Denver Law Review

Volume 79
Issue 4 *Symposium - Privacy*

Article 15

December 2020

Vol. 79, no. 4: Full Issue

Denver University Law Review

DENVER UNIVERSITY LAW REVIEW

VOLUME 79

2001-2002

FROM EDITOR

As you have most likely noticed by now, this year's Symposium issue has quite an exciting, new look. We decided to revive our "magazine" format - something first tried approximately thirty years ago. Our goal with this issue is to present interesting and informative articles, in a reader-friendly format, on a timely subject: privacy. In the wake of the largest terrorist attack on American soil, and with war looming, privacy concerns abound.

We chose writers from diverse backgrounds: attorneys, a bookstore owner, a privacy activist, and a former governor, just to name a few. You may not agree with everything they have to say, but we think you will find their articles thought provoking and timely. I want to thank each author for writing a superb article - and also thank each author for their patience. The magazine issue took a little longer than our usual law review issues, but we think you will agree that it is well worth the wait.

We hope you enjoy this new format and the articles within.

Sincerely,

Tanya L. Thiessen
Symposium Editor

Denver University Law Review (ISSN 0883-9409)
Summer 2002
The Denver University Law Review is published quarterly by the University of Denver College of Law through the Denver University Law Review Association.

Denver University Law Review
7039 East 18th Avenue
Denver, Colorado 80220
(303) 871-6172
dulr@student.law.du.edu
www.du.edu/law/lawreview
Cite as: 79 DENV. U. L. REV 2002.

Subscriptions: Subscriptions to the Law Review are $35.00 per volume (add $5.00 for foreign mailing). All subscriptions will be renewed automatically unless the subscriber provides timely notice of cancellation.
Single and Back Issues: Single issues of the current volume are available from the Association at $15.00 per issue. All previous volumes and issues of the Law Review are available exclusively from William S. Hein & Co., Inc., 1285 Main Street, Buffalo, NY 14209 (800) 828-7571.

Form: The Law Review generally conforms to The Bluebook: A Uniform System of Citation (Columbia Law Review Ass'n et al. eds., 17th ed. 2000) and to The Chicago Manual of Style (14th ed. 1993). It is the general policy of the Law Review not to keep unpublished sources used in articles, notes, or comments beyond their use for verification of citations. Inquiries as to the location of an unpublished source should be directed to the author of the article, note, or comment in which it is cited.
Manuscripts: Please address manuscripts to the Articles Editor, Denver University Law Review, 7039 East 18th Avenue, Denver, Colorado 80220. Manuscripts should be double-spaced and cannot be returned unless accompanied by a self-addressed, postage-paid envelope.
Previous nomenclature: Published as the Denver Bar Association Record from 1923 to 1928, Dicta from 1928 to 1965, and Denver Law Journal from 1966 to 1984.
Postmaster: Please send all address changes to Denver University Law Review, 7039 East 18th Avenue, Denver, Colorado 80220.

INSIDE

University of Denver College of Law

ADMINISTRATIVE OFFICERS

Daniel L. Ritchie, A.B., M.B.A., Chancellor
Robert Coombe, Ph.D., Provost
Craig Woody, B.A., Vice Chancellor for Financial Affairs/Treasurer
Carol Farnsworth, M.A., Vice Chancellor for Communications
Mary Ricketson, B.A., J.D., Dean of the College of Law
J. Robert "Jay" Brown, B.A., M.A., Ph.D., J.D., Associate Dean for Academic Affairs
Gary L. Alexander, B.A., M.L.L., J.D., Asst. Dean of Information Services and Library Director
David Ricciardi, B.S., Registrar
Iain Davis, B.A., Financial Aid Director
Keryn Goldstein, B.A., Chief Financial Officer
Sheila Green, B.A., M.A.L.S., Reference Librarian
Martha Kcister, A.B., M.A., M.L.S., International Law Librarian
Stephen Favreau, M.S., B.A., Asst. Dean of Administration
Lauri A. Mlinar, Director of Events
Nancy P. Nones, B.A., Administrator, International Legal Studies
Laura Dean, B.A., Director of Alumni Relations
Robin A. Ricker, B.S., Program Coordinator, Graduate Tax Program
Patty Powell, B.A., J.D., Dean of Student Services
Forrest Stanford, B.A., J.D., Director of Admissions
Tim Henderson, B.A., M.S., J.D., Director of Career Services
Shane Seymour, B.A., M.A., Executive Director of Development
Robert Yegge, A.B., M.A., J.D., Dean Emeritus
Professor of Law, Director, Legal Administration Program, Co-Director, Clinical Programs

FACULTY

Tanya Bartholomew, B.A., J.D., Legal Writing Professor
William M. Beaney, A.B., LL.B., Ph.D., Emeritus Professor of Law
Arthur Best, A.B., J.D., Professor of Law
Andrea Bloom, B.A., J.D., Legal Writing Professor
Jerome Borison, B.S., J.D., LL.M., Associate Professor of Law, Director, Student Federal Tax Advocacy Clinic
Burton F. Brody, B.S., J.D., LL.M., Professor of Law
J. Robert "Jay" Brown, Jr., B.A., M.A., Ph.D., J.D., Associate Dean of Academic Affairs, Professor of Law
Penelope Bryan, B.S., M.A., J.D., Associate Professor of Law
John A. Carver, Jr., A.B., LL.B., LL.D., Emeritus Professor of Law
Federico Cheever, B.A., M.A., J.D., Associate Professor of Law
Alan K. Chen, B.A., J.D., Associate Professor of Law
Christine Cimini, B.A., J.D., Assistant Professor of Clinical Programs
Alfred J. Coco, B.A., J.D., M.L.L., Emeritus Professor of Law
Roberto L. Corrada, B.A., J.D., Associate Professor of Law
Tami D. Cowden, B.A., J.D., Legal Writing Professor
Edward A. Dauer, A.B., LL.B., Dean Emeritus and Professor of Law
Kate Duba, B.A., J.D., Legal Writing Professor
Wendy Duong, B.S., J.D., LL.M, Assistant Professor of Law
K.K. DuVivier, B.A., J.D., Assistant Professor of Law, Director of Lawyering Process Program
Nancy S. Ehrenreich, B.A., J.D., LL.M., Professor of Law
Christopher Gehring, B.A., J.D., Legal Writing Professor
J. Wadine Gehrke, B.A., J.D., Assistant Professor of Clinical Programs
Rashmi Goel, B.A., LL.B., J.S.M., Assistant Professor of Law
Robert M. Hardaway, B.A., J.D., Professor of Law
Jeffrey H. Hartje, B.A., J.D., Associate Professor of Law
Timothy M. Hurley, B.A., J.D., Legal Writing Professor
Sheila K. Hyatt, B.A., J.D., Professor of Law
Sam Kamin, B.A., J.D., Ph.D., Assistant Professor of Law
Martin Katz, A.B., J.D., Assistant Professor of Law
Francis W. Jamison, B.A., J.D., Emeritus Professor of Law
Jan G. Laitos, B.A., J.D., S.J.D., John A. Carver, Jr. Professor of Law, Director of Natural Resources Program
Harry O. Lawson, B.A., M.S., Emeritus Professor of Law
Neil O. Littlefield, B.S., LL.B., LL.M., S.J.D., Emeritus Professor of Law
Lucy A. Marsh, B.A., J.D., Professor of Law
Esteban Martinez, B.A., M.A., J.D., Legal Writing Professor
Michael G. Massey, B.A., J.D., Legal Writing Professor
G. Kristian Miccio, B.A., M.A., J.D., LL.M., J.S.D., Assistant Professor of Law
Ved P. Nanda, B.A., M.A., LL.B., LL.M, LL.M., LL.D. (Hon.), Vice Provost for Internationalization, Evans University Professor, Thompson G. Marsh Chair, Director, International Legal Studies Program
Julie A. Nice, B.A., J.D., Professor of Law, Delaney Chair
Jim Otto, B.S., J.D., M.S., Director, Advanced Degree Programs in Natural Resources and Environmental Law
Stephen L. Pepper, A.B., J.D., Professor of Law
George W. "Rock" Pring, B.A., J.D., Professor of Law
John H. Reese, B.A., LL.B., LL.M., S.J.D., Professor of Law
Paula R. Rhodes, B.A., J.D., Associate Professor of Law, Director, LL.M. in American and Comparative Law Program
Edward J. Roche, Jr., B.B.A., J.D., Professor of Law
Howard I. Rosenberg, B.A., LL.B., Professor of Law
Thomas D. Russell, B.A., M.A., J.D., Ph.D., Professor of Law
John T. Soma, B.A., M.A., J.D., Ph.D., Professor of Law
Mary A. Steefel, B.A., J.D., LL.M., Legal Writing Professor
Celia R. Taylor, B.A., J.D., Associate Professor of Law
Mark A. Vogel, B.B.A., J.D., LL.M., Professor of Law, Director, Graduate Tax Program
Eli Wald, B.A., LL.B., LL.M., S.J.D., Assistant Professor of Law
Timothy B. Walker, A.B., M.A., J.D., Emeritus Professor of Law
James E. Wallace, A.B., LL.B., B.D., Ph.D., Emeritus Professor of Law
James L. Winokur, B.A., LL.B., Professor of Law
Robert B. Yegge, A.B., M.A., J.D., Dean Emeritus, Professor of Law, Director, Legal Administration Program, Co-Director, Clinical Programs
Edward H. Ziegler, Jr., B.A., J.D., LL.M., Professor of Law

JOB INSECURITY?

When It Comes To Workplace Surveillance Of Electronic Communications, Employers Are Free To Establish The Rules Of The Game

by Philip L. Gordon, Esq.

Introduction

In May, 2001, when federal judges on the United States Court of Appeals for the Ninth Circuit learned that, in at least one important respect, they were no different from millions of clock-punchers worldwide, they were outraged.[1] What was the startling revelation for these usually imperturbable appellate court judges? Mere bureaucrats in the Administrative Office of the United States Courts, a little known group of civil servants who administer the federal court system, were monitoring the federal judiciary's e-mail and Internet traffic, including the traffic of these Article III judges.[2] The perceived intrusion upon the seclusion of judicial chambers so incensed Judge Alex Kozinski that he took the highly unusual step of publicly denouncing the chief of the administrative agency in the *Wall Street Journal* and discussed his views on a nationally televised talk show.[3]

Ironically, in the years preceding this millennial epiphany, judges, practically all of whom came of age with the rotary dial telephone, had put in place a regime which has made it extremely difficult for workers to recover damages based upon their employers' review of e-mail and Internet communications. This situation has resulted from a judicial construction of the Federal Wiretap Act,[4] which effectively eliminates any statutory privacy protection for workplace e-mail and Internet use. With e-mail and Internet use steadily transforming the United States Postal Service into a quaint relic, the time is ripe for judges, and Congress as well, to re-think the law governing the privacy of e-mail and Internet communications. However, the events of September 11, 2001, have placed the issue of workplace privacy on the judicial and legislative backburner.

Consequently, employers, who are increasingly concerned about regulating the use of e-mail and Internet in the workplace, should view this regulatory vacuum as an opportunity to establish their own rules governing the use of these resources.[5] Moreover, employers have a range of electronic monitoring policies from which to choose. At one end of the spectrum is a policy aimed at protecting employers from abuse of their electronic communications systems through employee consent to unrestricted electronic monitoring. At the other extreme is a policy based upon the principle that electronic privacy should be a workplace benefit. Employers can tailor either policy to meet their own specific needs and the demands of their particular workforce.[6]

From The Rotary-Dial Telephone To The Apple Macintosh: The Evolution Of The Federal Wiretap Act

The 1960s were watershed years for wiretaps. By that time, tapping technology had been in use for decades with practically no restrictions or judicial oversight under federal law.[7] Then, the United States Supreme Court revolutionized the notion of communications privacy. In *Katz v. United States*,[8] the Court held that even someone who uses a public telephone booth can have an objectively reasonable, subjective expectation of privacy in the content of his telephone call, an interest protected by the Fourth Amendment from government intrusion.[9]

Congress responded to *Katz* by outlawing virtually all interceptions of telephone calls without judicial

authorization. Congress also strictly limited the circumstances in which a court could order a telephone wiretap.[10] However, the statute embodying this regime, the Federal Wiretap Act, was a creature of its time. The statute was premised upon a monolithic communications world inhabited only by AT&T and its copper telephone lines.

In the opening years of the 1980s, the world upon which the Federal Wiretap Act was premised changed slowly, but radically. Apple Computers began to market "The Macintosh," the first computer designed for consumption by the general public. Electronic mail was becoming a widespread means of communication. The cordless telephone represented the cutting edge of telephone technology. The answering machine had just recently become a "must-have" commodity. The divestiture of AT&T was a work in progress.

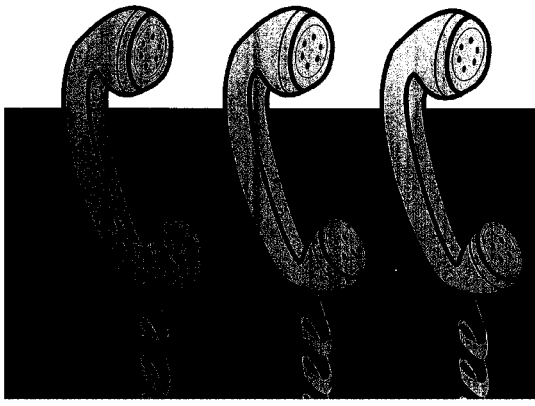
With this backdrop, Congress amended the Federal Wiretap Act in 1986, thereby extending the Act's coverage to "electronic communications."[11] In contrast to "wire communications" - transmissions of the human voice over telephone lines - "electronic communications" encompassed transfers of data not containing the human voice[12] (Napster, of course, was not yet on the radar).

