Human Rights in the 'War on Terror'

Edited by

RICHARD ASHBY WILSON
University of Connecticut

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE UNIVERSITY PRESS
Cambridge, New York, Melbourne, Madrid, Cape Town, Singapore, São Paulo

Cambridge University Press
40 West 20th Street, New York, NY 10011-4211, USA

www.cambridge.org
Information on this title: www.cambridge.org/9780521853194

First published 2005

Printed in the United States of America

A catalog record for this publication is available from the British Library.

Library of Congress Cataloging in Publication Data

Human rights in the War on Terror / edited by Richard Ashby Wilson.
p. cm.
Includes bibliographical references and index.
ISBN 0-521-85319-2 (hardcover) – ISBN 0-521-61833-9 (pbk.)
1. Human rights. 2. Civil rights. 3. War on Terrorism, 2001– 4. Terrorism – Prevention.
5. Iraq War, 2003. 6. International law. I. Wilson, Richard, 1964– II. Title.
JC585.H865 2005
323'.09'0511 – dc22 2005013325

ISBN-13 978-0-521-85319-4 hardback
ISBN-10 0-521-85319-2 hardback

ISBN-13 978-0-521-61833-5 paperback
ISBN-10 0-521-61833-9 paperback

For Margaret Wilkinson Wilson

Contents

Contributors

Thomas Cushman is Professor of Sociology at Wellesley College. He is the author of numerous books and articles on topics ranging from cultural dissidence in Russia to the war in Bosnia and Hercegovina. He is the founding editor of *Human Rights Review*, and the founding editor and current editor-in-chief of *The Journal of Human Rights*. Prof. Cushman was Mellon Foundation New Directions Fellow in 2002, and is a Faculty Associate at the Center for Cultural Sociology at Yale University. His most current work is an edited volume entitled *A Matter of Principle: Humanitarian Arguments for the War in Iraq*, University of California Press, 2005.

Richard Falk is the Albert G. Milbank Professor of International Law and Practice at Princeton University. His most recent books are *The Great Terror War* (2003), *Religion and Humane Global Governance* (2002) and *Human Rights Horizons* (2001). He served as Chairman of the Consultative Council, Lawyers' Committee on American Policy Toward Vietnam (1967–75) and he has been a member of international panels of jurors addressing 'Marcos' Policies in the Philippines', 'The Armenian Genocide', 'Reagan's War Against Nicaragua', 'Nuclear Warfare', 'Puerto Rico: A History of Repression and Struggle', and 'Amazonia: Development and Human Rights'.

Michael Freeman is a Research Professor in the Department of Government at the University of Essex. He was the Deputy Director of the Human Rights Centre from 1989 to 1999 and the Director of the MA in the Theory and Practice of Human Rights from 1991 to 2002. In addition, he served as the Vice President of the Association of Genocide Studies and Chair of the Human Rights Research Committee of the International Political Science Association (1997–2000). He is the author of *Human Rights: An Interdisciplinary Approach*

13. Our Privacy, Ourselves in the Age of Technological Intrusions

PETER GALISON AND MARTHA MINOW

After the terrorist attacks of 9/11, the United States government has elevated terrorism as the most important issue shaping government policies. What has happened and what should happen to legal protections of individual freedom in this context? Privacy is one of the individual freedoms in serious jeopardy due to post-9/11 governmental initiatives, yet it lacks comprehensive and clear definition in law and policy. Philosophically and historically, it may best be understood as a multivalent social and legal concept that refers simultaneously to seclusion, self-determination, and control over other people's access to oneself and to information about oneself. Even though its meanings are multiple and complex, privacy is closely connected with the emergence of a modern sense of self. Its jeopardy signals serious risk to the very conditions people need to enjoy the kind of self that can experiment, relax, form and enjoy intimate connections, and practice the development of ideas and beliefs for valued expression. The fragility of privacy is emblematic of the vulnerability of individual dignity and personal rights in the face of collective responses to terror and other enormous threats, real or perceived. In the face of narratives treating both technological change and security measures as either desired or inexorable, claims that privacy stands as a right outside of history, grounded in nature or divine authority, are not likely to prove persuasive or effective.

A partial, but insufficient, assurance for privacy can come from strengthening legally enforceable rights that safeguard a zone of individual autonomy – including rights that transcend the public/private distinction rather than bolster it. Similarly, some, but insufficient, protection for privacy can be built into designs for physical and electronic architecture affecting visibility and surveillance. And some, but insufficient, protection can come from public pressure

Thanks to Jeffrey Shih for research assistance and to Mario Biagioli, Julie Cohen, Arnold Davidson, and Richard Wilson for helpful comments.

to protect privacy understood as desire, expressed by individuals and groups through consumer markets,[1] politics, and even day-to-day relationships with one another. The same fate could befall the strategy of judicially enforceable individual rights. Unless individuals perceive and object to violations, legal challenges and political objections to invasions of privacy will neither arise nor culminate in judicial enforcement. Moreover, unless judges and legislators understand that large groups within the society expect and value forms of privacy that are under threat, they will not recognize or enforce them.

At the same time, failures to attend to privacy in the design of technology, the articulation and enforcement of laws, and in the mechanisms of markets and politics produce downward spirals, reducing both the scope of experiential privacy and people's expectation of and hope for privacy.[2] A vicious circle ensues: if people repeatedly experience telemarketers passing on their names, phone numbers, addresses, and purchasing records to others; if people are subjected to daily searches of their bodies and belongings as they enter buildings, board airplanes and trains, or drive near national borders; if people watch courts refuse challenges to governmental and corporate collection and sharing of personal information, the actual scope of privacy protections declines, and so does the motivation and willingness to demand privacy in any of these settings. Before we know it, such a downward spiral could affect the very sense of self people have – the sense of room for self-expression and experimentation, the sense of dignity and composure, the sense of ease and relief from public presentation. Although these features of experience have specific historical and cultural roots, and hardly describe all of human

[1] Perhaps the most familiar expression of desire these days is through consumer demand, generating market-based responses to private preferences, as suppliers offer privacy protections for a fee. Providers can try to build a taste for privacy by offering products and educating consumers. Whatever the source of the desire, absent individual desires for privacy, the market approach will be unavailing. For only if people demand and show a willingness to pay for privacy protections will consumer purchasing power make a difference. And even if individuals do want to pay, not all forms of privacy are amenable to market-based protection. No fee can be paid (to whom would it go?) to remove substantial information about oneself from the Internet. Political solutions can be prompted similarly by leaders and by grassroots and organized movements, each having the ability to affect the desires of individuals and groups as well as pressuring legislatures and administrators to adopt privacy-protecting rules and practices. Individuals who desire privacy in their everyday life can negotiate for it with their family, friends, and neighbors; in crowded homes, mutual practices of averting one's eyes and agreeing not to look through one another's papers and other belongings can secure some degree of privacy. Yet this approach offers no help where the risk of intrusion comes from strangers. Thus, not all forms of privacy are negotiable person by person.

[2] Recent works exploring the behavioral and normative dimensions of privacy demand and supply on the Internet include Hetcher 2001; Samuelson 2000.

experience, their erosion would amount to a genuine loss of sufficient significance to warrant deliberate concern, attention, and evaluation.

Too often in the past democratic nations have surrendered freedoms in the name of security with enormous cost and too often little benefit. The values of privacy deserve at least some restraints on restrictive measures, even if limited incursions could enhance security over the short term. Similarly, we might marginally increase security by trampling on other rights, such as habeas corpus, but thus far, the country has not made such a sacrifice (see *Rasul v. Bush*, 124 S. Ct. 2686 (2004)). The uncertainty and atmosphere of heightened risk resulting from terrorism should not automatically point toward invading the privacy of individuals. Given the limitations in any single strategy, a mixture of legal, technological, and market solutions offers the best hope for protecting privacy and the goods it stands for in the face of responses to terror, whether those responses are legitimate or illegitimate, and well-considered or ill-advised.

In the past, this and other nations have dramatically curtailed freedoms of speech and association while addressing a sense of internal and external security threats. A recent study of the treatment of freedom of expression during wartime in the United States concludes that in six historic periods, the United States government "went too far in restricting civil liberties" (Stone 2004: 524). Historians, judges, legislators, and other observers have come to condemn as fearful overreactions the Sedition Act of 1789, or President Abraham Lincoln's suspension of the writ of habeas corpus during the Civil War, the internment of Japanese Americans during World War II, the loyalty investigations during the Cold War, and the government treatment of anti-war protests during the Vietnam War (Ibid. at 525). Understandable fears and unscrupulous leaders give rise to repression beyond what circumstances warrant. Excessive restrictions of individual freedoms accompany superstitious beliefs that sacrifice and control of one thing – like personal freedom – would overcome general threats and danger. Privacy, like freedoms of speech and assembly, names a strand of individual liberty that has long faced jeopardy during security crises.

As we explore here, only a complex mix of legal, technological, market, and educational strategies hold realistic promise for confining governmental overreaching and undue restrictions on privacy. Laws can establish procedures that make invasions of privacy more difficult, but they can neither assure complete protection nor devise a perfect algorithm for reconciling privacy and security. Technology can be designed to restrict access to private information in degrees, and can establish filters to guard access to data depending upon the user, but it cannot create the desire for its use; nor does technology function

as well retrospectively (after data have been collected) as it does prospectively. Also, in the absence of either legal requirements or market domination, technological privacy protections do not produce coercive or uniform results. Education and market strategies might cultivate a demand for privacy, but both operate diffusely, and leave results to the decisions and behaviors of individuals and institutions. Without deliberate effort, a downward spiral can become a vicious circle, eroding privacy through legal permission, technological access to unprecedented amounts of personal information, and diminishing public expectations of privacy. Deliberate initiatives in law, technology, and market and educational strategies designed to generate desire could, in contrast, promote an upward spiral, moving up while rotating back and forth between positive desires on the one side and legal/technological constraints on the other. At stake is no less than sense of self – contingent in its historical origins and nonetheless highly valued – enabled by assurances of privacy.

I. Prologue: Lessons from the Terrorist Information Awareness Project

In early 2002, the Defense Advanced Research Projects Agency (DARPA), a research and development division within the U.S. Department of Defense, launched an undertaking it initially called the Total Information Awareness project (TIA). For political reasons it was renamed in April 2002 the Terrorist Information Awareness project (TPAC 2004).[3] The project developed advanced informational technology tools to use domestic and foreign databases in both governmental and commercial hands in order to search for "patterns that are related to predicted terrorist activities" (DARPA 2003: 14). TIA used mathematical algorithms and other features of governmental software to "mine" personal data. Its analysts began to develop scenarios for terrorist attacks, based on "historical examples, estimated capabilities and imagination" (Ibid.).[4]

[3] Probably the first public indication of the effort appeared in testimony by the Director of DARPA before the Senate Armed Services Committee. Fiscal 2003 Defense Request: Combating Terrorism, Hearing before the Senate Armed Services Committee, April 10, 2002 (statement of Dr. Tony Tether).

[4] This report, developed in response to Congressional and advocacy organization critics, includes consideration of privacy concerns notably in the use of tools such as human face recognition and other tools for identifying individuals (DARPA 2003: 31). The report explains that the Department of Defense would follow existing law to protect privacy and civil liberties, and that the appointment of a Federal Advisory Committee by the Secretary of Defense to address these issues demonstrated the importance the department attaches to privacy (Ibid.).

