I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

Introduction: The Information Economy, the War on Terror and the Evolving Landscape of Information Privacy Law

DENNIS D. HIRSCH*

The evolution of the law resembles the geologic transformation of the earth's surface. The existing legal framework sits at the top level, crusty and brittle but apparently solid and slow to change. Down below, immense pressures begin to build. They may arise from technological change. Or, they may result from social inequity, economic crisis, political discontent or any number of other causes. But build up they do, pushing their way ever more persistently towards the surface; demanding that the law transform itself to accommodate the new realities.

Sometimes these pressures erupt in the hot magma of major new legislation. Landmark statutes such as the Civil Rights Act of 1964[1] or

---

* Geraldine W. Howell Professor of Law, Capital University Law School. B.A. Columbia University, 1985; J.D., Yale Law School, 1991. I would like to thank Martha Landesberg, Associate Director, Privacy Policy and Education, U.S. Department of Homeland Security who co-edited many of the Notes in this volume, for her wise and insightful contributions. Martha gave generously of her time and expertise and contributed greatly to the students' learning experience and to their final products. I also thank the student authors themselves, who gracefully accepted editing suggestions and showed commitment and integrity during the writing process, as well as Editor-in-Chief Marjorie Yano, Issue Editor David Campbell, and all the other student editors whose contributions and diligence improved this issue. Finally, I would like to thank the International Association of Privacy Professionals (IAPP) whose generous support helped make it possible to produce this privacy issue and to distribute it to privacy professionals throughout the country. While each of these individuals and organizations made important contributions to this issue, any errors in this introductory essay are solely my own.

[1] 78 Stat. 241 (1964).

the environmental statutes of the 1970's[2] add new mountain ranges to the legal landscape. At other times, the pressures do not express themselves in legislation but instead generate a metamorphic process that shapes existing legal doctrines to new purposes in order to meet new needs. The bending of the covenant of quiet enjoyment so as to create the doctrine of constructive eviction – a legal contortion made necessary by the need to address deplorable living conditions in urban slums – represents this type of metamorphic change.[3] In still other instances, the pressures push forward vital legal questions as to which the law as yet has no answer and so reveal fissures and gaps in the legal terrain. The accreting sediments of judicial decisions, regulatory interpretations, and finely targeted legislation eventually fill these gaps with solid layers of new law and administrative rules. Finally, there are instances in which the pressure finds a way to release itself and disperse. Subsequent developments – technological, social, economic, political – relieve the forces pushing up from below. The result is a harmless vent of steam, or a new arrangement in the technological or social stratum that leaves the surface of the law all but unchanged.

So it is with information privacy law. In recent decades two tectonic shifts have put intense pressure on this body of law. The first is the revolution in information technology and the consequent rise of the Information Economy.[4] In a story that need not be repeated here, the transformation from analogue to digital technology has allowed private enterprises to collect, manipulate and communicate personal data at a volume and with a speed that that would have been unthinkable just a short time ago.[5] Companies have seized on this ability and used it to produce a dizzying array of new businesses,

---

[2] *See e.g.*, Clean Air Act, 84 Stat. 1676 (1970) (current version at 42 U.S.C. § 7401-7671q (2000)); Federal Water Pollution Control (Clean Water) Act, 86 Stat. 816 (1972) (current version at 33 U.S.C. § 1251-1387 (2000)); Resource Conservation and Recovery Act, 90 Stat. 2795 (1976) (current version at 42 U.S.C. § 6901-6991i (2000)).

[3] *See generally* WILLIAM B. STOEBUCK & DALE A. WHITMAN, THE LAW OF PROPERTY § 6.33, at 284 (3d ed. 2000) (discussing this development).

[4] *See generally*, DANIEL J. SOLOVE, MARK ROTENBERG & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 623-635 (2nd ed. 2006) (describing this development).

