THE FUTURE FACE OF THE WORLDWIDE DATA PRIVACY PUSH AS A FACTOR AFFECTING WISCONSIN BUSINESSES DEALING WITH CONSUMER DATA

TODD A. NOVA[1]

I. INTRODUCTION

Data privacy issues have become increasingly important in both international and domestic politics as intrusions such as unsolicited e-mail have become more prevalent and as the role of data as a commodity has become ever more apparent. This trend was brought to the forefront of the political arena by the 1995 creation of the European Union Data Directive[2] (hereinafter "E.U. Data Directive" or "Data Directive"), an E.U.-wide data privacy directive since mirrored by other countries that have either passed, or are considering passing, similar measures to prevent the use of personal data without the explicit consent of individuals.[3] One such example is a current data privacy act being proposed by Mexico's legislature.[4] With the national 'No-call' list debate in the U.S. as evidence of a growing public desire to protect privacy, one wonders not whether, but how much, inertial effect this global data privacy movement is likely to have on U.S. data privacy policy in the near future.

This article will attempt to examine the degree to which popular and economic pressure created by the E.U. Data Directive will cause a "ratcheting up" of U.S. privacy legislation from both

---

[1] B.A., Dartmouth College, 1998; J.D., University of Wisconsin Law School, December 2004. Special thanks to my parents, Gail and James, Ross Nova, and Kathryn Kehoe for all of their faith, support, advice and love. This Comment is dedicated to the memory of my grandfather, Dr. Louis Ross, M.D.

[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals wih Regard to the Processing of Personal Data and on the Free Movement of such Data, 1995 O.J. (L281) 31 [hereinafter E.U. Data Directive].

[3] Due to the limited scope of this article, it is only possible to touch on the data privacy legislation efforts of our closest primary trading partners: the European Union and Canada. For a brief discussion of the current status of privacy legislation progress in Australia and Japan, both of whom are considering privacy legislation, see John Bentivoglio et al., *Global Privacy Update*, 20 COMPUTER & INTERNET LAW. 1 (2003).

[4] *See* Deborah L. Vence, *Mexican Bill Could Affect U.S. DMers*, MARKETING NEWS, Oct. 14, 2002, at 5.

a national and state level, using Wisconsin's situation as emblematic of a number of states in the U.S.[5] Next, if any comprehensive act similar to the E.U. Data Directive were passed in the United States, how might it affect Wisconsin business in light of existing or possible state legislation and state court enforcement of data privacy rights? Finally, keeping these possible trends in mind, it will be useful to consider potential functional and economic impacts of data privacy legislation on the United States and Wisconsin.[6]

As mentioned previously, the constraints of this note require limiting the discussion of international privacy laws to our largest and closest trading partners, the E.U and Canada. Within this framework, the second section will provide background as to the recent history and statutory implementation of international privacy laws. After describing the current state of these laws, the third section will delve into the ratcheting function described above as performed by legislation and externalities such as the E.U. Data Directive's Safe Harbor provision[7] and popular support. With these ratcheting trends in mind, the fourth section will analyze the current direction of the modern privacy push in Canada, the U.S., and Wisconsin by looking at pending legislation and overall public sentiment. Fifth, it will be useful to attempt to predict the future face of global, U.S., and Wisconsin

---

[5] I borrow the term "ratcheting" as it applies to the global promulgation of privacy legislation from an article by Professor Gregory Shaffer of the University of Wisconsin Law School. In *Globalization and Social Protection: The Impact of E.U. and International Rules in the Ratcheting up of U.S. Privacy Standards* he writes:

> What happens in one jurisdiction can affect not only the playing field in other jurisdictions, but also the players' perceptions of their stakes. Data privacy regulations in Europe not only inform the tenor and context of debates in the United States, but also shape interest groups' appreciation of their options.

25 YALE J. INT'L L. 1, 38 (2000) [hereinafter *Globalization and Social Protection*].

[6] This focus is especially important in light of proposed legislation in Wisconsin that promises to establish a new $300 million venture capital seed fund. The disbursement of these funds and the future growth sectors of Wisconsin's economy should be informed by, among other factors, potential constraints on industries which rely on personal data. For the legislative text of Wisconsin's proposed seed fund, see S.B. 249, 2003 Leg., 96th Sess. (Wis. 2003).

[7] Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45,666 (July 24, 2000) [hereinafter Safe Harbor provision].

privacy policy while examining the likely future impacts of this privacy push from an economic and practical perspective.

II. The Current State of World Privacy Law: The European Union, United States, Canada, and Wisconsin

The U.S. and E.U. approaches to data privacy are generally viewed to be at opposite ends of the spectrum. Embodying the view many have regarding U.S. data privacy policy, it has been said that

> data privacy regulation in the United States is fragmented, ad hoc, and narrowly targeted to cover specific sectors and concerns. It is decentralized and uncoordinated, involving standard setting and enforcement by a wide variety of actors, including federal and state legislatures, agencies and courts, industry associations, individual companies, and market forces.[8]

The E.U. approach, on the other hand, has been said to represent the opposite tack. As Joel Reidenberg commented,

> Between the implementation in Europe of comprehensive legal protections pursuant to the directive on data protection and the continued reliance on industry self-regulation in the United States, trans-Atlantic privacy policies have

---

[8] *Globalization and Social Protection*, *supra* note 5, at 22. A more moderate description of the same sentiment states:

> The American approach to privacy has evolved as one of restraint. . . whereas the EU member states take an omnibus approach giving the state a pro-active preventative role. The fundamental difference in the American versus European conception of privacy is reflected most basically in the terms used to describe data privacy. Americans used the term 'privacy which can refer to the right to be free from the gaze of a 'peeping Tom' or the right to choose whether one wants her name distributed to telemarketers. Europeans use 'data protection,' which very specially addressed information generated by an individual's overt activity.

Julia Gladstone, *The U.S. Privacy Balance and the European Privacy Directive: Reflections on the United States Privacy Policy*, 7 Willamette J. Int'l L. & Disp. Resol. 10, 15 (2000).

> been at odds with each other. The rapid growth in e-commerce is now sparking the long-anticipated trans-Atlantic privacy clash.[9]

Regardless of the approach one favors, a brief survey of current international privacy law helps explain the origins of such a policy clash.

A. The European Union

In 1995, an effort was made to standardize the existing national privacy laws in the E.U., resulting in the E.U. Data Directive.[10] The E.U. Data Directive employs sanctions backed by regulatory authority as a means of creating a common standard aimed at eliminating the negative externalities of disparate national laws found throughout the E.U.[11] In effect, the term "Directive" requires each E.U. member state to adopt the standards defined therein within a limited time frame. Significant progress has been made throughout Europe to this end.[12] That said, the E.U. Data Directive forces E.U. member nations to set standards for the use of personal data that effectively require the owner[13] of the data to consent[14] to its use while limiting the uses to which the data at issue may be put.[15] Moreover, unlike the U.S. approach

---

[9] Joel R. Reidenberg, *E-Commerce and Trans-Atlantic Privacy*, 38 Hous. L. Rev. 717, 718 (2001). Mr. Reidenberg goes on to comment that

> The background and underlying philosophy of the European Directive differs in important ways from that of the United States. While there is a consensus among democratic states that information privacy is a critical element of civil society, the United States has, in recent years, left the protection of privacy to markets rather than law. In contrast, Europe treats privacy as a political imperative anchored in fundamental human rights.

Id. at 730–31.

[10] *Id.* at 731–32.

[11] *See* Marc Rotenberg, The Privacy Law Sourcebook 2002: United States Law, International Law, and Recent Developments 367–394 (2002). *See also Globalization and Social Protection, supra* note 5, at 2–3.

[12] Reidenberg, *supra* note 9, at 732.

[13] I use the term "owner" as a synonym for the subject of the data at issue.

[14] Article 2, section (h) of the E.U. Data Directive states: "the data subject's consent shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed."