An early description of the initiative explained how it would "detect, classify, identify, track, understand, and preempt," using biometric data, such as images of faces, fingerprints, iris scans, and transactional data, such as "communications, financial, education, travel, medical, veterinary, country entry, place/event entry, transportation, housing, critical resources, and government" (TPAC 2004: 15).[5] The Lawyers Committee for Human Rights described the data sources to be examined more vividly as encompassing: "religious and political contributions; driving records, high school transcripts; book purchases; medical records; passport applications; car rentals; phone, e-mail and internet search logs" (LCHR 2003).[6] Subject to such searches would be public records held by local, state, and federal government agencies, and databases purchased by the government from commercial vendors, such as credit card companies and retail stores. The project "would make available to government employees vast amounts of personal information about American citizens who are not suspected of any criminal conduct," according to lawyer Floyd Abrams, who served on the Technology and Privacy Advisory Committee ultimately created by Donald Rumsfeld, Secretary of the Department of Defense, to review TIA in response to public outcry (TPAC 2004: 63–4).

Considerable ambiguity about the TIA mission and scope contributed to public confusion and wide opposition to it. Differing descriptions conflicted over whether the project would produce a centralized database in government hands, aggregating data from governmental and the private sector, or the project would instead produce and deploy searching devices across public and private databases while leaving the privately owned data in private control (Markle Foundation 2003: 10).[7] The project generated doubts about the credibility and candor of its managers and about their commitment both to protect civil liberties and to guard against abuses of governmental power.

Whether it resulted from perception or reality, the director chosen to lead the project became a lightening rod for critics. The Director of the Information Awareness Office, established to oversee the initiative, was John Poindexter.

[5] Early DARPA ITA Slide, reproduced in TPAC 2004: 15.

[6] Report edited by Fiona Doherty and Deborah Pearlstein, and funded by The Atlantic Philanthropies, the John Merck Fund, the Open Society Institute, Mathew Dontzin, and Equal Justice Works fellowship. The Lawyers Committee changed its name recently to Human Rights First.

[7] Citing for comparison Poindexter 2002 . . . ("The relevant information extracted from this data must be made available in large-scale repositories with enhanced semantic content for easy analysis to accomplish this task") with DARPA 2003 . . . ("the TIA Program is not attempting to create or access a centralized data base that will store information gathered from public or privately held data bases").

A retired Navy Admiral and National Security Advisor to President Ronald Reagan, he had been convicted of conspiracy, lying to Congress, defrauding the government, and destroying evidence for illegally selling weapons to Iran and using the funds to provide secret and illicit support to a military force in Nicaragua in what became known as "the Iran Contra scandal" (Walsh Report; Weintraub 1986).[8] An appellate court overturned the conviction on the grounds that witnesses who testified against him in the criminal trial may have been affected by Poindexter's own testimony before Congress – and his own testimony was supposed to be protected by a grant of immunity. After the trial and the appeal, Poindexter worked at private sector technology companies, including Synteck Industries, where he helped to develop intelligence data-mining and information-harvesting software on government contracts and for private industry (Sutherland 2002).

In February 2002, Poindexter returned to government service to head the Information Awareness Office of DARPA. In August 2002, at the DARPA-Tech 2002 Conference, he explained TIA's strategy by noting that terrorists would have to engage in transactions, and those transactions would "leave signatures in this information space" (Poindexter 2002). The initiative would pursue more efficient and sophisticated ways to find and mine data for analysis and use. As the Lawyers Committee for Human Rights later pointed out, TIA would proceed with no prior judicial approval. Its searches would not be limited to instances where the government had suspicion about particular individuals or particular terrorist organizations. Instead, it would precipitate unprecedented, constant fishing expeditions into people's lives, and generate millions of searches falling short not only of the standard of probable cause, but actually any cause at all. An American Civil Liberties Union representative warned that data mining by TIA would "amount to a picture of your life so complete it's equivalent to somebody following you around all day with a video camera" (Baer 2003).

This image of the program as total surveillance was actually initially embraced explicitly by the government. DARPA named the project "Total Information Awareness." The initial logo posted on the TIA web-site presented an all-seeing eye on the top of a pyramid transformed from the eighteenth-century eye of providence on the Great Seal to an all-too practically oriented governmental panopticon with the slogan, "Knowledge is Power."[9] Although Director Poindexter noted the importance of protecting privacy

[8] The Aide was Oliver North.

[9] It is unclear whether this was meant as a secular version of the Great Seal's Providential eye, a reference to the Masonic sign, or some other cryptic visual reference of omnipresence.

and civil liberties, the DARPA presentation describing the program seemed remarkably indifferent to these issues (Poindexter 2002). Barry Steinhardt, Director of the American Civil Liberties Union Technology and Liberty Program, commented, "It is grimly appropriate that this Orwellian program is being sold to us in such an Orwellian Manner" (Responses 2003).

Sparked by a November 2002 *New York Times* column by William Safire, criticisms of TIA mounted in the press and in Congress. Critics questioned the effectiveness of TIA. They warned that it would generate as many as three million false identifications of individuals as terrorists each year (LCHR 2003: 27).[10] Critics pointed out that the project could create new occasions for governmental misuse of private data (Ibid.). Although the project had defenders, it elicited sharp objections across the political spectrum, from the Eagle Forum lead by Phyllis Schlafly on the right to People for the American Way on the left (Safire 2003). This generated sufficient pressure for the Assistant Secretary of Defense for Intelligence Oversight and the Inspector General of the Department of Defense to initiate review of the program. In December 2002, the Assistant Secretary conducted a review and then brought Intelligence Oversight regulations to the attention of DARPA. In January 2003, the Inspector General initiated an audit of TIA, and called for greater effort to "minimize the possibility for governmental abuse of power" (TPAC 2004: 17).[11]

A separate initiative of DARPA became even more controversial. In July 2003, Democratic Senators Byron Dorgon and Ron Wyden publicly investigated and castigated an experiment in creating a futures market in predicting terrorist events, a joint venture between the DARPA project and the business arm of *The Economist* magazine (CNN.com 2003; Mark 2003). Media coverage linked the terrorist futures venture and TIA as products of DARPA under Poindexter's leadership. In the face of the public outcry Poindexter resigned his post (Rennie 2003). Poindexter later explained that despite public misunderstandings, the TIA initiative had encompassed privacy protections.[12] Yet,

[10] Letter from Public Policy Committee, Association for Computing Literacy, to the Senate Committee on the Armed Services, January 20, 2003.

[11] Citing Department of Defense, Office of the Inspector General, Information Technology Management: Terrorism Information Awareness Program (D-2004-033) 4 (2003).

[12] This question by Spencer Reiss and answer by John Poindexter appeared in Reiss 2004:

> [Question:] So how do you persuade people that having the government peer into their lives is a good idea? [Answer:] Most people don't understand what we were trying to do. Too many opinions are formed based on sound bites from those who yell the loudest. One of the things we were working on was a "privacy appliance" that would conceal a person's identity until a case could be made against them. Congress killed that, too.

as columnist Safire pointed out, a person convicted on five felony counts for lying to Congress about the Iran-Contra affair was "hardly the person to ask elected officials to trust with unprecedented, unchecked power" (Safire 2003).

By the time the Inspector General released the results of the audit of TIA in December 2003, and specifically directed the TIA project to build privacy protections into the development process, Congress had already terminated funding for TIA (TPAC 2004: 18). Its Department of Defense Appropriation Act, passed September 25, 2003, permitted TIA work only in relation to counter-terrorism foreign intelligence, and the media optimistically declared that TIA was dead.[13] In fact, as the Technology and Privacy Advisory Committee to the Department of Defense reported, government agencies continued to undertake data-mining projects similar to TIA, but outside of the DARPA framework (Ibid.).

Indeed, in July 2003, the White House announced a multi-agency initiative, the Terrorist Threat Integration Center, to integrate and analyze terrorist-threat-related information, collected domestically and abroad (Ibid. at 28). Some of TIA's activities may have moved there (Ibid.). Placed under the Director of Central Intelligence, this effort is not subject to the oversight of Homeland Security. The initiative also moves police and law enforcement material within the CIA, despite a statutory prohibition against CIA use of police, law enforcement, or internal security powers (Ibid. at 29).[14] So if TIA's activities persist here or in other classified activities, they do so without public review and with real risk of violating existing law.

Other initiatives like TIA proceed as government agencies commission and pay for work in the private sector. Seisint, Inc., a private company, built the Multistate Anti-Terrorism Information Exchange (MATRIX) as a tool for local law enforcement agencies. It enables the data-mining activities launched by TIA based on analysis of drivers' and pilots' licenses, age and gender, ethnicity, and investigation records (*St. Petersburg Times* 31 May 2004; LCHR 2003: 17). Connecting patterns across public and private databases remains a strategy available to other governmental agencies fighting terrorism. It is within the current capability of government agencies to collect and analyze data about individuals within the United States, including citizens, persons with visas, and legal resident aliens (TPAC 2004: xi, 8). Meanwhile, private commercial

[13] See, e.g., *Denver Post* 31 May 2004; *Atlanta Journal-Constitution* 10 December 2003. DARPA had identified a range of technologies contributing to TIA, and there is no indication that termination of TIA involved terminating development or use of these other technologies (2003: Appendix B).

[14] Citing The National Security Act, 50 U.S.C. sec. 402-2(d)(1)(2002).

enterprises track the purchasing and Internet surfing behavior of millions of individuals, develop profiles of households containing demographic and lifestyle information[15] – and the government can obtain this information without any legal restriction, simply by purchasing it.

Intense negative response by the media and Congress (and advocacy organizations) to TIA may have led to its official termination, but the underlying activities of government anti-terrorist data mining that generated intense concerns about privacy and error most likely continue and do so with less prospect of public review. Like a ball of mercury, the data-mining activities scatter and grow less visible once subjected to pressure. Public concerns about privacy have generated more secrecy about the government activities that jeopardize personal privacy. The historic national commitment to the pairing of personal privacy and open government now shifts toward governmental secrecy and incursions on individual privacy.

This reversal grows from government actions well beyond TIA.[16] Departing from decades of practice, Attorney General John Ashcroft eliminated rules that had restricted FBI surveillance of religious, civic, and political organizations in the United States. Those rules, adopted after abuses by the FBI during the 1950s and 1960s, confined investigations to crimes that had already been committed. Now, in contrast, the FBI can infiltrate groups, monitor meetings, and collect and analyze data looking for patterns and other possible predictors of future terrorist activities even in the absence of evidence of a crime (Borger 2002; *Times-Picayune* 3 June 2002). After 9/11, without much debate,[17] Congress enacted the USA PATRIOT Act (2001). That law relieves the FBI of the obligation to produce individualized evidence in order to justify searching library and bookstore records, rental car records, school grades, medical records, financial records, and Internet sites. The Act allows the FBI to obtain telephone and Internet service records without any judicial oversight. To search the records of libraries, medical and financial institutions, and schools, the FBI now needs only to submit a request in secret to a special semi-secret tribunal, the Foreign Intelligence Surveillance Court, which hears in closed-door sessions the government's requests ex parte, without

[15] See, e.g., Directionsmag.com 3 December 1998; R. L. Polk & Co. 2005. See also McClurg 2003 (discussing Double-click and other consumer profiling and tracking enterprises).