[5] For a description, *see generally* Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1223-1241 (1998) (describing the information revolution and its impact on information privacy); Dennis D. Hirsch, *Protecting the Inner Environment: What Privacy Regulation Can Learn from Environmental Law*, 41 GA. L. REV. 1, 1-23 (2006) (same).

products and services. The use of and the demand for personal information has sky-rocketed. This has turned information privacy law, which seeks to protect such information, into a hotly contested terrain.

A second powerful force, following close upon the first, has brought equally intense pressure to bear on information privacy law. The tragic events of September 11, 2001 have given rise to an expanded national security apparatus that gathers huge amounts of personal data in order to identify and track potential terrorists and others who might threaten public safety.[6] This has generated controversies over such matters as warrantless wiretapping,[7] prosecutorial subpoenas demanding Internet search query and usage records,[8] and proposals for government web crawlers such as "Carnivore" that sniff the Internet for suspicious activity.[9] Developments such as these, and the legal issues they have spawned, have put further pressure on information privacy law.[10]

Each of the Notes in this volume selects one or more of the recent threats to information privacy and explores how the law is, or should be, changing in response to this new pressure. The Notes describe

---

[6] For an informative summary of these developments, *see* Peter P. Swire, *The System of Foreign Intelligence Surveillance Law*, 72 Geo. Wash. L. Rev. 1306 (2004).

[7] *See generally* Jennifer C. Evans, *Hijacking Civil Liberties: The USA PATRIOT Act of 2001*, 33 LOY. U. CHI. L.J. 933, 959-981 (2002) (describing this controversy).

[8] *See* Joseph Menn & Chris Gaither, *THE NATION; U.S. Obtains Internet Users' Search Records; Yahoo and Others Reveal Queries from Millions of People; Google Refuses. Identities Aren't Included, but the Data Trove Stirs Privacy Fears*, L.A. TIMES, Jan. 20, 2006, at A1.

[9] *See generally* E. Judson Jennings, *Carnivore: U.S. Government Surveillance of Internet Transmissions*, 6 VA. J.L. & TECH. 10 (2001) (describing this proposed technology which the government ultimately decided not to pursue).

[10] Of course, the Information Revolution and the War on Terror are not completely separate phenomena. They build on and reinforce one another. Commercial data brokers obtain government records through freedom of information requests, public records laws, or by purchase, and integrate them into their private databases. *See generally*, Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1149-1154 (2002) (describing how private companies collect digital public records). By the same token, law enforcement agencies and other government bodies commonly purchase from private data brokers vast collections of personal information that the law may have prohibited these public agencies from gathering on their own. DANIEL J. SOLOVE, THE DIGITAL PERSON 169-170, 174 (2004). The net effect is a dramatic increase in the collection and use of personal data that is putting intense new pressures on the law of information privacy.

eruptions of new legislation, metamorphic bending of legal doctrine, the opening of gaps and fissures in the law, and the release of pressure without the need for legal change. The geologic transformation metaphor can accordingly serve as a useful device for classifying and describing the Notes and the legal changes that they analyze.

Surveillance and Privacy Under the Obama Administration: The Foreign Intelligence Surveillance Act Amendments of 2008 and the Attorney General's Guidelines for Domestic FBI Operations, by Elizabeth Johnson, chronicles an "eruption" of new legislation. Johnson describes how the post-9/11 demand for more foreign intelligence information resulted in the passage of certain provisions of the USA PATRIOT ACT, the 2008 amendments to the Foreign Intelligence Surveillance Act, and the 2008 revision to the Attorney General's Guidelines for FBI operations. Johnson describes how these additions to the legal landscape opened the door to more warrantless surveillance for the gathering of foreign intelligence information and immunized from liability telecommunications companies that participated in such surveillance. She evaluates the arguments that civil liberties groups have put forward against these legal and policy developments, and those that national security officials have put forward in favor of them. In addition, she analyzes how the law in this area should develop in the future.

