DATA PRIVACY ISSUES - KNOW YOUR RIGHTS AND RESPONSIBILITIES

June 22 – 25, 2008

John L. Nicholson
Pillsbury
Washington, D.C.

Arthur McCombs
John Hopkins University
Baltimore, Maryland

Vadim Schick
Pillsbury
Washington, D.C.

Introduction

American colleges and universities are subject to significant regulation with respect to how they collect, store and use personal information of their students, employees, or patients. U.S. Federal laws provide a fragmented, sectoral approach to data privacy protection, offering separate laws protecting, *inter alia*, students' rights through the Federal Educational Records Privacy Act ("FERPA")[1], patients' rights through the Health Insurance Portability and Accountability Act ("HIPAA")[2], as well as personal financial information through the Graham-Leach-Bliley Act ("GLBA")[3]. In addition to these Federal laws, colleges and universities may be required to comply with the payment card industry data security standards ("PCI DSS")[4] if they process credit card payments (e.g., at the campus bookstore or restaurants/dining halls or for tuition or donations). As if that weren't a sufficiently complicated framework, many U.S. states have privacy laws of different types, covering a broad range of requirements, from collection and use of information to data breach notification provisions. California has long been the forerunner with regard to privacy law, and most states have selected aspects of California's laws to implement. At least 40 U.S. states, Washington, D.C., and Puerto Rico have enacted some kind of data breach notification law, and even within the data breach notification laws, there is broad variation with regard to information covered, breaches requiring notice, type of notice required and potential liability. For example, California has strict data breach notification laws that cover data (including medical data) about California residents regardless of where that data is actually held, and imposes limited liability for damages caused by such breaches on the merchants. Minnesota, in addition to its data breach notification law, imposes significant liability on merchants responsible for data breaches. Finally, for institutions with foreign students and international campuses, international regulations, such as the EU's directive

---

1 20 U.S.C. § 1232(g) (2008).

2 Pub. L. 104-191, 110 Stat. 1936 (1996).

3 15 U.S.C. §§ 6801-6809 (2008).

4 Payment Card Industry Data Security Standard, Version 1.1, Requirement 3 (September 2006) available at https://www.pcisecuritystandards.org/tech/pci_dss.htm (last accessed April 28, 2008).

regarding the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (the "EU Directive") and Canada's Personal Information Protection , [5] impose certain restrictions on the trans-border transfer of personal data. This paper offers a broad overview of the data privacy protection regime, as it applies to institutions of higher education. Part I provides an overview of the U.S. and international data privacy protection framework. Part II offers suggestions regarding ensuring compliance and minimizing risk of data breach. Finally, Part III provides some guidelines for handling a data breach, if one occurs.

Part I: Overview of Data Privacy Regulation

A. United States (Federal) Framework

The United States has no single definition for protected personal information, only definitions specific to individual statutory and self-regulatory regimes. Congress has been reluctant to enact comprehensive legislation protecting all of an individual's private information. Instead, federal authorities focused on a few industries and sectors where it is foreseeable that disclosure of personal information could result in harm to the individual. Most notable are health care, with the passing of HIPAA in 1996, and financial institutions, with the enactment of GLBA in 1999.[6]

In many ways, Congress has been reactive, rather than proactive, in passing data privacy legislation. The Video Privacy Protection Act of 1988 was passed after reporters gained access to titles of videos rented by Supreme Court nominee Robert Bork, which led some critics to joke that in the United States "video rentals are afforded more federal protection than are medical records."[7] The murder of Hollywood actress Rebecca Shaffer by a stalker who got her address from the California Department of Motor Vehicles led to the enactment of the U.S. Driver's Privacy Protection Act of 1994.[8] Consumer concerns over misuse of their phone numbers by telemarketers led to the Do-Not-Call Implementation Act of 2003, establishing the Do-Not-Call Registry administered by the Federal Trade Commission.[9] Similarly, growing concerns from Internet Service Providers (ISPs) and consumers regarding e-mail spam resulted in the Controlling the Assault of Non-Solicited Pornography And Marketing Act (CAN SPAM) of 2003.[10]

The Family Educational Rights and Privacy Act of 1974 ("FERPA") currently governs the privacy of students' education records in the United States. Originally enacted in 1974,

---

[5] *See* Council Directive 95/46, The Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L281) 31 (EC) [hereinafter EU Directive].

[6] 42 U.S.C. § 201 (2087); 15 U.S.C. § 6801 (2008).

[7] Trevor Shaw, Dir. Gen., Audit & Review, Office of the Privacy Comm'r of Can., International Perspectives on Privacy & Security, Address to the Dep't of Homeland Sec. Data Privacy & Integrity Comm. (Sept. 28, 2005), available at www.privcom.gc.ca/speech/2005/sp-d_050928_ts_e.asp (last accessed April 28, 2008).