At the same time, Congress passed an accompaniment to the Federal Wiretap Act, which sometimes is referred to as the Stored Communications Act.[13] This statute protects stored electronic communications in two limited respects. First, an anti-hacking provision prohibits unauthorized access to "a facility through which an electronic communication service is provided," such as a server, for purposes of obtaining access to electronic communications stored in that facility.[14] Second, the statute imposes upon those who provide electronic communications services to the public, such as an Internet Service Provider ("ISP"), an obligation to maintain the privacy of electronic communications stored on their own servers.[15]

The Judicial De-Clawing Of Federal Statutory Protections For The Privacy Of E-Mail And Internet Communications

The practical effects of this dichotomy between electronic communications and stored electronic communications became apparent only as claims under the Federal Wiretap Act based upon the unauthorized review of e-mail began to trickle through the judicial pipeline. The seminal case in the area, *Steve Jackson Games, Inc. v. United States Secret Serv.*,[16] did not involve workplace monitoring, but rather the Secret Service's review of un-retrieved e-mail stored on the hard drive of a computer seized from a company offering an electronic bulletin board service.[17] The United States Court of Appeals for the Fifth Circuit held that the Secret Service's conduct was not actionable under the Federal Wiretap Act because the Act prohibits only "real-time" interceptions of electronic communications, i.e., the acquisition of the content of the communication *while the communication is in transmission.*[18] Because the e-mail reviewed by the Secret Service was in electronic storage, the Federal Wiretap Act did not apply. However, the Secret Service did not escape *Steve Jackson Games* scot-free. The Fifth Circuit's opinion notes that the Secret Service did not challenge the district court's finding that its agents had violated the Stored Communications Act by reviewing the un-retrieved e-mail without authorization from the service provider, without the consent of either party to the communications reviewed, and without judicial authorization.[19]

Steve Jackson Games opened the door to unrestrained monitoring of workplace e-mail and Internet use. Until relatively recently, software capable of "real-time" interception of e-mail and Internet communications was not even commercially available. Consequently, employers seeking to monitor employee e-mail and Internet use had no choice but to retrieve the content of those communications from electronic storage on the



" The statute was premised upon a monolithic communications world inhabited only by AT&T and its copper telephone lines."

employer's server. Moreover, unlike the Secret Service in *Steve Jackson Games*, an employer can not be held liable under the Stored Communications Act for retrieving employee e-mail from its own server because that statute expressly excludes the system provider from liability.[20] The Stored Communications Act also is inapplicable to an employer's retrieval of e-mail permanently stored on an employee's hard drive because the Stored Communications Act protects electronic communications only when in intermediate or temporary storage.[21]

The Fifth Circuit's construction of the Federal Wiretap Act to prohibit only "real-time" interception of e-mail and Internet use dominated the judicial scene until the United States Court of Appeals for the Ninth Circuit addressed the issue in January 2001.[22] Perhaps as a precursor to its outcry against e-mail and Internet monitoring by the Administrative Office of the United States Courts, the Ninth Circuit in *Konop v. Hawaiian Airlines*[23] held that the acquisition of the content of an electronic communication may be actionable under the Federal Wiretap Act even if the electronic communication is not in transmission when the acquisition occurs.[24] In that case, Konop, an airline pilot, maintained a closed bulletin board for pilots to speak critically about both union representatives and company officials.[25] Konop alleged that an airline executive violated the Federal Wiretap Act by using false pretenses to obtain access to, and to review, messages on the bulletin board.[26] The Ninth Circuit, rejecting the Fifth Circuit's construction of the Act in *Steve Jackson Games*, held that the airline executive's actions constituted an interception under the Act.[27] Relying in part upon its holding in *United States v. Smith*,[28] that the unauthorized retrieval of a voice mail message constituted an interception under the Federal Wiretap Act,[29] the *Konop* court stated that there was no reasoned basis for distinguishing between voice mail and electronic mail.[30]

Philip L. Gordon is a shareholder in the Denver office of Littler Mendelson, P.C., a national labor and employment law firm, and a fellow of the Privacy Foundation. Mr. Gordon specializes in counseling employers on privacy issues and representing employers in privacy-related litigation

The proponents of workplace privacy had a short-lived victory. In a startling reversal, revealed shortly before the September 11 terrorist attacks, the panel in *Konop* withdrew its opinion *sua sponte*, with one judge dissenting.[31] The majority's brief opinion provides no reason for this highly unusual action.[32] The majority might have belatedly realized the potential impact of the panel's original decision on law enforcement, thus explaining the panel's hasty retreat from its novel holding. If the retrieval of stored e-mail does constitute an interception under the Federal Wiretap Act, then law enforcement authorities must obtain court authorization and comply with the Federal Wiretap Act's stringent limitations on interceptions before, for example, obtaining access to e-mail on an ISP's servers. By contrast, the Stored Communications Act, which otherwise regulates access by law enforcement officials to electronic communications in storage at an ISP, establishes a much lower threshold and much less stringent requirements for access to stored electronic communications.[33]

Congressional Reconstruction Of Federal Privacy Protections For E-Mail And Internet Use Is Not On The Horizon

The prevailing statutory construction leads to bizarre results in the employment context. Communications by telephone — whether wire-line, cordless, or cellular — enjoy full protection under the Federal Wiretap Act.[34] Federal law also protects the most obvious piece of junk, snail mail, from unauthorized interception.[35] By contrast, under *Steve Jackson Games* and its progeny, electronic mail enjoys no protection under the Act unless intercepted in real-time.[36] Put another way, employers cannot obtain the contents of telephone communications in any form without risking liability under the Act, but employers can review employee e-mail and Internet use with impunity so long as they do not intercept the content of the communication in real-time.[37]

This is not the first time that the Federal Wiretap Act has resulted in an arguably irrational stratification of means of communication. In 1986, when Congress expanded the Federal Wiretap Act to encompass "electronic communications," Congress contemporaneously and expressly excluded cordless telephone communications from the Act's coverage.[38] Congress reasoned that the general public could readily attain the radio portion of a cordless telephone conversation that resulted from the transmission between the handset and the base unit. Consequently, the cordless telephone user could not have an

objectively reasonable expectation of privacy in his cordless telephone conversations.[39]

This "cordless" exclusion, like the real-time construction of the word "interception," resulted in a boon for law enforcement. Numerous reported cases decided under the Federal Wiretap Act after 1986 analyzed motions filed by criminal defendants to suppress the contents of cordless telephone conversations acquired by a police scanner, or even a neighbor's baby monitor.[40] Relying on the Congressional exclusion, courts uniformly denied these motions to suppress, whether based upon the Act or upon the Fourth Amendment.[41]

Notwithstanding this law enforcement benefit, Congress eliminated the "cordless exclusion" in 1994.[42] Congress concluded that the distinction between unprotected calls over cordless telephones and protected calls over cellular and wire-line telephones had become untenable. Even though it was commonly known that others could easily acquire the radio portion of a cordless telephone call, the use had become so widespread that society could no longer tolerate unrestrained interceptions of this means of communication.[43]

A similar congressional reversal of the distinction between wire communications and electronic communications resulting from the judicial construction of the term "interception" is not on the horizon. In the wake of September 11th, Congress probably will not amend the Federal Wiretap Act to put the interception of stored electronic mail on an equal footing with the interception of telephone calls. To do so would impose new constraints on law enforcement when society is focused on the war on terrorism and the need to ensure personal security.

If anything, Congress signaled its approval of the judicial distinction between real-time interception and retrieval from storage when it passed anti-terrorism legislation in October 2001, popularly known as the USA Patriot Act. That statute, among other things, removed voice mail from the scope of the Federal Wiretap Act.[44] As a result, telephone calls, like electronic mail, now enjoy federal statutory protection only when intercepted in real-time.

How Employers Can Fill The Judicial And Legislative Vacuum

Until Congress takes action, the e-mailer's situation today will remain similar to the man in the sidewalk telephone booth in *Katz*, or the cordless telephone user between 1986 and 1994. The means of communication has become a part of everyday life but its use is potentially perilous.

From the employer's perspective, this situation has advantages in the workplace. The e-mail system can pose a potential threat by, for example, allowing the transmission of trade secrets off site with the press of a button. In addition, Internet use can interfere with the intended business purposes of the employer's system resources through, for example, the downloading of pornography. Also, the circulation by e-mail of provocative messages could raise the specter of discrimination or sexual harassment claims. Given these risks, employers are appropriately concerned about these abuses and their potential costs. In the absence of judicial or legislative limits, employers have the freedom to protect themselves from these risks as long as they do not intercept the content of electronic communications in real time without first obtaining their employees' consent.[45]

By the same token, unrestricted electronic monitoring may stifle beneficial uses of e-mail and the Internet. Privacy spawns creativity, and the rapid interchange of ideas through e-mail can accelerate the creative process. But, if an employee fears that a supervisor who monitors the mail will swat down an unorthodox idea, she might be less willing to express herself. With respect to personal activities, a modicum of privacy may ultimately benefit the employer. After all, which course of conduct is more efficient: fifteen minutes of surfing Amazon.com's Web site or one hour on a secret mission to Barnes & Noble located several blocks from the office?

This question remains: how should an employer regulate the use of e-mail and the Internet in the workplace? The answer will depend upon an array of factors including, for example, the employer's own objectives, the maturity and sophistication of the employer's workforce, the function of e-mail and Internet communications in the particular workplace, and whether trade secrets are accessible in electronic format.

Those employers who view their electronic communications system as a threat could deter abusive conduct with a policy designed to send a clear signal to employees that if they abuse the employer's system, they will be caught and disciplined. Some of the principal points of this type of policy would state the following:

1. The electronic communications system and all communications sent, received, or stored by the system are the property of the employer;

2. The employer reserves the right to monitor, read, copy, print, and distribute the content of all electronic communications, including e-mail and Web sites visits, sent, received, or stored by the system;

3. How the monitoring will be effectuated;

4. By signing the employer's

continued on page 575

Little Brothers Are Watching You:

The Importance of Private Actors in the Making of Fourth Amendment Law[1]

It is something of a truism in criminal procedure (as elsewhere in constitutional law) that unless the conduct of a government agent is involved, the Constitution is not implicated.[3]

Thus, if a Federal Express employee acting on her own initiative opens a shipped package that turns out to contain drugs and then gives these drugs to law enforcement, no search has occurred.[4] Similarly, if a hotel manager searches the room of a guest and then turns over any contraband he finds to the government, no search has occurred.[5] So long as the private citizen is acting as such and not at the direction or encouragement of law enforcement,[6] the government is free to use the discovered material without concern for its exclusion at trial.[7] To the extent that actions by private actors ever find their way into our consideration of criminal procedure, it is generally to prove this point: only the government and its agents can be found to have violated the Fourth Amendment.

In this essay, I argue that this focus on state action has distracted both scholars and practitioners from an important point: the interrelationship between privacy vis-à-vis private actors and privacy vis-à-vis the government. While it is true that the absence of a state actor means that a Fourth Amendment search has not been conducted, it does not follow from this fact that Fourth Amendment doctrine is unaffected by such invasions of privacy. Quite the contrary: I argue that the more privacy an individual surrenders to private actors, the less privacy he will have from the government. The more we become inured to our neighbors, employers, creditors, and advertisers having greater and greater access to areas we think of as private, the more we run the risk that the government will have unfettered access to them as well.

The principal basis for this argument is the Supreme Court's decision in *Katz v. United States*[8] and the line of precedent that it has spawned. In *Katz*, the Supreme Court stated that a search occurs and the Fourth Amendment is implicated whenever the government invades an area in which an individual has a reasonable expectation of privacy.[9] The Court held that whether an

"INSTEAD of asking whether the place searched...is a place entitled to Fourth Amendment protection...the question became whether the defendant behaved in a way that demonstrated his subjective belief that the place searched was entitled to protection..."

individual is entitled to Fourth Amendment protection depends not on where the search of the object takes place, but rather on how the individual and society treat that area.[10] Thus, as the court put it:

> [T]he Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection . . . [b]ut what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.[11]

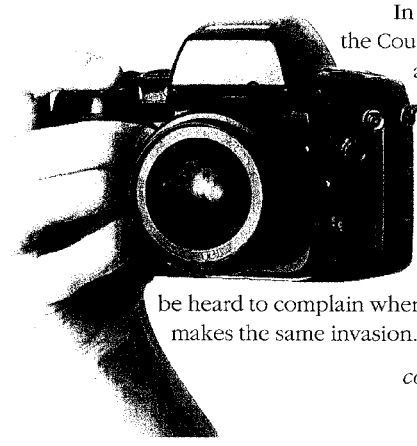
Instead of asking whether the place searched — in *Katz* a public phone booth — is a place entitled to Fourth Amendment protection in the abstract, the question became whether the defendant behaved in a way that demonstrated his subjective belief that the place searched was entitled to protection, and whether society is willing to validate that belief as reasonable.[12]

On a case-by-case basis over the last thirty-five years, the contours of the Fourth Amendment under *Katz* have come into focus. I argue that one thing that has become very clear is that even things in which one generally has a very high privacy interest — one's home, one's business records, etc. — can be searched by the government without implicating the Fourth Amendment if one has permitted others to have access to these things. If an individual has given up a reasonable expectation of privacy in his property or information by exposing them to the view of others, he cannot attempt to deny the government similar access to these areas.