Other Notes tell a story that is more akin to the metamorphic bending and shaping of the law than to the eruption of new statutes. *Me, Myself, and My Avatar: The Right to the Likeness of our Digital Selves,* by Oliver Khan, considers the emergence of virtual worlds, such as *Second Life* or *World of Warcraft,* in which users participate in multi-player games through avatars or characters that represent them. Khan explains that game makers and others have begun to exploit commercially these individual avatars and characters by using them in advertisements and for other business purposes. The problem is that an avatar can sometimes bear a striking resemblance to the player who fashioned it. Khan explores whether courts can stretch and shape the common law right to publicity in order to protect against this new form of commercial appropriation of another's likeness. He also examines whether federal copyright laws would pre-empt such an expanded state law right.

Come Fly the (Unfriendly?) Skies: Negotiating Passenger Name Record Agreements Between the United States and the European Union, by Marjorie Yano, also focuses on a metamorphic legal process. Yano describes how the United States pressed the European Union to provide detailed information about passengers bound for the United States as part of its post-9/11 effort to attain better aviation security. In 2004, the U.S. and the E.U. reached an agreement on the

transfer of this passenger name record ("PNR") data. The E.U.'s 1995 Data Protection Directive created a potential sticking point. It required that any such agreement ensure "adequate" protection of personal data. The Note describes how, mindful of the U.S.'s national security concerns, the European Commission interpreted and molded the Directive's adequacy requirements so that the PNR agreement would fit within them. The European Parliament successfully challenged this interpretation in the European Court of Justice. The Note discusses this legal battle over the 1995 Directive and chronicles the negotiation of a subsequent, 2007 agreement that appears to have resolved the issue. The Note details the potential privacy risks posed by transfers of PNR data and the steps that the Department of Homeland Security has taken to mitigate these risks.

Living Our Lives Online: The Privacy Implications of Online Social Networking, by David Hector Montes, focuses on the rise of social networking sites, the threats that they pose to children, and the risks that they create for anyone who exposes personal information in this new medium. Montes focuses on the case of Megan Meier, the teenager who committed suicide after the mother of a former friend, pretending to be a teenage boy, initiated and then broke off a Myspace relationship with her. He examines how federal prosecutors, eager to indict the mother, sought to stretch and bend the contours of federal felony laws so that they would encompass her behavior. The federal prosecutors failed to win a conviction on the felony charges. They achieved a misdemeanor conviction premised on the unusual proposition that the mother had violated the Computer Fraud and Abuse Act when she failed to adhere to the Myspace terms of use agreement. An appeals court reversed the conviction on the grounds that criminalizing an individual's violation of a web site's terms of agreement would turn many millions of Americans into criminals. In his Note, Montes strongly condemns the defendant's actions in the Megan Meier case. But he also raises important questions about the propriety of stretching existing criminal laws to encompass novel, digital crimes and suggests better ways to address these new harms. Moving beyond cyberbullying, Montes also examines the ways in which employers and law enforcement agencies collect personal information from social networking sites, the social benefits of these practices, and the risks that they pose for individual privacy. He discusses the conceptual and operational difficulties involved in developing a legal framework to reduce social networking sites' impacts on information privacy.

Several Notes chronicle instances in which technological and social developments have exposed fissures and gaps in the legal fabric. *It's Personal: Privacy Concerns Associated with Personal Health*

Records, by Kristen Carl, describes the rise of digital personal health records and explains how they have revealed a significant gap in the legal protection of medical information. As Carl explains, the Health Insurance Portability and Accountability Act ("HIPAA") sets up privacy protections for most electronic health records managed by HIPAA-covered entities such as hospitals or doctor's offices. However, the statute likely does not govern personal health records that individuals create themselves through such services as Google Health or Microsoft Health Vault. Such personal health records can contain fully as much sensitive medical data as those that hospitals and doctors maintain. HIPAA's failure to cover them constitutes a major gap in the legal structure for protecting personal health information. Carl examines ways in which legal resources, including certain provisions of the recently passed American Recovery and Reinvestment Act of 2009, might be employed to fill this gap.