[8] Francesca Bignami, *Transgovernmental Networks vs. Democracy: The Case of the European Information Privacy Network*, 26 MICH. J. INT'L L. 807, 819 (2005).

[9] *See* Do-Not-Call Implementation Act of 2003, Pub L. 108-10, 117 Stat. 557 (2003).

[10] *See* CAN-SPAM Act of 2003, Pub. L. 108-187, 117 Stat. 2699 (2003).

Congress has amended FERPA nine times, most recently under the USA Patriot Act of 2001.[11] FERPA regulates the access to, amendment of, and disclosure by schools of education records.[12] All schools receiving funds from any US Department of Education program must comply with FERPA, and parents or eligible students either over the age of 18 or attending post-secondary schools are protected by FERPA.[13]

As part of its requirements for schools' disclosures of educational records, FERPA mandates that in order for a post-secondary school to release any information from a student's school record, the school must first obtain written permission from the eligible student.[14] Many exceptions to this consent requirement exist, including disclosure to, *e.g.* other school officials with "legitimate educational interest"; other schools to which a student is transferring; and to authorities performing audits or enforcing relevant Federal laws.[15] Schools may also disclose information from education records pursuant to a subpoena or court order or information that constitutes "directory information".[16] According to the current rules under FERPA and the accompanying regulations, "directory information" includes an eligible student's name, address, telephone number, date and place of birth, honors and awards and dates of attendance.[17] However, a student retains the right to request that a school not disclose "directory information".[18]

On March 24, 2008, the Department of Education released additional proposed amendments to the FERPA regulations.[19] All public comments on the proposed legislation must be submitted to the Department of Education by May 8, 2008.[20] The amendments seek to incorporate prior legislative amendments and two Supreme Court FERPA decisions into the legislation, as well as address disclosure concerns raised by the tragic shootings that occurred at Virginia Tech in 2007.[21] Generally, the purpose of the proposed regulations is to clarify the existing privacy regime under FERPA rather than significantly substantively alter the rules. A few examples of proposed changes to the current legislative structure include: specifying that an eligible student's social security number is not directory information; permitting schools to disclose information pursuant to an outsourcing relationship; and allowing schools more

---

[11] *See* "Legislative History of Major FERPA Provisions" available at http://www.ed.gov/print/policy/gen/guid/fpco/ferpa/leg-history.html (last accessed April 28, 2008).

[12] *See* 20 U.S.C. § 1232(g) (2008).

[13] Under FERPA, parents have the rights of access and amending educational records until the student turns 18 or attends a postsecondary institution. Once an eligible student possesses FERPA rights there are only very limited circumstances under which a parent may access the eligible student's records (*e.g.* if the parents claim the eligible student as a dependent under the Federal tax regime). *See* "FERPA General Guidance for Students" available at http://www.ed.gov/print/policy/gen/guid/fpco/ferpa/students.html (last accessed April 28, 2008).

[14] *Id.*

[15] *Id.*

[16] *See* 20 U.S.C. § 1232(g) (2008).

[17] *Id.*

[18] *Id.*

[19] *See* Federal Register, Vol. 73, No. 57/ Monday March 24, 2008, Proposed Rules, pp. 15574-15602.

[20] *Id.*

[21] *Id.*

flexibility in its disclosure of information in connection with a health or safety emergency.[22] Because the proposed amendments were released to the public so recently, little commentary about the future state of university FERPA compliance has been published at this time.[23] However, a few blogs have commented on the proposed regulations, noting that a major outcome of the proposed legislation would be to provide greater flexibility to colleges and universities in disclosing eligible student information in the "interest of health and safety".[24]

Despite the fact that a detailed discussion is outside the scope of this paper, U.S. colleges and universities should also be aware of HIPAA due to its application to college and university health centers and any institution with a medical school. HIPAA is the Federal statute that provides for privacy and standardized transmission of health records and information. This statute specifically applies to health plans, health care clearinghouses, and providers that are covered by the regulation (called "covered entities") that transmit health records. HIPAA protects "individually identifiable health information" which includes demographic information collected from an individual that is either created by a health care provided or relates to treatment of an individual.[25] The lead agency for HIPAA management and enforcement is the Department of Health and Human Services.