[15] Article 7 of the E.U. Data Directive provides:

discussed subsequently, the E.U. Data Directive covers both public and private records, thus staying true to its stated purpose of comprehensive data protection.[16]

More to the point, the E.U. Data Directive limits data use of businesses operating, or who wish to operate, under the auspices of the E.U. while providing means for enforcement of its provisions, lest companies circumvent the Directive by "storing" data in non-compliant countries.[17] The E.U. Data Directive's proverbial stick regarding these inevitable attempts is a provision that allows for both sanctions[18] and for the prevention of the transfer of data to any noncompliant third party countries.[19] Needless to

---

> Member States shall provide that personal data may be processed only if:
> (a) the data subject has unambiguously given his consent; or
> (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
> (c) processing is necessary for compliance with a legal obligation to which the controller is subject; or
> (d) processing is necessary in order to protect the vital interests of the data subject; or
> (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
> (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

E.U. Data Directive, *supra* note 2, at 40.

[16] Article 2 of the E.U. Data Directive defines the relevant parties:

> (e) 'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller
> (f) 'third party' shall mean any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data
> (g) 'recipient' shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients.

E.U. Data Directive, *supra* note 2, at 38–39.

[17] Reidenberg, *supra* note 9, at 733.

[18] EU Data Directive, *supra* note 2, at 45.

[19] *Id.* at 46.

say, this particular article has created no small amount of umbrage for businesses in the United States, as U.S. actors are directly affected by international law. The reasons for the consternation caused in the United States most likely result from the somewhat amorphous requirement that:

> The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations. Particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.[20]

This is not to say that a noncompliant country must either strictly meet the E.U. Data Directive requirements or be shut out completely. Rather, states themselves are encouraged to force compliance. The Data Directive reads:

> Where the Commission finds, under the procedure provided for in Article 31 (2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.[21]

In addition to these provisions, individual recourse is provided for in that every member state must allow for judicial remedy in the event it is believed that an individual's rights, as described by the E.U. Data Directive, have been breached.[22] The effect of this provision on litigation in Europe and the potential ramifications for litigation in the U.S. are still unclear, as enforcement actions are still relatively rare.[23] Nevertheless, common

---

[20] *Id*. at 45–46.

[21] *Id.* at 46.

[22] *Id*. at 45.

[23] There have been few Safe Harbor enforcement actions in the United States thus far. *See* Gregory Shaffer, *Extraterritoriality in a Globalizing World: Regulation of Data Privacy*, 97 AM. SOC'Y INT'L L. PROC. 314 (2003) [hereinafter *Extraterritoriality in a Globalizing World*]. *See also infra* note 123. Even in the E.U., where

sense dictates that provisions employed to deal with an international patchwork of data privacy policies invoking the full power of the E.U.'s economy to restrict data transfers with companies in the United States and other countries could be both politically and economically damaging.[24]

Quite aside from issues of international enforcement, the mere creation of the E.U. Data Directive has not led to the harmonious incorporation of its principles within the Union. In addition to the fact that few European states met the October 1998 transition deadline, some nations, most notably France, have yet to implement the Directive as required while others, such as Ireland and Luxembourg, did not implement the Directive until as late as 2002.[25] The fact that a number of member states missed the 1998 transition deadline illustrates the difficulty of implementing such sweeping legislation in the face of so many factors. Also indicative of this difficulty is that Germany, Ireland, Luxembourg and the Netherlands only enacted the required legislation in response to the E.U. Commission taking them to the European Court of Justice for failure to implement the Data Directive requirements.[26] Still, all candidate E.U. countries finally have associated E.U. Data Directive legislation, save Turkey, though even that country is considered to be close to implementing similar such legislation.[27]

---

enforcement is guided by Data Directive Provisions, the E.U. Commission has acknowledged that

> [i]ndeed, international transfers appear to be an area where the lack of enforcement action creates such a gap. National authorities are supposed to notify the Commission when they authorize transfers under Article 26 (2) of the Directive. Since the Directive came into operation in 1998, the Commission has received only a very limited number of such notifications.

Report from the Commission: First Report on the Implementation of Data Protection Directive (95/46/EC), COM(03) 265 final at 19 [hereinafter Report from the E.U. Directive Commission].

[24] Reidenberg, *supra* note 9, at 739.

[25] *See* Report from the E.U. Directive Commission, *supra* note 23, at 7.

[26] *Id*. at 3, n. 1.

[27] *Id.* at 13.

Still, despite this legislation, divergences in implementations of the E.U. Data Directive have caused difficulties in enforcement and in the creation of a consistent privacy protection regime.[28] As the E.U. Directive Commission states, "Many of the divergences detected nevertheless do stand in the way of a flexible and simplified regulatory system and are still therefore of concern (see for example the differences in the notification requirements or the conditions for international transfers)."[29]

Some of the specific problems encountered in implementation of the E.U. Data Directive are less than surprising. For example, the E.U. Directive Commission complains of underfunded and thus under-utilized enforcement actions, "patchy" compliance by data controllers,[30] and, as an explanation for the lack of compliance, a "low level of knowledge of their rights among data subjects."[31] Another problem cited by the Commission is a lax attitude, generally, regarding the E.U. Data Directive, which they say, "in addition to being in contravention of the Directive – risks weakening protection in the E.U. as a whole, because with the free movement guaranteed by the Directive, data flows are likely to switch to the 'least burdensome' point of export."[32] Finally, the E.U. Directive Commission acknowledges that the E.U. Data Directive's requirements must be reviewed for conflicts with other existing national laws in order to become truly effective – a review which has yet to take place.[33]

While the E.U. Data Directive is a comprehensive and structured set of requirements, it is by no means a panacea for the ills of data mining and manipulation. The extensive implementation across both member and candidate countries, however, indicates

---

[28] *Id.* at 12.

[29] *Id.*

[30] E.U. Data Directive, *supra* note 2, at 38, states:

> (d) 'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law.

[31] Report from the E.U. Directive Commission, *supra* note 23, at 12.

[32] *Id*. at 19.

[33] *Id.* at 15.

the strong inertia gathered by the concepts embodied by the E.U. Data Directive and show that this comprehensive set of data privacy guidelines will ultimately prove successful.[34]

B. The United States

For all of the implementation difficulties encountered with the E.U. Data Directive, the current state of privacy law in the United States is significantly less ordered and, some argue, less effective.[35] Specifically, "[i]t is decentralized and uncoordinated, involving standard setting and enforcement by a wide variety of actors, including federal and state legislatures, agencies and courts, industry associations, individual companies, and market forces."[36] Nonetheless, it is useful to provide a summary of some of the major privacy laws as they currently exist in the United States and Wisconsin, as it will indicate the specific nature of privacy legislation in the United States as narrowly targeted and, often, only in response to public scandals.[37]

First, one of the few federal omnibus acts with aims similar to those of the E.U. Data Directive is the Privacy Act of 1974 (hereinafter "Privacy Act").[38] The aim of this act was to "promote governmental respect for citizens' privacy by requiring federal agencies to observe certain guidelines in the use and disclosure of citizens' personal information."[39] The act requires that no federal agency disclose personal information without consent of the individual whose data is at issue unless certain exemptions come into effect.[40] Additionally, the Privacy Act requires that each disclosure be tracked,[41] that any individual be

---

[34] *See generally Globalization and Social Protection*, *supra* note 5, at 6. Professor Schaffer discusses the concept of inertia, also termed "spill-over" or "ratcheting." There, he comments, "Foreign regulation can, in particular, affect domestic actors' appreciation, their stakes and their political leverage. EU regulatory policy can thereby affect U.S. policies and commercial practices, and vice-versa. I refer to this as the theme of transnational institutional interdependence."

[35] *Id.* at 22.

[36] *Id.*

[37] *Id.* at 25.

[38] 5 U.S.C.A. § 552a (1996) [hereinafter Privacy Act].

[39] Rotenberg, *supra* note 11, at 43.

[40] Privacy Act, *supra* note 38, § 552a(b).