Of course, in these cases one rarely waives an interest in property or information explicitly. Instead, in a number of contexts, courts have inferred from a defendant's actions that he could not have had a privacy interest in his activities, or that such an interest could not be reasonable. For example, in *California v. Greenwood*[13], the Supreme Court held that no search occurred when police removed trash that Greenwood had placed by the side of the road for collection.[14] Without explaining whether Greenwood had demonstrated that he did not expect his discarded trash to be kept secret, or whether that expectation of privacy, even if actually entertained by the defendant, was not reasonably held, the Court simply reasoned that there could not be a reasonable expectation of privacy in something consciously abandoned.[15]

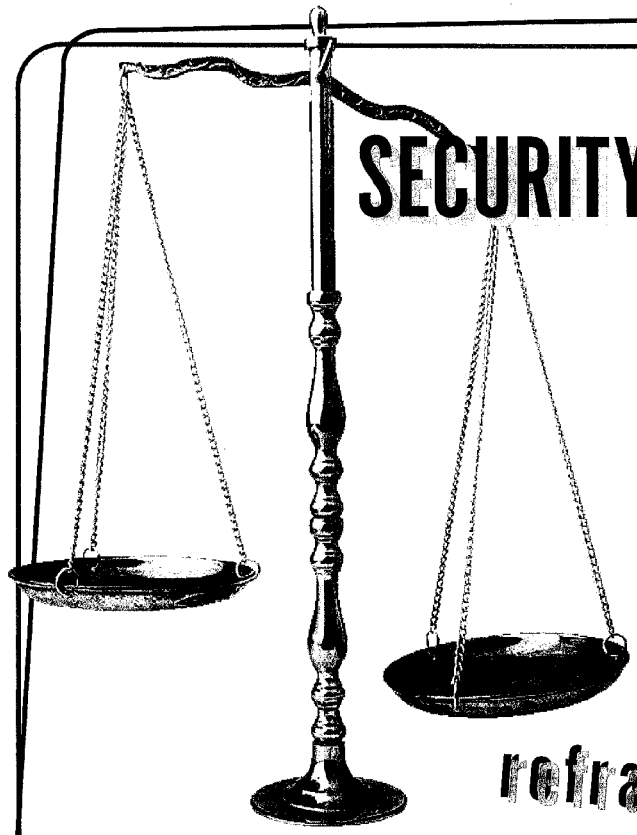
The Court's reasoning was clearly influenced by the fact that by putting the trash in front of the house, Greenwood had made it available not just for sanitation workers but for anyone else who happened by. The Court stated, "[i]t is common knowledge that plastic garbage bags left on or at the side of a public street are readily accessible to animals, children, scavengers, snoops, and other members of the public."[16] Furthermore, the Court reasoned, the sanitation workers themselves, once in possession of the trash, might have conveyed it to anyone else.[17] Thus, because the police officers merely did what any other member of the public could have done — looked through the trash that had been left out — they did not invade Greenwood's reasonable expectation of privacy.

In reaching this conclusion, the Court analogized to other, earlier examples of this line of reasoning. For example, in *Smith v. Maryland*[18] the Supreme Court held that the installation and use of pen registers — devices that allow law enforcement to access and record all of the numbers dialed from a particular phone — was not a search subject to the requirements of the Fourth Amendment. The Court held that the installation and use of these devices (by the phone company at the direction of law enforcement) was not a search because in the course of using his phone, the defendant voluntary conveyed information to the phone company about the numbers he was dialing.[19] Thus, Smith knew (or at the very least should have known) that he was transmitting this information to a third party, and "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[20] Similarly, in *United States v. Miller*,[21] the Supreme Court ruled that records held by banks may be subpoenaed without invoking the Fourth Amendment. The reasoning was the same: "The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."[22] Like Greenwood putting out her trash, Smith and Miller had essentially abandoned their privacy interests by allowing others access to their information.[23]



In still other contexts, the Court has held that when an individual has simply failed to protect herself from an invasion of privacy that a member of the public could have made, she will not be heard to complain when the government makes the same invasion. For example, in

continued on page 553



SECURITY VS. PRIVACY

reframing the debate

By Shaun B. Spencer*

— "Freedom and fear are at war."**

This essay explores several dimensions of the debate between security and privacy that accompanies many anti-terrorism and law enforcement proposals.

The debate is often framed, either implicitly or explicitly, as a balancing of the tangible harms that a security proposal would prevent, against the intangible harms that an intrusion on privacy would cause. This approach presents the choice between, for example, the disastrous effects of a terrorist airline hijacking, and the relatively minor feeling of discomfort that might flow from presenting a national ID card before boarding. Given those limited choices, what right-thinking person would not choose the latter? This framework of balancing tangible against intangible harms is not merely a rhetorical strategy selected by the proponents of security measures. It is also a way of understanding the debate that flows naturally from the perception that privacy is a mere abstraction, a luxury with little concrete value.

This essay focuses on three ways in which the tangible-versus-intangible decision making framework both overvalues security and undervalues privacy. First, the framework is incomplete because it fails to account for the many unintended consequences that usually flow from security measures. The cumulative effect of those unintended consequences gradually erodes society's very conception of privacy. Yet the tangible-versus-intangible framework implicitly focuses on short-term benefits and consequences, necessarily excluding the long-term effects on privacy.

Second, the contextual specificity that characterizes the tangible-versus-intangible framework overemphasizes the harms on the tangible side of the scale. By embedding the choice between security and privacy in a concrete factual context (such as boarding a plane), the framework all but guarantees that people will decide to guard against the tangible harms.

Finally, the framework draws a false distinction between tangible breaches of security and intangible intrusions on privacy. In fact, the tangible results that

security proposals promise are often empirically suspect. Instead, security proposals serve largely intangible goals, such as allaying people's fears. In contrast, privacy intrusions can have quite tangible consequences that disrupt and inhibit social behavior.

I. UNINTENDED CONSEQUENCES AND THE EXPECTATION-DRIVEN CONCEPTION OF PRIVACY

The tangible-versus-intangible framework described above invariably understates the impact of any particular security measure on privacy. This is so for two related reasons. First, the framework fails to account for the many unintended consequences that inevitably accompany most privacy-intrusive security measures. Second, the framework ignores the fact that our conception of privacy is vulnerable to incremental encroachment not only by the initial security measure, but also by the unintended consequences that follow.[1] The tangible-versus-intangible framework, however, implicitly focuses on short-term benefits and consequences, and therefore excludes long-term effects on privacy.

A. Unintended Consequences

Unintended consequences come in several different forms. The first is secondary use, which occurs when information created or collected for one purpose is used for another, or when an information collection technique developed for one purpose is used for another.[2] One of the most widely acknowledged examples is the Social Security number (SSN). After Congress passed the Social Security Act, the newly-formed Social Security Board[3] had to find a way to track each worker's lifetime earnings, social security contributions, and benefits.[4] The Board assigned a number to each account, and assured citizens that the SSN was to be used solely to identify citizens' retirement accounts.[5] Yet in 1943, President Roosevelt ordered all federal agencies developing their own identification systems to use the SSN "exclusively."[6] Over the next five decades, the SSN's uses spread like wildfire, and by 1998 the Secretary of Health and Human Services acknowledged that the SSN was "in such extraordinarily wide use as to be a *de facto* personal identifier."[7] Today, someone who refuses to divulge her SSN will find it practically impossible to conduct everyday transactions.[8] This is not a peculiarly American phenomenon. Identifying numbers in Canada, Australia, the Netherlands, and Austria have all been put to widespread secondary uses.[9]

Secondary uses can flow to government as well as from it. For decades, direct marketers have collected vast stores of personal information about potential customers. Data profiling has become far more comprehensive with the rise of the Internet, which has put a great deal more personal information at profilers' disposal. Consumers, however, might be surprised to learn that businesses are not just sharing profiles with one another - they are sharing our profiles with law enforcement as well.[10] Sometimes law enforcement need not even ask for the information. Hosts of businesses reportedly opened their customer records to law enforcement agencies in the aftermath of September 11, often in violation of the privacy policies that they claimed they would honor when they collected the data.[11] Moreover, the USA Patriot Act[12] dramatically expanded the types of information about our Web surfing that any "governmental entity" - not merely law enforcement agencies - may monitor without a warrant.[13]

Consumers...might be surprised to learn that businesses are not just sharing profiles with one another - they are sharing our profiles with law enforcement as well

The second kind of unintended consequences are disclosures due to insufficient safeguards over personal information.[14] Any centralized database is vulnerable to hacking, even in such supposedly secure organizations as the Internal Revenue Service.[15] Accidental data disclosures have also become increasingly common. For example, credit agency Experian, drug manufacturer Eli Lilly & Co., and healthcare provider Kaiser Permanente, have all mistakenly divulged confidential information online.[16] Eli Lilly recently entered into a consent decree with the FTC concerning the accidental disclosure of the e-mail addresses of nearly 700 patients with mental illnesses, which Eli Lilly collected through its Prozac.com Web site.[17] Similarly, the House Energy and Commerce Committee recently took its Web site offline after discovering that an internal database concerning the Enron investigation "was left exposed to anyone with a Web browser."[18]

In addition to human error, there is the problem of human corruption. Centralized information is always at the mercy of dishonest or corrupt individuals willing to use it for their own personal or political gain. The abuses of J. Edgar Hoover and Richard Nixon are legendary.[19] But abuses of centralized databases and government surveillance are routine, rather than mere historical anomalies. Many security threat models predict that one percent of an organization's staff will always "be willing to sell or trade confidential information."[20] For example, in a five-year period, 127 employees of the California Department of Motor Vehicles were disciplined "for facilitating ID fraud."[21] Similarly, a Virginia notary public was recently convicted of "helping thousands of undocumented immigrants . . . illegally obtain Virginia

driver's licenses" and ID cards.[22] Until September 21, 2001, Virginia allowed applicants to prove residence with identity papers and a notarized affidavit.[23] *The Washington Post* reported that seven of the September 11 hijackers had obtained Virginia ID cards using that same loophole.[24]

A chilling General Accounting Office report details abuse of centralized crime databases by FBI and other law enforcement officers.[25] The National Crime Information Center ("NCIC") "is the nation's most extensive computerized criminal justice information system" consisting of a centralized database at FBI headquarters "and a coordinated network of federal and state criminal justice information systems."[26] "[I]nsiders pose the greatest threat to NCIC because they know the system and can misuse it by obtaining and selling information to unauthorized individuals, such as private investigators, or altering or deleting information in NCIC records."[27] The report found numerous incidents where insiders disclosed NCIC information to "unauthorized persons, such as private investigators, in exchange for money or other rewards."[28] In one case, a former Arizona law enforcement officer used NCIC information he obtained from three other officers to track down and murder his estranged girlfriend.[29] A Pennsylvania terminal operator used the NCIC to conduct background searches for her boyfriend - a drug dealer - who used the information to determine whether his new clients were undercover agents.[30] And in the tradition of Nixon's "dirty tricks," some local officials unlawfully used NCIC information to discredit political rivals.[31]

B. Incremental Encroachment and the Expectation-Driven Conception of Privacy

In any privacy-related debate, it is important to understand that privacy is generally defined by our own expectations.[32] Judicial privacy doctrines developed under the Fourth Amendment and in tort law define the scope of privacy by reference to whether an individual has a reasonable expectation of privacy in a particular context.[33] Even legislative action on privacy issues reflects social expectations of privacy. Given the variety of powerful interests that might be adversely affected by privacy-protective legislation, such legislation is extremely unlikely to pass unless it is supported by strong public perceptions of what is appropriately kept "private" in a given context.[34] Privacy, in short, is only as extensive as we believe it is.

This expectation-driven conception renders privacy vulnerable to incremental encroachment. Sweeping intrusions into the private sphere may fail because they conflict with firmly held expectations of privacy.[35] However, repeated moderate intrusions by governments and institutions capable of influencing social behavior can gradually erode expectations of privacy. The necessarily imprecise nature of group preferences means that we usually find a "gray area" where societal expectations are unsettled. The gradual erosion of privacy occurs through repeated incursions into this gray area.[36]

Thus, the effects of any single encroachment in fact reach much farther than the tangible-versus-intangible framework can acknowledge. The tangible-versus-intangible framework focuses too narrowly on the present, to the exclusion of the inevitable unintended consequences that will diminish privacy expectations far more than the initial security proposal. The framework commonly examines the extent to which a given proposal would intrude on our *current* expectations of privacy, and asks whether that intrusion is worth the promised security benefits.

To take just one example, proponents of a national ID card might suggest that limiting such a card to uses at borders and airports would have only minimal privacy implications, in part because people are already used to showing some form of ID when they travel.[37] But that view ignores the unintended consequences that would inevitably follow the creation of a card, even for initially limited purposes.[38] The urge to expand the uses of a biometric-based national ID - and the centralized database that would inevitably support it[39] - would be irresistible. A centralized database would facilitate the card's uses by government agencies responsible for welfare benefits, law enforcement, and medical data.[40] Businesses would push to use the national ID card, perhaps at first for credit and banking purposes, but eventually for as many purposes as the SSN and driver's license are currently used.[41]