Is Financial Privacy Preventing Legitimate Research, by Peter Williams, points to another gap in the law. As Williams explains, financial researchers today have an increased need for mortgage loan data. They need this information in order to understand better the recent economic crisis and figure out how to prevent such an event from happening again. Existing law stands in the way. The Gramm-Leach-Bliley Act's privacy provisions deter financial institutions from revealing mortgage loan information by making it costly and difficult for them to do so. Williams warns that this is preventing researchers from doing important work on how to avoid future crises. What is missing from the legal fabric, Williams argues, is a research exception to the GLB Act's privacy requirements. He proposes a regulatory model, premised on the HIPAA research exception, for adding this feature to the legal structure.

Finally, as was mentioned above, there are situations in which further technological, social and economic changes can defuse growing pressures without the need for significant legal change. The law remains relevant insofar as it can facilitate, or inhibit, such non-legal solutions. Two of the Notes discuss potential adaptations of this type. *Sexually Transmitted Identification*, by James Helmink, examines the rise of highly popular web sites that allow a person to find sexual partners on the Internet. Helmink explains that such web sites render ineffectual the social and reputational networks that once enabled people to identify safe sexual partners. They thereby increase the risk of contracting sexually transmitted diseases (including HIV/AIDS) and create a pressing need for other ways to verify the sexual health status of a prospective partner. The problem is that such verification mechanisms, which entail sharing highly sensitive medical health information, pose a threat to individual privacy. Helmink

surveys technological solutions to this (technologically-created) problem. He considers new types of web sites at which one would be able to check another's sexual health status, Smartphone applications that would allow one to disclose test results only to a specified person for a limited amount of time, and smart card technologies that could enable the holder to record the results of a rapid STD test and share it anonymously with others. He identifies the core qualities, including data security and privacy protections, that any such technology would need in order to prove effective, and evaluates each mechanism in light of these criteria. Helmink locates his discussion within the context of tort law, particularly tort actions against those who infect others or who fail to warn of such infection. He analyzes how the new technologies might affect this area of law, particularly the doctrine of assumption of the risk.

Copyright, Data Protection, and Privacy with Digital Rights Management and Trusted Systems: Negotiating a Compromise between Proprietors and Users, by Saif Khan, describes another technological threat to information privacy and suggests both technological and legal solutions to it. Khan describes the emergence of digital rights management ("DRM") and trusted systems – two technologies designed to monitor and control the use of copyrighted works so as to support the asserted property rights of the content creators. He explains that such technologies can, in some instances, enhance information privacy by preventing unauthorized individuals from accessing medical records and other collections of personal data. Yet copyright owners can also use DRM and trusted systems to monitor who is using a given piece of content (e.g. a book, film, or song), how they are using it, and when they are doing so. Taken to the extreme, such technologies can extend surveillance to virtually all uses of intellectual and media content. This would radically shrink the private realm in which most us are accustomed to consuming such content, thereby chilling intellectual and aesthetic exploration. Khan surveys proposed technological and legal solutions that would preserve many of the copyright-enhancing features of DRM and trusted systems, while simultaneously ensuring greater anonymity and protection of the users' personal information.

The ongoing transformation of information privacy law that the Notes in this issue depict is one of the most compelling and significant legal stories of our time. Just as it can be pleasing to view a natural landscape, so it can be interesting to view a legal landscape that has completed its evolution and reached a mature phase. But it is far more exciting to see the evolutionary process itself unfold and to watch the landscape take shape as this is happening. That is what the Notes in this issue show us. They give us a front-seat view of the

process of legal change as it is occurring right now in the field of information privacy law. They also do what no observer of geologic change ever could. They implicitly acknowledge that it is we *humans*, not impersonal forces of nature, who ultimately determine the course of legal evolution, and they propose how we might intelligently make the choices that lie ahead.