[41] *Id.* § 552a(c).

allowed to access her record upon request,[42] and that each agency publish information in the Federal Register detailing what systems exists and the content of each of those systems.[43] Importantly, however, this act applies only to federal agencies, in contrast to the broad-based applicability of the E.U. Data Directive. Moreover, enforcement mechanisms originally intended to give this act traction have fallen by the wayside.[44]

Another more recent federal act addressing such privacy concerns is the Graham-Leach-Bliley Act of 1999 (hereinafter "GLB Act"),[45] which addresses privacy concerns by giving the Federal Trade Commission the authority to police the privacy practices of "financial institutions."[46] Financial institutions, as contemplated by the GLB Act, include a broad range of actors who extend credit to customers as well as those providing appraisal services for personal property and can include banks and car dealers, among others.[47] Each entity that falls under the auspices of the GLB Act must: 1) notify its customers of its privacy policies, 2) disclose the conditions under which personal information will be released to third parties and 3) allow customers to choose not to allow their personal information to be shared with third parties.[48] Although encouraging, certain provisions dilute the efficacy of the GLB Act, including provisions which allow third parties to use personal information if that party is marketing on behalf of the institution that owns the data.[49] Still, if the

---

[42] *Id.* § 552a(d)(1).

[43] *Id*. § 552a(e)(4).

[44] ROTENBERG, *supra* note 11, at 43, notes that:

> As originally drafted, the Privacy Act would have created a Federal Privacy Board to act as an oversight and enforcement mechanism. The final Act, however, created a far more limited body, the Privacy Protection Study Commission. . . [which made] numerous recommendations for change. The Commission was dissolved following the release of its report.

[45] Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999).

[46] John T. Soma et al., *An Analysis of the Use of Bilateral Agreements Between Transnational Trading Groups: The U.S./EU E-Commerce Privacy Safe Harbor*, 39 TEX. INT'L L.J. 171, 185 (2004).

[47] *Id.* at 185–86.

[48] *Id.*

[49] *Id.* at 187.

provisions of the GLB Act are violated, the FTC has the authority to initiate criminal prosecution where an actor has knowingly violated GLB Act provisions.[50]

The next federal act deserving attention here, mainly due to its high profile, is the Freedom of Information Act (hereinafter "FOIA"), also promulgated in 1974.[51] Though certainly a step forward in terms of privacy rights, its scope is similar to the Privacy Act in that it only allows citizens access to all federal agency records.[52] Moreover, FOIA was expanded in 1996 by the Electronic Freedom of Information Act Amendments to "include access to electronic records and databases in electronic format, if such format is requested. The amendments also require agencies to expedite the processing of certain FOIA requests."[53]

Next, the Telecommunications Act[54] requires that telecommunications carriers protect consumer information such as calling patterns, billing information, and home addresses of subscribers.[55] Again, while this act is certainly important in terms of protecting consumer data, its scope could be described as little more than limited.

While it is possible to list the other acts put forth by Congress, it would not prove useful to this inquiry, as federal privacy legislation in the United States is something of a patchwork of laws relating to relatively specific areas of consumer data.[56] As has been said quite succinctly by Professor Shaffer, "Rather than engage in a converted effort to protect individual privacy, in most cases, Congress has simply reacted to public scandals."[57] This point becomes clear by looking at the names of the other privacy acts currently in force.[58] These include the Right to Financial Privacy Act of 1978,[59] the Cable Communications Policy Act of

---

[50] *Id.*

[51] 5 U.S.C.A. § 552 (1974).

[52] ROTENBERG, *supra* note 11, at 64 (describing the similarities between the acts).

[53] *Id.*

[54] 47 U.S.C.A. § 222 (1996).

[55] ROTENBERG, *supra* note 11, at 248.

[56] *See Globalization and Social Protection*, *supra* note 5, at 25.

[57] *Id*.

[58] *Id*. Professor Shaffer initially brought forth this point.

[59] 12 U.S.C.A. § 3401 (1978).

1984,[60] the Video Privacy Protection Act of 1988,[61] the Employee Polygraph Protection Act of 1988,[62] the Driver's Privacy Protection Act of 1994,[63] and the Children's Online Privacy Protection Act of 1998.[64] The point has been made that "[a]s a result, in the United States, 'video rentals are afforded more federal protection than are medical records.'"[65]

C. Canada

Generally, Canada's approach to privacy protection stands in opposition to the laissez-faire approach taken by the United States. Beyond viewing individual privacy as a fundamental right, the Supreme Court of Canada has found individual privacy to be an essential component of freedom.[66] Canadian courts have even gone so far as to recognize a violation of individual privacy rights as a tort.[67] Furthermore, while the United States has yet to implement any comprehensive privacy legislation, Canada has forged ahead and become the newest entrée into the world privacy legislation arena.[68] Importantly, this legislation both portends similar such legislation here in the United States and affects American businesses by imposing additional costs associated with compliance.[69] Should the influence of these Canadian requirements ever be minimized, it is important to note that "our

---

[60] 47 U.S.C.A. § 551 (1984). This act essentially mirrors the consumer privacy protections for telecommunications companies found in the Telecommunications Act.

[61] 18 U.S.C.A. § 2710 (1988).

[62] 29 U.S.C.A. § 2001 (1988).

[63] 18 U.S.C.A. § 2721 (1994).

[64] 15 U.S.C.A. § 6501 (1998).

[65] *Globalization and Social Protection*, *supra* note 5, at 25 (quoting Sheri Albert, Smart Cards, Smarter Policy: Medical Records, Privacy and Health Care Reform 13 (1993)).

[66] *See* Juliana M. Spaeth et al., *Privacy Eh!: The Impact of Canada's Personal Information Protection and Election Documents Act on Transitional Business*, 4 Vand. J. Ent. L. & Prac. 28, 31 (2002) (citing R. v O'Connor, (1995) 4 S.C.R. 411).

[67] *Id.* (citing Canada v. Southam, Inc., (1984) 2 S.R.C. 145).

[68] *Id*. at 29.

[69] *Id.*

trade with Canada is roughly equivalent to our combined trade with Japan, China, Germany, and the United Kingdom."[70]

Turning to the specifics of Canada's privacy regime, Canada's Personal Privacy Protection and Electronic Documents Act ("PIPEDA"), which is similar to the Data Directive, aims to protect the personal information of Canadians by governing commercial use of personal information by both domestic and foreign collectors of such data.[71] Moreover, PIPEDA's stated purpose is to balance the individual's need for privacy with the obvious economic need for access to some of the collected data.[72]

PIPEDA demands that when "collecting, using, or disclosing Canadians' personal information in the course of a commercial activity. . ., the Act requires compliance with ten specific obligations."[73] These obligations are: 1) accountability, 2) identifying purposes, 3) consent, 4) limiting collection, 5) limiting use, disclosure and retention, 6) accuracy, 7) safeguards, 8) openness, 9) individual access, and 10) challenging compliance.[74] Broadly, the first requirement, accountability, mandates that "entities are responsible for all personal information under their control."[75] Second, entities must inform people of reasons for the collection of their information.[76] "Consent" requires that individuals, save certain circumstances, consent to the use of their data.[77] The

---

[70] *Id.*

[71] *Id.*

[72] Personal Information Protection and Electronic Documents Act, S.C., c.5, s. 3 (2000) (Can.). [hereinafter PIPEDA] states:

> The purpose of this Part is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

Id.

[73] Spaeth, *supra* note 66, at 33.

[74] PIPEDA, *supra* note 72, at c.5, sched. 1.

[75] Spaeth, *supra* note 66, at 34.

[76] *Id.*

[77] *Id.*

"limiting collection" requirement mandates that data only be collected for the identified reasons.[78] Next, "limiting use, disclosure, and retention" means that the same data may not be used for purposes other than those for which it was originally obtained.[79] Sixth, the accuracy requirement maintains that information used must be, in a word, accurate.[80] Seventh, the "safeguards" requirement demands that data be protected effectively.[81] Eighth, the "openness" requirement forces organizations to make information available regarding their data policies.[82] Ninth, "individual access" means that information about "whether organizations have collected, used, or disclosed their personal information" must be provided upon written request.[83] Finally, "challenging compliance" allows individuals the opportunity to complain to companies regarding suspected non-compliance, and those companies must act to remedy any such failure.[84]

Turning now to enforcement, PIPEDA is enforced internally via a series of measures which allow for a mixture of self-help, access to the court system, and the assistance of a Canadian Privacy Commissioner.[85] Internationally, the enforcement mechanisms of this legislation are less clear than those put forth by the E.U. Data Directive. The most obvious effect this will have on American companies is on their attempts to obtain personal data from Canadian companies who are themselves forced to comply with PIPEDA's requirements.[86] Beyond this somewhat obvious ramification, however, the jurisdictional problems created by the amorphous nature of data storage and transfer pose interesting questions that have yet to be fully considered.[87]

---

[78] *Id.* at 36.