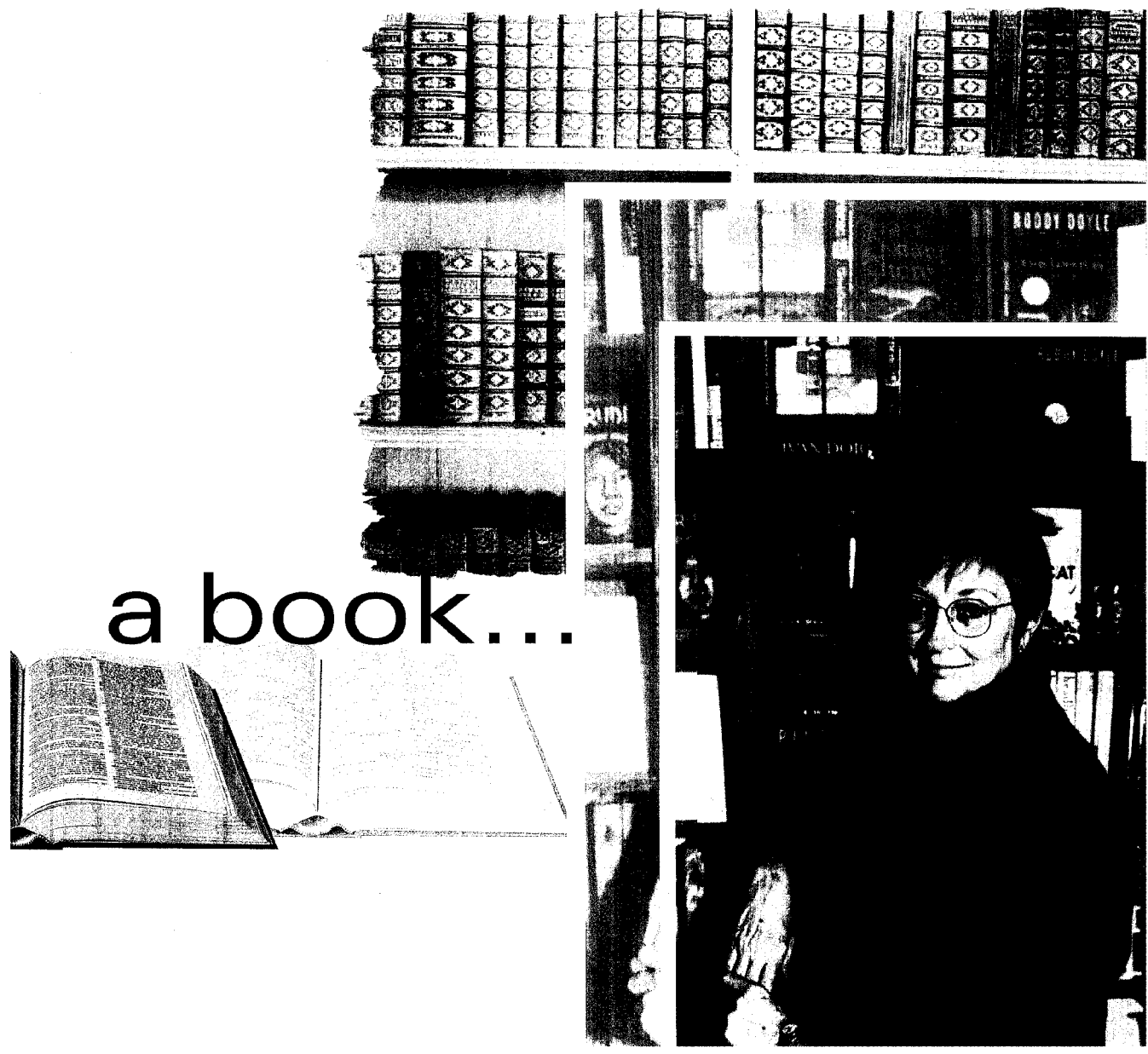
Such plans are already underway. The American Association of Motor Vehicles Administrators ("AAMVA") recently proposed uniform national standards for all state-issued driver's licenses, which would encode a variety of information about each license holder, including a "biometric identifier."[42] Companies are already marketing scanners that can not only read, but also store, information from the AAMVA-standardized driver's license.[43] Scanners are being marketed to bars, restaurants, car dealerships, and convenience stores, and suggested for use by health clubs, personal trainers, and for the general retail market.[44] AAMVA itself has proposed sharing its model with banks, the travel industry, car rental agencies, insurance companies, and retailers.[45] Furthermore, as illustrated above, centralized databases are ripe for abuse from within and without, and increase dramatically the chance for accidental disclosures. As these uses and abuses accumulated in incremental steps, we would gradually come to expect less and less privacy in a variety of contexts - clearing the way for further encroachment. Each inch of ground that society yields in the private sphere renders the next inch more vulnerable. Yet the tangible-versus-intangible framework ignores these long-term effects by limiting its temporal focus to the present.

continued on page 554

judging

On March 17, 2000, the Tattered Cover Book Store received a "subpena" from the Drug Enforcement Agency ("DEA") and I began a fight to save the First Amendment.

by Joyce Meskis



a book...

On March 17, 2000, the Tattered Cover Book Store received a "subpena" from the Drug Enforcement Agency ("DEA"). The "subpena" required that the Tattered Cover turn over the purchase records of one of the store's customers. Specifically, it asked for the record relating to a mail order purchase, in addition to all other transactions by this particular customer.

I immediately faxed the "subpena" to our attorney, Dan Recht, who informed me that it was an unenforceable administrative subpoena.[1] We discussed the First Amendment implications of this request. Dan said he would call the DEA agent. Dan informed the agent of our First Amendment concerns and stated that the Tattered Cover would not turn over the information based on this administrative request. He invited the agent to obtain a real subpoena that we would then litigate. The agent indicated to Dan that he did not want to do so, and Dan was left with the impression they were going to let it drop.

We thought the matter was over. However, early in April Dan received a call from Fran Wasserman at the Adams County District Attorney's office. Mr. Wasserman told Dan that a search warrant was being sought in order to obtain the information that the DEA "subpena" had requested from the Tattered Cover. Dan felt that Mr. Wasserman hoped to avoid the search warrant by getting Dan's permission to obtain the information. Dan asked if he could have until the end of the next business day before any action was taken to give him time to contact his client. Mr. Wasserman agreed.

I was incredulous when Dan called to tell me about his conversation with Mr. Wasserman. A search warrant! No opportunity for further judicial review! We agreed to mull over the situation and discuss it the following day. However, before we had an opportunity to have that conversation, there were four law enforcement officers (soon to be joined by a fifth) in my office, search warrant in hand. I could not believe it! I raised the First Amendment issues, talked about the *Kramerbooks* case, which put a greater burden on authorities when it came to searches and seizures of constitutionally protected material,[2] all to no avail. The officers allowed me to contact Dan, who persuaded them to hold off on the execution of the warrant for a week after a series of conversations with the officers and Mr. Allen, in the Denver District Attorney's office, who had signed off on the warrant.

The search warrant had been narrowed somewhat from the original request. It required the Tattered Cover to turn over detailed information concerning the mail order shipment, plus all transactional information relating to that same customer during a one-month period.

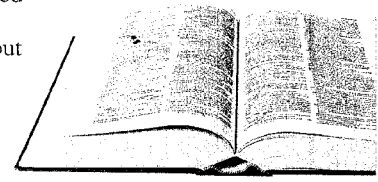
We filed for and received a temporary restraining order halting the execution of the search warrant. This allowed us to litigate the subpoena in the Denver District Court. That case was heard in October 2000, and the judgment rendered half a loaf to each side. Judge J. Stephen Phillips denied authorities (the North Metro Drug Task Force) access to our customer's purchase records over the one-month period. However, the judge ordered the Tattered Cover to provide the information regarding the specific mail order shipment it had contained.

The facts leading up to the search warrant unfolded over time. Apparently, late in 1999 and early in 2000, the North Metro Drug Task Force was investigating a suspected methamphetamine lab in a trailer home in Adams County. During the course of that investigation, they sifted through the trash outside of the home. In so doing, they found the leavings of a meth lab as well as an empty mailing envelope with a Tattered Cover mailing label on it addressed to a person living in the trailer home. That label also had an invoice number printed on it which could be used to identify the shipment.

The leavings of a meth lab found in the trash gave police probable cause to obtain a search warrant for the trailer home. In searching the home, they found a small meth lab in a bedroom. They also found two new looking books on the manufacture of methamphetamines. Neither had Tattered Cover inventory control stickers on them. One was still in a wrapper. Testimony in court also alleged that neither had the appearance of having been read.

The police found that there were as many as five or six individuals living in or frequenting the trailer home. They concentrated on identifying the occupant of the bedroom. A list of suspects emerged, our customer being Suspect A. Suspect A's address book was found in the bedroom, along with other documents with the names of other individuals. A lot of effort went into building the prosecution of this case, but it all came to a screeching halt with the issue of trying to tie the meth books to Suspect A. The police testified that they saw this as a "piece of the puzzle."

However, when Fran Wasserman was approached to sign off on the search warrant in Adams County, he refused to do so. He indicated to the officers that more investigation was needed. He asked them to check the books for fingerprints and told them that they needed to interview the suspects connected with the trailer home. They proceeded to dust the books, but found no useful fingerprints. The officers did not do the interviews in compliance with Mr. Wasserman's request. Instead, they sought the search warrant from another jurisdiction-Denver.



I knew very little about the investigation when the police arrived at the Tattered Cover with the search warrant from the Denver County Court. As our conversation unfolded, I asked one of the officers if our customer (Suspect A) had been contacted so that permission could be obtained for me to turn over the information. The officer said that they had not because the suspect was not the sort to give permission. I thought that might indeed be true if those particular books regarding the manufacture of methamphetamine had been sent in the mailer. If they had not, our customer may have given permission for the police to find out what had been in the mailer. In any case, it seemed to me that there was little to lose in asking, and something might be

gained. The officer stressed that they just wanted the information regarding the mail order shipment. I asked the officer what would happen if this did not reveal what they expected it to. He replied that they would then take the next step, which I interpreted to mean that they would seek additional records from the Tattered Cover.

The officers made it clear that they were not investigating the Tattered Cover for illegal activity. I was sure that was the case, because the Tattered Cover is a law-abiding business. I tried to make it clear that the Tattered Cover did not intend to stand in the way of a criminal investigation. As an establishment, we are in agreement with authorities that meth labs are a scourge on the community. We support the police in the difficult job they do. But, for the Tattered Cover, an individual consumer's book purchase has serious First Amendment implications. We also believe that it is incumbent on the police to protect and honor our First Amendment rights. This case requires a balancing of the necessity of the information the government seeks against important constitutional protections.

As the afternoon wore on, I asked one of the officers how having a book in one's possession could play a role in a conviction for illegal activity. He replied that it could be introduced into evidence to establish the suspect's state of mind. Curiously, months later he would say that the information regarding the book purchase was sought to establish residency in the bedroom (the police had residency in the trailer home established). Why then, did the police only focus on the books about methamphetamines? Were there other books in the bedroom? What would have been the outcome if the Tattered Cover had not sold the meth books to this suspect? Would that have freed Suspect A of suspicion? I did not think that was likely. How important exactly was this "piece of the puzzle?" Was a "compelling need" (a higher standard than probable cause) clearly established? Given all of the evidence, would there still have been a case without the books? Conversely, if the whole case hung on the books, was it a viable case?

...he would say that the information regarding the book purchase was sought to establish residency in the bedroom... Why then, did the police only focus on the books about methamphetamines?

Some have asked me why I did not declare victory after the decision of the District Court. Would turning over this information really impact our freedom to read? I believe it would. Therefore, the Tattered Cover decided to appeal the decision of the District Court. Briefs were submitted to the Colorado Supreme Court and the oral arguments were heard on December 5, 2001. I am writing this at the end of February 2002 as we await the decision of the court.

While the Tattered Cover is not arguing that the First Amendment enjoys absolute protection, it is arguing that there should be and is a higher standard of protection. It is, after all, one of the very most important pillars of our government. In the *Kramerbooks* case, a District of Columbia District Court Judge ruled that Kenneth Starr, in his subpoena of Monica Lewinsky's book purchase records, could not have unfettered access to such information in his investigation of President Clinton's activities. She ruled that he must demonstrate a compelling need for the information as it relates to such an investigation, which is a higher standard than probable cause.[3] That case never made it to the next step

continued on page 555

Tattered Cover v. Thornton:

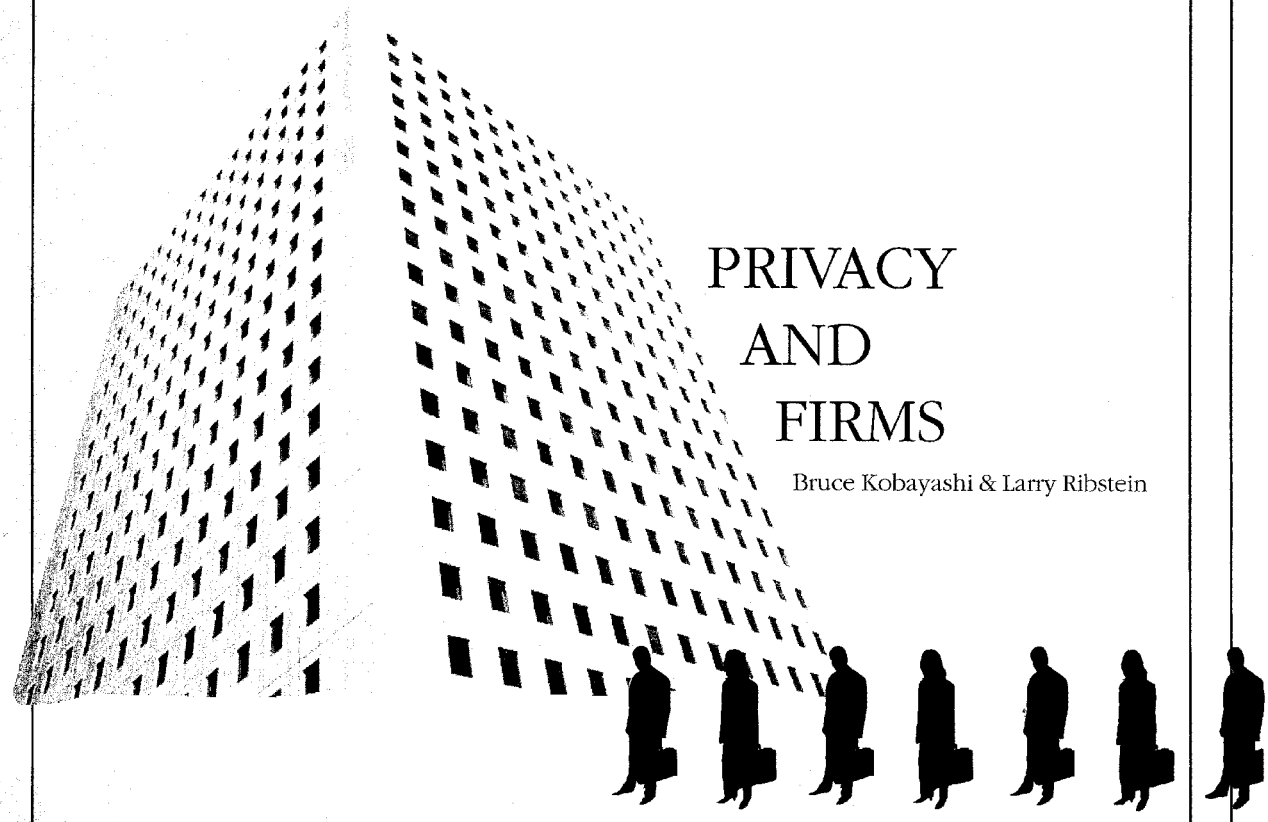
by Corey Ann Finn

The Colorado Supreme Court handed down *Tattered Cover v. Thornton* on April 8, 2002.[1] The court found in favor of Joyce Meskis' bookstore, the Tattered Cover, holding that the search warrant of a bookstore customer's purchase record was unconstitutional.[2]

In 2000, the Drug Enforcement Agency and the North Metro Task Force were monitoring a trailer in Adams County, Colorado, because they suspected that its occupants were manufacturing methamphetamine.[3] Having searched through the trash of the trailer and having executed a search of the trailer pursuant to a warrant, investigators needed to connect one of four occupants of the trailer to the meth lab found in the trailer's bedroom. Suspecting a connection between the books found in the bedroom on the manufacture of methamphetamine and an empty mailer from the Tattered Cover found in the trash, investigators served the Tattered Cover with a DEA administrative subpoena, requiring information about the order sent to Suspect A and all other purchases made by the suspect. About this initial subpoena, the Colorado Supreme Court said that "[u]sing such a subpoena was ordinarily a successful technique for DEA officers, though such a subpoena lacks any force or legal effect."[4] Meskis, through her attorney, informed investigators of her unwillingness to comply because of her concern for the privacy of the bookstore's customers.