U.S. colleges and universities may be subject to GLBA. Colleges and universities are generally not exempt from GLBA compliance. To the extent that an institution of higher learning engages in lending funds (whether to students or faculty), collecting loan payments, or facilitating the process of applying for financial aid, the institution may be considered a "financial institution" subject to GLBA regulation. There are two categories of compliance requirements under GLBA: the Safeguarding Rules and the Privacy Rules. The Privacy Rules govern the use and disclosure of personal nonpublic information. The Safeguarding Rules set forth requirements with respect to the manner in which financial institutions are expected to protect nonpublic information in their custody or control. Any institution of higher learning that complies with FERPA and the regulations promulgated pursuant to FERPA is considered to be in compliance with the Privacy Rules. However, there is no similar accommodation for institutions of higher learning in connection with the Safeguarding Rules. The Safeguarding Rules require financial institutions to develop, implement and maintain a comprehensive security program consisting of administrative, technical and physical safeguards to protect against the unauthorized use or disclosure of nonpublic personal information.

Additionally, any college or university that extends credit to students may be subject to the new rules on *Identity Theft Red Flags and Address Discrepancies Under the Fair and*

---

[22] *Id.*

[23] We anticipate that further commentary will be published by June 22, 2008 to discuss during the NACUA conference.

[24] See *e.g.*, The Chronicle of Higher Education News Blog, "Education Department Proposes New Student-Privacy Rules", March 24, 2008 available at www.chronicle.org (last accessed April 28, 2008); *see also e.g.* The Bazelon Center for Mental Health Law, "Proposed Rules Expand Disclosure of Student Information," April 15, 2008 available at www.bazelon.org/issues/education/takeaction/4-08FERPAregs,htm (last accessed at April 28, 2008).

[25] 45 C.F.R. § 160.103 (2008).

Accurate Credit Transactions (FACT) Act of 2003.[26] These rules implement § 114 and § 315 of the FACT Act, which specifically call for "establishment of procedures for the identification of possible instances of identity theft" and "reconciling addresses."[27] The rules require: (1) financial institutions and creditors to develop and implement a written "Identity Theft Prevention Program" to detect, prevent and mitigate identity theft in connection with certain covered accounts, (2) credit and debit card issuers to assess the validity of notifications of changes of address in conjunction with a request for a new card, and (3) any user of consumer credit reports to implement reasonable policies and procedures when a consumer reporting agency sends a notice of address discrepancy.[28] The new identity theft and address discrepancy rules took effect on January 1, 2008. Affected entities have been given ten months to review their current practices, develop security programs, and implement the necessary changes before full compliance is expected by November 1, 2008.

Finally, the ongoing "War on Terror" has produced another set of reactionary Congressional legislation that significantly affects citizens' privacy rights, most notably the USA PATRIOT Act of 2001.[29] This may have particular repercussions for research universities which may be pressured by the federal government to disclose personal information of any U.S. or foreign national working on sensitive projects at that university. While the details of this and other anti-terrorism-related legislation are outside of the scope of this paper, it is important to note that these provisions affect the basic privacy rights of both American citizens and non-U.S. citizens studying or working at U.S. institutions of higher learning.

B. PCI Standards

In December 2004, Visa and MasterCard announced an agreement to align their data security programs for merchants and third party processors, which led to the creation of a standard known as the Payment Card Industry (PCI) Data Security Standard (DSS). PCI DSS was designed to guard against attacks that involve theft and subsequent misuse of cardholder information, and consists of twelve requirements (though each requirement includes a few sub-requirements).

The twelve PCI DSS requirements include: *building and maintaining a secure network* (Requirement 1: Install and maintain a firewall configuration to protect cardholder data and Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters); *protecting cardholder data* (Requirement 3: Protect stored cardholder data and Requirement 4: Encrypt transmission of cardholder data across open, public networks); *maintaining a vulnerability management program* (Requirement 5: Use and regularly update anti-virus software and Requirement 6: Develop and maintain secure systems and applications); *implementing strong access control measures* (Requirement 7: Restrict access to cardholder data by business need-to-know, Requirement 8: Assign a unique ID to each person with computer

---

[26] The rules have been promulgated by Department of Treasury Office of the Comptroller of the Currency, the Federal Reserve System, the Federal Deposit Insurance Corporation, the Department of Treasury Office of Thrift Supervision, the National Credit Union Administration, and the Federal Trade Commission.

[27] Pub. L. 108-159 §§ 114, 315 (2003).

[28] *See* Federal Register, Vol. 72, No. 217, Friday November 9, 2007 at 63718.

[29] *See* USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

access, and Requirement 9: Restrict physical access to cardholder data); regularly monitoring and testing networks (Requirement 10: Track and monitor all access to network resources and cardholder data and Requirement 11: Regularly test security systems and processes); and maintaining an Information Security Policy (Requirement 12: Maintain a policy that addresses information security).