[79] *Id.*

[80] *Id.*

[81] *Id.*

[82] *Id.* at 37.

[83] *Id.*

[84] *Id.* at 37–38.

[85] "The Commissioner has essentially five ways of ensuring that organizations comply with Canada's privacy laws: (1) investigating complaints; (2) mediating disputes; (3) auditing personal information practices; (4) publicly reporting abuses; and (5) seeking remedies in Federal Court" *Id*. at 38.

[86] *Id.*

[87] *Id.* at 38–39.

D. WISCONSIN

As has already been discussed, privacy law in the United States is something of a patchwork of state and federal law. Thus, a brief discussion of the current state of Wisconsin's privacy regime is useful to businesses operating in Wisconsin who should consider both the current state of privacy law and its likely future shape. Not surprisingly, Wisconsin's privacy law regime mirrors that of the United States as a whole in that it is, in essence, a loose conglomeration of laws.[88] Wisconsin common law has dealt extensively with public records access,[89] but effectively not at all in regard to the transmission of personal information in a context contemplated by either the E.U. Data Directive or PIPEDA.

Interestingly, Wisconsin currently has in place statutory provisions dealing with data privacy.[90] Still, it has been argued that the broad nature of Wisconsin's privacy statutes make them almost unenforceable, since there is no provision for a private cause of action.[91] It has been said that, "Notwithstanding the

---

[88] *See* Michael K. McChrystal et al., *Invasions of Computer Privacy*, WISCONSIN LAWYER, Oct. 1998, at 25.

[89] *See, e.g.,* Hathaway v. Joint School Dist. No. 1, City of Green Bay, 342 N.W.2d 682 (Wis. 1984).

[90] The Wisconsin statute dealing with offenses against computer data and programs provides in part:

> (a) Whoever willfully, knowingly and without authorization does any of the following may be penalized as provided in pars. (b) and (c):
>
> Modifies data, computer programs or supporting documentation.
>
> Destroys data, computer programs or supporting documentation.
>
> Accesses computer programs or supporting documentation.
>
> Takes possession of data, computer programs or supporting documentation.
>
> Copies data, computer programs or supporting documentation.
>
> Discloses restricted access codes or other restricted access information to unauthorized persons.

Wis. Stat. § 943.70(2) (2001-02).

Wisconsin law also states that "The right of privacy is recognized in this state. One whose privacy is unreasonably invaded is entitled to the following relief. . ." Wis. Stat. § 895.50(1)

[91] McChrystal et al., *supra* note 88, at 25.

sweep of Wisconsin's computer crimes statute, the extent of computer privacy remains very much in doubt."[92] Perhaps most importantly, the data's subject is not protected in Wisconsin since "The statute is most limited. . . in that its protection seems to run only to the owner or possessor of the data, computer, or program."[93] For common law precedent in Wisconsin, one needs to turn to federal law for guidance.[94] That said, while there are no formal channels for protecting data privacy, standard tort and contract remedies have been employed with varying degrees of success.[95] Nonetheless, this regime can hardly be called coherent or extensive relating to its protection of an individual's data. Without embarking on an analysis of various common law options for addressing data privacy concerns (for example, a duty of reasonable care may exist to protect information, but what if the data is stolen and then purchased by a third party?), it can be safely said that, currently, "[t]hese questions await dispositive treatment by Wisconsin courts."[96]

III. The Ratcheting of Global Privacy Laws: How Externalities Effect Privacy Law Inertia

Considering the above survey of the E.U., United States, Canada and Wisconsin privacy regimes, one can see that global privacy concerns are becoming increasingly prevalent. With the continued maturation of the internet and the information economy, these concerns will only grow in importance. It is this increase in visibility that has led numerous observers to conclude that the United States will face growing pressure to better protect the privacy of its citizens with privacy laws similar to those promulgated by the E.U. and Canada.[97] As such, some attention

---

[92] *Id.*

[93] *Id.*

[94] For example, the more seminal cases like *U.S. v. Katz*, 389 U.S. 347 (1967), are typically cited. Moreover, there is no option in Wisconsin for private enforcement of the state's data protection statute and "no reported Wisconsin decision directly addresses the issue." McChrystal et al., *supra* note 88, at 28.

[95] McChrystal et al., *supra* note 88, at 28.

[96] *Id.* at 27.

[97] *See*, *e.g.*, Gladstone, *supra* note 8; Reidenberg, *supra* note 9; *Globalization and Social Protection*, *supra* note 5.

should be paid to the notion that international externalities will likely encourage privacy law development in the United States.[98]

From a popular perspective, the privacy debate continues to mushroom, as one might gather from a brief survey of recent articles as well as recent media attention given to the issue.[99] Moreover, evidence suggests that, while most Americans are blissfully unaware that their personal information is being disseminated without their express consent,[100] they would object heartily if made aware of the true extent to which an individual's data is disseminated. When asked whether they felt forcing a standardized website policy would better protect their personal information, 86% of adult Americans agreed.[101] Still, only 13% of adult Americans believe that the government will help them protect their personal information.[102] For example, the recent scandal that arose when JetBlue Airways sold 5 million passenger itineraries to a defense contractor to aid in testing a concept profiling system – a violation of its own privacy policy – shows just how eager Americans can be to defend their privacy when they realize that it has been compromised.[103] Moreover, numerous high-profile consumer advocacy groups have pinpointed this desire for comprehensive privacy legislation, with one such group, The Annenberg Public Policy Center, writing that "[o]ur findings. . . indicate that consumers want legislation that will help them gain access to and control over all information collected about them

---

[98] *Globalization and Social Protection*, *supra* note 5, at 55.

[99] Without citing the specific articles, a quick internet search reveals thousands of related articles from magazines and newspapers including Time, PC World, The Financial Times, The New York Times, The Washington Post, and more. Additional, seemingly numerous television and radio programs have been devoted to the topic as well.

[100] A recent study indicated that about 57% of adults using the internet mistakenly believe that web-sites with privacy policies are not gathering or sharing personal information. When presented with a privacy description describing what companies actually do with their personal information, 85% of adults did not accept the online privacy policy. Joseph Turow, *Americans & Online Privacy: The System is Broken, Annenberg Public Policy Center* (2003) *at* http://www.annenbergpublic policycenter.org.

[101] *Id*. at 3.

[102] *Id.*

[103] *See* Ryan Singel, *JetBlue Shared Passenger Data*, WIRED NEWS (Sept. 18, 2003), *at*: http:// *www.wired.com*/news/privacy/0,1848,60489,00.html.

online."[104] Other such groups, including the Electronic Privacy Information Center, have been at the forefront of the public push for a comprehensive data privacy regime. All things considered, it is safe to say that wide public support exists for comprehensive privacy legislation. To wit, the recent success of the national "do not call" list bolsters the idea that when presented with the option of protecting personal information, Americans will jump at the opportunity.[105]

Most recently, popular support for privacy-related legislation has been exemplified by the recent House of Representatives' near unanimous passing of an anti-spam bill in November of 2003, interestingly titled "Controlling the Non-Solicited Pornography and Marketing Act," by a vote of 392-5.[106] The fact that this bill was passed so resoundingly, after a number of similar such bills have failed to pass in recent years, seems to portend the recognition of public frustration by the United States legislature. The stated purpose of the bill supports this assertion, as it reads, "The convenience and efficiency of electronic mail are threatened by the extremely rapid growth in the volume of unsolicited commercial electronic mail. . . Most of these unsolicited commercial electronic mail messages are fraudulent or deceptive in one or more respects."[107] Despite the markedly different focus and tone of this bill as opposed to past privacy legislation, however, one can once again see the legislative reaction to an isolated political issue rather than the broader privacy concerns spawned by the nature of the information economy.[108]

It is axiomatic that public support is vital for the implementation of this type of legislation in the United States. This public support will not alone, however, force the creation of a comprehensive privacy law. This is perhaps best evidenced by the fact that no such legislation has yet been enacted. That is not to say, however, that this will not happen. Externalities created by international legislation which imposes requirements on American

---

[104] Turow, *supra* note 100, at 4.