Investigators then sought and received a warrant from a Denver County court, which they attempted to execute. Pursuant to Meskis' attorney's request, the district attorney who signed off on the warrant voluntarily stayed its execution so the bookstore could litigate it (in fact, the Tattered Cover did receive a Temporary Restraining Order from the court).

continued on page 570



PRIVACY AND FIRMS

Bruce Kobayashi & Larry Ribstein

Questions concerning the extent to which privacy should be governed and what the rules should be.

Employees and employers have competing interests in disclosing

Privacy is a loose collection of principles, particularly including a property right in information and an interest in a protected personal sphere.[1] In general, there are questions concerning the extent to which privacy should be governed by default or by mandatory rules, and what these default or mandatory rules should be.

Privacy raises particularly difficult and important questions in the employment context. Employees and employers have competing interests in disclosing and preventing disclosure of information. For example, firms may want to share information with their employees about customers, trade practices and technology that helps the employees do their jobs. This raises the concern that employees will reap private advantage by selling or otherwise transferring this information to third parties during or following their employment. This concern could reduce firms' willingness to share such information with employees, and can suppress incentives to develop information or inventions.[2] At the same time, excessive protection of the employers' information could reduce employees' mobility and the flow of valuable information in society.

Employers, in turn, need information about employees in order to evaluate them for hiring and to monitor them while they are employed. Employees have an incentive to disclose because employers' information costs affect the cost of employment and ultimately jobs and compensation. But employees also may have an interest in keeping some information private to protect their personal space or to hide shirking or other bad acts that are detrimental to the firm.

Appropriately balancing employers', employees' and society's interests in workplace privacy contributes to social wealth by encouraging efficient employment relationships. This requires sensitivity to the unique characteristics of the economic activity that gives rise to the specific organizational form chosen by a given firm. It follows that balancing may best be achieved by enforcing firms' contracts. Contracts covering employment issues in general, and privacy in employment in particular, are among the nexus of contracts that are the central characteristic of a firm.[3] Since efficient restrictions add value to the firm by protecting its proprietary information and ability to monitor employees, employers and employees usually are better off if contracts are enforced than if they are not. To be sure, employees may prefer *ex post* not to be bound by restrictions on disclosure and not to be monitored by the employer. But employees are better off *ex ante* to the extent that they share in the value of efficient arrangements through higher compensation.

That is not to say that enforcing contracts is always efficient. There may be some role in this area as in other areas of intra-firm contracting for legal regulation. For example, restrictions on the dissemination of employer information or on employee mobility may benefit both employees and employers but reduce social wealth because of their negative effects on development of intellectual property and competition. Employers' intrusions into employee privacy may be privately wealth maximizing within the firm, but have social costs in terms of the loss of individuality. Thus, it may be tempting to regulate these contracts.

But in order to fully evaluate such regulation, it is important to measure costs as well as benefits. The full costs of regulating employer/employee contracts

appear only from an understanding of the role these contracts play in the overall operation of the firm, and an appreciation of the second-best alternatives parties would resort to if regulation precludes first-best contracts. For example, restricting protection of employer information can inhibit firms from disseminating confidential business information to employees[4] and, in turn, force revision of relationships with employees. Protecting the privacy of employees' information can inhibit monitoring of employees and force employers to resort to non-agency-type relationships.

This paper is both normative and positive. It shows why contracts regarding these issues *should* be enforced. It also shows that the contracts are enforced despite seemingly mandatory state rules preventing enforcement. The key to understanding the positive analysis is to see the enforcement issue in the *interstate* context, where both employers and employees are free to choose the states in which they live, contract, and sue.

Part I presents an overview of the theory of the firm and its implications for privacy. Part II discusses the issues regarding privacy of the employers' information, including enforcement of contracts between employers and employees from intra- and interstate perspectives. Part III discusses privacy issues concerning employees, again including enforcement of contracts.

I. THE THEORY OF THE FIRM AND PRIVACY

Economic activity is carried out within a firm when the costs of using market transactions are relatively high.[5] Within a firm, a nexus of longer-term contracts that direct activity and restrain the behavior of the transactors replaces spot transactions directed by market prices.[6] The form of these contracts is shaped by the nature of the transactions and information costs the parties face. One circumstance in which the cost of using market transactions is high is team production. Team production occurs when individual resources are combined so that the value of the combined output exceeds the sum of the outputs of the individual resources, and it is costly to determine an individual's marginal contribution to team output.[7] Increasing the cost of monitoring an individual's effort level increases moral hazard costs, ceteris paribus. Moreover, if the team resources become specialized to the team, individual members can opportunistically "hold up" the team by threatening to withdraw team resources under their control unless they receive a larger share of the team's marginal product.[8]

The use and production of confidential business information is an example of the team production problem. Team production is present because the value of information produced by many individuals exceeds the sum of the values of each individual's separate information. Moreover, the value of the combined information is often maximized when it is then widely disseminated among members of the team, as opposed to being closely held by management. Thus, to maximize the value of team production, individuals must be induced to disclose their valuable private information to the firm, and the firm in turn must be able freely to disseminate the information among team members.

The inherent attributes of information can, however, make both types of disclosures costly. First, it is difficult to monitor individuals' use of the team's information because information is intangible, thereby facilitating hidden behavior,[9] and plastic in the sense that it can be used in many different ways.[10] This deters sharing of valuable information and reduces the value of team production.[11] Individuals may fail to disclose valuable information to the team, inadequately safeguard valuable information, or use disclosed information for their own benefit at the team's expense,[12] by direct or indirect disclosure to competitors.[13]

Second, it is difficult to design mechanisms for encouraging disclosure by individual team members. Prior to disclosure, the discloser may be unable to convince others of its value. Indeed, even after disclosure it may be difficult to value the marginal contribution of an individual's information.[14] If the owner of the information has been unable to strike a bargain prior to disclosure, it may lose the value of the information on disclosing it because, absent legal protection, the potential buyer or others may disseminate it.[15] These problems may lead to "adverse selection" in the sense that team members are induced to disclose only low quality information.[16] A team member also may be able to use his private information to hurt the team, or threaten to do so unless he is given a larger share of the benefits the team creates.

The firm must devise ways to solve these problems of moral hazard and opportunism associated with the disclosure and use of information by individuals in the firm. This includes restricting individuals' access to valuable information, and developing incentives to create information. The firm can promulgate rules apportioning the value of the firm's information among team members, contract with employees to restrict their behavior during and after their employment, and monitor employees'

"...firms' incentives to share information with their employees may be affected by the risk that employees will disclose this information with others"

creation and use of information. These rules and contracts may involve intrusions into the employee's "privacy" and restrictions on the employee's "freedom." But such "intrusions" are no more onerous than terms contained in licensing agreements that serve to restrict the "freedom" of the licensee.[17] Both types of restrictions facilitate the voluntary production and dissemination of information.

How a firm addresses these problems depends on several factors. First, firms differ in the extent to which their activities use resources and information that are costly to monitor and expose the firm to opportunistic behavior. Second, employees vary in their costs of reduced privacy and ability to move to other jobs. These differences can be expected to produce many different approaches to protecting information.

Firms' contracts also depend on legal rules precluding enforcement of some types of contractual restrictions. For example, rules that protect employees' privacy can increase firms' monitoring costs by precluding them from using some types of intrusive surveillance techniques. Firms then will have to use less preferred methods of reducing the costs of employee moral hazard. Firms may not only switch to less intrusive and effective monitoring methods, but also make more fundamental changes in the way they conduct their business. For example, firms' increased exposure to tort and criminal liability resulting from diminished ability to effectively monitor employees may induce firms to replace employees with independent contractors, thereby effectively altering the scope of the firm.[18] Also, reducing firms' abilities to protect their information also may reduce dissemination of information with the firm and potential marginal benefits of team production.

The desirability of legal rules prohibiting enforcement of agreements that restrict employee privacy and mobility must consider several issues in addition to the substantive nature of such rules, including whether such rules should be mandatory or default rules, what legal regime will apply to a contract between a firm and its employees, and how such rules should be made. For example, if a wide variety of approaches would be optimal, default rules may be superior to mandatory rules, and different types of firms may need different default rules. Under these circumstances, a decentralized, bottom-up approach to legal restrictions may be preferred to a top-down, centralized uniform approach.[19] Finally, while different firms may prefer a wide variety of approaches, a given firm may prefer that a particular rule apply uniformly to all members of a firm. Otherwise, forum shopping by mobile employees of multi-state or multi-jurisdictional firms can result in the non-uniform and non-optimal application of rules regulating the employer/employee relationship.[20] This suggests that parties should be able to enter into enforceable contracts by choosing which law governs the employee/employer relationship.[21]

II. PROTECTING EMPLOYERS' INFORMATION

This Part builds on the general discussion in Part I by discussing more specifically the employment contracts that protect dissemination of employer information and the costs and benefits of enforcing these contracts. It shows that, while enforcing these contracts usually is efficient, there may be some justification for state laws restricting enforceability. However, the politics of such laws suggests that state regulation may be excessive. In particular, states may internalize the benefits of using these laws to protect local interests while imposing costs out of state. This Part also shows that this problem ultimately can be disciplined by the parties' ability to locate and litigate in jurisdictions that enforce efficient contracts. Subpart A discusses the countervailing considerations that drive contracts in this area. Subpart B discusses state provisions and enforcement of contracts regarding these issues, including the default rule protecting trade secrets and customized contracts regarding ex-employees' competition and disclosure. It shows that, viewing the issues solely from an intrastate perspective, states have perverse incentives not to enforce efficient contracts. Finally, subpart C discusses the interstate dynamic that disciplines state law inefficiency.

A. THE BASIC PROBLEM

As discussed in Part I, firms' incentives to share information with their employees may be affected by the risk that employees will disclose this information with others. Employees may do so by either straight sale or by effective sale in the form of employment. During employment, the firm can monitor employees' misuse of information, subject to restrictions on such monitoring resulting from privacy considerations discussed in the next Part. The employer's biggest problem, therefore, may be the employee's use of the information to compete with her former employer after leaving employment.

From the standpoint of the employer's and employee's joint welfare, the optimal contractual restrictions depend on the risk to the employer associated with the employer's disclosure of proprietary information; the value to the employer of disseminating the information to the employee compared to alternative relationships in which information is not shared with the agent, and the costs to the employee of being restricted from sharing information that the employee may have helped create and that is inherent in the employee's expertise. For example, the employer may have developed customer lists or technical information that the employee must have in order to be able to sell or develop the product. However, if dissemination of the information to the employee is likely to lead to the further disclosure of the information to competitors, sharing this information will result in a significant reduction in the value of the employer's valuable informational property right. The employer's only alternative to restricting disclosure may be a less productive relationship with the employee. However, the employee may have also contributed to the

development of the employer's products and its clientele. Also, a highly specialized employee may be unable to separate her own expertise from that of the employer. Variations on these facts would produce different levels of optimal restrictions on information in particular relationships.

The policy analysis is complicated by social costs of contracts regarding dissemination of employer information. Dissemination of information may be valuable to the amount of innovation.[22] Conversely, inability to protect proprietary information may reduce incentives to produce it in the first place.[23] Thus, default rules and contract enforcement matter.

B. ENFORCEMENT OF CONTRACTS: INTRASTATE PERSPECTIVE

This subpart discusses the basic law of enforcing contracts that protect employers' information. It assumes that the relevant law is that provided by a single state. Subpart C widens the perspective to the multi-state scenario.

1. The default rule: Trade secrets law

Trade secrets law most directly protects the employer's business information. However, this law has important gaps, and may be costly and uncertain to apply.[24] Thus, employers must supplement default legal protection of trade secrets by actively monitoring employees' theft of information and with other contractual protection, including non-competes, as discussed in the next subsection.