[16] See LCHR 2003: i–xviii, 3–14 (reviewing government policies to restrict release of information to the public about governmental activities, to expand treatment of materials as classified for security reasons, and to limit Congressional oversight).

[17] Michael Moore's documentary film, 'Fahrenheit 9–11', charges that most of the legislators adopted the law without reading it – but one representative captured on film reported that did not differentiate this bill from others.

participation of the target or the target's lawyer (LCHR 2003: 16–17).[18] Congressional efforts to examine how the FBI is actually using these powers have been rebuffed by the Department of Justice (Ibid. at 17). State governments have already produced and used the multistate crime and terrorism database known as the MATRIX to look for patterns in data to identify potential terrorists.[19] Most of these actions have triggered little public reaction. Even when there has been criticism in the media or Congress, the expansive governmental powers persist, without oversight or accountability. For example, public criticisms of airline watch lists developed by the Transportation Security Administration after 9/11 remain exempt from judicial review and existing laws ensuring individuals access to and opportunity to correct government records (LCHR 2003: 26). Government contracts with private companies for the collection of personal information may elude legal rules constraining government and protecting individual privacy (see Hoofnagle 2004).

When exposed to view, airline watch lists and the Total Information Awareness project trigger criticism by advocacy groups, elected representatives, and media. This suggests both widespread low-level discomfort with invasions of privacy and the frailty of privacy rights. (During the first part of 2004, Senator

[18] Discussing sections 215 and 505 of the USA PATRIOT Act. Some defend the PATRIOT Act provisions as necessary; others argue that they do not alter the standards protecting individual privacy (see *National Law Journal Roundtable* 2003: 19). For example, Alice Fisher, former deputy assistant attorney general in the Department of Justice, explained that "A grand jury can issue a subpoena for just these records in a library in a regular criminal investigation, and it often has." But Ann Beeson, associated legal director of the American Civil Liberties Union, argues that the Section 215 orders operate like warrants, unlike subpoenas, because they cannot be challenged prior to compliance and instead are immediately executable. David Sobel comments that the USA PATRIOT Act transforms the role of the Justice Department from prosecuting crimes to "anticipating and preventing them," which changes the role of intelligence and investigation pursued by the government. (Ibid. at 21).

[19] The Multi-State Anti-Terrorism Information Exchange (MATRIX) is described on its website this way:

> This technology helps to identify, develop, and analyze terrorist activity and other crimes for investigative leads. Information accessible includes criminal history records, driver's license data, vehicle registration records, and incarceration/corrections records, including digitized photographs, with significant amounts of public data records. This capability will save countless investigative hours and drastically improve the opportunity to successfully resolve investigations. The ultimate goal is to expand this capability to all states. http://www.matrix-at.org/, visited August 24, 2004.

The American Civil Liberties Union filed suit challenging the use of the MATRIX by Michigan because it allegedly violates a 1980 law prohibiting police from sharing confidential information without legislative permission or approval from a citizen oversight group (Baldas 2004) (describing MATRIX, and suit, filed as *Milliken v. Sturdivant*, No. 04-423728CZ, Wayne Co. Mich. Cir. Ct.).

Edward Kennedy found himself on the no-fly list some five times – and eventually cleared up the error by phoning Ashcroft, not an option available to most citizens.) As government initiatives in data gathering and analysis become less available to review by the media, the Congress, and by private individuals, privacy erodes. So does public awareness of these developments. What might this mean for democracy, for self-government, and for checking centralized governmental authority? And what might these developments mean for the conceptions and experiences of the self?

II. Privacy: Conceptual and Legal Frailties

The vulnerability the legal conception of privacy produces is a result of its plural and diffuse nature. Predicated on plural and at times inconsistent social values, constructed by judges without a clear grounding in legal text or tradition, and wedged within a distinction between public and private spheres that limits the scope of legal remedies, legal privacy faces predictable competition and likely defeat. The very structure of privacy as an individual right, subject to countervailing state interests, is too crude to deal effectively with shifting social relationships; it is also adrift from foundational ideas that could withstand the politics of the moment. Jeopardy to privacy is jeopardy to the space for individual self-invention that our society celebrates.

A. Multiple and Contingent Values. Noting the multiple complexity and even contradictory notions encompassed by privacy has become commonplace among scholars. Robert Post commented, "Privacy is a value so complex, so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings, that I sometimes despair whether it can be usefully addressed at all" (2001: 2087). The content of privacy and the very idea that something called privacy is of value remain historically and culturally contingent. It is possible to trace a boundary between public and private life to practices in ancient Greek and Roman societies, with the private referring to home, dominated by the patriarch, and the public referring to the realm of self-governance, reserved for citizens (see Arendt 1958; Solove & Rotenberg 2003: 27). This divide between public and private is less helpful in describing many non-Western societies. It also does not capture well the conception of individual privacy that people invoke against intrusive searches by government agents, surveillance of consumer transactions and health status by commercial entities, and monitoring Internet use of web-sites by an individual user. Privacy as a claim by an individual is a call to control access to one's self or information about oneself in relation to neighbors, strangers,

employers, and government actors. Yet it also refers to the ability to make a personal decision about reproduction, contraception, marriage, or adoption without interference from others, and especially without restrictions imposed by the government.

As these descriptions suggest, the term "privacy" evokes a cluster of ideas, rather than a sharply chiseled concept. Some scholars propose conjunctive definitions. They acknowledge that privacy has come to denote related but distinct concepts, such as the ability of individuals to find seclusion and also control over access to their person and to information about themselves (Allen 1988: 46–7; Westin 1967; Solove & Rotenberg 2003: 31–2; DeCew 1997: 75; Kang 1998: 1202). Others try to find a core theory underlying distinct concepts,[20] such as the right to be let alone, or personhood, or intimacy, but none has secured widespread agreement.

Robert Post notes that contrasting and at times conflicting theories animate different conceptions of privacy. Privacy could be an avenue for dignity and a vehicle for expressing shared norms about self-respect and respect for others, but it also could be a route for freedom and experimentation, including resistance to shared norms (Post 2001: 2095). "Privacy as dignity seeks to eliminate differences by bringing all persons within the bounds of a single normalized community; privacy as freedom protects individual autonomy by nullifying the reach of that community" (Ibid.). Although it is not so obvious that dignity requires conformity rather than social enforcement, Post's analysis offers an intriguing lens unto somewhat paradoxical features of a norm that requires for its effectiveness widely shared practices and, once effective, affords individuals latitude for unique and even rebellious action.

Daniel Solove argues for abandoning the search for the essence of privacy and instead proposes viewing privacy as a set of ideas that bear "family resemblances" to one another, in the sense that Ludwig Wittgenstein developed; then he argues we can address issues of privacy pragmatically in light of particular circumstances (2002: 1098, 1128). Somewhat analogously, turning to the translation of conceptions of privacy in the law of privacy, Jerry Kang and Benedikt Buchner propose abandoning arguments over whether to locate privacy rights within a framework of property law or instead within a framework of fundamental human rights (2004). Instead, they suggest that analysis should proceed functionally by asking whether and when societal interests should override individual choices, when should governmental rules fortify individual preferences for privacy (Ibid.). Even that approach leaves

[20] Daniel J. Solove drew this useful contrast between the cluster approaches and the core concept approaches to privacy (2002: 1087).

undecided the scope of concerns to be registered by a privacy analysis, and the resolution of conflicts between privacy and public interests such as security and public health.

The emergence of privacy as a right within American law reflects development of a sense of the private self that needs seclusion and finds violation in the capture and distribution of information without consent. In 1965, the United States Supreme Court struck down as unconstitutional a statute criminalizing the distribution of information and medical advice about contraception (*Griswold v. Connecticut*, 382 U.S. 479 (1965)). The plaintiffs' lawyers organized a test case, now known as *Griswold v. Connecticut*, to challenge the arrest of individuals who had counseled married couples about contraception. This circumstance held considerable appeal for the Court because the law intruded upon "the intimate relation of husband and wife," and therefore violated a right of privacy older than the Constitution itself (Ibid. at 482). Thus the Court focused on the locus of greatest protection for privacy – the marital home – although specifically under scrutiny was the communication between the couple and the physician.

The Court's majority had trouble, however, finding language inside the Constitution to root a right to privacy. The opinion by Justice Douglas cast about for a hook and listed several that seemed close (Ibid. at 484).[21] But, finding no clear basis for a right to privacy, Justice Douglas proceeded in his opinion for the majority to scout out "penumbral rights of privacy and repose," lying around the edges of rights explicitly stated in the Constitution (Ibid. at 480). Conducting a tour of the Constitution, his opinion pointed to First Amendment freedoms of association, privacy in one's associations, and freedoms to teach and to learn and to choose how one's children should learn; the Third Amendment's prohibition against the quartering of soldiers in private homes; the Fourth Amendment's ban against unreasonable searches or seizures; the Fifth Amendment protection against self-incrimination; and the Ninth Amendment's reservations of rights retained by the people, even if not enumerated in the text. One commentator suggested that Justice Douglas here "skipped through the Bill of Rights like a cheerleader: 'give me a P . . . give me an R . . . an I . . . ,' and so on, and found P-R-I-V-A-C-Y as a derivative or

[21] Citing the First Amendment right of association, the Third Amendment prohibition against the quartering of soldiers in any house, the Fifth Amendment protection against self-incrimination, and the Ninth Amendment retention of rights not enumerated in the Constitution. See also Ibid. at 482 (discussing prior decisions recognizing the right of parents to select the child's schools and the right to study a particular foreign language). The Court here reread these cases to form a right to privacy even though the cases themselves arose centrally as conflicts over the treatment of religious and ethnic identities in schooling. See Minow 1987.

penumbral right" (Dixon 1976: 84). Another argued as a matter both of logic and legal drafting, the explicit textual reference to some but not other features of privacy – including the right against self-incrimination, but not a right to reproductive choice – would indicate that the framers of the Constitution did not intend to protect the unmentioned features (Henkin 1974: 1422).

The unsatisfying nature of the majority opinion prompted even the individual justices who agreed with the result to write concurring opinions. Each groped for a place in the Constitution's text on which to ground the right used to reject the ban on contraceptive advice (*Griswold*, 381 U.S. at 486, 499). Two of the nine justices found the entire enterprise preposterous and objected in their dissenting opinion that the Court's majority arrogated power, without the authority of Constitutional language, to impose federal judicial policy preferences (Ibid. at 507, 527). Justice Black, joined by Justice Stewart, explicitly criticized the Court's majority for seeking to turn into constitutional principle the effort by Warren and Brandeis to recast common law tort remedies as "right to privacy" (Ibid.).

What has emerged through case-by-case constitutional adjudication is not one right to privacy but instead several distinct lines of cases. One, emanating from *Griswold v. Connecticut*, protects decision making by individuals over the intimate matters of marriage and procreation from "undue burden" or other intrusions by state regulation.[22] A related strand protects individuals in their intimate relationships including, but not limited to, marriage (*Lawrence v. Texas*, 539 U.S. 558 (2003)). Neither of these ideas produces absolute protection and instead they call for "balancing" the private interest and competing public purposes.