[105] Federal Trade Commission Press Release, *Do Not Call Registrations Exceed 50 Million*, Sept. 17, 2003, *at*: http://www.ftc.gov/opa/2003/09/dncnumbers030917.htm.

[106] S. 877, 108th Cong. (2003).

[107] S. 877, 108th Cong. § 2(a)(2) (2003).

[108] *See Globalization and Social Protection, supra* note 5.

companies have been perhaps the strongest factor in the ratcheting of world and U.S. privacy law. As Professor Shaffer has written, "Because the E.U. Directive applies to data transfers worldwide, it has extra-jurisdictional effects. United States businesses feel the greatest impact because they engage in more European transactions than other foreigners. . ."[109] In essence, beyond the economic, and thus indirectly political, drivers of policy, "[t]he E.U. Directive has drawn attention to data privacy issues in the United States. It has pressed U.S. governmental authorities to address the adequacy of current U.S. data privacy regulation in order to fend off a regulatory conflict with the European Union."[110]

While it would be interesting to discuss the externalities imposed by Canada's PIPEDA, the more extensive, and thus more influential, E.U. Data Directive provisions more greatly affect U.S. privacy concerns. More specifically, while the ideals embodied by the E.U. Data Directive have had some influence, the rubber hits the road in the form of the Data Directive's enforcement provisions.

While public outcry, as discussed above in relation to the recent anti-spam legislation, has resulted in the promulgation of additional privacy law enhancement in specific areas, it is mainly the enforcement provisions of the E.U. Data Directive that have forced the extra-legislative creation of privacy law in the United States aimed at creating individual U.S. corporate compliance with the E.U. Data Directive.[111] Specifically, the E.U. Data Directive has spawned the creation of a Safe Harbor provision meant to allow for individual self-certification of U.S. businesses that must be deemed in compliance with the E.U. Data Directive.[112] Effectively, the unilateral enforcement provisions of the E.U. Data Directive achieved what political pressure could not:

---

[109] *Id.* at 55.

[110] *Id.*

[111] The E.U. Data Directive has "pressed U.S. businesses to enhance self-regulatory efforts to forestall E.U. restrictions on data transfers to the United States. . .[and] United States businesses are now on the defensive about their practices. So are officials in the U.S. Department of Commerce who represent U.S. business interests abroad." *Globalization and Social Protection*, *supra* note 5, at 55–56.

[112] The final Safe Harbor documents were negotiated by the U.S. Department of Commerce and accepted by the E.U. on July 28, 2000. The provisions are detailed in 65 Fed. Reg. 142 (July 24, 2000).

namely, that U.S. businesses protect the information of European citizens.[113]

Specifically, the Safe Harbor provision principles require that businesses inform individuals about how and why information is collected and disseminated, provide an option to "opt-out" of general information use and "opt-in" for more sensitive information, require third parties who obtain individuals' data to adhere to the same standards, take reasonable measures to ensure data security, take reasonable steps to ensure that data is used for the stated purposes and is kept accurate, grant individuals access to their information and provide a mechanism for correcting errors, and provide sufficient compliance enforcement mechanisms.[114] These Safe Harbor provisions require that a company must

---

[113] Regarding this assertion, it has been said that, "Many of the Member States that vociferously accused the United States of interference with their domestic policies have now, through the power of the E.U., exercised extraterritorial authority on the United States through the Data Privacy Directive." Barbara Crutchfield George et al., *U.S. Multinational Employers: Navigating Through the "Safe Harbor" Principles to Comply with the E.U. Data Privacy Directive*, 38 AM. BUS. L.J. 735, 736 (2001) (citations omitted).

[114] Specifically, the Safe Harbor Principles require:

> NOTICE: An organization must inform individuals about the purposes for which it collects and uses information about them, how to contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure. This notice must be provided in clear and conspicuous language. . .
> CHOICE: An organization must offer individuals the opportunity to choose (opt out) whether their personal information is (a) to be disclosed to a third party(1) or (b) to be used for a purpose that is incompatible with the purpose(s) for which it was originally collected or subsequently authorized by the individual. . .
> For sensitive information (i.e. personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual), they must be given affirmative or explicit (opt in) choice if the information is to be disclosed to a third party or used for a purpose other than those for which it was originally collected . . .
> ONWARD TRANSFER: To disclose information to a third party, organizations must apply the Notice and Choice Principles. . .
> SECURITY: Organizations creating, maintaining, using or disseminating personal information must take reasonable precautions to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction.
> DATA INTEGRITY: Consistent with the Principles, personal information must be relevant for the purposes for which it is to be used. . . To the extent necessary for those purposes, an organization should take reasonable steps

> join a private sector-developed privacy program that includes effective enforcement mechanisms such as the TRUSTe or BBB Online Seal program, or (2) develop and pronounce their own privacy policies in conformity with the Principles, or (3) self-certify to the Department of Commerce that the company is already subject to a sector-specific statute, regulation or legal requirement, or (4) commit to adherence with the Principles in contracts with parties transferring data from the E.U. in accordance with E.U. authorized model contracts."[115]

The adoption of these provisions is evidence of the ratcheting effects of global privacy legislation. That is, there is little doubt that these Safe Harbor provisions would not exist but for the requirements of the E.U. Data Directive.[116] To wit, their very existence is a direct response to the requirements imposed by the Data Directive.[117]

Still, these provisions and self-certification requirements would doubtless fail to force the ratcheting of privacy policy without the enforcement mechanisms put in place and assented to by the E.U. These mechanisms include the self-certification process, whereby a corporate officer must certify that the corporation meets five main criteria which effectively state that a company must, among other requirements: 1) provide the details of

---

> to ensure that data is reliable for its intended use, accurate, complete, and current.
> ACCESS: Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate. . .
> ENFORCEMENT: Effective privacy protection must include mechanisms for assuring compliance with the Principles, recourse for individuals to whom the data relate affected by non-compliance with the Principles, and consequences for the organization when the Principles are not followed. . ."

65 Fed. Reg. 142 (2000) at 45667-668.

[115] George et al., *supra* note 113, at 765. These principles effectively mirror the privacy requirements required by the E.U. Data Directive, thus explaining the E.U.'s acceptance of the exception. *Id.* at 766–67.

[116] Prior to the E.U.'s acceptance of the Safe Harbor provisions, this response could already be seen as businesses promoted "'self regulation' as an alternative to E.U. regulation" thus pressing them "to raise their internal standards. Suddenly, businesses and business associations. . . develop[ed] a plethora of data privacy protection 'principle,' 'guidelines,' model contracts, and other schemes." *Globalization and Social Protection*, *supra* note 5, at 72–73.

[117] *See* George et al., *supra* note 113, at 766–67.

how it will use personal data, 2) provide a description of its privacy policy, 3) detail the statutory body that has jurisdiction to hear any claims regarding trade practice and privacy, 4) name any privacy organizations to which it belongs, and 5) detail its method of verification.[118]

While these provisions comport with the spirit of the E.U. Data Directive, the ratcheting effect would likely not be initiated without stringent remedies to force compliance. Though aimed at encouraging businesses to adopt private enforcement remedies, the effectiveness of these enforcement provisions has been questioned.[119] Anecdotally, however, the fact that 146 corporations, including General Motors, Gateway, Ernst & Young, and Disney, have self-certified with the FTC indicates that these enforcement provisions have been at least somewhat effective.[120] These enforcement provisions include the ability to petition the enforcement resolution bodies subscribed to by the offending corporation for sanctions, the requirement that failures be reported to the governmental body with jurisdiction over the corporation, review by the FTC to determine whether section 5 of the FTC Act prohibiting unfair or deceptive trade practices has been violated and, ultimately, removal from the Safe Harbor list if persistent failures occur.[121]

Locally, this ratcheting effect on Wisconsin mirrors the analysis already undertaken regarding the relative lack of attention to this issue in the state. Thus, the effect on the state is limited to the broader federal and international requirements such as those already discussed regarding the Safe Harbor provision.

---

[118] 65 Fed. Reg. 142, at 45669-670.

