Introductory Essay for "Privacy Law Year in Review, 2005-2006"

PETER P. SWIRE*

This essay introduces our second issue of Privacy Law Year in Review. In preparing this essay, I was struck by the sheer volume of privacy law developments. Major topics in each annual volume are: government information collection; financial privacy; medical privacy; privacy on the Internet and in commercial databases; and privacy internationally. The volume also includes two special topics that have not been the subject of previous publication: a cross-sectoral review of auditing for privacy and a systematic analysis of the privacy laws of California, the state that has become a major source of U.S. privacy laws.

The essay first briefly describes the nature of Privacy Law Year in Review. It then provides a summary, in fewer than 2,500 words, of privacy law developments in 2005-2006.

I. THE TASKS OF PRIVACY LAW YEAR IN REVIEW

The principle goal of Privacy Law Year in Review is to create a trustworthy, non-ideological, and clearly-written annual review of developments in privacy law. It is one of three annual issues of *I/S: A Journal of Law and Policy for the Information Society*. I am the Faculty Editor for this issue. Also serving the journal are Peter Shane of the Moritz College of Law, who is overall Faculty Editor of the journal, and the Managing Editor, Sol Bermann, who has broad experience in the privacy field. Other current I/S issues include "Cybersecurity and Policy" and "Federal Secrecy After 9/11." Information about *I/S* is available at http://www.is-journal.org.

As was true for our inaugural issue, we are delighted that this issue of Privacy Law Year in Review will be distributed to all members of the International Association of Privacy Professionals ("IAPP"). The IAPP has grown rapidly in recent years and expects to have over 3,000 members by early 2007. Privacy Law Year in Review is distributed in hard copy to all IAPP members, and members also can sign up for passwords to get online access to all other *I/S* issues.[1] As part of our collaboration with IAPP, we at the Moritz College of Law have now written the official curriculum for the Certified Information Privacy Professional examination. Sol Bermann, students from *I/S*, and I have written the book of training materials for publication in the fall of 2006.[2]

The format of Privacy Law Year in Review is designed to be useful to the largest possible number of readers. We believe the approach here will benefit both experts in each sub-field and people who are looking at a topic for the first time. Each article includes an abstract to guide the reader to relevant material. In addition, the articles introduce key legal materials, such as HIPAA or the Gramm-Leach-Bliley Act, so that persons who are inexperienced in that area can get a basic orientation, while also providing a more detailed analysis and citations for recent developments. In that way, readers who are especially interested in one topic gain an

---

* C. William O'Neill Professor of Law and Judicial Administration, Moritz College of Law of The Ohio State University. From 1999 until early 2001, Professor Swire served as Chief Counselor for Privacy in the U.S. Office of Management and Budget.

[1] For IAPP members who wish to activate their online access, contact Kimberly MacNeill, IAPP Membership Services Coordinator (207.351.1500 x113/kim@privacyassociation.org).

[2] PETER P. SWIRE & SOL BERMANN, INFORMATION PRIVACY: OFFICIAL REFERENCE FOR THE CERTIFIED INFORMATION PRIVACY PROFESSIONAL (International Association of Privacy Professionals 2006).

understanding of the state of the art, as well as footnotes that guide the reader to the full text of statutes, regulations, cases, and other primary materials.[3]

The topics for this issue were selected in the fall of 2005. The dedicated student authors researched and wrote drafts through the end of the 2006 academic year, under the supervision of Sol Bermann, myself, and student Issue Editors Katherine Delaney and Elizabeth Hutton. Edits were completed in the fall of 2006 under the guidance of student Issue Editors Kirk Koehler and Gene Park, and this essay was completed in October, 2006.

II. An Overview of Privacy Law in 2005-2006

This part of the essay gives my commentary and summary for the articles contained in "Privacy Law Year in Review, 2005-2006."

A. Government Information Collection

The past year has seen numerous, high-profile issues in the area of government information collection and use. From the fall of 2005 through early 2006, Congress debated the reauthorization of the USA-PATRIOT Act, many of whose provisions were due to sunset at the end of 2005. Eventually, most of the government authorities in the 2001 version of the law were reauthorized. The new law contained only modest changes, such as somewhat greater judicial review of "Section 215 orders," a mechanism for requiring those holding records to provide them to the government.