A distinct legal notion of privacy – mentioned by Justice Douglas in *Griswold* – stems from the Fourth Amendment protection against unreasonable searches or seizures.[23] Once limited to physical intrusions into an area protected by the Constitution, this notion of privacy was recast by the Supreme Court to "protect people and not simply physical 'areas'" (*Katz v. United States*, 389 U.S. 347 (1967)). In seeming to broaden protection of privacy from the physical locales of home or office to persons, the Court actually

[22] See *Eisenstadt v. Baird* (1972); *Roe v. Wade* (1973); *Webster v. Reproductive Health Services* (1989); *Planned Parenthood of Southeastern Pennsylvania v. Casey* (1992).

[23] "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation and particularly describing the place to be searched, and the persons or things to be seized." U.S. Constitution, Amendment IV. The Supreme Court developed a doctrine excluding from the evidentiary base in criminal trials evidence obtained in violation of this guarantee, but debates over the scope and viability of that doctrine have grown broad and intense. See, e.g., *United States v. Leon*, 468 U.S. 897 (1984).

also introduced considerations that can erode privacy protections. Justice Harlan articulated the scope of the Fourth Amendment protection in terms of two requirements: an actual subjective expectation of privacy, held by the individual, and an assessment that society should treat that expectation as "reasonable" (Ibid. at 360). These requirements are patently flexible. They lend themselves to downward reductions of the amount of privacy either by the simple assertion of a judge – whose rejection of a privacy claim immediately shrinks what is reasonable to expect – or by shifting social and commercial practices. The Supreme Court has acknowledged that individuals may expect the contents of their garbage to be private but nonetheless denied constitutional protection to trash left for collection in an area accessible to the public (*California v. Greenwood*, 486 U.S. 35 (1988)). In that one act, the Court told people not to expect privacy in the refuse they leave out for garbage collection. Similarly, helicopter surveillance of the interior of a partially covered greenhouse in the backyard of a residential home does not violate constitutionally protected privacy because five members of the Supreme Court concluded it would not be reasonable to expect privacy there (*Florida v. Riley*, 488 U.S. 445 (1989)).

The Courts can further diminish the scope of legal privacy protections by narrowly interpreting what counts as a "search" that should trigger Fourth Amendment protections, and by linking the definition of a search, like the content of reasonable expectations, to shifting social practices and growing uses of new technologies. The Court did treat a thermal-imaging device outside a home as a search because it would identify the presence of heat lamps, often used in marijuana production that would otherwise not be visible from outside the building (*Kyllo v. United States*, 533 U.S. 27 (2001)). The Court's definition of a search in that context emphasized that the thermal-imaging device "is not in general public use." Hence, changing uses could alter what counts as a search (Ibid. at 41).

Mindful of plural qualities of privacy as a normative ideal, judges have created legal doctrines that are attentive to competing considerations and evolving circumstances. Yet in so doing, the judges may have produced legal concepts that are circular or even self-defeating. The very requirements articulated by judges to implement a legal conception of privacy may lead to its demise. Jeffrey Rosen recently argued that the "reasonable expectation of privacy" is a circular notion, offering no independent purchase on knotty problems and therefore no real protection for privacy (2000: 60).[24] Robert Post, in reply, has agreed that there is a kind of circularity in the notion,

[24] Scholars and judges have criticized the standard as circular. See LaFave 1966: 393–4; Posner 1979: 188; *Minnesota v. Carter*, 525 U.S. 93, 97 (1998).

but nonetheless argues that the reasonable expectation test is not determined entirely by law but also by social norms derived outside of law (2001: 2094).

Here, Post argues that legal privacy grows from two distinct and even conflicting social norms (without specifying their cultural roots or historical origins). On the one hand, there is a social norm of dignity behind privacy: "Privacy as dignity locates privacy in precisely the aspects of social life that are shared and mutual. Invading privacy causes injury because we are socialized to experience common norms as essential prerequisites of our own identity and self-respect" (Ibid. at 2094). On the other hand, privacy refers to a valued space for freedom, a location for trying out and exposing parts of our identity that we conceal before other people (Ibid. at 2095). "Privacy as dignity safeguards the socialized aspects of the self; privacy as freedom safeguards the spontaneous, independent, and uniquely individual aspects of the self" (Ibid. at 2096). If Post is right, the legal conception of privacy is inherently unstable as it contains internally conflicting social norms.

Whether they are as Post describes or take some other shape, the social norms behind the legal conception of privacy are historically contingent. When buffeted by other social forces, such as wartime public and media frenzy or collective fears about terrorism (often abetted by political figures), the social values behind privacy provide even less sturdy legs for holding up an enforceable legal conception. Legal conceptions of privacy that depend on social expectations lack both the coherence and content to resist pressures to cut back on individual privacy. Especially when those pressures come from security demands, or from the seeming inexorability of new technologies, they are likely to diminish or even elide both the social wellsprings and the legal protections for personal privacy.

B. The Public-Private Distinction and the State Action Doctrine. Echoing ancient Greek and Roman ideas, American law assumes and enforces a distinction between the public sphere and the private sphere, and this very distinction is a source of vulnerability for legal enforcement of personal privacy for several reasons. First, as critics for at least 100 years have emphasized, the use of law to define and regulate the boundaries between public and private puts law – and public officials like judges and police officers – in control of the very scope of privacy, rendering what is private subject to public control.[25] Jamie Boyle argues that, "the central fear of the liberal political vision

[25] Theorists known as legal realists launched many critiques of the public/private distinction in their work that flourished between 1890 and 1945. See generally Horwitz 1982; Fisher, Horwitz & Reed 1993.

is that unrestrained state power will invade the private sphere. And yet the only force available to police the state is the state" (1992: 1434; see also Peller 1985). This warning is most powerful when, as is increasingly the case now, the state combines secrecy with invasions of privacy.

Second, persistent ambiguity over the meaning of the public/private distinction makes it an unreliable tool for protecting privacy. Does "public" refer to government? Or to anything that is not private? Does private refer to the family and home, or to anything that is not government? The ambiguity revolves around the status of the marketplace and civil society. Should employment settings be viewed as public or private? How about commercial exchanges? Or clubs? If viewed as public, each of these settings is properly subject to public values, such as nondiscrimination. If viewed as private, then each should be granted latitude and even seclusion from public surveillance and norms. Third, courts created the "state action doctrine" to monitor the scope of constitutional rights such as equal protection, liberty, and freedom from intrusive searches. Those rights, therefore, attach only when state actors threaten private persons – and they do not apply even when profoundly jeopardized by corporations, religious entities, or other private actors.

Thus, the United States Constitution makes state action a prior requirement for most constitutional provisions affecting liberty, and it is within the concept of liberty that courts tend to identify privacy.[26] State action is required to trigger the protections of freedoms of speech, religion, and assembly, the right to be secure against unreasonable searches or seizures, the right to due process before deprivations of life, liberty, or property, the right to equal protection of the law, and the right to vote. The protection of privacy, as recognized by judges under the Fourteenth Amendment's due process clause, is tethered to the state action requirement and thus applies only to threats by government actors.

In efforts to aid the civil rights movement, many courts during the 1960s construed the scope of state action broadly to apply to an ostensibly private entity if in practice it performed a government function or worked entwined with governmental aid or involvement. Over the past few decades, the Supreme Court has cut back on the scope of state action and therefore reduce the reach of rights predicated on it. This enlarges the ability of governments to bypass constitutional requirements simply by shifting previous government tasks to the private sector. A private school, educating children and financed almost exclusively by government funding, can manage

[26] This discussion draws upon Minow, *Privacy and Privatization* (draft Aug. 2004).

its employment disputes like a private employer and avoid the due process rules governing government bodies because private as well as public entities historically have provided education (*Rendell-Baker v. Kohn*, 457 U.S. 830 (1982)). A commercial company can pursue its own enforcement for breach of contract without following due process rules, even if such rules would apply if a sheriff or court played a role in such enforcement (*Flagg Brothers, Inc. v. Brooks*, 436 U.S. 149 (1978)).[27] The Court thus has come to define the government function test for state action restrictively by asking if the function is exclusively assigned to government rather than by looking, as scholars have suggested, to the kind and scope of power exercised (see Friendly 1969: 222; Choper 1979).

The definition of state action affects whether the collection and distribution of personal information must be subject to the strictures of the Constitution, such as the warrant requirement of the Fourth Amendment or the protection against self-incrimination in the Fifth Amendment. Because data collected by supermarkets and drug stores in exchange for discount cards are then available for sale to government as well as other purchasers, the government can easily acquire information in two steps without complying with the rules that attach if it pursued the information directly.

Privacy rights can be installed beyond the Constitution's commands. They can be enforced without state action through statutes when legislators have the power and will to act. Congress has adopted statutes regulating private conduct in the absence of state action.[28] Yet commercial lobbying groups may secure limitations in the statutes or in the regulations or enforcement patterns that vitiate the goal of protecting individual privacy. When legislation leaves privacy protections up to individual consent, companies condition purchases and services on waivers of individual privacy claims; that is cheaper for the companies and also affords access to the consumers' information to enhance marketing and sales. Recently, the U.S. Congress adopted the Graham-Leach-Bliley Act to authorize financial institutions to share personal information, especially to facilitate business between affiliated financial institutions. The

[27] For a probing analysis of the issues raised by the case, see Brest 1982.

[28] See, e.g., Section 605, Federal Communications Act of 1934. Later, Congress articulated the norm in the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. sections 2510–20, but it exempts wiretaps for national security purposes. The Electronic Communications Privacy Act of 1986 establishes the current framework that includes an avenue for suppressing contents of intercepted electronic communication. The law does permit electronic surveillance if one of the parties to the communication consents. Congress also adopted the Right to Financial Privacy Act, 39 U.S.C. sections 3401–22, to prevent banks and other financial institutions from disclosing a person's financial information to the government, absent a subpoena or search warrant.

law empowers federal agencies to establish standards to strengthen the security and confidentiality of personal information held by financial institutions and to protect against unauthorized access. Yet, the dominant approach taken by the agencies thus far is to presume that the financial institutions can share consumer information, as long as consumers have a chance to opt out of the sharing systems. Practically speaking, by placing the default position to favor sharing, most of the information will indeed be available for distribution. People too often do not understand the stakes or take the effort to opt out through densely written release forms.

The limitations of constitutional analysis, the vagaries of statutory coverage, and the frailty of individual vigilance, taken together, expose personal privacy to massive challenge by corporate and market activities. Governmental purchases of commercial information accomplish an end-run around the checks otherwise applicable when government seeks personal information. Government uses of subcontracting, vouchers, and other techniques of privatization similarly water down or bypass privacy restrictions that attach to public action.

C. The Weakness of an Individual Rights Framework. Constituting legal protection of privacy through an individual right tethers privacy protections to an uncertain anchor. This uncertainty is pronounced in this age when rights are subjected to constant balance, against societal interests, and when the theoretical foundations for rights are disputed or absent. The contemporary style of judicial interpretation of constitutional rights in the United States has led Alexander Aleinikoff to call this an "age of balancing" (1987). He argues that the metaphor aligns constitutional adjudication with a calculus of utilities and with an ad hoc approach to issues that impairs the development of stable and predictable legal rules (Ibid.). Framed as an entitlement of the individual, to be weighed against the interests of the state, an individual's privacy must do battle with potentially powerful needs of majorities (Greer 2003). It also presumes a degree of individual autonomy and bargaining power that departs from many people's lived experiences, and leaves the enforcement of privacy to the assertion of claims by people with sufficient motivation, time, and money. Also, the rights framework affords little latitude for conceptualizing, much less for resolving, conflicts among multiple rights-bearing individuals.