[119] Frits Bolkestein, European Commissioner for the Internal Market, supported adoption of the Safe Harbor principles "despite the fact that Parliament was concerned about the fact that remedies open to individuals appeared to be too weak" and left available the option to revisit negotiations if the available remedies proved inadequate. George et al., *supra* note 113, at 778–79 (quoting http://www.europa.int/comm/internal_market/en/dataprot/news/ (July 13, 2000)).

[120] The Safe-Harbor List of Companies, *available at http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/+safe+harbor+list*.

[121] 65 Fed. Reg. 142, at 45673-674.

All things considered, it is safe to say that the externalities imposed by international privacy law have forced the Department of Commerce and, by proxy, U.S. corporate interests to respond and ratchet U.S. privacy law where the U.S. legislature has failed to respond. Without discussing the merits and ramifications of this development, the question now becomes what future effects this ratcheting will have on U.S. and state privacy law regimes and, subsequently, how this will affect U.S. and Wisconsin businesses.

IV. The Current Legislative and Public Sentiment Push

The end-game of this privacy regime ratcheting remains to be seen. Nonetheless, a survey of existing public and governmental sentiment, coupled with a discussion of national and international public sentiment regarding data privacy, shows that the privacy concerns embodied by the Data Directive, PIPEDA, and the Safe Harbor provision show no signs of abating. In fact, this survey, coupled with a review of pending data privacy legislation, indicates that the world's privacy regime is likely in its infancy. To this end, it is useful to undertake a brief review of the current legislative and public sentiment drivers of international data privacy rights.

A. Current Privacy Regime and Public Sentiment in the European Union

Focusing, at least briefly, on the current state of public and legislative sentiment in the E.U. is vital, considering the indirect influence that the E.U. Data Directive has already exerted on Canada, Hong Kong, Japan, Thailand, and Australia, just to name a few.[122] Perhaps the most significant indicator of this influence was the Data Directive's ability to force the implementation of the Safe Harbor provisions. That is, the potential loss of the European Union market surely drove the creation of these provisions, given the aforementioned reluctance of the United

[122] These countries have all implemented significant legislation aimed at protecting personal data in line with the E.U. Data Directive. For a good survey of these laws see Nicole A. Wong et al., *Privacy and Marketing Issues*, 755 PLI/Pat 11 (2003).

States to implement any broad-based privacy regime.[123] Recognizing the current influence of the E.U. strengthens the assertion that it will exert significant and growing economic and legislative pressure. After all, as a block, it is the largest single market in the world.[124] When one couples this realization with the fact that the E.U. expanded from fifteen to twenty-five member states in 2004, giving it a combined population larger than that of the United States, Canada, Japan, Australia, and New Zealand combined, it is impossible to ignore the large market leverage the E.U. will enjoy.[125] Moreover, the influence such market dominance wields over external political machinations is clear given the substantial political influence and reach of the United States after World War II. It thus makes sense to review the potential future state of E.U. data privacy protections before moving on to explore that of the United States, Canada, and Wisconsin.

At first, the very nature of an E.U. Directive requires that its member states adopt its provisions, thus requiring some form of compliance from any companies wishing to trade with a member state. Again, the prospect of a gigantic twenty-five member trading block adhering to these provisions makes the Data Directive almost impossible to ignore. Couple the coming creation of this European super-state with the stated commitment to the principles of the Data Directive as described in its preamble,[126] and it becomes clear that the Data Directive will serve more as a floor than as a ceiling on data privacy protections.

The current state of the Data Directive bolsters this assertion. In its First Report on the Implementation of the Directive, the Commission of the European Communities found that "[a]lthough the Data Protection Directive incorporates high standards of protection, most individuals (4113 out of 9156 or 44.9%)

---

[123] Additionally, the rise of information technology has hastened globalization as well as the interdependence of the U.S. and E.U. economies. *Extraterritoriality in a Globalizing World, supra* note 23. Professor Shaffer explains this trend, writing, "Companies depend on information flows not only in their relations with third party suppliers, customers, consultants, marketers, and other service providers, but also internally, within their complex networks of transnational affiliates, joint ventures, and partnerships."

[124] *Id.* at 317.

[125] *Id*.

[126] E.U. Data Directive, *supra* note 2, 31–38.

considered the level of protection a minimum."[127] In discussing the statistic, the Commission acknowledges that, as it was comprised of survey responses, it "cannot be considered representative."[128] This seems to telegraph the Commission's opinion that the Data Directive represents the minimum, rather than the maximum, standards that should be employed in protecting personal information. The tenor of the entire report, in fact, supports this assertion.[129] More specifically, the work plan for better implementing the Data Directive states, "A general, serious concern indicated above is that the level of compliance, enforcement and awareness appears not to be at an acceptable level."[130] To this end, the Commission lists ten action items for improved implementation of the Data Directive that focus on improved implementation and increased enforcement of the objectives.[131] As such, it is clear that the E.U. is wholly committed to the Data Directive and to pursuing broad based and consistent enforcement of its provisions in the near future. It is therefore the opinion of this writer that the E.U. will continue to refine, strengthen, and enforce the provisions and philosophies of the Data Directive, with the ultimate implication being that businesses in the United States and Wisconsin should get used to adhering to international, as well as national and state, business regulations in the data realm.

B. Current Privacy Regime and Public Sentiment in the United States

As discussed above, the current privacy regime in the United States is something of a patchwork of individual laws resulting in protection for relatively specific types of personal information. Nonetheless, whether by external legislative ratcheting or by public pressure, federal legislative efforts appear to be moving toward greater privacy protections for individual data. Though no comprehensive legislation has yet been passed, various bills currently in the House of Representatives indicate

---

[127] Report from the E.U. Directive Commission, *supra* note 23, at 9.

[128] *Id.*

[129] *See generally id.*

[130] *Id.* at 22.

[131] *Id.* at 22–26.

that privacy concerns are coming to the forefront of legislators' minds in the United States. For example, a survey of current House Bills shows titles such as the Global Internet Freedom Act,[132] the Wireless Privacy Protection Act,[133] and the Defense of Privacy Act.[134] Descriptions of these Bills further indicate a leaning toward protecting individual data privacy.[135]

Beyond pending legislation, recently implemented legislation bolsters the contention that privacy restrictions in the United States will only become more stringent as they come in line with E.U. and international requirements as well as with simple constituent sentiment. The Health Insurance Portability and Accountability Act (HIPAA) of 1996 may be the most comprehensive example of such legislation, affecting a broad range of patient data while prescribing specific requirements for the transfer of that data.[136] Moreover, again illustrating the broad reach of the E.U. Data Directive, it has been noted that, "[a]lthough the purposes espoused for enacting HIPAA seem to be purely domestic in character, it may be that HIPAA is the needed cure for healthcare compliance with the E.U. Directive."[137] The other most recent and most well known such legislation includes the COPPA Act of 1998, aimed at protecting children's online privacy.[138]

Interestingly, in reflecting the role of public perception on driving legislation, it has been said that the HIPAA Act was part of a "concerted effort to restore trust in the healthcare system by limiting access to personal health information."[139] Inherent in

---

[132] H.R. 48, 108th Cong. (2003).

[133] H.R. 71 108th Cong. (2003).

[134] H.R. 338 108th Cong. (2003).

[135] *See generally* EIPC Bill Track, *available at http://www.epic.org/privacy/bill_track.html* (contains tracking information and related bills).

[136] Health Insurance Portability and Accountability Act, Pub. L. No. 104-91, 110 Stat. 1936 (1996).

[137] Ryan Lowther, *U.S. Privacy Regulations Dictated by E.U. Law: How the Healthcare Profession May be Regulated*, 41 COLUM. J. TRANSNAT'L L. 435, 451 (2003). For a review of HIPAA concerns from a Wisconsin perspective, see Timothy A. Hartin, *New Federal Privacy Rules for Health Care Providers*, WISCONSIN LAWYER , April 2002, at 14.

[138] 15 U.S.C.A. § 6501 (West. Supp. 1998).