Depending upon how many payment transactions a college or a university processes each year, the payment card associations may require the school to validate its compliance with PCI DSS through an on-site assessment performed by an independent third party assessor. For example, Level 1 compliance is reserved for more than six million Visa or MasterCard transactions per year or more than 2.5 million American Express transactions a year. Level 2 covers 150,000 to 6 million transactions for Mastercard; 1 million to 6 million transactions for Visa; and 50,000 to 2.5 million transactions. Level 3 covers 20,000 to 1 million Visa e-commerce transaction; 20,000 to 150,000 e-commerce MasterCard transactions; and less than 50,000 American Express transactions. Level 1 requires an annual on-site PCI data security assessment performed by a qualified third party auditor and signed by an Officer of the complying school, and a quarterly network scan performed by a qualified independent scan vendor. Levels 2 and 3 require an annual PCI self-assessment questionnaire by the school and a quarterly network scan performed by a qualified independent scan vendor.

C. States' Laws

California was one of the first states in the country to regulate privacy and, today it has the most comprehensive framework of state-level privacy laws in the country.[30] California privacy laws are also some of the most stringent in the country, requiring safeguards for a wide variety of resident's personal information. As such, most of the privacy laws in existence in other states encompass some aspect of the California privacy framework. Understanding California's privacy laws offers insight into the breadth of state privacy laws in existence throughout the country.

California privacy laws cover a broad set of subject areas including: arrest records, cable television subscriber information, check printing, computer crimes, credit card numbers, credit reporting, debt collection processing, motor vehicle records, ecommerce, employment records, false personation, financial records, invasion-of-privacy, investigative consumer reports, insurance information, medical records, police records, school records, sex offender registration, stalking, tax records, telephone records and solicitation, video store lists, voter registration records, and wiretapping. A notable component of California's privacy laws is that in a number of cases, the laws reach beyond California state borders. Many of this state's privacy laws apply to any entity that stores a California resident's information or transacts business with a Californian, regardless of where that entity is located. For colleges and universities, this means that as long as one student on campus is from California, your institution may be subject to California privacy laws.

[30] Article 1, Section 1 of the California Constitution states: "The right to privacy is an inalienable right granted to all people under the California Constitution."

One of the most significant areas of state-level privacy regulation relates to data breach notification. Forty states, the District of Columbia, and Puerto Rico have enacted data breach notification laws. The primary purpose of these laws is to establish guidelines for when entities that store personal information must inform individuals that their information has been compromised. Three states' laws, California, Minnesota and Georgia, provide a survey of the different data breach notification approaches.

California's data breach notification law, which was the first law of its kind when adopted, requires entities to immediately notify residents if certain unencrypted personal information is compromised.[31] The law specifically requires notice if the breached personal information is coupled with the resident's first name, or first initial, and last name. The personal information that triggers the California statute includes: (1) social security numbers; (2) driver's license numbers or California Identification Card numbers; (3) account numbers, credit or debit card numbers, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (4) medical information; or (5) health insurance information. Under this law, notice must be given in "the most expedient time possible and without unreasonable delay."[32] Furthermore, if immediate notice is not offered, residents have a private cause of action for damages and injunctive relief. The California data breach notification law now serves as the model for most other states.

Minnesota's approach is notable because not only does this state have a standard data breach notification provision, but in 2007 it became the first state to codify one of the PCI standards.[33] This particular Minnesota law imposes strict liability on merchants following a data breach if the merchant retains credit or debit card security data after the transaction is completed. The law specifically prohibits storage of "card security code data, the PIN verification code number, or the full contents of any track of magnetic stripe data." By requiring the destruction of this type of sensitive authentication data immediately following a transaction, the Minnesota law gives legal effect to Requirement 3 of the PCI DSS.

Finally, Georgia's law represents one of the more lenient data breach notification statutes in the country. The Georgia law only applies to information brokers, defined as "any person or entity who, for monetary fees or dues, engages in whole or in part in the business of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring, or communicating information concerning individuals for the primary purpose of furnishing personal information to nonaffiliated third parties."[34] This definition includes entities such as Choicepoint and other marketing firms, but specifically excludes Georgian governmental agencies. Colleges and universities are also likely outside the scope of the Georgia law.

California, Minnesota and Georgia illustrate the different types of data breach notification laws in existence, however, there is still tremendous variation among each of the existing state statutes. In particular, most data breach notice laws have divergent standards related to the type

---

[31] CAL CIV CODE §§ 1798.29; 1798.82 (2008).

[32] CAL CIV CODE § 1798.82(a) (2008).

[33] MINN. STAT. §§ 325E.61, § 325E.61 (2008).