2. Express contractual protection: Non-compete covenants

Although employees may become involved in industrial espionage and outright theft, while they are with the firm it would seem that the threat of dismissal would deter most direct misuse of corporate information.[25] However, after the employee leaves, firing the employee obviously is no longer a viable sanction for misuse of information and the employee has much stronger incentives to abuse corporate information. The employee might sell the information outright, but more often is likely to try to use the information as leverage in getting another job or as the basis for a competing business. As noted above, relying on trade secret law alone may not be an effective means to prevent such abuse of employer information. Thus, the most important protection in this setting is through the use of covenants not to compete.[26] These contracts impede employees from effectively selling the information by pursuing lines of work after employment where the information is most valuable. The agreements also serve several other functions, including ensuring the retention of unique talent, and protecting the firm's investment in training employees.[27]

Covenants not to compete are not always enforced under state law. The main question regarding enforcement concerns the scope of the restriction. Most states enforce "reasonable" restrictions,[28] although they may differ on standards of reasonableness. Some states have strong statutory policies against enforcement set forth in statutes. In particular, the California statute provides, "every contract by which anyone is restrained from engaging in a lawful profession, trade, or business of any kind is to that extent void."[29]

The states appear to have several reasons for not enforcing these agreements. First, where the agreement restricts the employee more than appears necessary to protect the employer's property rights, the agreement may be anti-competitive — that is, it may prevent employees with valuable expertise from working for competitors. Also, employers may try to piggyback competition restrictions onto protection of information by disclosing more trade secrets to employees than the job requires in order to justify broad restrictions.[30] Second, some courts appear to be concerned with inequality of bargaining power between employer and employee, perhaps attributable to employees' lack of market power or sophistication. Third, Ronald Gilson has argued that enforcing non-competes reduces positive externalities of information sharing between firms that can permit the growth of high-tech corridors.[31]

These arguments may or may not justify non-enforcement.[32] In general, even if non-compete agreements have costs, it is important to consider whether the benefits of enforcement discussed above outweigh the costs. Even if the court imposes a seemingly mild "reasonableness" restriction, it may be hard for employers to design a restriction that is both broad enough to protect their information and narrow enough to satisfy the courts. Thus, holding agreements unenforceable may impede protection of employers' information. This seems particularly clear where alleged costs are internalized between the employer and employee.

With respect to the argument that the agreements are anticompetitive, it is not clear why employers in general should be deemed to have enough market power in the employment market to render their employment agreements suspect. Just as employers compete for valuable employees at the time of employment, so they must compete as to the terms of employment, including terms that restrict employees' mobility. Thus, employers would internalize the costs of these agreements through the wages they must pay employees to agree to the covenants. Indeed, it would seem that employers would have to pay employees more than the agreements are worth as restrictions on competition since employees, whose human capital is not diversifiable, could be expected to be averse to the risks of immobility.

Perhaps the competition argument reduces to an argument that the employers have unfair bargaining leverage over employees. But again, it is not clear why this would be the case throughout the employment market. Moreover, covenants not to compete are most prevalent with respect to the most highly trained workers and professionals, who are presumably most able to protect

themselves contractually. Although legal restrictions on non-competes may make workers better off than they would be without the restrictions, it is not clear whether this is efficient or in any sense fair. Non-enforcement of the covenants may transfer wealth from employers and low human capital workers to high human capital workers.[33] Even if employers do have bargaining leverage, restrictions on non-competes may accomplish little, since employers can use their leverage to reduce the employees' compensation to adjust for the inability to impose a non-compete, or substitute other devices that may be inferior from the employers' standpoint but hurt employees as much or more than non-competes. For example, employers have the option of simply disclosing less information to employees.

With respect to Gilson's argument that non-competition agreements may impose social costs by impeding the flow of information, it is not clear when this benefit of restrictions is outweighed by the social costs of reducing incentives to produce information or making employment relationships less efficient. All of this is not to say that restrictions on non-competition agreements are never efficient. The benefits of certain types of restrictions certainly outweigh the costs for some types of economic activities. But the opposite will be true for other types of economic activities. Even if legislation or common law rules that restrict enforcement of non-competition agreements enforce efficient norms or practices for the former subset of activities,[34] applying such laws to the latter set of activities will be socially costly. Thus, there is room for experimentation with and competition among various regimes. This raises the question, discussed in the next subpart, whether jurisdictional choice leads to efficient rules.

C. THE INTERSTATE PERSPECTIVE

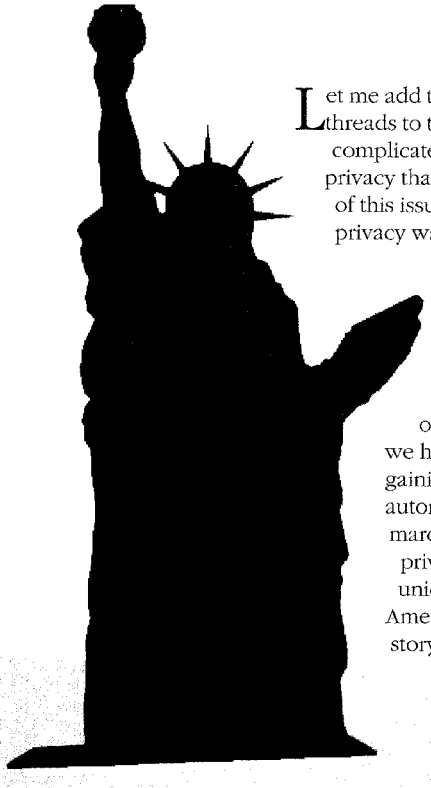
Gilson suggests that states should be able to decide what policy they will follow regarding enforcement of non-competes because employers can leave states that inadequately enforce contracts and protect property rights.[35] But a state's regulation may apply to employers who have offices in multiple states, that seek to recruit in the regulating state, or whose employees are being recruited by an employer in the regulating state. The national or international scope of many modern firms makes it costly for them to structure their businesses so that they avoid operation in states with undesirable rules. This may enable states — particularly a large, economically powerful state like California — to impose the costs of its competition policy on firms elsewhere while local firms get the benefits. Conversely, California's firms are subject to the costs of other states' inadequate regulation while they must play by local rules in doing business locally. This problem of "spillover" of regulatory costs suggests that state competition may lead to inefficient results.

Firms' practical inability to avoid undesirable state regulation is partly attributable to default choice-of-law rules regarding enforcement of contracts that make it difficult for employers to predict whether their agreements will be enforceable in these interstate situations. Restatement (Second) of Conflicts indicates the range of considerations courts may take into account:

> (1) The rights and duties of the parties with respect to an issue in contract are determined by the local law of the state which, with respect to that issue, has the most significant relationship to the transaction and the parties under the principles stated in § 6.
>
> (2) In the absence of an effective choice of law by the parties (see § 187), the contacts to be taken into account in applying the principles of § 6 to determine the law applicable to an issue include:
>
> (a) the place of contracting,
>
> (b) the place of negotiation of the contract,
>
> (c) the place of performance,
>
> (d) the location of the subject matter of the contract, and
>
> (e) the domicil, residence, nationality, place of incorporation and place of business of the parties. These contacts are to be evaluated according to their relative importance with respect to the particular issue.
>
> (3) If the place of negotiating the contract and the place of performance are in the same state, the local law of this state will usually be applied, except as otherwise provided in §§ 189-199 and 203.[36] The general factors that guide choice of law under this section are:
>
> (a) the needs of the interstate and international systems,
>
> (b) the relevant policies of the forum,
>
> (c) the relevant policies of other interested states and the relative interests of those states in the determination of the particular issue,
>
> (d) the protection of justified expectations,
>
> (e) the basic policies underlying the particular field of law,
>
> (f) certainty, predictability and uniformity of result, and
>
> (g) ease in the determination and application of the law to be applied.[37]

Thus, for example, a court might apply the law of the raiding employer's state rather than that of the employee's or employer's state, even if the employee originally resided there, because of the raiding state's strong policy favoring sharing information. The regulating state might be able to have it both ways, since in the reverse situation its own interest in protecting local

continued on page 555



Privacy and Public Policy

by Richard D. Lamm
Professor,
University of Denver

Let me add two modest threads to the incredibly complicated fabric of privacy that is the subject of this issue. First, privacy was an almost alien concept to America's founding settlers, and we rightly can be proud of the progress we have made in gaining individual autonomy. The march toward privacy is a uniquely American success story. Second, although this has been an American success story, we should take great care not to lose, in the name of privacy, some of the efficiencies modern technology has made available to government.

America was not born in or with privacy. Both government and neighbors intruded on one's "privacy" in ways unthinkable today. Americans lived mostly in small, confined communities where everyone knew everyone else's business. Your neighbor's business was your business, and state authority often backed this up.[1] A citizen could, and often would, be turned in by a neighbor for adultery, wife beating, dressing immodestly, flirting, homosexuality, masturbation, sodomy or violation of "community religious and moral values."[2] New Englanders thought nothing of spying on and interfering with their neighbor's most intimate affairs, in order, as one Massachusetts man said in 1760 "not to suffer sin in My Fellow Creature or Neighbor."[3] Most prosecutions in colonial courts were for moral offenses. The Puritans made homosexuality, masturbation, sodomy and bestiality capital offenses, and flirting in a lascivious manner and failure to attend church on Sunday were matters for prosecution.[4] People would gather around the post office and demand a public reading of their neighbor's private letters considered to be of special interest, and travelers often would find themselves sharing a bed with a stranger at an inn.

In most states, citizens were compelled to fund religion and their "souls" were public business. Nine colonies funded churches; the separation of church and state existed only in Rhode Island, Delaware, New Jersey and Pennsylvania.[5] Until the mid-nineteenth century, American citizens publicly financed churches, usually Congregational or Anglican.[6]

No clear delineations existed between the "public" sector and the "private" sector. The government often performed its functions by requiring citizens to perform municipal jobs. If a municipality had a public need it would often enlist its citizens to perform it. Street cleaning and paving were accomplished by obliging each person and business in the city to clean or repair the street abutting his house or shop. Many functions considered public today were mandated to be performed by the citizenry, and charters were issued to private individuals to collect fees for many municipal services like toll roads and education. Sanctions were issued against private persons for failure to perform their public duties.[7] A person's life and lifestyle were closely connected to that of his or her neighbor. People's private actions were subject to public monitoring, and their time was subject to appropriation by the community.

The thinking behind the American Revolution and the Constitution changed this dramatically. People were no longer "subjects" but "citizens," and republicanism eliminated the Crown's prerogatives and granted them to state legislatures. Government ceased controlling matters of personal morality. Public taxation was expanded, and public and private functions separated. Public education was initiated, and separation of church and state expanded gradually, with Massachusetts being the last state to abolish a state funded church in 1833.[8] While strong pressures to conform to certain moral standards existed, the structure of those post-Revolutionary War institutions that separated the public and private sectors started America down the road to autonomy and privacy.

My second point is that while there are dangers of ignoring or under-reacting to the issues raised by privacy, there are also dangers of overreacting. The threat to personal privacy and the Orwellian implications of our surveillance technologies are awesome, worrisome, intrusive and liberty threatening. Many, including Ronald

Corbett and Gary Marx, have pointed out the dangers of a surveillance society: "Such a society is transparent and porous. Information leakage is rampant. Barriers and boundaries –distance, darkness, time, walls, windows, and even skin –that have been fundamental to our conceptions of privacy, liberty and individuality give way."[9]

In this issue, others articulately illustrate this danger to life, liberty, autonomy and dignity. But in an attempt to balance the scales somewhat, I would like to point out some examples of efficiency and effectiveness that will be precluded if we overreact. For twenty years, I was on the front lines of the battle between the concepts of privacy and the promise of new technologies to enhance government efficiency and citizen convenience.

Building prisons is immensely frustrating for most state governors. Corrections has been one of the fastest growing parts of state budgets for the last 25 years. That is certainly true of Colorado. I personally have investigated and helped adopt the use of modern surveillance devices in corrections and have been the subject of criticism for doing so. I believe we can make use of some modern surveillance technologies without fear that our society will become like that of Orwell's *1984*. We can save the taxpayers' money and, at the same time, offer more humane settings for offenders. However, we must think through the privacy issues.

I believe we can make use of some modern surveillance technologies without fear that our society will become like that of Orwell's *1984*.

The use in corrections for surveillance of non-violent offenders within the community allows them to hold jobs, continue to support their families, and even allows us leave some offenders in the community for their entire sentence. Surveillance technology allows the state to expedite a phased reentry of incarcerated inmates into society. It is more economical and humane than a $25,000-a-year prison cell. A central monitoring system allows the state to monitor offenders day and night, and conduct random checks at anytime of day. Only the offender and authorities need know of the surveillance's existence, and offenders can maintain a job.

Many states have installed video cameras in state patrol cars to the mutual benefit of both state patrol officers and the public. Big Brother? Hardly. Surveillance allows cleaner arrests and gives us a record on those rare occasions something goes awry. Similar video cameras surround the Governor's mansion and also monitor the State Capitol during non-working hours. Cheap, efficient, effective.

Likewise, sobriety check stops on heavy drinking nights prove to be a very powerful tool with minimum intrusion. Clearly, a short stop by the state police and a brief exchange with the driver is a powerful tool against the biggest highway killer, drunk driving. I admit this was a controversial issue, but I supported it and found it a useful tool against drunk drivers during high-risk holidays.

Requiring people entering the State Capitol or City and County Building to go through security gates is unfortunate but necessary, and hardly merits the excess rhetoric that greeted its arrival. Likewise, some schools in high-crime areas have found it necessary to institute scanning devices. While we may feel sad that such measures are necessary, they hardly signal the fall of the Republic.

Electronic tolls on roads, tunnels and bridges add immensely to an efficient transportation system. Surveillance will allow many new innovations, like direct charging by vehicle type, weight, location and time of day. We stand on the threshold of "smart highways" which have great promise in easing traffic delays, but all of these innovations involve privacy issues. I believe the concerns are valid but manageable. Some of these technologies can function without collecting personal or vehicle specific information. There are privacy enhancing technologies which allow us to adopt the technology, yet limit the manner, means, and data collected. We must give great thought to how this information is safeguarded and used, and certainly to whom has access to it. As we have all seen with driver's licenses, it is possible to balance individual privacy with public need.

Obviously, we do have to consider the cumulative impact of all of these minor intrusions and the many others of a similar character. The total effect of these minor intrusions into privacy can clearly be more than the sum of their parts, and it is well worth debating whether we are entering a time of permanent, unceasing surveillance of the citizenry. We must also worry about "function creep," where initially reasonable technologies overreach and become oppressive. But from a public policy standpoint, it is hard to believe that we can run a populous modern state without using technologies that have the potential to threaten privacy. This will be an incredibly important balancing act.