[139] Lowther, *supra* note 137, at 451 (citing Lisa J. Sotto, *Privacy Concerns in the Health Care Industry*, 632A PLI/Pat 803, 836 (2001)).

this statement is that there was some semblance of distrust of the healthcare industry that needed to be remedied. Interestingly, this statement mirrors closely that portion of the Commission of the European Communities report indicating that most individuals in the E.U. viewed the Data Directive as providing only the minimum level of protection.[140] That is, whether in the United States or the E.U., there would seem to be some sense of a right to privacy inherent in western culture. As the internet age continues to make it easier to invade this right, it seems logical that public pressure to protect will increase, thus making data protection legislation more likely.

From a more anecdotal perspective, public sentiment has helped support this legislative drive. Again, the national "do not call" list's success indicates the American public's strong desire for privacy protections.[141] Indeed, the complete lack of public outcry over any of the more recently enacted privacy legislation supports the argument that legislators would do well to further support privacy legislation. In fact, nothing to this point indicates that lawmakers will back off from implementing further privacy legislation.

For example, the FTC's ability to invoke enforcement mechanisms for Safe Harbor violations indicates the government's growing willingness to support and enforce privacy protections.[142] Specifically, Microsoft entered into a consent decree with the FTC where it agreed to be monitored for twenty years under the threat of serious civil penalties. In this instance, Microsoft was charged with violating its own stated privacy policies for its .NET Passport system.[143] Further examples include JetBlue Airways' attempted sale of passenger data and Northwest Airlines' sale of its passenger data for use by the Department of Homeland Security. Finally, public outcry over perceived privacy and ethical violations is occurring with greater frequency. As such, pending and recently enacted legislation, coupled with various instances of public support for such legislation, show that the United States

---

[140] Report from the E.U. Directive Commission, *supra* note 23, at 9.

[141] *Do Not Call Registrations Exceed 50 Million*, *supra* note 105 (indicating that over 50 million people had placed their names on the "do not call" list by September of 2003).

[142] *See Extraterritoriality in a Globalizing World*, *supra* note 23, at 315–16.

[143] *Id.* at 316.

is starting to get serious about implementation of privacy protection provisions.

C. Current Privacy Regime and Public Sentiment in Canada

While reviewing the E.U. privacy push is valuable for the reasons already mentioned, namely that its direction drives the likely future of worldwide privacy policy, a brief review of Canada's privacy push is useful simply because our national trade with the country has reached significant proportions. Specifically, U.S.-Canada trade was over four hundred billion dollars in 2000.[144] Again, this sum is approximately equal to the sum of our trade with Japan, China, Germany, and the United Kingdom.[145] That said, Canada's recent 2001 PIPEDA Act[146] is of primary importance since its success will likely dictate not only the future face of privacy legislation in Canada, but will also affect the face of privacy legislation in the United States through both example and by a ratcheting of externalities similar to those discussed in relation to the Data Directive. Moreover, the broad scope of PIPEDA, coupled with the Canadian court system's commitment to privacy protection, removes the need for turning to anecdotal evidence of public support as a driver for heightened privacy legislation. Rather, one might infer that the combination of clear legislative and clear judicial support indicates fairly broad public support of privacy protection in Canada.

While Canada may have thus far exhibited a stauncher commitment to privacy regulations than has the United States, this is not to say that Canada's political spectrum is without trouble in this arena. In fact, the Quebec government has challenged the constitutionality of the Act, thereby threatening the law's very existence.[147] The suit is expected to make its way to Canada's Supreme Court in late 2004 or early 2005.[148] The suit has given voice to various opponents of the plan and must certainly give

---

[144] Spaeth et al., *supra* note 66, at 29.

[145] *Id.*

[146] *Id.*

[147] Michael Geist, *Fighting Privacy Law Questionable*, The Toronto Star, Jan. 19, 2004, at CO2.

[148] *Id.*

pause to any individual hoping for implementation of overarching privacy legislation in the United States. Certainly, if provincial interests are able to hijack privacy legislation in an environment where there is a considerably deeper commitment to privacy than in the United States, one must question the prospects for similar comprehensive legislation in this country.

To be sure, the outcome of this litigation should be closely watched and its outcome viewed as instructive for any similar such attempts in this country, not only for the prospects of such legislation here if such a suit is unsuccessful, but also for the potential economic ramifications if defeated. Since PIPEDA received the E.U.'s seal of approval in 2002, all threat of data blockage between the two entities was removed.[149] Should PIPEDA be found unconstitutional, this approval will be lost and the ramifications could be severe, with each province being required to obtain its own adequacy finding and the law's removal creating a variety of other regulatory costs which may severely hamper Canada's economy.[150]

D. Current Privacy Regime and Public Sentiment in Wisconsin

For a variety of reasons, a review of Wisconsin's privacy regime vis a vis the United States privacy regime shows few differences, mainly due to a lack of attention to consumer privacy issues in the state. For this reason, the bulk of consumer privacy regulations affecting the state have been implemented by the federal government. This is evidenced by the fact that Wisconsin's privacy statute "surprisingly has been the source of limited judicial attention with relatively few published court opinions providing shape to this important law."[151] Additionally, there appears to be a relative lack of commentary or attention to privacy issues in the state. As such, the blanket statement that the Wisconsin privacy regime and public sentiment in the state mirror relatively closely the discussion of the federal situation above must be

---

[149] *Id.*

[150] *Id.*

[151] Bradden C. Backer, *A Federal Court's Recent Rejection of a Wisconsin Court of Appeals Decision Narrowly Construing the Right of Employee Privacy Compounds Uncertainty about Wisconsin's Privacy Protections*, Wisconsin Lawyer, Sept. 2003, at 22.

made for a relative lack of state attention to these issues. It should be noted that this is in no way a negative. Rather, a basic exposure to economics offers the defense that a broad-based, federalized system of privacy regulations reduces inefficiencies created by complicated provincial procedures. For these reasons, the suggestion is made here that interested parties in Wisconsin focus on national and international privacy legislation development for guidance as to what will affect local Wisconsin business.

V. Economic and Other Consequences of Universal Privacy Policies: Balancing the Scales

The costs associated with the burgeoning international privacy regime are not insignificant. To be sure, these costs "will likely result in compliance, transaction, operation, and opportunity costs for U.S. businesses."[152] In Europe, there has been scant talk about the economic ramifications of the overall Data Directive. This may be because of the coincidence of the Data Directive's implementation with the overall effort to integrate Europe and add additional member states to the E.U. That is, the task of separating the actual ramifications of the Data Directive from the extraordinary amount of background noise generated by the formation of a new E.U. with a new single currency and the resultant economic upheaval would be a tall task, indeed.

Still, the general costs associated with Safe Harbor compliance in the United States are likely to mimic, at least somewhat, those of Data Directive compliance in the E.U. A typical description of the costs associated with privacy regulation contends that "costs stem from the Directive's requirement that businesses maintain detailed records of the purposes for which the data was collected and processed. Furthermore, in situations where businesses must obtain the data subject's informed consent before transferring the data, data subjects may elect not to permit the disclosure of their personal information."[153] This analysis then goes on to detail the damages associated with a reduction in information available for decision making, transaction costs associated with acquiring information, lowered productivity

---

[152] Tracie B. Loring, *An Analysis of the Informational Privacy Protection Afforded by the European Union and the United States*, 37 Tex. Int'l L.J. 421, 441 (2002).

[153] *Id.*

due to increased costs and, ultimately, increased prices for consumers.[154] Similar commentators even go so far as to lament that "[i]nternet privacy legislation may sound a death knell for a developing industry."[155] They argue that certain businesses providing privacy verification would become obsolete should the legislature pass comprehensive privacy legislation.[156]

While such points are valid, they are relatively easy to make and also view the problem in a vacuum. When considering these points, one must also look at the alternative problems that, for example, a hospital with a website might currently have. Specifically, the hospital has to deal with the Privacy Act of 1974, HIPAA, COPPA and any relevant state requirements that may be in place. Surely, there are costs associated with maintaining such varied standards. While it is beyond the scope of this article to argue that these costs would be greater than implementation of a singular privacy regime similar to the Data Directive, analyses of the costs of such implementation tend to ignore the realities of the current framework of numerous and unrelated privacy laws and the legal oversight nightmares they create. Additionally, such analyses tend to ignore the fact that the lack of a federal standard decreases efficiency by increasing oversight costs while reducing system visibility.[157]

In addition to factoring the costs associated with the current privacy regime, it is also useful to consider specifically some of the costs claimed to stem from the Data Directive. One example sometimes used regarding individuals exercising their right to inquire into how their data is being used is likely an insignificant problem. Specifically, over 62% of data controllers surveyed by the Commission of the European Communities did not believe responding to data requests was a significant resource drain. In fact, most either did not have figures available or received fewer than ten requests.[158] This statistic is used not to show that the costs of implementing the Data Directive are insignificant, but

---

[154] *Id.*

[155] Angela Vitale, *The E.U. Privacy Directive and the Resulting Safe Harbor: The Negative Effects on U.S. Legislation Concerning Privacy on the Internet*, 35 VAND. J. TRANSNAT'L L. 321, 354 (2002).