[34] GA. CODE §§ 10-1-910-911 (2008).

of breach that triggers notice, the timing requirements of notice, and exemptions for notification if encrypted data is compromised or other factors are satisfied. These divergent data breach notification standards can present compliance challenges, and, as such, national legislation to unify these standards is being debated. In fact, there are currently two measures being considered at the federal level. These proposed measures include the Data Accountability and Trust Act and the Personal Data Privacy and Security Act of 2007.[35] Each of these pieces of legislation would pre-empt existing state data breach notification laws, however, there is no indication that immediate progress will be made on either of these initiatives.

D. International Data Privacy Regime

The groundwork for the international data privacy regime was laid in the 1970s, with the development and adoption of the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (the Guidelines) promulgated by the Organization for Economic Cooperation and Development (OECD).[36] OECD Guidelines included provisions regarding notice, consent, transfers, access, integrity, and safety of personal information.[37] In 1995, the EU Parliament passed the EU Directive, which set a minimum standard for EU member states' comprehensive legislation on data privacy protection.[38] Broadly, the EU Directive allows private entities to collect only a limited amount of protected personal data and only for a specific permitted purpose. Further, such companies are required to provide notice to data subjects regarding the purpose for which the information is being gathered, and also may be required to obtain consent from the data subjects in order to use or disclose the information to a third party. Finally, the EU Directive closely regulates transborder transfers of protected data, and allows for imposition of serious sanctions against violators.

At the time of passage of the EU Data Directive, Canada occupied the middle of the spectrum of data privacy protection, somewhere between the laissez-faire approach of the United States, and the strictly regulated European model. However, Canada has been gradually moving closer and closer to the European Union. With PIPEDA's passage in 2000 and its full implementation in 2004, the European Union recognized Canada as providing "adequate" data privacy protection, which connotes protection at least equal to the one afforded by the EU Directive. PIPEDA brought significant changes to how businesses use Canadians' personal information.

Both the EU Directive and PIPEDA adopt extraordinarily broad definition of "personal information."[39] The EU Directive covers all information "relating to an identified or identifiable natural person."[40] Specifically, the European Union's definition of "personal data" means "any

---

[35] H.R. 958, 110th Cong. (2008); S. 495, 110th Cong. (2008).

[36] OECD, OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA [hereinafter OECD GUIDELINES] available at http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html (last accessed April 28, 2008).

[37] *Id.*

[38] *See* EU Directive, *supra* note 5.

[39] *See* EU Directive, *supra* note 5, at art. 2(a); PIPEDA, 2000 S.C., ch. 5 § 2(1) (Can.).

[40] *Id.*

information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."[41] PIPEDA applies to entities using or disclosing such information during the course of a "commercial activity", which includes selling or leasing donor, membership or other fundraising lists (the latter being crucial to any development efforts for universities or hospitals.)[42] Table 1 does not provide a complete list of protected data, but gives an impression of just how far the various data protections laws of the European Union and Canada can reach.[43]

Table 1: Sample Protected Personal Data or Information

• First name or initials • Last name • Video programming activity • E-mail address • Internet Protocol (IP) address • Personnel files • GPS data • Payment History • Income • Military History • Criminal charges, convictions, certain court records • Merchandise and product order history • Financial transaction information • License and certificate numbers • Account numbers • Internet URLs • Device identifiers (serial numbers on blackberries, phones) • Hospital dates of: birth, admission, discharge, and death • Geographic subdivisions smaller than a state (street address) • Health Plan beneficiary numbers • Customer loyalty program records and details	• Employment History • Body identifiers (tattoos, piercings) • Education records • Descriptive consumer listings • Customer relationships • Credit reports and credit scores • Credit card purchases • Loan or deposit balances • Credit card numbers • Vehicle identifiers (license plate numbers) • Conversations (recorded or overheard) • Voting history • Debit card numbers • Biometric identifiers (DNA, finger, iris, and voice prints) • Information concerning children • Medical care information • Unique identifiers that can be attributed to a specific individual • Full-face (and comparable) photographic images • Service subscription history • Fax number • Telephone number • Fraud alerts

[41] *Id.*

[42] PIPEDA, 2000 S.C., ch. 5 § 4 (Can.). Canadian law gives an equally broad scope to the definition of commercial activity, defining it as "any particular transaction, act or conduct that is of a commercial character, including selling, bartering or leasing of donor, membership or other fundraising lists."

[43] *See, e.g.*, Rebecca Herold, *Privacy, Compliance and International Data Flows: White Paper*, NET IQ at 4 (June 2006).