The individual rights framework is especially weak in the absence of explicit textual support for the right and in a moment of history when allusions to natural rights or God-given rights do not resonate widely. Michael Ignatieff, who has asked whether an era of human rights is ending because of the global fight against terrorism,[29] offered a searing challenge to the "idolatry" of international human rights, and his challenge reverberates for all systems of individual rights (2002b). A secular state cannot rely on religious ideas to bolster rights, but turning legal rights into a new secular religion would mistakenly treat law as the source for defining all that is good and desirable. Instead, Ignatieff argues, rights should be predicated on the minimal respect for a space of individual decision making.

Even this minimal conception of rights partakes of the pretense that rights are "out there" rather than names for commitments people want to hold onto even in the face of countervailing arguments. What is missing is the language to acknowledge their contingency even while using rights as tools or techniques to resolve knotty problems. Conventionally, privacy protections invoke images of walls or swords and shields. Perhaps such images are necessary to reinforce the essentially rights claims that can irritate the minority. Yet the balancing methodology, and the perpetual availability of countervailing arguments render privacy weak from start to finish. Perhaps acknowledging the frailty of rights would avoid disillusionment with legal action that does find a compromise or directly caters to anti-privacy interests. Despite ambiguity and complexity, privacy has grown up alongside a notion of the self that can be fashioned – and jeopardy to privacy spells danger for that sense of self as well.[30]

D. Privacy and the Self. In different ways and in different contexts, we find ourselves with a conception of privacy that keeps running aground. First, we looked at the seemingly unavoidable clash between an understanding of privacy that depends on subordinating individuals within a community to shared norms, and on the other side the devotion precisely to freedom for the individual to depart from the norms of that same community. Then we found ourselves caught in a second, seemingly paradoxical situation, in which the individual seeking privacy from the state is forced to look to the state to define the boundary between private and public and then to keep the state squarely on the far side of that border. The paradox plays itself out even in the internal workings of legal doctrine, where only state actors are constitutionally liable for privacy violations even as government actors – judges – decide who is and

[29] Ignatieff 2002a.

[30] For a useful effort to explore more flexible elements in a concept of privacy, see Nissbenbaum 2004.

who is not a state actor for these purposes. Finally, as we look to privacy as a right or collection of rights, we find ourselves unsuccessfully looking for permanent, free-standing principles beyond history or politics, and yet no potential principles seem robust enough to reach across present contexts and changing political realities – let alone across time.

We suggest starting with, rather than fleeing from, the recognition of the historical contingency of privacy notions. The roots of privacy in specifically liberal political ideas serves to elevate the significance of the individual, enforce the distinction between a public and private realm, and constrain the state to protect individuals through laws and rights. Privacy centrally advances and protects a concept of a distinctive self, unmoored from station, time and destiny, that emerges from a prior century of liberal thought into social practices in parts of the United States and Europe by the late nineteenth century. The centrality of a particular notion of self to the resulting legal and political norms cannot be overstated. Self-expression, self-assertion, self-determination – all these and others make that dependence explicit, but the dependence is there even when the word "self" is not. Indeed, the origins of a "self" as a concept are far older than the specific form of modern selfhood that we intuitively want to protect with concepts of privacy. The pre-Socratics most certainly were concerned with a self that needed cultivation through isolation and testing. And medieval writers certainly took much to turn on the nature of the individual soul as key to selfhood. A reflective self figures as a theme in the Renaissance (Bloom 1999). But only in a Pickwickian sense could we say that people of ancient or medieval times thought about the plastic invented self, implied in our current usage of privacy.

The history of the self has different aspects, but its history in the United States and Europe has been played out, largely (though in important ways not exclusively) through the body. When the ancients sought to cultivate the self by meditation or isolation, by deprivation; when the German Bildungsroman of the nineteenth century moved the hero toward a completion of the self through a voyage; when the French formed their secondary schools in the early nineteenth century to teach its young men how to assert "le moi" – these were all techniques to create a self in a particular image (Goldstein 1994). Indeed, there are many techniques for reinforcing certain forms of selfhood. Architecture can be built to annihilate the sense of individual importance or can be constructed to glorify the individual, even to repeat the human face and body in the structures in which we live. A legal system can elevate or subordinate the individual; elevation has been the direction of law in the United States with increasing force after the Civil War and subsequent constitutional amendments.

One of the architectural markers of apartments in the late nineteenth century was a radical distinction between public and private places. Certainly in the wealthier houses (bit by bit imitated in more modest homes) public sectors of the living space were dedicated to display. A foyer (sometimes dining room) offered a kind of routing station after the reception area, beyond which only the family would pass. After these open and quasi-open spaces, were the sacred precincts of the bedrooms. These were hidden from public view, beds and sexuality needing cover from sight (Guerrand 1990).

Within the bourgeois apartment, the restriction of smells came more slowly. Britain mandated flush toilets, hygienists pressed for sanitary kitchen facilities – air, clean water, removal of odors became an obsession principally during the last half of the century (Ibid. at 370–4). It is against this socio-spatial background that Samuel Warren and Louis Brandeis' 1890 "Right to Privacy" needs to be viewed. These authors began by invoking the ancient protection of life and property: assault on body, cattle, or land could be defended. It was their ambition, however, to *extend* "property" to the intangible domain. "Much later," they wrote, "came a qualified protection of the individual against offensive noises and odors, against dust and smoke, and excessive vibration." Here Brandeis and Warren were indeed taking up a very current campaign that was in the process of re-making the boundary of the self, hygienic and architectural transformations that extended the protective cocoon of self hood from the body and possessions as such and widened them considerably. Judges, invoking common law, could sanctify this new sphere of the self: "thoughts, emotions, and sensations demanded legal recognition" (Warren & Brandeis 1890).

If privacy was augmented, then intrusions – trespasses – too would appear in a correspondingly broader scope. The particular kind of trespass using [the] penny press to circulate portraits and gossip were felt especially by members of the upper classes who found themselves the target of scurrilous rumors, but the very phenomenon of this kind of "mechanical devices" was itself of relatively recent construction, and even more recent registration as an emotional intrusion. "To satisfy a prurient taste the details of sexual relations are spread broadcast in the columns of the daily papers," and some retreat, some refuge from this "advancing civilization" would demand a sanctum sanctorum, a zone into which prying eyes could not peer (Ibid. at 196).

Caring for this zone of privacy took many forms. Collecting became a hugely important activity of the late nineteenth century – family archives, stamps, rocks, seashells, antiques, art. These were all at once a gesture (alongside, for example, diary keeping) against death, a retreat into domesticity, a small-scale imitation of aristocratic splendor, and a rejection of the exterior

social world. Collecting was a way of making the self – a technology as it were – completely irrelevant as a form of self-construction in the time of the Stoics. As Michelle Perrot has put it, "the ubiquity of collecting is one of the most telling facts of nineteenth-century upper-class history" (Perrot 1990: 545). This may make it plainer why Warren and Brandeis took up the issue in the historic essay:

> Suppose a man has a collection of gems or curiosities which he keeps private: it would hardly be contended that any person could publish a catalogue of them, and yet the articles enumerated are certainly not intellectual property in the legal sense, any more than a collection of stoves or of chairs (1890: 203).

Precisely because the self was in flux in the late nineteenth century, the work necessary to preserve and develop it was visible. In times of stability such efforts might fade into the unseen. Warren and Brandeis toyed with the idea that conscious creation of artistic or literary works might be worthy of protection but everyday conduct not. Such a distinction, it might be said, would encourage creative work.

> This contention, however plausible, has, in fact, little to recommend it. If the amount of labor involved be adopted as the test, we might well find that the effort to conduct one's self properly in business and in domestic relations had been far greater than that involved in painting a picture or writing a book.... (Ibid. at 204).

Making a (private) life was, so to speak, its own aesthetic creation, and the protection of that life-as-art was in and of itself worthy, perhaps *most* worthy, of protection. It would be insufficient, in their view, to find protection only in the scope of property law to guard against the publication of private expression – for example, in a written letter; a right to privacy would be needed for the sake of peace of mind and the sense of "inviolate personality," not merely for any economic value (Ibid. at 210, 205).

This creation had its locus in part in property – the prying eye of the press camera, for example, might be seen as an extended trespass. But some aspects (lists of items in one's collection) were not in any literal sense a material trespass. In short, Warren and Brandeis' defense of privacy are in a transition moment of the self; privacy as defense of that expanded self was – and is – in historical flux. This is crucial not just theoretically, but practically. Once we see how the boundaries of the self change, we also should come to understand how the associated boundaries dividing public from private and state from individual cannot be legislated or judged once and for all time. But the slow variability of the self over the course of the nineteenth century, for example, should not be conflated with moment-to-moment arbitrariness. The sense of

self is not ephemeral in that way. Even when we want to change the boundaries of the private, it may not be something willed otherwise in a moment – as our sense of shame and modesty makes abundantly clear.

Bringing to visibility the techniques of the self – as Michel Foucault and Pierre Hadot have argued[31] – shows how the self is historical, not transcendental. Because it has changed over time and place, privacy – designed to create a penumbral region around the self – is also variable. That the sense of privacy should vary as much as it does from culture to culture today, even among Anglo-American and continental European countries, is less of a surprise if we recognize that there are also differing senses of self. For example, long-standing differences in conceptions of the relation of each person to duty and state characterize even a cursory contrast between the United States and Germany. So when we, with Robert Post, reflect on the tensions between privacy associated with conformism and privacy associated with freedom, we need to return to the specific underlying concept of the self that is so indissociably attached to privacy.

To look at the self as constituted through technologies is to open up a series of questions. What are our methods (ethics) now, individually or collectively, for *intentionally* cultivating the self? How do our educational institutions, churches, courts, armed forces, and psychiatric hospitals function (discipline) in this regard? How do developments affect the shaping of the self even without intentional aim to do so? The full range of these techniques leave open other possibilities, including self-shaping technologies that are chosen for many different reasons – but are not at all necessarily in *order* to shape the self. These days one thinks of new technologies, from films and surveillance devices to Internet searches, on-line games, on-line affinity groups, and chat rooms. In a variety of ways, these produce subtle shifts but also potentially profound changes in how a self is created, presented, and subject to surveillance, display, or manipulation.

For example, older concepts of the self were bound up with kinship relations determined more by affect than by biology. Indeed, for quite some time, courts insisted upon the father-child relationship even in cases where the biology (determined by blood type) proved that the father had not, so to speak, "fathered" the child. According to anthropologist Marilyn Strathern, kinship relations have recently undergone a major transformation as genetic information increasingly defines connections where before they had not. Genetic

[31] On the notion of the 'technique of self' from Foucault and Hadot, see Focault 1986: 43–5; Foucault, L'Herme/neutique du subject (2001); Hadot 1995. See also Davidson 1994; Martin, Gutman & Hutton 1988. For application to scientific techniques of the self, see Galison 2004.

information has led to new duties – including some codified legally – to pass along information about genetic (medical) predictions of dangerous conditions to genetic relatives. The family, as she puts it, becomes "informational" (Strathern 2003: 180–4). As we might by now anticipate, when features of the self as deep-going as kinship are affected, privacy issues cannot be far behind, entering as soon, for example, as people start demanding the protection of DNA sequences that might predict future medical difficulties. At the practical level will employers be allowed to discriminate based on genetic defects? Would carrying a BRCA mutation that might predispose one to breast or ovarian cancer open up the possibility of social exclusion? Does privacy in the physician-patient relation break down when genetic disease might affect a relative – is there an obligation here to break confidentiality? Alteration in privacy codes affecting DNA data could, in these and other ways, re-shape our sense of who we and others are; conversely, if we come to identify ourselves increasingly in terms of our DNA, that may generate new pressures to enforce genetic privacy (Weaver 1997; Green & Thomas 1998; Sudell 2001).