[156] *Id.*

[157] *See* Spaeth et al., *supra* note 66.

[158] *See* Report from the E.U. Directive Commission, *supra* note 23, at 9.

rather to demonstrate that blanket assertions about generalized costs are worth little without statistical support. Most criticism centered on implementation costs tends to lack such support.

As such, an accurate cost-benefit analysis is difficult to provide. Perhaps this is because the Data Directive and related Safe Harbor requirements are relatively recent, or perhaps it is because the rapid and extreme changes in the global economy create background noise that is impossible to separate from the actual effects of such legislation.[159] As such, it is useful to focus on complying with existing international privacy standards while attempting to learn from mistakes made in such implementation. After all, as argued above, the ratcheting function that has already spread versions of the Data Directive all over the world, and has affected the United States directly via the Safe Harbor provisions, is unlikely to abate.

While it is likely the case that privacy laws will only become more stringent as ratcheting mechanisms operate by forcing those interested in competing in the global marketplace to comply with E.U. driven privacy standards, it must be acknowledged that "alleged E.U. over-regulation can limit the commercial operations of U.S. enterprises."[160] Nonetheless, international inertia for privacy legislation indicates that while the United States may be able to affect the structure of such legislation, it is unlikely that it will be able to stop it from advancing.[161]

VI. Application: The Likely Future Face of U.S. and Wisconsin Privacy Policy

The ratcheting functions of the international privacy regime discussed above make it likely that the United States will continue to move to adopt transatlantic institutional standards

---

[159] Most commentary which purports to address the effects of privacy regulations on American companies tends to focus on the requirements placed on these companies, with only passing attention to the effects. *See, e.g.,* Dean William Harvey & Amy White, *The Impact of Computer Security Regulation on American Companies*, 8 Tex. Wesleyan L. Rev. 505 (2002).

[160] *See Extraterritoriality in a Globalizing World*, *supra* note 23, at 314.

[161] In considering the ways it might affect legislation, case studies of the effects of privacy legislation on U.S. businesses are useful. *See* Michael E. Staten & Fred H. Cate, *The Impact of Opt-In Privacy Rules on Retail Credit Markets: A Case Study of MBNA*, 52 Duke L.J. 745 (2003).

driven by the Data Directive model.[162] Moreover, the rate of this change is likely to be hastened by the fact that the E.U. market, which is already larger than that of the United States, is only going to become larger and exert more institutional influence as it grows with the potential addition of new member states.[163] Simply stated, the current state of the United States privacy regime, already looking more like the E.U. model with the adoption of provisions such as the Safe Harbor, will continue to migrate toward a universal standard, prodded by the ever growing influence of the E.U. marketplace.[164] This change is being driven not only by the prospect of access to the European market, but also by the need for access to the world market, which is clearly migrating toward the E.U. standard.[165]

From a Wisconsin perspective, the relative lack of attention to comprehensive privacy legislation and the lack of common law precedent in the state context[166] means that federal legislation controls in this realm. This author argues that this will prove advantageous for Wisconsin businesses, as they will need only worry about federal and international concerns without having to navigate potentially conflicting state standards in addition. This is not to say that the legal challenges facing Wisconsin data exporters and importers are insignificant in this realm. Quite the contrary, navigating data regulations imposed by the E.U., Canada, Japan, and all of our other large trading partners will prove precarious, at best. At least one thing is clear, however: due to the enormous current and potential scale of its economy, the E.U. Data Directive model will be the driver for both change and international consistency.

---

[162] Gregory Shaffer, *Reconciling Trade and Regulatory Goals: The Prospects and Limits of New Approaches to Transatlantic Governance Through Mutual Recognition and Safe Harbor Agreements*, 9 COLUM. J. EUR. L. 29, 73 (2002).

[163] See *http://europa.eu.int/abc/governments/index_en.htm* for recent updates as to EU member status.

[164] "The E.U. Directive is the world model for privacy legislation. This is the reality. The latest trend, however, is to find a balance between the E.U. and U.S. models. Canada and Australia are adopting this strategy, and Japan has this model in draft form." Douglas Sacks, *Mexican Data Protection Legislation Looms*, TARGET MARKETING Feb. 1, 2003, at 15.

[165] *See id.*

[166] *See* Backer, *supra* note 151, at 23.

This likely creation of an international privacy regime, while not driven by the United States, could prove beneficial macroeconomically. This point is best proven by analogy to the drivers for the federal pre-emption doctrine, namely that consistency in rules prevents provincial interests from frustrating the functions of a national market.[167] Similar to this doctrine, rather than attempt to reconcile federal requirements including HIPAA, COPPA, the 1974 Privacy Act and other legislation with additional state requirements, the clarification that one overarching standard could provide would certainly help mitigate, if not overcome, the expenses associated with Data Directive and Safe Harbor compliance actions.

Additionally, data protection is beneficial from a public sentiment standpoint. While some may dismiss the calls for privacy legislation as unnecessary, cumbersome, or counterproductive, even the Direct Marketing Association has recognized the need for some form of standardization as a means of protecting its industry from consumer backlash leading to even harsher legislation.[168] Other commentators have found the costs associated with the Safe Harbor standards to be less cumbersome than expected due to current U.S. legislation while finding that such compliance provides a variety of other benefits, including positive public relations.[169] As such, the likely fact that the United States and Wisconsin will have to operate under Data Directive requirements, be it through national legislation or Safe Harbor compliance, promises to make the privacy landscape easier to navigate while providing additional tertiary benefits.

VII. Conclusion

A review of a variety of privacy legislation regimes around the world shows that a standardized law of data protection is making its way around the world, driven by the requirements put

---

[167] *See* Geist, *supra* note 147.

[168] The chair of the DMA's International Council Operating Committee wrote that, "Privacy legislation is a positive. The introduction of privacy legislation in a country should be viewed as good news. Privacy abuse by a small percentage of direct marketers can create a consumer backlash that affects the entire industry." Sacks, *supra* note 164.

[169] David A. Castor, *Treading Water in the Data Privacy Age: An Analysis of Safe Harbor's First Year*, 12 Ind. Int'l & Comp. L. Rev. 265, 283–86 (2002).

in place by the E.U. Data Directive as well as the tremendous threat of restricted access to the gigantic E.U. trading block. Already the United States finds itself in the substantial minority of developed nations who have yet to adopt any comprehensive data protection legislation. As such, it is evident that the current state of privacy affairs will not last much longer, and the United States will be forced to adopt its own law requiring broad-based compliance with a law similar to that of the Data Directive. Moreover, the lack of individual state legislation or common law on the topic means that this federal legislation will control data transfers and protection.

In Wisconsin, businesses dealing with consumer data hoping to expand their core competencies internationally can no longer rely on compliance with state or federal law, since federal law appears behind the international curve and since Wisconsin law has yet to affirmatively address the issue in any meaningful way. Rather, state businesses considering international trade would do well to implement processes and protections in line with the E.U. Data Directive so as to avoid future costly retrofitting of information technology systems, processes and policies in addition to being protected in the event that the Safe Harbor provisions are made to require enhanced privacy protections. While perhaps cumbersome and costly for now, such retrofitting in the future would have exponentially greater costs.[170]

---

[170] A variety of studies have concluded that costs to modify software processes increase exponentially with time. *See, e.g.*, Carmine Mangione, *Software Project Failure: The Reasons, The Costs*, CIO UPDATE, Jan. 3, 2003, *at*: http://www.cioupdate.com/reports/article.php/1563701. Re-engineering of systems, therefore, is to be avoided.