The EU places unique and severe restrictions on the export of personal information from the European Union by private actors.[44] Protected data may be transferred outside of the European Union only to a country with "adequate" data privacy protections, meaning protections substantially similar to or greater than those offered by the EU Directive. The EU Directive allows for transfers of personal information to an entity in a country that does not guarantee an adequate level of privacy protection and that has not assented to Safe Harbor or implemented binding corporate rules if: (1) the data subject unambiguously consents to the transfer; (2) transfer is necessary for the performance of a contract between the data subject and the business; (3) transfer is necessary for the entry and/or performance of a contract between the business and a third party for the data subject's benefit; (4) transfer is justified on "important public interest grounds" or for purposes of a lawsuit; (5) transfer is necessary to protect the vital interests of the data subject; or (6) information is from a database to which the public has routine access because of national laws on access to documents.[45] EU member states may create other exceptions to the transborder transfer restrictions, but they must notify the European Commission and other member states of any such exemptions.[46]

PIPEDA also regulates transborder transfers of protected data. PIPEDA applies to information gathered prior to its enactment, and applies to non-Canadian businesses gathering information about Canadians.[47] However, non-Canadian entities' obligations under PIPEDA are unclear once the information is transferred and then stored outside of Canada. American colleges and universities gathering information on perspective students, employees or patients are certainly affected by PIPEDA while collecting the information in Canada, or acquiring it from a Canadian partner, because PIPEDA's secondary data transfer requirement forces Canadian businesses to include PIPEDA's privacy requirements in all contracts contemplating transfer of Canadians' personal information abroad.[48]

European authorities take data subjects' complaints and corporate compliance in general very seriously. "The EU nations have assessed millions of dollars in fines for noncompliance with the EU Data Protection Directive and applicable country privacy laws," writes Rebecca Herold, "with a couple of the highest to date running at 840,000 Euros (approximately US$900,000) and 1.08 million Euros [(approximately US$1.16 million)] . . . [and many] of these actions have been related to moving data over country borders to a receiving country that is not considered as having adequate data protection requirements, such as the United States."[49] For example, in 2001 Spain alone imposed fines against 500 companies totaling over $13 million, and the EU member states plan to conduct joint audits of data protection in health insurance

---

[44] Public actors are allowed much more leeway in using or disclosing personal information to a third party for diplomatic or national security reasons. *See* EU Directive, *supra* note 5 (see Chapter IV – Transfer of Personal Data to Third Countries, Articles 25-26).

[45] *See* Bignami, *supra* note 8, at 826; *see also* EU Directive *supra* note 5, art. 7.

[46] One example of an exception is allowing a transborder transfer if a contract between an and the receiving party outside the EU—specifically, not a "safe" country for personal information—renders that party liable in tort for any loss or theft of the personal information. *See* Bignami, *supra* note 8, at 826.

[47] *See* PIPEDA, 2000 S.C., ch. 5 § 4 (Can.).

[48] *Id.*

[49] Herold, *supra* note 43, at 1.

companies.[50] Canadian authorities have also remained vigilant, launching 1700 investigations in 2002 alone. In 2003, Canada completed 278 PIPEDA compliance investigations, and the number went up to 379 investigations in 2004.[51] However, the Privacy Commissioner in Canada is significantly under-funded. If Canadian Parliament gives the Privacy Commissioner greater funds, as requested in her 2005-06 Annual Report, the Commissioner will likely increase the number of audits and investigations.[52]

Table 2: Relevant Legislation in U.S., Canada and the E.U.

	United States	**Canada**	**European Union**
Relevant Statutes	*No overarching data privacy legislation or scheme* Important "sector" federal legislation: - FCRA (1970)[53] - Privacy Act (1974) - Telecom Act (1996) - HIPAA (1996) - COPPA (1998)[54] - GLB (1999) - CAN SPAM (2003) - FERPA (200_)	PIPEDA (2000) and "substantially similar" provincial laws Other important federal legislation: - Privacy Act (1985)	The EU Directive (1995) and member states' laws
Enforcing Agencies	FTC is responsible for enforcement of businesses' compliance with the Safe Harbor provisions and relevant privacy legislation. Department of Education is responsible for enforcement of compliance with FERPA.	Administered by the Privacy Commissioner (established in 2000); Office of the Superintendent of Financial Institutions (OSFI) supervises offshoring of data during outsourcing transactions for financial institutions.[55]	Administered and enforced by the member states' commissions and by the European Data Protection Supervisor on the Union level.

[50] *Id*.

[51] *Id*.

[52] Office of the Privacy Comm'r of Can., *Annual Report to Parliament 2005: Report on the Personal Information Protection and Electronic Documents Act*, 3 (2006) available at http://www.privcom.gc.ca/information/ar/200506/200506_pa_e.pdf (last accessed April 28, 2008); *see also* Herald, *supra* note 43, at 1 ("privacy enforcement authorities have stated that they are just getting started and expect enforcement to increase markedly").