America was not born with privacy as a way of life, but we have grown up with it. Privacy has become indispensable to our personal lives and what we value

continued on page 566

Supermarket Cards:
The Tip of the RETAIL SURVEILLANCE Iceberg

by Katherine Albrecht, Ed. M.
CASPIAN - Consumers Against Supermarket Privacy Invasion and Numbering[1]

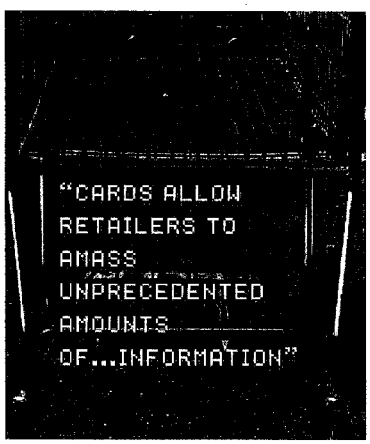
SECTION 1: INTRODUCTION AND BACKGROUND

The good news is, marketers know so much more about you that they can precisely tailor their marketing messages. The bad news is, marketers know so much more about you even when you would prefer your anonymity. One man's relevance is another man's intrusion. Big Brother has truly arrived, with a grin and a fist full of coupons.[2]

- Frequency Marketing in the 21st Century

Love 'em, hate 'em, or merely tolerate them, there is no escaping the fact that supermarket cards have become a fixture of the American retail landscape. Since first appearing in the early 1990's, card-based purchase tracking programs, variously known as loyalty, frequent shopper, reward, or club cards, have spread quickly throughout the grocery industry. In January 2000 it was estimated that 60% of U.S. grocers required a card to obtain discounts,[3] and today eight of the top ten U.S. grocery retailers own at least one supermarket chain with a card program in place or a trial underway.[4]

Promoted as savings devices by the grocery industry, cards allow retailers to amass unprecedented amounts of longitudinal information on consumer purchase and eating habits. Each time a shopper scans a card at the checkout lane, a record of the items purchased, the time, the store location, and the payment method are added to the shopper's profile. Along with millions of other records, this profile is stored in an enormous "data warehouse" (frequently a secure facility run by a marketing company under contract to several different supermarkets) where it can be analyzed in detail or simply stored until a later use is found for it.



A storm on the horizon

...she has resigned herself to those moments of simmering anxiety she sometimes feels when she hands over her card at the grocery store. 'It's like sitting in your beachfront property watching the storm warnings, hoping the hurricane doesn't hit you,' said Arden Schell, 58, of Arlington. 'It's the kind of thing you worry about but you don't know how to put a stop to it.'[5]

- Robert O'Harrow, Jr., Washington Post Reporter, quoting Virginia Shopper Arden Schell

Though the majority of American households have signed up for at least one supermarket card,[6] high rates of program participation do not necessarily mean that consumers are comfortable with the programs. A growing segment of the population has begun to express deep concerns about the privacy implications of using supermarket cards.

Shoppers like Arden Schell are correct in sensing a storm on the horizon. Today, not only can marketers and product manufacturers access a dizzying array of data on supermarket shoppers through the use of cards and related technologies, but soon social agencies, health insurance companies, law enforcement, the

United Nations, criminals, and lawyers may also begin clamoring for their own up-close view of shoppers' personal food shopping habits.

By allowing their grocery purchases to be tracked and recorded, consumers leave themselves vulnerable to threats from these sources. This article sets out to document these risks and provide information to enable shoppers to make informed decisions about whether or not to participate in supermarket card programs.

Why fight supermarket cards?

The food business is far and away the most important business in the world. Everything else is a luxury. Food is what you need to sustain life every day. Food is fuel. You can't run a tractor without fuel and you can't run a human being without it either. Food is the absolute beginning.

- Dwayne O. Andreas, Former Chairman of the Board, Archer Daniels Midland Company

At first glance it may seem odd that a privacy researcher would conduct an in-depth analysis of something as mundane as supermarket cards, especially considering how many other invasive technologies have sprung up in the last decade. But while other privacy-violating technologies may be flashier, few have the pervasive reach of the lowly grocery card. Virtually every American family patronizes a supermarket,[8] and since food is essential for survival, obtaining it is perhaps the least negotiable of consumer activities. Supermarket practices arguably have greater potential to impact society than those of any other retail channel.

The grocery cards in their wallets provide many shoppers with their first glimmer of awareness about retail surveillance. Though the most egregious privacy violations in the commercial sphere occur far from the average consumer's experience and awareness, grocery cards provide tangible evidence of their existence. Tracked back to their source, the cards lead the investigator to a staggering host of complex strategies to watch, record, and control consumers on an enormous scale.

Background of supermarket card programs

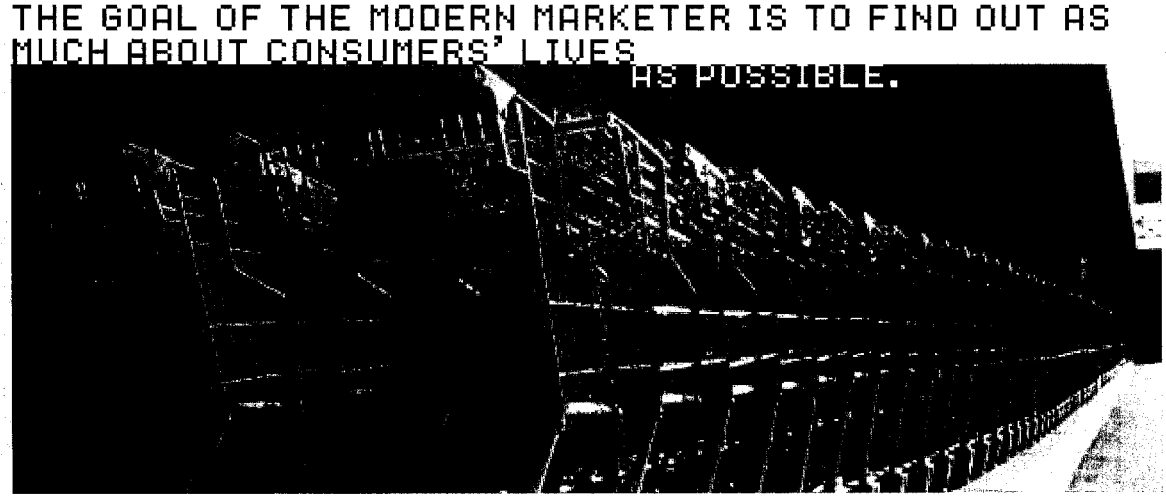
Loyalty schemes are not gestures made by philanthropic superstores.[9]

- Mark Price, Waitrose Supermarket Executive

Understanding how supermarkets have come to embrace the card concept can provide a framework for understanding the privacy implications of cards. The goal of the modern marketer is to find out as much about consumers' lives as possible. In the past, marketers were frustrated by the fact that many consumers do not want to provide information about themselves to strangers. Marketers had to pay for people to provide them with information about their purchases (a fair arrangement based on mutual consent), but since the industry could not to afford to pay all American shoppers to be tracked, for years it limped along with what it could glean from the occasional survey or focus group.

Then the marketers hit on an idea. Rather than use money as the carrot to entice people into surrendering private information about their shopping habits, they could use it as a stick to punish people into surrendering that information. And what's more, if they did it right, consumers might never be the wiser.

Fast forward ten years, and here we are — the supermarket card is a fixture in virtually every shopper's wallet. By withholding access to sale prices, marketers have coerced tens of millions of Americans into surrendering data that they would never have revealed voluntarily. Even though discounts on overstocked and seasonal items have been around for thousands of years, shoppers can now only receive discounted prices if they comply with the supermarket's surveillance agenda by serving as unpaid research subjects. And punishment for refusal (the stick) is harsh: anyone refusing to participate is penalized in the form of higher prices — sometimes to the tune of double or more for a given grocery item.[10]



It's brilliant that the marketers didn't have to give anything up in the process. Ostensibly, the cards are designed to save shoppers money, so participating consumers should see their grocery bills drop significantly as soon as the programs are implemented. However, when prices at Kroger were compared before and after the introduction of a card program in Indiana in 2000,[11] exactly the reverse was found to be true — sale prices on identical items went up after the cards. Nevertheless, given a choice between mediocre discounts with the card, or no discounts at all without it, most consumers capitulate and sign up.

Consider how many shoppers would still choose to be monitored if there were no punishment for refusal, and the motivating factor (the stick) quickly becomes apparent.

The industry talks out of both sides of its mouth

On the surface, customers view the card as a tool to receive discounted prices or other incentives. Marketers, on the other hand, use the cards to learn about their shoppers.[12]

- Ann Raider, Marketing News

Most people, amazingly enough, look at what's going on with that card and don't connect that we have the data. For those of you in this room [MIT media lab] I have no doubt that you know we have access to data on you. But for a lot of consumers, it's a frightening thing.[13]

- Curt Avallone, VP of Marketing and New Technology, Stop & Shop Supermarket

While industry trade publications openly discuss the data collection function of cards, the supermarkets carefully avoid mentioning data collection to customers. Instead cards are promoted through advertising and promotional materials as "savings" devices to "reward" loyal shoppers.

Shoppers are intentionally kept unaware of the privacy implications associated with cards. When first announcing its involvement with the supermarket loyalty card concept a few years back, Catalina Marketing Corporation (CMC) hired a public relations agency, the CGI Group of New York, to "minimize media coverage linking CMC with unethical obtrusive database marketing."[14]

CGI proudly stated on their website that "despite questions from the press regarding privacy issues not one resulting story mentioned the (privacy) issue."[15] The campaign to squelch discussion of privacy within the media, coupled with extensive advertising, served to keep these concerns from many shoppers' awareness in the initial phases of card introduction in this country.

Unfortunately, many shoppers only discover that the card is a data collection device (rather than a savings device) after several months — or even years — of regular use. By that time the store has already collected a large dossier of information on the individual and for many shoppers it feels too late to complain. Though many people then contact the stores asking to have their records expunged (only to be told in most cases that their data is now the property of the store), most consumers simply accept the situation as an unfortunate *fait accompli* since to do otherwise would require admitting to their previous ignorance and explaining a history of "voluntary" card usage.

Consumer acceptance levels are debatable

Because many studies on consumer acceptance levels of supermarket cards have been commissioned or conducted by companies with a financial stake in the outcome, it is difficult to gauge the true acceptance levels for cards among consumers. Independent research is needed to accurately determine how consumers feel about data collection, price considerations, and other factors that play a role in consumer card usage. When asked, grocery executives point to internal surveys as evidence that consumers support their card programs.[16] Indeed, it is probably true that if store representatives ask shoppers, "Would you use a loyalty card if it meant you could save money on your groceries?" many may well answer yes. However, consider the results if a survey were to ask this, more truthful question:

> If your supermarket required you to provide personal information and carry a card to be eligible for sale prices (the same sale prices you already get today), and furthermore, used that card to make a record of all of your purchases in perpetuity with the goal of extracting more money from you, leaving you no way to manage or expunge that record and leaving it vulnerable for use against you in a variety of ways, would you approve?

The majority of shoppers would probably answer with an emphatic and resounding "NO!"

SECTION 2: USE AND ABUSE OF SUPERMARKET DATA

Can supermarkets be trusted with data?

Whenever concerns about data collection are raised, supermarkets point to their privacy policies, particularly their promise not to share card data with third-parties. Despite this promise, many chains routinely sell large amounts of card purchase data to outside marketing and manufacturing companies, justifying this practice on the grounds that they remove "identifying information" before sharing the records. But is shopper card data, minus a name and address, really anonymous?

Data reidentification

A computer process called "reidentification" can allow marketers to re-attach names and addresses to "anonymous" records — even after all so-called "identifying information" has been removed.[17] The process works by combining the "anonymous" data set with outside information to pair up items that are uniquely associated to individuals. For example, using only birth date and full ZIP code it is possible to identify 97% of the Cambridge, Massachusetts population.[18]

The U.S. General Accounting Office recently expressed alarm over the reidentification trend which it says enables

marketers and other "data snoopers" to identify specific individuals on the basis of very limited information.[19] The U.S. Census Bureau is so concerned about reidentification by marketers that it recently took pains to "blur" census records before releasing them.[20]

Unfortunately, the average supermarket IT department is unlikely to invest in complex and expensive "blurring" procedures before selling "anonymous" or "aggregate" shopper card purchase information to data-hungry marketers, meaning that your personal information could easily fall into the marketers' hands. Researchers predict that reidentification risks will increase as the amount of data available on individuals continues to grow.[21]

Internal risks

Unbeknownst to most shoppers, the information contained in their supermarket card records may extend far beyond mere grocery purchases, name, address and phone number. In the early stages of card introduction, many stores required a social security number or driver's license number (or both) to receive discounts — and would not issue a card without them.[22] Today, because many stores' shopper cards double as "check cashing cards," such identifying information is still routinely collected from millions of grocery consumers without raising an eyebrow. Even shoppers who do not want check cashing privileges are often encouraged to provide additional information, such as their date of birth, on card applications.

The problem is that once the store has shoppers' identifying information, it can easily obtain detailed intelligence on other aspects of their lives. A Florida company, AccuData, aggressively markets a product it calls a "penetration profile" to grocers.[23] These profiles are designed to augment the grocery purchase data collected on customers with a wealth of additional information about them from outside databases.[24] AccuData recommends that supermarkets attach the profiles to customer data files so they can better analyze the "geodemographic, psychographic and purchasing characteristics" of their unsuspecting customers.[25]

Data collected in this way not only violates customers' expectation of privacy, but it is also subject to internal security risks. The IT staff of a typical supermarket has access to all information contained in the store's shopper card records. This data is often held on insecure computer systems where even low-ranking employees have access. Here it is subject to both human error and employee corruption.