New technologies may render unavailing the late nineteenth-century notions of privacy as a guardian against unwanted journalistic or neighborly prying eyes. That older conception was in essence *territorial*; many recent extensions of property try to generalize a simple "no trespass" rule: from don't cross my field, don't touch my cattle, to don't survey my hard drive, don't check my library records. Some specific metaphors, such as firewalls, can be helpful in articulating notions of privacy in worlds created by new technologies (Pohlmann & Crothers 2002). But it would be a mistake to treat such metaphors as fully mapping onto the new realms and risks permitted by new technologies. Data mining, analogized to invasion of territorial space, would be nothing more than an extension of someone looking through a crack in your fence, each individual bit of information obtained simply adding to a heap of wrongly obtained bits. Yet, such territorial conception seems seriously incomplete in the contexts of virtual reality, information technology, and markets for personal information. The territorial conception of privacy critically understates what is lost if such data mining proceeds without any limitations. To understand what is at risk requires attending to how the computer has made possible the combination of different forms of information that would have been, a century ago, unimaginable. Getting a list in a few seconds of anyone in the United States who subscribes to a Middle Eastern newspaper, watches Al-Jazeera, is between ages 20 and 35, and who traveled to Washington on the day of a major political demonstration is but a few clicks away. When that bureaucrat at TIA or one of its successors performs such a search and you are named by the state, it is not just "information" that

has been gathered. This e-interpellation goes farther than the information separately considered – by the very act of naming you as a suspect (or "person of interest") you have changed status in the eyes of others who know about this, and if you come to know or fear, in your eyes as well. Correlating state databases (including taxes, criminal records, social security, voting registration) with private databases (purchases, travel, on-line clicks) does more than merely assemble a tad more information here or there. It undermines the very concept of a private life.

Can privacy, linked to a conception of private spaces, be sufficient to guard the jeopardy to selves that ensues from such surveillance of personal data mining? There is something far too crude in the image of the physical invasion of specific locales as the threat to privacy. Simple extensions of the legal conception of privacy neglect the degree to which retrospective assertion of a right comes too late, once databases are linked and mined, or secret governmental hearings are in process. Such an "invasive" picture fits many kinds of privacy violation, but it ignores the slow, but nonetheless powerful changes in the self that have occurred since the late nineteenth century and continue today. Is a fallen hair still your property and is its sequencing rightly described as an act of trespassing? Or, more dramatically, if your brother's DNA is sampled – perhaps because he was arrested, perhaps because he was caught up in a DNA dragnetting sweep, perhaps because he was in the military – then *your* DNA is also largely known. But your DNA was known *without* any territorial intrusion on your body or property: the sequencing could even have taken place without your knowledge and based on no strand of your hair or scraping of your skin. By sampling your brother, your DNA code could well have been cracked while you were, in fact, on the other side of the world. Similarly, if publicly available data sets are mined in concert, where – in what *place* would one locate the "intrusion"? No, territorial concepts of self and privacy simply are not expansive enough to capture the totality of issues surrounding our current condition (Grand 2002; Kaye 2001).

Still, if we believe that privacy talk enters with historically fluid concepts of the self, then we may be able to understand the weakness of privacy-as-right. As popular as it may be to see many features of social life as contingent on particular historical and cultural practices, acknowledging this feature of privacy and the sense of self it presupposes and supports seems particularly problematic because we expect stability in privacy and the self. Granted the conception of self has changed over time; this explains why the privacy right always seems too particular to capture the putative universality of rights talk that Michael Ignatieff calls rights as secular religion. But the self does not change moment to moment; we must not infer from this that the contingency

of the concept necessarily implies the uselessness of a defensible, mid-scale notion of privacy. A venerable oak may have a history, it surely was not always there, but it can just as surely occupy a central position in our town square's landscape. Pursuing a concept of privacy (and its associated sense of self) that is neither eternal nor ephemeral offers an avenue toward protections that are robust, without positing an imagined, and quickly deflected, universal ought.

III. A Complex Strategy for the Pursuit of Privacy Protections

The double danger that threatens the concept of privacy is this: on one side, if privacy is taken to be a universal, eternal notion then we are tempted to posit rigid principles that define it. But this very rigidity makes privacy frail – to take privacy as territorial, for example, is to be thoroughly unprepared for a new world of data mining, infra-red searches, DNA dragnetting, or computer hacking.[32] On the other side, if privacy is taken to be a matter for every local subculture, every passing fad and every individual whim, then we are left at the beck and call of every new technique of surveillance, market intrusion, or nosy neighbor. Our view is twofold: first, that privacy is not well defined in isolation – it takes its significance from its association with a widely (but not universally) shared notion of self. And second, the self is itself historically embedded, changing slowly relative to the headlines of the daily paper, but significantly over historical time – the self of the Renaissance or Greek Antiquity is not the self of the late nineteenth century. Privacy and the self are neither eternal nor ephemeral. On this picture privacy is the label we give to the protective penumbra that surrounds this historicized self – privacy marks the penumbral edge of selfhood.

Certainly it is all too easy to expect categories to fall into the eternal or the ephemeral: something is true for all time or a mere and local construction. But privacy, like race, may be neither. For years we have known that race as an immutable hereditary essence is nineteenth century in origin – we can even prize apart the conditions of its appearance and growth in European and American culture. But to track the genealogy of race is not to dismiss its power: race grips us today as it did a century ago. Our experiences with the built environment, hygiene, sexuality, or warfare have similar middle-term histories: here are worlds neither eternal in their structure nor changeable at the drop of a hat. What categories like these (privacy, self, race, sexuality) have in common is that they are often taken to be trans-historical – unlike,

[32] For discussions of these technologies and the legal issues they raise, see Dodson 2000; Ditzion, Geddes & Rhodes 2003; Regnier 2004.

say, clothing fashion or architectural idiom. Privacy and the self need to be understood precisely as of this mid-range type: powerful, robust, relatively long-lived – and yet changing markedly over the course of the centuries.

Both the notion of privacy and the sense of self it protects are contingent on historical, technological, and political shifts; privacy is linked to the historical development of a sense of self during late nineteenth century in the United States and Western Europe.[33] Perhaps implicit in its contingency lies the greatest promise of privacy. Entwined with the emerging notions of a sense of individual self capable of free choice, experimentation, and self-invention, the specific conception of privacy emerging in American law enables the creativity and the spirit of liberty that exemplify the nation's contributions to human civilization. No doubt the self is continuing to change. There is no reason to expect that the bourgeois architecture of the late nineteenth century and the patterns of collecting, cleaning, diary-writing, alongside sound- and smell-proofing, were the final word on defining selfhood. Our current world is making use of new technologies that may well re-define the self. Who is to say what the long-term effect will be as an ever-increasing number of people spend more and more hours trying on new personalities and even identities on-line, around the non-virtual globe?[34] The conception of the self nurtured in private, experimenting with choice and self-invention could well be extending and shifting in the new environment, even as it depends on the sphere of the private invented only over the past century or so.

With this historicized conception of privacy in mind, we come at the end of this chapter to three conclusions. First, the idea that by sacrificing personal privacy we will achieve security at best reflects faulty analysis or magical thinking and at worst seeks to excuse failures to attend to immediate and difficult security dangers that require no sacrifice of privacy. Sacrificing personal privacy does nothing to defend those ferociously toxic chemical plants that stand upwind from major cities or to secure the major repositories of plutonium, highly enriched uranium, nuclear weapons, or radioactive waste.

[33] We do not mean to make claims of either similarity or difference with conceptions of the self in other parts of the world – but do mean to note the historical and regional contingency of such conceptions. In addition to historical contingency, privacy as an idea is likened to contingent privileges of class and contingent features of gender identity. Thus, privacy may embody privileges associated with wealth. The ability to seclude oneself, to control who has access to viewing oneself, or to imagine freedom to shape one's identity free from intrusions by others imply control over sufficient resources even to develop these as aspirations. Privacy may also carry important gendered dimensions; certainly, control over one's reproductive choice has been largely conceived as a special concern for women, given the disparate burdens pregnancy carries for women compared with men.

[34] See Haraway 1991; Mitchell 2003; Turkel 1997.

These fundamental dangers to our security have yet to receive priority. At the same time, successful law enforcement efforts, such as arrests of major al Qaeda leaders, did not result from trolling through millions of private e-mails, correlating their contents with the book borrowing or video rentals; it has come from targeted cell phones and pavement-pounding police work. To date, it is at most a tiny minority of terrorists who have been convicted as a result of data mining consumer and government records. It is not clear that even such techniques – rather than targeted searches based on reasonable suspicions of individuals – have generated any arrests or detentions (see Schneier 2003; CSTCT 2002). It strikes us as worse than foolish to imagine that the sacrifice of something we value – privacy – is in and of itself the means to increase security. Sacrifice for the sake of sacrifice is magical thinking, a kind of haywire homeland potlatch. Instead of blindly opening up our reading, our communication, our purchases, and our travel to commercial and governmental mining, we can and should demand that priority be given to the real security failings that represent real and enormous threats. In the absence of such steps, it is tempting to interpret the invasions of privacy through massive governmental surveillance and data mining as part of the efforts by leaders to claim they have advanced security, when they have not, to heighten fears in order to maintain political control, or to appeal to an irrational notion that sacrifice and pain will exchange for safety and deliverance.

Second, given the complexity of the self, trying to reduce the privacy concept to a purely utilitarian framework is like steamrolling a statue to capture its essence in the simpler space of the two-dimensional plane. Such flattening may make security and privacy look like a simple balancing act – twelve ounces of each on the two sides of the scale – but it does nothing to acknowledge the space people need to deliberate, to try out new ways of acting or different ways of speaking. To imagine we could weigh against security what we call privacy pretends that we can transform these ends into quasi-quantifiable means, and to conduct a charade that anything could ever win against security. Because in such a flatland view, utility always will make security measures trump, even if the security gains are at best marginal or speculative, or a political performance designed to reassure us that we are doing something in the face of panic and unease. It is all too easy for each of us to exaggerate fear and minimize values like privacy, or the associated sense of freedom for self-development and the experience of dignity. To ask "what is the utility of dignity" is to offer it up for sacrifice.

