Introductory Essay for "2004 Privacy Year in Review"

PETER P. SWIRE*

As the Faculty Editor of this issue, it is with great pleasure that I write this Introductory Essay for "2004 Privacy Year in Review." This Essay first describes the recent growth of privacy law, especially in the United States, and then explains the reasons that we have created this first volume of "Privacy Year in Review." The Essay then turns to the nine articles that constitute the Year in Review, and highlights key developments in the areas of government information collection, Internet privacy, medical privacy, financial privacy, international developments, privacy torts, Voice over Internet Protocol and privacy, biometrics, and Radio Frequency Identification Devices.

I. THE GROWTH OF PRIVACY LAW AND THE NEED FOR "PRIVACY LAW: THE YEAR IN REVIEW"

The idea for an annual review of privacy law arose early in discussions about creation of this journal, *I/S: A Journal of Law and Policy for the Information Society.* Professor Peter Shane of the Moritz College of Law had the vision to begin the new journal. Sol Bermann, who created the successful series of PrivacyCons from 1999 to 2003 and now works at Moritz, was enthusiastic about assisting with a privacy issue.

I agreed to participate in the Journal on one simple condition – the Journal should play a distinctive and useful role in the area of privacy. As we considered possible ways to meet this goal, we settled on the idea of creating a trustworthy, non-ideological, and clearly-written annual review of developments in privacy law. The volume in your hands is the first of what we hope and expect will be an ongoing series.

We have created a format that is designed to be useful to the largest possible number of readers. The format we have developed seeks to serve both experts in each sub-field and people who are looking at a topic for the first time. Each article has a clear table of contents to guide the reader to the relevant material. Each article introduces the 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. Each article also provides more detailed

* Professor of Law and John Glenn Scholar in Public Policy Research, 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.

analysis and citations for recent developments. In that way, readers who are especially interested in one topic gain an 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.

This issue responds to the new professionalization of privacy law in the United States. As recently as a decade ago, practically every privacy professional in the country would be among the couple of hundred people in attendance at either the Computers, Freedom, & Privacy conference or the Privacy & American Business annual conference. Today, by contrast, no one meeting hall could possibly host all the privacy professionals. The HIPAA medical privacy rule has required a privacy official to be named for essentially every health care provider, insurer, and clearinghouse in the country.[1] The Gramm-Leach-Bliley financial privacy law applies to all banks and other financial institutions, requiring expert privacy advice in connection with notice, opt-out, and other issues. The vast majority of companies doing business on the Internet have privacy policies posted. In the federal government, there has been a gradual institutionalization of privacy, with Privacy Impact Assessments now required for new computer systems and Chief Privacy Officers named for each federal agency. For companies doing business globally, the European Union Data Protection Directive has helped to spur almost all developed countries to increase their level of privacy regulation. In all of these settings and more, numerous lawyers and other professionals encounter privacy law in their daily work.

One story from personal experience suggests the extent of the change. When I has hired by the Clinton Administration in early 1999 to work on privacy policy, we did not even know what to call the position. If the term "Chief Privacy Officer" had been invented yet, we had never heard of it. After some fussing, we settled on the title of "Chief Counselor for Privacy." The lack of a position title reflected the novelty of what we were trying to achieve, to somehow build good privacy policy into the daily activities of a large organization, the United States government.

The contrast with today is striking. Instead of everything being invented for the first time, a growing number of CPOs today are

---

[1] When drafting the rule, the Department of Health and Human Services reported the number of health care providers in 1997 at about 700,000. 65 Fed. Reg. 82,462, 82,780 (Dec. 28, 2000) (reporting that 563,000 small health care providers constituted 82.6% of all providers). The number of entities covered by HIPAA, each of which is required to name a privacy official, is considerably larger than that, including all health care plans and clearinghouses, and notably including the large number of corporations that self-insure under ERISA.

following in the footsteps of a previous CPO in their organization. The International Association of Privacy Professionals now has a certification program for privacy professionals, complete with an examination. In short, even compared with 1999, we now have much more of a "profession" of privacy.

Along with professionalization comes specialization and division of labor. How many of us feel competent to provide advice in all these areas: HIPAA; Gramm-Leach-Bliley; the Fair Credit Reporting Act; Section 5 of the Federal Trade Commission Act; the European Directive; the privacy torts; and the specialized governmental rules, from the Electronic Communications Privacy Act to the Privacy Act itself? At some level, we recognize that these topics all implicate privacy law. There are many analogies and important lessons that each one of these topics can provide for the other topics. In addition, the fields often overlap, such as when the medical privacy rule has special provisions for the bank payments system or a data spill can implicate enforcement under multiple laws. With that said, it is hard enough for us to keep up with developments in our particular field. Few of us indeed feel confident that we are familiar with the entire privacy landscape, or even know where to go to learn quickly about neighboring fields.