As the reauthorization debate was underway, the New York Times published its first story about a National Security Agency program to intercept certain calls between the United States and overseas, without any participation by the Foreign Intelligence Surveillance Court or other judicial supervision. The initial story was followed by reports of two other major surveillance programs. First, the Electronic Frontier Foundation filed suit based on a witness who stated that he saw large-scale access by the government to major phone switches. Second, USA Today reported that the phone calling records of up to 50 million Americans had been turned over by telephone companies to the NSA. The facts and legal status of these three programs were highly contested at the time of this writing, in the fall of 2006. In the first holding on the merits, a district court in Michigan held that the program described in the New York Times was unconstitutional.[4] That holding is now under appeal, and next year's Privacy Year in Review will examine these programs in greater detail.

At the federal level, this issue describes other major developments. The period 2005-2006 saw the first significant implementation of the Intelligence Reform and Terrorism Prevention Act, enacted in late 2004. Among other developments, the Act created a new Privacy and Civil Liberties Oversight Board in the White House, and its members were confirmed in February, 2006. The period 2005-2006 saw continued privacy debates about development of the "Secure Flight" program, which is designed to pre-screen airline passengers against terrorist watch lists. This program remains in the planning and testing phase and is intended to replace the earlier CAPPS II program, which was canceled due to privacy concerns.

A major theme for privacy in the government sector is how authentication of individuals should proceed in the future. In 2005-2006, the State Department proposed new U.S. passports, which would use Radio Frequency Identification ("RFID") chips to communicate from the

---

[3] In some instances, this issue of Privacy Law Year in Review refers back to material in the inaugural issue. Subscribers to *I/S*, including IAPP members, can access earlier issues online.

[4] ACLU v. NSA, 438 F. Supp. 2d 754 (E.D. Mich. 2006).

passport to machine readers, for biometric and other information. Critics complained that this use of RFIDs would be a security risk, because unauthorized persons could detect a U.S. passport and potentially read, or "skim," personal information. As described in a chapter on this topic, the State Department in response revised the passport proposal, retaining RFIDs but creating an anti-skimming cover and other safeguards.

At the state level, authentication is also a major privacy issue. States are required to implement standardized drivers licenses by 2008, under the terms of the REAL-ID Act. Privacy advocates criticize REAL-ID as a de facto national identity card. State governments have voiced objections, especially concerning the expense and unfunded mandates of REAL-ID. As of the fall of 2006, the U.S. Department of Homeland Security has not issued the proposed rules for how states should implement REAL-ID. Thus, there may be considerable pressure to extend the 2008 statutory deadline or otherwise to change the law's requirements, due to the lack of time for motor vehicle agencies to put major changes in place by 2008.

B. FINANCIAL PRIVACY

Authentication has similarly been an issue in the financial services sector. The key question has been whether the risks in online financial transactions should dictate more than "one-factor authentication," such as a password. The Federal Financial Institutions Examination Council, comprised of the federal financial regulators, has now issued guidance calling for "strong" authentication by the beginning of 2007. The FFIEC specifically states: "[w]here risk assessments indicate that the use of single-factor authentication is inadequate, financial institutions should implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risks."[5] Historically, the financial services sector has often adopted security and other information technology measures that then spread to other sectors. Other sectors, therefore, should be aware of heightened authentication measures for banking and other financial services.

The period 2005-2006 saw important implementation of the Fair and Accurate Credit Transactions Act ("FACTA"), the 2003 update to the Fair Credit Reporting Act ("FCRA"). Three rules are especially significant. First, the banking agencies issued a major regulation restricting the use of medical information in the extension of credit. Medical information is now generally prohibited as a factor in making lending decisions, subject to a number of exceptions. This regulation addressed a gap under the HIPAA medical privacy rule, which applies to health care providers but not generally to lenders and other financial institutions. Second, the banking agencies explicitly supported the use of "layered privacy notices" in opt-out solicitations of credit or insurance under the FCRA. The wordy privacy notices under the Gramm-Leach-Bliley Act ("GLBA") have received a great deal of criticism for being legalistic and difficult for consumers to read. The banking agencies have now officially supported having notice in layers – a short and readable notice about the key points, with links to a longer notice for consumers who wish to learn the details. Third, security requirements under GLBA were supplemented by a new requirement that financial institutions and their agents must implement risk-based measures for the proper disposal of personal information. Financial institutions who contract out for disposal are also required to provide for safe disposal in the terms of the contract.

This period saw continued developments under GLBA. One issue, which also arises under other privacy laws, is how personal information will be handled during the discovery process.