Finally, we believe that no single kind of intervention – not law by itself, not technology by itself, and not the individual exercise of our desires and choices by themselves will be adequate to protect privacy. If we take seriously

the protection of privacy – protection of the dignity of the self – we must pursue complex and multiple means. Our best chance at this will necessarily involve a kind of complementarity among the law, technology, and desire. Law provides institutional checks on power, transparency of decision making and results, and recompense for violations and mistakes. Technology steers action and can provide complete deterrence of invasive action through the hardware and software designed to collect and analyze data or monitor conduct and presence. Technology also creates possibilities for open expression. Desire – whether expressed in markets, political action, or private conduct – is generative, imaginative, pressurizing. Our desired choices can shape the self. The role of each is not, of course, completely independent – experience with certain technologies can certainly shape the self, the law can sometimes deter, and our desires themselves can drive us towards transparency.

But each has its limits. Law can all too often be beholden to politics. It is, by its very means, slow, reactive, and responsive to pressures of politics and power. Legal protections, even if successfully adopted, require the desires and courage of victims to complain and judges for enforcement. Technology can be too rigid – no sooner is there a measure to protect e-privacy then a hacker arrives with a countermeasure. If technology is too rigid, desire can be so flexible that we can find ourselves giving up privacy in the enthusiasm of a demagogic moment. We can draw on the strengths of law, technology, and desire to complement and substitute for each other's limitations.

The idea of such complementarity may be more familiar from more mundane concerns. After all, defending such an abstract aspect of what we care about is at least as hard as protecting our bodies in automobiles. On the road we rely on hardware (soft dashboards, shatterproof glass, airbags, and seatbelts). We count on laws that restrict speeding, limit alcohol, and channel traffic. And we demand proactive good sense, the right management of desires on the part of drivers as they handle intrinsically dangerous machines: prosaic as it is, courtesy does matter at 65 miles per hour.

In coming to terms with privacy we will need a mix of this kind, even if it will need to be significantly more complicated. We need legal rules that anticipate rather than merely react – that affect the structure of technology, for example.[35]

[35] "In thinking about guidelines, the government should start with the basic architecture – what is the appropriate level of protection for different types of information, and what kinds of standards and procedures might provide that protection. The current legal framework governing access to and use of privately held data is a patchwork quilt of different standards for information with similar sensitivity (such as wire, cable, and Internet

We need new technologies that will no doubt include anonymizing software, cryptography, and hardware that make much more difficult what currently are easy intrusions into the monitoring of our on-line lives, purchases, and travel. Privacy in the coming generation will require architecture, both of the electronic and bricks-and-mortar type designed to provide refuge from inquiry more sophisticated by far than any of the prying eyes of the press presented to Warren and Brandeis seventy-five years ago. And we will have to make use of our own decisions, our own desires, as we express our choices in the marketplace, to be sure, but not only there. We need to educate ourselves about our tendencies to overemphasize dangers and the short term and inadequately to imagine the circle of concern.[36] And we will need to demand publicity about decisions affecting our privacy. Without the investigative work of a newspaper columnist, the details of the Terrorist Information Awareness project may well never have surfaced publicly, though when they did, people demanded change. That democratic process of oversight becomes all but impossible as new developments moved behind the wall of classified secrets. Opportunities for knowing what is going on are central to the development and expressions of desires – and here maintaining scrutiny of governmental secrecy and vigilance over personal privacy remain vital legal strategies. Some sense of a right to privacy will be needed, even while we recognize that rights talk will have to be flexible enough to change with changing technological and political times. No single measure will protect us on the interstate; no magic bullet, technological, juridical, or decisional, can sufficiently guard our sense of self.

How much we want to protect privacy implicates what space and latitude we preserve for selfhood. How we *want* to exercise the self, so to speak, is more than a personal question. Our decisions about the Terrorist Information Awareness project and the USA PATRIOT Act redefine the reach and ambition of government surveillance; they re-align the boundary between public and private, and the very scope for self-creation for everyone in the nation. James Scott's powerful book, *Seeing Like A State* (1998), depicts the statistical vision of the rising nation-state from the early eighteenth century forward (see Anderson 1991). We are now in a position to determine how we want the state to see today and therefore how the state and individual should relate to one another both in pragmatic roles – who can read what – and symbolically – what would we prefer that the state *not* see such that an individual can explore the world with a measure of openness?

Reading privacy together with the conception of the self brings forward other values, like human dignity, which we do not want to throw away simply to signal commitment against an amorphous network of criminal terrorists. Our sense of dignity, our sense of self are tied up with our most valued freedoms to grow, to raise our children with self-respect, to nurture the deliberative democracy we have been proud of for 225 years. Posing the question of privacy in terms of self and dignity not only helps us understand the historicity of these notions, but it also underscores the stakes we have in their protection.

Devastating as it was, the bombing of the World Trade Center was also a warning. It was not only a warning from the terrorists, but also a warning from inside our own political culture that we must reckon, urgently, with the aspects of our civil life that we value most deeply. Privacy is not a dangerous luxury to be thrown away like cigarettes on the deck of a wartime freighter plying the dark North Atlantic night. Privacy is the name we give the edge of the dignified self, a boundary we need to protect even if, especially if, we find ourselves once again under siege.

communications) and inappropriate or nonexistence standards for other kinds of information. See www.markletaskforce.org for matrices about this. The complexity of these rules, and the confusion they engender, may cause government officials to be reluctant to take lawful and necessary action to gather important counterterrorism information for fear of crossing a vague line. At the same time, these rights offer little assurance to the public that their rights are adequately protected. . . . New guidelines should, at a minimum, address the following: (1.) government acquisition and use of private sector data; (2.) government retention of the data; (3.) sharing of the data by the acquiring agency with other agencies for purposes other than counterterrorism; and (4.) accountability and oversight" (Markle Foundation 2003: 32–6). It is tempting to explore the common law as an avenue for relief/checking by private individuals against commercial entities (see McClurg 2003). Yet contractual terms can easily evade common law duties.

[36] "By sensationalizing 'newsworthy,' but low-risk, dangers, [the media] generate a sense of panic that quickly cascades through society. People routinely overreact to vivid depictions of frightening, but low-probability, dangers. Lurid reports of sniper shootings, for example, send ripples of fear through a community, triggering excessively cautious responses. This can have a devastating effect on society when the precipitating event is a terrorist attack or espionage in wartime. In such circumstances, the 'excessively cautious' response may not be merely to avoid the sniper's haunts but to insist that government detain and depart aliens, anarchists, or Muslims because of an exaggerated sense of the danger they pose to the nation" (Stone 2004: 533). See also Nussbaum 2003.

REFERENCES

Aleinikoff, T. A. (1987). 'Constitutional Law in the Age of Balancing'. 96 *Yale Law Journal* 943.

Allen, A. L. (1988). *Uneasy Access: Privacy for Women in a Free Society*. Totowa, NJ: Rowland & Littlefield.

Anderson, B. (1991). *Imagined Communities: Reflections on the Origin and Spread of Nationalism* (revised edition). New York: Verso.

Arendt, H. (1958). *The Human Condition*. New York: Doubleday.

Atlanta Journal-Constitution. 'Balance Information With Privacy'. 10 December 2003, p. 22A.
Baer, S. (2003, January 5). 'Broader U.S. Spy Initiative Debated; Poindexter Leads Project to Assess Electronic Data, Detect Possible Terrorists; Civil Liberties Concerns Raised'. *Baltimore Sun*, p. 1A (quoting Jay Stanley of the American Civil Liberties Union).
Baldas, T. (2004, August 9). 'ACLU Takes on "Matrix" Crime, Terrorism Database'. *National Law Journal*, p. 4.
Bloom, H. (1998). *Shakespeare: The Invention of the Human*. New York: Riverhead Books.
Borger, J. (2002, May 21). 'Shamed FBI's Snooping Powers Increased'. *The Guardian* (London), p. 18.
Boyle, J. (1992). 'A Theory of Law and Information: Copyright, Spleens, Blackmail, and Insider Trading'. 80 *California Law Review* 1413.
Brest, P. (1982). 'State Action and Liberal Theory: A Casenote on Flagg Brothers v. Brooks'. 130 *University of Pennsylvania Law Review* 1296.
California v. Greenwood, 486 U.S. 35 (1988).
Choper, J. (1979). 'Thoughts on State Action: The "Government Function," and "Power Theory" Approaches'. *Washington University Law Quarterly* 757.
CNN.com. (2003, July 30). 'Amid furor, Pentagon kills terrorism futures market'. Inside Politics. Available at: http://www.cnn.com/2003/ALLPOLITICS/07/29/terror.market/index.html.
Committee on Science and Technology for Countering Terrorism (CSTCT). (2002). *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*. National Research Council of the National Academies. Washington, D.C.: National Academies Press.
DARPA (2003, May 20). *Report to Congress Regarding the Terrorism Information Awareness Program*. Available at: http://www.globalsecurity.org/security/library/report/2003/tia- di_report_20may2003.pdf.
Davidson, A. (1994). 'Ethics as Ascetics: Foucault, The History of Ethics and Ancient Thought'. In J. E. Goldstein (Ed.), *Foucault and the Writing of History*. Cambridge: Blackwell.
DeCew, J. W. (1997). *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*. Ithaca, NY: Cornell University Press.
Denver Post. 'Virtual Borders vs. Civil Liberties'. 31 May 2004, p. C-07.
Directionsmag.com. (1998). 'Acxiom's InfoBase Profiler Via the Acxiom Data Network is First Consumer Data Product to Provide Census and Household-Level Demographic Data and Scores in Sub-Second Time'. 3 December 1998, Press Release, Acxiom Corp. Available at http://www.directionsmag.com/press.releases/index.php?duty=Show&id=80.
Ditzion, R., Geddes, E., & Rhodes, M. (2003, Spring). 'Computer Crimes'. *American Criminal Law Review*, vol. 40, issue 2, p. 285(52).
Dixon, R. (1976). 'The "New" Substantive Due Process and the Democratic Ethic: A Prolegomenon'. *Brigham Young University Law Review* 43.
Dodson, A. J. (2000, Winter). 'DNA "Line-Ups" Based on a Reasonable Suspicion Standard'. *University of Colorado Law Review*, vol. 71, issue 1, pp. 221–54.
Eisenstadt v. Baird, 405 U.S. 438 (1972).