The annual review of privacy law is designed to address this problem. In one volume, privacy students, advocates, and professionals get an outline of today's issues, an introduction to topics with which they are less familiar, and an in-depth set of references for a person's areas of special interest. If the annual review succeeds as we hope, then many readers will include it as one of the small set of volumes kept in handy reach of one's desk.

Before describing the contents of this year's issue, it may be helpful to describe how the volume was produced, and also to solicit readers' suggestions about how to improve the volume in future years. The intensive research and writing for this volume was done by a group of about 15 students at the Moritz College of Law who are on the staff of *I/S: A Journal of Law and Policy for the Information Society*. I did privacy training sessions with the students before they began their papers. Shannon Rogers, a 2L at Moritz, did a wonderful job as Issue Editor in riding herd on the students, maintaining quality control and keeping the project on schedule. Sol Bermann, now a Staff Attorney at Moritz, used his considerable privacy expertise while working closely with Shannon and the other students. I reviewed the papers at the draft and final stages. John Morris of the Center for Democracy and Technology was kind enough to draw on his own immersion in issues concerning VoIP (Voice over Internet Protocol).

He agreed to write the article on VoIP and Privacy when we had a gap in our coverage by students.

Looking ahead, we welcome thoughts from you about how to make next year's volume more useful. For the format, have we managed to introduce you effectively to new areas while also providing enough depth in your areas of special interest? Do the articles provide the right amount of analysis? Do they provide helpful citations to let you dig deeper where you need to do so? Are there other goals we should seek to achieve in the volume in future years?

As for the substance, we expect to add one feature for next year's volume. For a number of years there has been an annual bibliography of privacy-related scholarship prepared for the Defamation and Privacy Section of the American Association of Law Schools. Professor Daniel Solove of the George Washington University Law School prepared the bibliography in 2004. For future years, our plan is to include that bibliography in the *I/S* "Privacy Year in Review."

On substance, we welcome your thoughts on whether we have covered the topics that you find most important. Our tentative plan at this point is to have annual chapters at least on government data collection, medical privacy, financial privacy, Internet privacy, and international topics. We also plan to have "special topics" each year, which this year cover VoIP and Privacy, biometrics, and RFIDs. Looking ahead, we might benefit especially from persons who could contribute articles on topics that the students do not cover. For instance, our students do not always have the language skills or access to materials to do the best possible job on developments in countries outside of the United States. Perhaps readers familiar with those developments would wish to write articles in the future. There may well be other topics where readers have particular expertise and would wish to write for inclusion in future volumes.

II. AN OVERVIEW OF PRIVACY LAW IN 2004

This part of the Essay gives my commentary and summary for the nine articles in "2004 Privacy Year in Review."

A. GOVERNMENT INFORMATION COLLECTION

The inaugural issue of "Privacy Year in Review" includes some events before 2004 to describe the current state of federal information collection. The theme of professionalization of privacy is furthered by the E-Government Act of 2002, which requires a Privacy Impact Assessment as part of the acquisition of new federal computer

systems. Considerable controversy has accompanied screening programs, especially at the Department of Homeland Security. This article describes the evolution of CAPPS II into Secure Flight, as well as developments on No-Fly Lists and vetting of flight personnel.

There has recently been increasing public debate about the related issues of data mining by the government, information sharing among parts of the government, and information sharing between the private and public sectors. The Total Information Awareness Program was de-funded by Congress in 2003, but published reports show that many other data mining projects are in various stages of development. December 2004 saw enactment of the Intelligence Reform and Terrorism Prevention Act of 2004. That statute created a National Intelligence Director and authorized creation of a wide-ranging network for information sharing among intelligence agencies. As a quid pro quo for the increased data sharing, the Congress created a Privacy and Civil Liberties Board in the Executive Office of the President. At the time of this writing in April, 2005, President Bush has not made any appointments to that Board.

At the state level, there have been efforts to put privacy policies on government web sites and otherwise try to build privacy into E-Government functions. The most controversial issue at the state level has been the creation of the Multi-State Information Terrorism Exchange (MATRIX), which facilitates information sharing and data mining among participating states. Although 15 states had agreed to participate in MATRIX by early 2003, that number dropped to five full participants by 2004, in part due to privacy concerns.

B. INTERNET PRIVACY

During the 1990s especially, much of the public debate about privacy in the United States was about the ways that data would or would not be collected as people used the Internet. The legal regime for Internet privacy, however, was essentially limited to Section 5 of the Federal Trade Commission Act, which prohibits "unfair or deceptive" trade practices. Enforcement actions have continued under Section 5 and the Children's Online Privacy Protection Act, but the biggest changes in 2004 arose as some of the darker sides of the Internet became apparent.