[53] Fair Credit Reporting Act, 15 U.S.C. § 168 *et seq*. (2008).

[54] Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-06 (2008).

[55] George Takach, *Canada: Outsourcing and Offshoring: Myths, Realities, The Hurdles and How to Do It Right*, MONDAQ BUS. BRIEFING, July 20, 2006, available at http://www.mondaq.com/article.asp?articleid=41386&searchresults=1 (last accessed April 28, 2008). *See also* Canadian Office of the Superintendent of Financial Institutions available at http://www.osfi-bsif.gc.ca/osfi/index_e.aspx?ArticleID=3 (last accessed April 28, 2008).

	United States	Canada	European Union
Relevant State and Province Legislation	Many States, including California and Georgia, adopted more stringent data privacy legislation	Alberta, British Columbia, and Quebec have their own data privacy legislation that was recognized to be substantially similar to PIPEDA. PIPEDA still applies in other provinces, and applies to all inter-provincial data transfers.	Each member state has adopted its own data privacy legislation, which must be in accord with the EU Directive.

Part II: Key Considerations for Colleges and Universities

As mentioned above, U.S. colleges and universities are subject to significant regulation with respect to how they collect, store and use personal information of their students, employees, or patients. Schools collect and use information from perspective applicants (many of whom are under 18), parents of applicants and students, alumni and their partners and spouses, and, of course, donors. Schools collect personal information, including sensitive financial information, in a great variety of ways: the Internet, mail and telephone solicitation, and campus events. Finally, schools collect information from a huge range of geographies: numerous U.S. states and foreign countries (including from citizens of the E.U. and Canada). Thus, compliance with the mosaic of various data privacy protection regulations is crucial to any school. This Part II offers a few general guidelines for achieving such compliance.

First, accountability serves as the cornerstone of compliance with privacy laws. Every school collects, stores and uses personal information regarding its students, employees, or patients, and each such school is ultimately responsible for keeping all personal information safe. This primarily means that colleges and universities should adopt privacy policies which comply with basic principles of data privacy protection and train the relevant staff with respect to these policies. Organizations should appoint an individual or team within such organization (e.g., a chief privacy officer or a similar senior executive) who will be responsible for compliance and will have the ability to address complaints. In the for-profit higher education industry, it is important to note that subsidiaries and affiliates may be considered separate entities under international privacy laws, and may require additional staff and resources for compliance. Significantly, university leadership must provide meaningful support and sponsorship to its privacy specialists.

Second, some jurisdictions, certainly European countries and Canada, may require the "knowledge and consent" of the data subject for collection, use or disclosure of personal information.[56] There are a few exceptions to this general rule on both sides of the Atlantic,

[56] Further, both EU and Canada require that personal information must be collected and used only for the specific, stated purpose. For example, if an Italian citizen requests information regarding Johns Hopkins' Bologna center for admission purposes, Johns Hopkins may not disclose or use his information for donation solicitation or cross-selling other its partners products. Thus, schools should limit the collection and use of protected personal information accordingly. If your school has campuses or partnerships in Europe or Canada, and does not monitor

including disclosure for law enforcement, artistic, and journalistic purposes. Consequently, schools should be aware of what data they are collecting, using, or disclosing, and in what jurisdictions.

Colleges and universities should also consider using waiver and consent forms for its applicants, potential applicants and students, and implement clear privacy policies for visitors to its Web sites. Schools must make their privacy policies and procedures transparent. They have to make readily available to individuals specific information about their policies and practices relating to the management of personal information.

Third, schools should develop and implement procedures to keep the personal information they have is necessary, accurate, complete, and up-to-date (including, where applicable, whether the identified purpose for collecting and using such information are accurate and up-to-date). The data subject should have the right to access the information held by the school. In some instances, schools may be required to inform the data subject (upon request) of the existence, use, and disclosure of his or her personal information and provide access to that information. Data subjects must be able to challenge the accuracy and completeness of the information, and schools must amend the information accordingly. The simplest way for any institution to comply with these requirements is to include contact information of its privacy office on its Web site and/or in its published privacy policy. Also, data subjects should have the ability to file a complaint directly with the college or university regarding the school's use of personal information. Schools should implement procedures to receive, investigate, resolve, and respond to all such complaints.

Finally, schools should effect policies to safeguard protected information (such as classification or authorization schemes for accessing information) and have the technological savvy to protect such data from loss or theft. One of the surest ways to safeguard personal information is not to keep it at all. Among other things, schools should work to minimize or eliminate the use of Social Security numbers. In fact, PCI standards demand that all credit card data (including magnetic data) is purged within hours of the relevant payment transaction. Therefore, schools should regularly dispose of protected personal information, especially once the original purpose for collecting such information is fulfilled, and should provide training to faculty and administration staff regarding the financial, operational and reputational risks associated with unauthorized disclosure of data.