---

[5] The Federal Deposit Insurance Corporation, Federal Reserve Board, Office of the Comptroller of the Currency, Office of Thrift Supervision, and the National Credit Union Administration. FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL, AUTHENTICATION IN AN INTERNET BANKING ENVIRONMENT 1, http://www.ffiec.gov/pdf/authentication_guidance.pdf (last visited Oct. 31, 2006).

The case law remains somewhat unclear, but recent cases have supported allowing personal financial information to go to the other parties in litigation, subject to protective orders. An ongoing issue is how the two major financial privacy statutes interact for purposes of preemption of stricter state privacy laws. GLBA does not preempt stricter laws, but the FCRA now does. The biggest recent battle has been in California, where a stricter financial privacy law was eventually held to be preempted by the FCRA. We can expect continued disputes in the future as states seek to draft stricter financial privacy laws that appear to be permissible under GLBA but may be struck down as within the scope of the FCRA.

C. MEDICAL PRIVACY

In health care privacy during 2005-2006, one generally successful area was the response to Hurricane Katrina. The HIPAA privacy rule contains explicit provisions for natural and other emergencies, and these provisions appeared workable under their first major test.

There has been less success to date in the area of enforcement. HHS has received over 20,000 privacy complaints since the privacy rule went into effect in 2003, but it has yet to bring its first civil enforcement case. For criminal enforcement, the Office of Legal Counsel, in the Department of Justice, issued an opinion in 2005 that took a very narrow view of the criminal provisions of HIPAA. (I have written elsewhere about why I believe that opinion is bad law and bad policy.)[6] Happily, federal prosecutor Peter Winn published an article in 2006 with an innovative approach, based on the idea that employees of covered entities owe a duty to their employers to follow the privacy rules.[7] Three cases have now been brought by U.S. Attorneys under this new theory, but the main Justice Department has failed to bring any cases in response to over 200 criminal referrals from HHS.[8]

At several recent conferences, I have heard regulated companies urge HHS to enforce HIPAA more effectively. They emphasize that it is difficult to get management support for privacy and security activities if HIPAA is seen as a paper tiger. Another reason to have a credible enforcement program is to lay the foundation for the major shift to electronic clinical health records during the next decade. Opinion surveys show that privacy and security concerns are the biggest obstacle to adoption of electronic health records. A chapter in this issue examines the justifications, actions needed, and barriers to adoption for the shift to such records.

D. PRIVACY ON THE INTERNET AND IN COMMERCIAL DATABASES

The period 2005-2006 saw ongoing litigation and legislative activity in a number of areas related to the Internet. Enforcement continued by the Federal Trade Commission and the states where Web sites violated their own privacy policies, both for children's Web sites and more generally. Spam litigation rose in volume, brought especially by Internet service providers and state Attorneys General. For spyware, there were new lawsuits brought by the Federal Trade Commission and by the states. Federal spyware legislation did not advance, but a number of states now have spyware laws as a variation on their general prohibitions against unfair and

---

[6] Peter P. Swire, *Justice Department Opinion Undermines Protection of Medical Privacy*, CENTER FOR AMERICAN PROGRESS, June 7, 2005, http://www.americanprogress.org/issues/2005/06/b743281.html.

[7] Peter Winn, *Who is Subject to Criminal Prosecution Under HIPAA?*, http://www.abanet.org/health/01_interest_groups/01_media/WinnABA_2005-11.pdf (last visited Oct. 30, 2006).

[8] The third indictment became public after the chapter on medical privacy was completed. Press Release, Federal Bureau of Investigation Miami Field Division, Two Charged in Computer Fraud, Identity Theft and Health Care Fraud Conspiracy (Sept. 8, 2006), http://miami.fbi.gov/dojpressrel/pressrel06/mm20060908.htm.

deceptive trade practices. Phishing – the use of the Internet to trick users into providing personal information – became a larger phenomenon. As with spam and spyware, phishing is now generally illegal. The challenge in each instance is how to have effective enforcement, especially as a larger proportion of the attacks on consumers come from outside of the United States.

The period 2005-2006 is when social networking sites, such as MySpace and Facebook, finally took off after years of predictions that they would do so. One chapter here examines the privacy and security problems that are beginning to emerge on social networking sites.

The trend toward security breach notification statutes continued during this period. Over thirty states now have such statutes, all modeled at least in part on S.B. 1386, the law passed in California in 2002. One chapter here examines major examples of state laws and also discusses the multiple proposals for federal legislation that were considered in Congress in 2005-2006.