Perhaps the biggest new area of legal concern came from the overlapping categories of "spyware," "malware," and "adware." Utah and California passed laws in this area in 2004, prompting a major effort at the national level to pass uniform legislation. Although the

federal law did not pass in 2004, some legislation will likely emerge in the near future.

Unsolicited commercial e-mail, or "spam," continued to plague users and prompt legal attention. The CAN-SPAM Act of 2003 went into effect in 2004, leading to a variety of regulatory and litigation developments and continued legislation at the state level. Unwanted e-mails became more than simply annoying in 2004, as the number of "phishing" or "spoofing" attacks grew enormously. Enforcement actions at the federal and state level sought to use the Computer Fraud and Abuse Act, new statutes against identity theft, and other legal tools to crack down on hacker attacks and fraud on the Internet.

Another new federal statute is the Fraudulent Online Identity Sanctions Act of 2004, which concerns the contact information that people provide when they register for domain names on the Internet. This law creates a rebuttable presumption that people who provide inaccurate contact information and who then commit a crime using the domain will have "willfully" committed the crime.

There was active litigation in 2004 under the Electronic Communications Privacy Act, most notably the *Councilman* case in which a First Circuit panel appeared to expand the ability of an Internet Service Provider to read e-mails sent to its customers.[2] Among other areas of active litigation were John Doe suits by the recording industry seeking to learn the identities of individuals that may have downloaded copyrighted music.

C. MEDICAL PRIVACY

The medical privacy rule under the Health Insurance Portability and Accountability Act went into full effect on April 14, 2003. The security rule under the same statute took full effect on April 21, 2005. For the enormous health care industry, which now accounts for about 15% of GDP, there has thus been considerable and ongoing activity to modernize their data practices. In addition, the importance of privacy and security to health care will likely continue to grow as medicine makes the transition to having electronic medical records for most Americans.[3]

---

[2] I participated in two amicus briefs in the case, seeking a rehearing en banc in the First Circuit and then briefing the en banc court on the merits. For a repository of the documents in the case, see http://www.eff.org/legal/cases/US_v_Councilman.

[3] The Markle Foundation, under the Connecting for Health project led by Carol Diamond, has been energetically involved in trying to assure privacy and security during this transition to EMRs. *See* www.connectingforhealth.org.

The article here provides an overview of HIPAA and then looks most closely at early enforcement under the medical privacy rule. By the end of July, 2004, the Office of Civil Rights ("OCR") in the Department of Health and Human Services had received over 7,500 privacy complaints, with more arriving at a rate of over 100 per week. Despite this volume, OCR at the time of this writing has not yet brought its first enforcement action. By contrast, the Department of Justice brought the first HIPAA criminal prosecution in 2004 and surprised many observers by prosecuting an individual employee of a health care provider. The article here explores the controversy about whether an individual, as opposed to the covered entity, can be subject to HIPAA prosecution. My personal view is that the HIPAA criminal statute does apply to individuals; otherwise, the substantial jail terms written in the statute would apply only to a miniscule portion of covered entities, the solo practitioners who are both individuals and covered entities. Many commentators have overlooked the fact that the criminal provisions are separate parts of the statute from the civil provisions, and each part of the statute should be interpreted on its own terms.

The medical privacy article next examines how HIPAA intersects with two related areas of the law. There is a significant controversy about the extent to which general medical privacy rules should apply to genetic data. There are also significant ongoing issues about which state laws are considered "stricter" than HIPAA, and thus continue to have effect even after the national rule has gone into effect.

D. FINANCIAL PRIVACY

The year 2004 saw continued implementation of two major statutes, the Gramm-Leach-Bliley Act of 1999 and the money laundering provisions under Section 326 of the USA-PATRIOT Act. For GLBA, the statute's broad definition of "financial institution" was held not to apply to certain software companies and to attorneys engaged in activities such as tax counseling. Other litigation clarified the interaction of GLBA with state and local law, including several cases where courts upheld release of non-public personal information for use in discovery in litigation. For money laundering, the regulations issued in 2003 led to several specific enforcement actions in 2004.

The biggest developments in financial privacy, though, concerned changes to the Fair Credit Reporting Act resulting from the Fair and Accurate Credit Transactions Act of 2003 ("FACT Act"). Many of the implications of the FACT Act are not yet clear, because the agencies

have not issued most of the implementing regulations. To date, the most prominent litigation has concerned the scope of the Act's preemption provision. Congress clearly broadened preemption compared with previous law. Courts have tended to find preemption, however, only to the extent of an inconsistency with the Act's provisions, and more litigation is likely in determining what counts as an "inconsistency." The private right of action that exists under the FCRA also continues to produce a steady stream of case law, with perhaps the most important development being cases that seem to expand liability on the furnishers of inaccurate credit data, and not only on the credit bureaus themselves.