In addition to general compliance with data privacy laws, colleges and universities should take steps to confirm that they are compliant with PCI DSS by (i) auditing and updating (where appropriate) the existing data retention policies and practices, including regularly monitoring any updates to the PCI DSS; (ii) auditing the existing payment processing hardware and software and data transmission practices; (iii) if certain hardware/software is known to be non-compliant, procuring agreements for new hardware or software should require compliance; (iv) reviewing school's existing contracts with service providers and updating any such agreements to reflect any new data retention provisions; and (v) working with third-party providers to ensure their compliance with Minnesota's Plastic Card Security Act, specifically by including provisions in

---

or capture the purposes for which personal information is gathered, or whether it is continually used for different purposes, your school should dedicate some resources to resolving this issue.

the all relevant contracts in order to indemnify the school in cases where the service provider has breached the Act.[57] Finally, each institution should prepare an incident response plan to be implemented in the event of a data breach. Preparing the plan before it is needed provides the opportunity to develop the plan in an organized manner by a team of clear-headed individuals with an appropriate combination of expertise. The plan should identify the members of the incident response team, including who is responsible for leading the response to any incident, and should cover all of the activities described in the next section.

Part III: Handling a Data Breach

For most entities, whether they are businesses or colleges or universities, the question is not whether a data breach will happen, but when and how severe it will be. Once a data breach is discovered,

- Determine whether the breach is ongoing (e.g., a cracker still accessing the data) and, if so, have the information systems group shut it down;
- Notify the incident response team who will implement the incident response plan (assuming one has been developed);
- Decide whether to inform any law enforcement agency and, if so, determine which one(s);[58]
- Determine the data that has been affected and the affected data subjects (this may require sophisticated forensics, and may take weeks);
- Determine the jurisdictions in which each affected data subject resides;
- Identify the "trigger" thresholds (e.g., unauthorized access, misuse) in each such jurisdiction;[59]
- Figure out which thresholds (if any) were met;
- Determine whether to limit the individuals notified to those required by law;[60]
- Analyze obligations in each affected jurisdiction (e.g., manner and content of notification; whether the state attorney general must be notified, whether the three credit bureaus must be notified and time limits);
- Determine whether to offer "extras" (e.g., free credit monitoring, toll-free information line) and, if so, which ones;
- Decide whether to have in-house personnel send the notifications, or to engage a third party to send them;
- Choose the mode of communication to be used for the notifications;

---

[57] Schools doing regular business with residents of Minnesota should confirm that they are not storing card security data in violation of the Plastic Card Security Act.

[58] The incident response plan should include a list of pertinent law enforcement agencies, and of specific individuals (with contact information) within them who might appropriately be informed. For example, the state of New Jersey has regulations that indicate that the Division of State Police should be notified within 48 hours of the discovery of a security breach involving New Jersey residents.

[59] For example, Maryland's law requires notice if there is a reasonable likelihood of misuse of the data, and Montana requires notice to the credit bureaus whenever the notice letter suggests to *any* Montana resident pulling a copy of the credit report.

[60] For example, the plan might specify that if notifications are required in any state, notifications will be sent to every affected person, regardless of residence or legal obligation. Such a decision will simplify somewhat the tasks that must be included in the plan.

- Determine the content of the notifications;
- Send the notifications (or have them sent by the pre-selected third party); and
- Arrange for remediation of the problem.

Part IV: Conclusion

International data privacy laws are extremely complex and varied, and it is important for colleges and university administrators to seek counsel from in-house or outside privacy experts on compliance issues. The EU's privacy regime is particularly daunting, considering that the European Union has twenty-seven members, each with its own set of privacy laws. Furthermore, data privacy protection in the United States is governed by an intricate patchwork of federal sectoral legislation, private (though nearly universally applicable) PCI standards, as well as dozens of state-specific laws and regulations. This is a new and a fast-developing field, and consulting with a privacy expert is the best way to ensure that an organization will not violate any of the applicable laws, which can potentially save the organizations much time and money.

Acknowledgements and Disclaimer

The panelists would like to thank Meighan O'Reardon, an associate in Pillsbury Winthrop Shaw Pittman's Global Sourcing group, for her significant contributions to this paper. Panelists also extend their thanks to Maureen Dwyer, Amanda Grenter, Anne Friedman and Rachel Wilson for their help.

The comments and opinions contained herein do not constitute legal opinion and should not be regarded as a substitute for legal advice.