Security breaches at information brokers ChoicePoint and LexisNexis made headlines during this period. Data breaches at those companies occurred near the time that Washington Post reporter Robert O'Harrow released his investigation of the industry, in the book *No Place To Hide*.[9] One chapter here examines the information broker industry, including legislative proposals that would create new privacy and security regulations for the industry. An area of particular focus has been on the rules for government access to commercial databases.

E. PRIVACY INTERNATIONALLY

This volume addresses a number of issues about privacy internationally, especially in the European Union ("EU"). The Lindqvist decision by the European Court of Justice has become well-known for its broad definition of "personal data" under the EU Directive on Data Protection.[10] The broad scope of the EU privacy directive, coupled with its limits on transferring data out of Europe, has spurred continuing efforts to clarify the legal status of data exports from Europe. In 2005, EU privacy regulators issued a Working Document for approval of "binding corporate rules." Proponents hope these rules will provide a clearer basis for multinational companies' data activities.

The continuing strictness of European data protection law has been subject to counter-pressures, especially from government initiatives to use personal information to combat terrorism. The Council of Europe Cybercrime Convention has been widely adopted in Europe and was ratified by the U.S. Senate in August 2006, despite concerns from privacy groups that it allows too much data sharing in the name of fighting online crime. In the United Kingdom, there have major legislative initiatives that have raised concerns from privacy advocates. For instance, the Identity Cards Bill was enacted by the Parliament in 2006. Similar to the REAL-ID Act in the United States, there are numerous technical and political issues that create the possibility of significant amendment before full implementation. On the international level, the handling of passenger name records has been a source of ongoing controversy between the European Union and United States. After the European Court of Justice struck down an earlier agreement on jurisdictional grounds, the European Union and United States announced a new agreement on the subject in October 2006.[11]

---

[9] ROBERT O'HARROW, JR., NO PLACE TO HIDE (2005).

[10] In re Lindqvist, Case C-101/01, 2004 All E.R. 561, *available at* http://curia.europa.eu/jurisp/cgi-bin/form.pl?lang=en&Submit=Submit&docj=docj& numaff=C-101%2F01&datefs=&datefe=&nomusuel=&domaine=&mots=&resmax=100.

[11] Press Release, Department of Homeland Security, Statement by Homeland Security Secretary Michael Chertoff on Passenger Name Record Agreement with European Union (Oct. 6, 2006), http://www.dhs.gov/xnews/releases/pr_1160772588688.shtm.

This issue also gives the first significant account, in English, of Argentina's data protection regime. At least a half-dozen Latin American countries have had "habeas data" causes of action in their constitutions, under which an individual can bring a private right of action to correct or destroy personal information that violates constitutional norms. In addition, Argentina and other countries in Latin America have passed expansive data protection laws, often using the law of Spain as a model. Organizations doing business in Latin America are thus facing a growing number of privacy laws, with Argentina as a useful case study for emerging compliance issues.

F. Special Topics: California and Privacy Auditing

Privacy Year in Review 2005-2006 has two special chapters this year, on topics that have not been addressed to date in the privacy literature. The first is a systematic examination of privacy law developments in California. California most famously took the lead in enacting data breach legislation. This chapter, however, catalogues specific California laws in the following areas: (1) a state constitutional right to privacy; (2) medical information; (3) financial information; (4) government information collection; (5) laws concerning the Internet and computer privacy issues; (6) criminal laws on issues such as identity theft and computer crime; and (7) the state Office of Privacy Protection. The chapter specifically seeks to explain, for organizations that operate on the national stage, when and where California privacy laws apply.

The second special topic is how auditing now occurs for privacy issues. For private-sector activities, there are specialized audit requirements for health care (HIPAA), financial services (GLBA), and under the Sarbanes-Oxley law. For the federal government, audits are required under the Federal Information Security Management Act. Federal agencies are now required to have a Chief Privacy Officer, and that Officer is expected to oversee privacy audits of the agency. In addition, there are proposals to improve auditing for privacy, such as the "immutable audit logs" supported by the Markle Foundation Task Force on National Security in the Information Age. By comparing current audit requirements in various sectors, the chapter may help clarify when and how audits should be done for uses of personal information.

III. Conclusion

Keeping abreast of all the data privacy and security issues has become a daunting challenge. For subscribers to one of the daily privacy news updates, a typical day can easily have a half-dozen separate news stories. One of our aspirations for Privacy Law Year in Review is to cut through the clutter. With this overview essay and more detailed chapters that provide needed detail, we hope Privacy Law Year in Review will become a source that professionals, advocates, and academics turn to throughout the year.

We welcome your suggestions for how to make Privacy Law Year in Review even more helpful in coming years.