E. INTERNATIONAL

In the area of international privacy, the article this year focuses on two countries that have recently expanded the sweep of their privacy legislation. Canada passed the Personal Information Protection and Electronic Documents Act ("PIPEDA") in 2000. Initial phases of PIPEDA applied to federally regulated entities and to organizations providing health services. In 2004, the Act became a truly national privacy law, applying to all commercial entities that process personal information. To show the actual legal workings of PIPEDA, the Article examines *Eastmond v. Canadian Pacific Railway*, where video surveillance of employees was subjected to a four-part balancing test. Under the facts of the case the video surveillance was upheld, but the case creates a roadmap for possible other employee challenges in the future.

Japan enacted its Personal Information Protection Act in 2003, and application to the private sector went into effect on April 1, 2005. With this law, Japan adopted an omnibus privacy law that is broadly similar to PIPEDA, the E.U. Data Protection Directive, and the laws in many other countries that have now enacted ominibus laws. One significant difference between the Japanese statute and the E.U. Directive is that the former does not have restrictions on trans-border flows such as those in the Directive. Nonetheless, the decision to implement omnibus privacy laws by major trading partners Canada and Japan further isolates the United States in its unique, sectoral approach to privacy protection.

F. PRIVACY TORTS AND A FREE PRESS

The next article examines the sorts of legal rules that were addressed in Brandeis and Warren's famous 1890 article in the

Harvard Law Review on *The Right to Privacy*.[4] Brandeis and Warren were concerned about the invasions caused by nosy journalists and photographers. Today, cameras and other recording tools are becoming digitized, miniaturized, and ever less expensive. This article therefore examines the current status of defamation and the privacy torts of intrusion upon seclusion, public disclosure of private facts, false light, and the right of publicity. The focus of the article is on the evolving status in the courts of the newsworthiness doctrine and other legal doctrines by which the First Amendment right of a free press is weighed against the claims of individual privacy.

G. THIS YEAR'S SPECIAL TOPICS

As the first of three special topics this year, John Morris of the Center for Democracy and Technology has written about privacy issues implicated by the rapid development of Voice over Internet Protocol ("VoIP"). Morris pithily explains the technological variations of VoIP deployments, and highlights the privacy issues that accompany each configuration. Perhaps the biggest current debate is the extent to which the federal government will have the legal ability to "pre-clear" new Internet Protocol systems, as the government already does under the Communications Assistance for Law Enforcement Act of 1994. Morris has been a leader in the Federal Communications Commission proceedings on this issue, and he explains how greater government involvement may promote public safety, but at a possibly significant price in privacy and in the innovation of new technologies.

The two remaining special topics for this year are biometrics and Radio Frequency Identification Devices (RFIDs). These are two emerging areas where there is likely to be greatly increased privacy regulation in coming years. The biometrics article briefly surveys the technical state of the art. It looks at the legal issues especially as they arise in the US-VISIT program of biometrics for foreign visitors to the United States and in systems that pair biometrics with smart cards. The article also looks at legal issues arising from DNA databases. The RFID article also explains the technology before showing the early standard-setting and other policy activity that is beginning to address how privacy can and should be maintained in RFID systems.

My own view is that emerging issues such as biometrics and RFIDs are showing the weaknesses of the traditional American

---

[4] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

approach to privacy protection. There has been remarkably little policy development in the federal government on how privacy should be protected as these technologies become more prevalent. This is true even though government agencies are pushing the deployment of biometrics and may well be large users of RFIDs. As the sheer volume of privacy issues continues to grow – as reflected in the many topics covered in this volume – it becomes increasingly attractive to have a more organized and consistent approach to privacy policy and law. It is daunting to imagine how to achieve this consistency, but I believe a growing number of organizations and privacy professionals are recognizing the limitations of the American ad hoc approach.

III. CONCLUSION

As we were going to press, I/S was delighted to reach agreement with the International Association of Privacy Professionals to have this issue distributed to all of its over 2,000 members. This agreement provides encouraging evidence of the usefulness of the volume in your hands. Our thanks to Trevor Hughes and the IAPP Board for working with us, and we hope to continue the relationship with our next issue, due out in the fall of 2006.

In conclusion, we welcome you to read this, our first issue of "Privacy Year in Review." Special thanks to Dean Nancy Rogers of the Moritz College of Law, Peter Shane, Sol Bermann, Shannon Rogers, and all the students at *I/S: A Journal of Law and Policy for the Information Society* who have worked so hard to create this volume.

Our goal in this effort has been to provide a readable, dependable, and non-ideological resource for students, advocates, policy makers, and privacy professionals. With your help we can hope to make this volume even more useful in future years. Please do share with us your suggestions and comments, so that the Privacy Year in Review for 2005 and future years will be even better.