Executive Summary of the Independent Counsel Investigation (the Walsh Report). Available at: http://www.fas.org/irp/offdocs/walsh/execsum.htm.
Fisher III, W. W., Horwitz, M. J., & Reed, T. (Eds.). (1993). *American Legal Realism*. New York: Oxford University Press.
Flagg Brothers, Inc. v. Brooks, 436 U.S. 149 (1978).
Florida v. Riley, 488 U.S. 445 (1989).
Foucault, M. (1986). *History of Sexuality, vol. 3: The Care of the Self* (R. Hurley, Trans.). New York: Vintage.
Friendly, H. (1969). *'The Dartmouth College Case and the Public-Private Penumbra'*. Austin: University of Texas.
Galison, P. (2004). 'Image of Self. In L. Daston (Ed.), *Things that Talk*. Cambridge: Zone Books.
Goldstein, J. (1994). 'Foucault and the Post-Revolutionary Self: The Uses of Cousinian Pedagogy in Nineteenth-Century France'. In J. Goldstein (Ed.), *Foucault and the Writing of History*, pp. 99–115. Oxford: Blackwell.
Grand, J. S. (2002, August). 'The Blooding of America: Privacy and the DNA Dragnet'. *Cardozo Law Review*, vol. 23, issue 6, pp. 2277–323.
Green, R. M. & Thomas, A. M. (1998). 'DNA: Five Distinguishing Features for Policy Analysis'. 11 *Harvard Journal of Law and Technology* 571.
Greer, S. (2003, September). 'Constitutionalizing Adjudication Under the European Convention on Human Rights'. *Oxford Journal of Legal Studies*, vol. 23, issue 3, pp. 405–433(29).
Griswold v. Connecticut, 381 U.S. 479 (1965).
Guerrand, R.-H. (1990). 'Private Spaces'. In M. Perrot (Ed.), A. Goldhammer, (Transl.), *A History of Private Life, vol. 4: From the Fires of Revolution to the Great War*, pp. 359–74. P. Ariès and G. Duby (general Eds.). Cambridge, MA: Belknap Press, Harvard University Press.
Hadot, P. (1995). *Philosophy as a Way of Life*. New York: Blackwell.
Haraway, D. J. (1991). *Simians, Cyborgs, and Women*. Routledge.
Henkin, L. (1974). 'Privacy and Autonomy'. 74 *Columbia Law Review* 1410.
Hetcher, S. (2001). 'Changing the Social Meaning of Privacy in Cyberspace'. 15 *Harvard Journal of Law and Technology* 149.
Hoofnagle, C. J. (2004, Summer). 'Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect, Process, and Package Your Data for Law Enforcement'. *University of North Carolina Journal of International Law and Commercial Regulation*, vol. 29, no. 4, pp. 595–637.
Horwitz, M. (1982). 'The History of the Public/Private Distinction'. 130 *University of Pennsylvania Law Review* 1423.
Ignatieff, M. (2002a, February 5). 'Is the Human Rights Era Ending?' *New York Times*, p. A29.
———. (2002b). *Human Rights as Politics and Idolatry*. Princeton, NJ: Princeton University Press.
Kang, J. (1998). 'Information Privacy in Cyberspace Transactions'. 50 *Stanford Law Review* 1193.
Kang, J. & Buchner, B. (2004, Fall). 'Privacy in Atlantis: A Dialogue of Form and Substance'. *Harvard Journal of Law and Technology*, vol. 18, no. 1. Available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=626942.

Katz v. United States, 389 U.S. 347 (1967).
Kaye, D. H. (2001, Summer). 'The Constitutionality of DNA Sampling on Arrest'. *Cornell Journal of Law and Public Policy*, vol. 10, issue 3, p. 455(55).
Kyllo v. United States, 533 U.S. 27 (2001).
LaFave, W. (1966). *1 Search and Seizure* (3rd ed.), section 2.1(d), pp. 393–4.
Lawrence v. Texas, 539 U.S. 558 (2003).
Lawyers Committee for Human Rights (herein "LCHR"). (2003). *Assessing the New Normal: Liberty and Security for the Post-September 11 United States*. New York. Available at: http://www.humanrightsfirst.org/pubs/descriptions/Assessing/AssessingtheNewNormal.pdf.
Mark, R. (2003, July 29). 'Pentagon Folds Hand in Online Terrorism Futures Scheme'. Available at: http://dc.internet.com/news/article.php/2241421.
Markle Foundation (2003). *Creating a Trusted Information Network for Homeland Security: Second Report of the Markle Foundation Task Force*. Available at: http://www.markletaskforce.org/Report2_Full_Report.pdf.
Martin, L. H., Gutman, H., & Hutton, P. H. (Eds.). (1988). *'Technologies of the Self: A Seminar with Michel Foucault'*. Amherst, MA: University of Massachusetts Press.
McClurg, A. J. (2003). 'A Thousand Words Are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling'. 98 *Northwestern University Law Review* 63.
Minnesota v. Carter, 525 U.S. 93, 97 (1998).
Minow, M. (1987). 'We, The Family: Constitutional Rights and American Families'. *Journal of American History*, vol. 74, no. 3, p. 959.
Mitchell, W. J. (2003). *Me^{++}: The Cyborg Self and the Networked City*. Cambridge, MA: MIT Press.
Multi-State Anti-Terrorism Information Exchange (MATRIX). Available at: http://www.matrix-at.org/. Accessed on 24 August 2004.
National Law Journal Roundtable (2003, April 26). 'Patriot Act Attacked'. 26 April 2003, p. 19.
Nissbenbaum, H. (2004). 'Privacy as Contextual Integrity'. 79 *Washington Law Review* 119.
Nussbaum, M. (2003). 'Compassion and Terror'. In J. P. Sterba (Ed.), *Terrorism and International Justice*, pp. 229–52. Oxford: Oxford University Press.
Peller, G. (1985). 'The Metaphysics of American Law'. 73 *California Law Review* 1151.
Perrot, M. (1990). 'The Secret of the Individual'. In M. Perrot (Ed.), A. Goldhammer, (Transl.), *A History of Private Life, vol. 4: From the Fires of Revolution to the Great War*, pp. 457–548. P. Ariès and G. Duby (general Eds.). Cambridge, MA: Belknap Press, Harvard University Press.
Planned Parenthood of Southeastern Pennsylvania v. Casey, 505 U.S. 833 (1992).
Pohlmann, N. & Crothers, T. (2002). *Firewall Architecture for the Enterprise*. John Wiley & Sons, Inc.
Poindexter, J. (2002, August 2). 'Overview of the Information Awareness Office'. Prepared remarks for delivery at DARPATech 2002, Anaheim, CA, Aug. 2, 2002. Available at: http://www.fas.org/irp/agency/dod/poindexter.html.
Posner, R. (1979). 'The Uncertain Protection of Privacy by the Supreme Court'. *Supreme Court Review* 173, 188.
Post, R. C. (2001). 'Three Concepts of Privacy'. 89 *Georgetown Law Journal* 2087.

Rasul v. Bush, 124 S. Ct. 2686, 159 L. Ed. 2d 548, 72 U.S.L.W. 4596, 2004 U.S. LEXIS 4760 (2004).
Regnier, T. (2004, Spring). 'The "Loyal Foot Soldier": Can the Fourth Amendment Survive the Supreme Court's War on Drugs?' *UKMC Law Review*, vol. 72, issue 3, pp. 631–68.
Reiss, S. (2004, May). 'Poindexter Confidential'. *Wired Magazine*, Issue 12.05. Available at: http://www.wired.com/wired/archive/12.05/poindexter.html.
Rendell-Baker v. Kohn, 457 U.S. 830 (1982).
Rennie, D. (2003, August 1). 'Admiral Behind Terrorist Futures Market "To Quit"'. *Daily Telegraph* (London), p. 20.
'Responses by Center for Democracy and Technology and Other Civil Liberties Organizations to TIA Report' (herein "Responses") (2003, August 20). Available at: http://www.cdt.org/security/usapatriot/030520cdt.shtml.
R. L. Polk & Co. (2005). 'Automotive Profiling System'. Available at: http://www.polk.com/products/aps.asp.
Roe v. Wade, 410 U.S. 113 (1973).
Rosen, J. (2000). *The Unwanted Gaze: The Destruction of Privacy in America*. New York: Vintage.
Safire, W. (2003, February 13). 'Privacy Invasion Curtailed'. *New York Times*, p. 41.
Samuelson, P. (2000). 'Privacy as Intellectual Property?' 52 *Stanford Law Review* 1125.
Schneier, B. (2003). *Beyond Fear: Thinking Sensibly About Security in an Uncertain World*. New York: Springer-Verlag.
Scott, J. C. (1998). *Seeing Like a State: How Certain Conditions to Improve the Human Condition Have Failed*. New Haven: Yale University Press.
Solove, D. J. (2002). 'Conceptualizing Privacy'. 90 *California Law Review* 1087.
Solove, D. J. & Rotenberg, M. (2003). *Information Privacy Law*, p. 27. New York: Aspen Publishers.
St. Petersburg Times (Florida). 'Total Information Awareness II?' 31 May 2004, p. 12A.
Stone, G. R. (2004). *Perilous Times: Free Speech in Wartime from the Sedition Act of 1789 to the War on Terrorism*. New York: W. W. Norton & Co.
Strathern, M. (2003). 'Emergent Relations'. In M. Biagioli & P. Galison (Eds.). *Scientific Authorship*, pp. 169–94, chapter 7. New York: Routledge.
Sudell, A. (2001). 'Comment: To Tell or Not to Tell: The Scope of Physician-Patient Confidentiality When Relatives Are at Risk of Genetic Disease'. 18 *Journal of Contemporary Health Law and Policy* 273.
Sutherland, J. (2002, February 18). 'No more Mr Scrupulous Guy'. *The Guardian* (United Kingdom). Available at: http://www.guardian.co.uk/g2/story/0,3604,651950,00.html.
Technology and Privacy Advisory Committee (herein "TPAC") (2004, March 1). *Safeguarding Privacy in the Fight Against Terrorism: Report of the Technology and Privacy Advisory Committee to the Department of Defense*. Available at: http://www.mipt.org/pdf/Safeguarding-Privacy-Fight-Against-Terrorism.pdf.
Times-Picayune (New Orleans, LA). 'Plots at Public Meetings?' 3 June 2002, p. 4.
Turkel, S. (1997). *Life on the Screen: Identity in the Age of the Internet*. New York: Touchstone.
United States v. Leon, 468 U.S. 897 (1984).

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (herein "USA PATRIOT Act"), Pub. L. No. 107–56, 302(a) (1), 115 Stat. 272 (2001).
Warren, S. D. & Brandeis, L. D. (1890). 'The Right to Privacy'. 4 *Harvard Law Review* 193.
Weaver, K. D. (1997). 'Genetic Screening and the Right Not to Know'. *Issues in Law & Medicine*, vol. 13. no. 3, p. 243.
Webster v. Reproductive Health Services, 492 U.S. 490 (1989).
Weintraub, B. (1986, November 26). 'Iran Payment Found Diverted to Contras; Reagan Security Advisor and Aide Are Out'. *New York Times*, p. A1.
Westin, A. F. (1967). *Privacy and Freedom*. London: Bodley Head.

14. Are Human Rights Universal in an Age of Terrorism?

WIKTOR OSIATYNSKI

To answer the question posed in the title it is useful to distinguish between human rights as the set of rules and human rights as principles. It also distinguishes between human rights and the philosophy of human rights. In 1948, there existed a cross-cultural consensus on rights as principles and on basic tenets of the philosophy of human rights. Recently, the consensus over principles and over the philosophy of human rights has broken down. The events of September 11 did not start this process; it merely accelerated it, and the war on terrorism brought it to a point that could be beyond repair. Therefore, our task today should not be to restore the consensus over the philosophy of human rights, but to detach the rules from – once universal, albeit no more – principles so that we could rescue human rights norms and find the most adequate means to enforce them.

To understand better this thesis, a brief overview of the development of human rights is in order.

The Original Consensus on Human Rights

The Universal Declaration of Human Rights (UDHR) adopted by the United Nations in December 1948 reflected a broad consensus between various ideas, values, and cultures. Even though the idea of individual rights was of Western origin, it was the non-Western countries that pushed for the adoption of the Declaration, against some reluctance of the Western governments (Lauren 1998: 165–71). Leaders and philosophers from Latin America, Asia, and the Middle East joined Western intellectuals and activists in support of human rights (Glendon 2001).

The final version of the Declaration proclaimed the values of individual liberty, democracy, and participation, as well as social and economic rights. Latin American governments also placed great emphasis on labor rights and