On the error front, stories abound of sensitive personal data stored on corporate computers being accidentally revealed to the public. One recent case involved Travelocity.com inadvertently posting the names, addresses, phone numbers, and e-mail addresses of 45,000 customers on its website for a period of several weeks before the error was discovered.[26] On the corruption front, it was recently alleged that AOL employees have been providing criminals with subscribers' passwords and account information to make fraudulent purchases.[27] One hacker said, "AOL's biggest security risk is corrupt employees who will straight up give away info for a price."[28]

There are also a number of disquieting cases where Internet companies reneged on their privacy policies during hard times by attempting to sell customer purchase data to the highest bidder (e.g., Toys.com[29] and Voter.com[30]). Companies have also retroactively eased privacy restrictions to allow them to reveal previously collected customer data (e.g., Amazon.com,[31] e-Bay,[32] and Yahoo[33]).

These are only the publicly reported cases. Larry Ponemon, a privacy expert who has conducted hundreds of corporate privacy audits both for PricewaterhouseCoopers and later as an independent privacy consultant,[34] reports that only 19% of financial businesses actually adhere to their privacy policies.[35] The reality is that whenever sensitive data is collected there is always a risk that it can be revealed in error, misused, or abused — and privacy policies offer little protection against these threats.

Personal injury and family law

Shopper cards have already begun cropping up in personal injury and family law cases. A California shopper named Robert Rivera sued Safeway-owned Vons supermarket after slipping on a yogurt spill in the store and fracturing his kneecap.[36] A mediator allegedly told Rivera's attorney, M. Edward Franklin, that Vons planned to introduce Rivera's liquor purchase records at trial to paint him as an alcoholic.[37] In another case, a man's supermarket card records indicating purchases of expensive wine were used against him in a divorce proceeding as evidence that he could afford to pay more alimony than he had claimed.[38]

Other security risks

The keychain versions of supermarket cards pose their own security risk. Anyone finding a shopper's keys has the potential to gain access to the data linked to it. Stop & Shop Supermarket in Boston gave a customer's name, unlisted home phone number, and residential address to a complete stranger who had found the customer's keys using the shopper card number on the key chain card.[39] The potential for danger is obvious if a criminal has the key to a person's front door and knows both his or her address and phone number.

In late 2001, a radio producer in Dallas obtained similar information from Safeway-owned Tom Thumb Supermarket.[40] She called Tom Thumb's toll free customer service line claiming to be a stranger who had found a set of keys in the parking lot (though they were actually her own). The customer service representative used the customer number from the key chain tag to quickly obtain her name and home address, which he then freely gave out to her (a supposed stranger) over the phone.[41]

Tom Thumb later apologized for the incident, explaining that the employee had made an error by sharing the information.[42] However, the company's explanation simply

underscores the point that no retailer can guarantee human error will not lead to disclosure of customers' personal information.

Shopper card records and health

HMO's may soon have shopper card data

Supermarket cards record more than just purchases; they make a record of the actual food people put into their bodies. Because they contain nutritional information for tens of millions of Americans, supermarket databases offer a potential gold mine for anyone who wants to monitor the eating habits of individuals and groups of people.

One U.S. supermarket chain, Royal Ahold-owned Stop & Shop, has already poured $3 million into the development of a very disturbing software program called SmartMouth to tap this potential.[43] SmartMouth can sift through the millions of supermarket card records Stop & Shop has collected on shoppers over the past eight years to create nutritional profiles on each individual cardholder.[44] If a customer has been overindulging in sugar and fat or ignoring a doctor's warning to cut back on sodium, the supermarket — or anyone else with access to the database — can find out with just a few mouse clicks.

While Stop & Shop has temporarily shelved the program, its future plans for SmartMouth are perhaps the most alarming I have yet encountered with regard to shopper cards: Stop & Shop executive Curt Avallone recently made the shocking admission that his company is considering "an HMO alliance" with "three or four health organizations" to make use of the SmartMouth program and Stop & Shop customer records.[45]

The staggering potential to form longitudinal nutritional profiles on their subscribers is not lost on health insurance companies, who could use the information to deny coverage, set rates, or use a person's lifetime eating habits to deny medical procedures such as heart bypass operations and dialysis. HMO subscribers' medical records and their food purchase records could become so intertwined that eating habits could ultimately become part of a patient's standard medical chart.

Stop & Shop is not the only company that has expressed an interest in linking card data to health records. Boots, a major British pharmacy retailer, offers medical and dental insurance plans linked to its "Advantage Card,"[46] which can also serve as a chip-based credit card.[47] Boots even encourages shoppers to donate their organs through a check box at the bottom of the card application, explaining on their website that "joining through Boots provides you with a combined Advantage Card and Organ Donor scheme card in one plus the peace of mind that your donor details are safely stored on the NHS [National Health Service] Organ Donor Register."[48]

Boots hopes to someday link its frequent shopper card with customers' medical records, health insurance, and social security information,[49] and the "smart card" industry here in the U.S. is clamoring for the same thing.[50]

The use of shopper card records to track health problems could be of interest to some members of the legal community, who have begun contemplating class-action suits against snack food companies.[51] Both attorneys and food manufacturers may soon develop a keen interest in who bought what, when, and in what quantities, along with individuals' health records to either instigate or fend off lawsuits.

If shopper card records are allowed to evolve into de facto health records, they will become an obvious target for government agencies wishing to claim their own piece of the information pie. Already, a chip-based "Health Passport card" (which uses a microchip to store and retrieve health information and "redeem nutrition benefits") has been issued to welfare recipients in three U.S. cities.[52] Disturbingly, the card, which is required to purchase groceries under the Women, Infants and Children (WIC) program, links food purchase information with medical assessments, health records, and immunization records, thus allowing WIC officials to closely scrutinize the nutritional makeup of a family's weekly shopping.[53] Observers in Wyoming, one of the program's test locations, say that eventually the Health Passport program could be expanded to include all citizens in the state, not just those receiving public assistance.[54]

Government health organizations want access to shopper card records

Anything recorded is subject to control.
- Katherine Albrecht, CASPIAN[55]

"Public health" has already been used as justification for three British supermarket chains to violate their privacy policies by offering card records to the government. With very little prompting, these chains agreed to release shoppers' purchase records to health officials to track the consumption and health effects of genetically modified (GMO) foods.[56] The study, which was fortunately cancelled, had planned to link store records and health databases seeking links between GMO food purchases and a variety of health problems, apparently without obtaining the permission of the shoppers concerned.[57]

Scottish health officials would like access to shopper card records to facilitate "the monitoring and evaluation of the various initiatives to promote improved [Scottish] diet."[58] Calling such data "invaluable," their report says that they plan to "consult the major supermarkets to explore the feasibility of accessing this data and to examine with them the scope for other uses to which loyalty card data might be put."[59]

Most worrisome of all, the World Health Organization (WHO) recently stated that one of its major objectives is to "*maintain global databases* for monitoring, evaluating, and reporting on the world's major forms of malnutrition, the effectiveness of nutrition programmes, and progress towards achieving targets at national, regional and global levels."[60] The global database would be a component of the WHO's larger plan

to "prevent, reduce and eliminate malnutrition worldwide,"[61] implying that the WHO envisions a more active role for itself in the global food arena than the mere collection and analysis of data. Will the United Nations someday demand shopper card records from around the world to form the basis of the WHO's "global database"?

Regardless of the good intentions of health officials, it is imperative that citizens keep grocery records out of government hands. Allowing governmental bodies to monitor and evaluate citizens' purchase and consumption of food could lead to various forms of control over the food supply — one area of life where politics should play no role.

Shopper card records, profiling, and law enforcement

Federal agencies practice profiling

The same software used by grocery marketers to analyze purchase records and predict future behavior is also being used by accountants at the Department of Defense (DOD) to keep tabs on 40,000 DOD employees.[62] When an employee uses his or her "government purchase card" the transaction is analyzed against the employee's personal information and previous purchase history.[63] Then the purchase is compared with profiles of "data patterns that might indicate improper use."[64]

The problem is that the program doesn't always work. Officials admit it needs "some fine tuning" after observing its unsettling tendency to make false accusations.[65] Over a recent three-month test period, the software caused 345 individuals to be put under investigation for making "suspicious purchases," many of which later turned out to be legitimate.[66] Unfortunately, worries over falsely accusing the innocent have done little to dampen the agency's enthusiasm for the data-mining program; the DOD plans to expand its use in coming years.[67]

The DOD will have plenty of company. The IRS may soon "feed data from every entry on every tax return, personal or corporate, through filters to identify patterns of taxpayer conduct."[68] The agency hopes to compile and store detailed information in taxpayer databases that can be sifted through in search of irregularities.[69] Given the insight into household income that eating habits provide, the IRS might find grocery records a tempting target for inclusion in the database. British revenue authorities have already demanded customer purchase records from supermarkets in the U.K. to investigate whether shoppers' spending habits match the lifestyles indicated by their tax returns.[70]

Of course, no one scans a grocery card with the expectation that their data will wind up in the hands of the IRS. Nevertheless, data given to retailers for one purpose has a disquieting tendency to wind up in someone else's hands. Selective Service once came under fire for using a list of children's addresses and birthdays from Farrell's ice cream parlors to mail out reminders about Selective Service registration.[71] Farrell's had originally collected the information to offer free ice cream cones on kids' birthdays.[72]

Profiling by law enforcement

Law enforcement agencies are already making use of shopper card records. DEA agents obtained the supermarket card records of individuals in Arizona to check for large purchases of plastic bags (presumably for packaging drugs).[73] In theory, shopper card records could be used to trigger this type of investigation whenever *any* purchase fits a "suspicious profile." Soccer moms getting ready for a bake sale could someday find themselves face-to-face with federal authorities asking them to justify their Ziploc purchases.

While the notion of federal authorities rifling through customer databases in search of irregularities may seem unbelievable, former president Bill Clinton has suggested that they do just that. Referring to "suspicious behavior," Clinton was recently quoted as saying, "More than 95% of the people that are in the United States at any given time are in the computers of companies that mail junk mail and you can look for patterns there."[74]

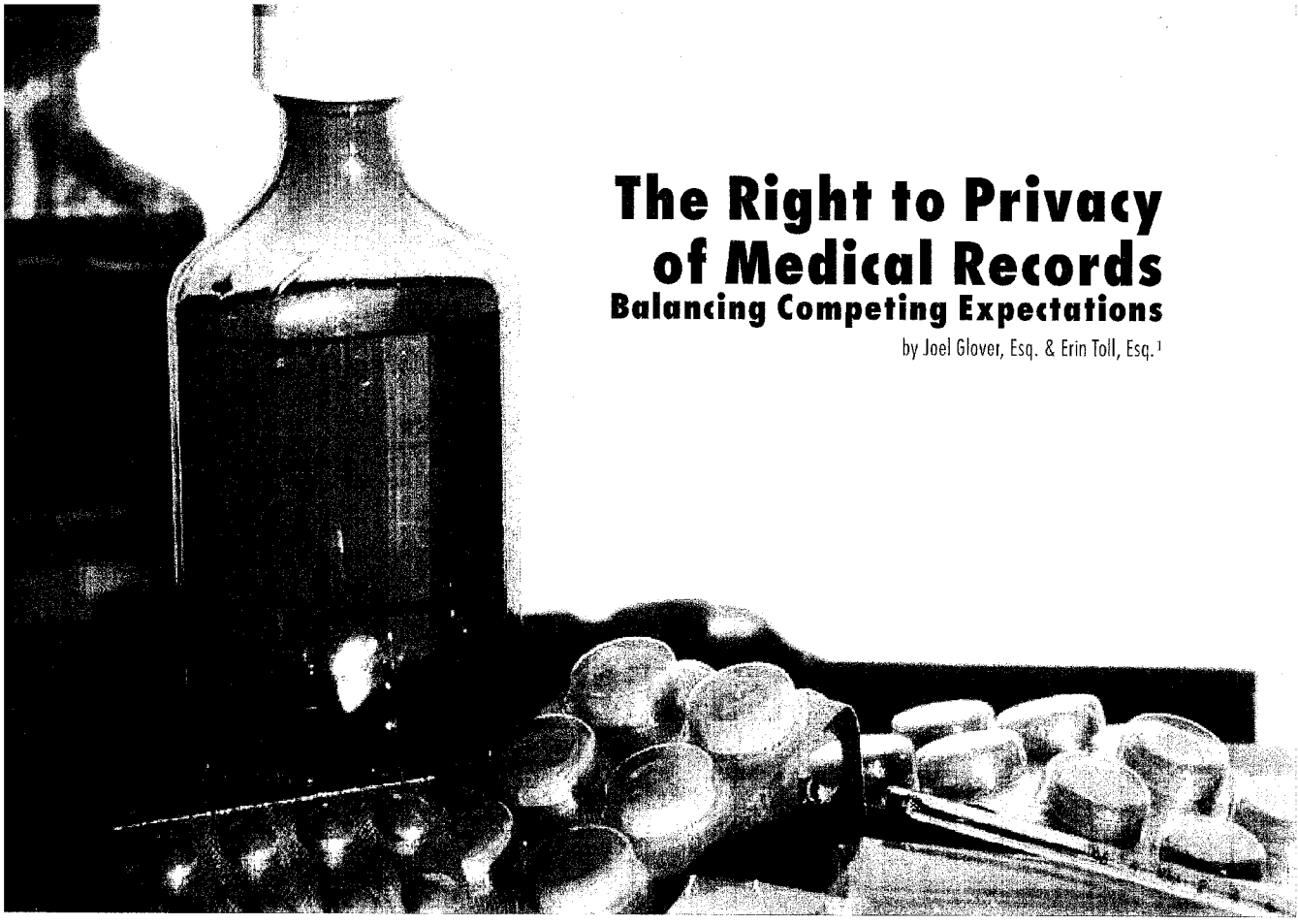
If the Police Federation of England and Wales has its way, it will soon be routine for U.K. law enforcement officials to review grocery records in search of "unusual" or "suspicious" behavior. The Federation has called for the more than 300 separate database records that exist on U.K. citizens — ranging from their supermarket purchase records to their driver's license information — to be merged into one super-database for easy access by law enforcement.[75]

Once the data is thus linked, they have asked for "artificial intelligence systems to watch and listen,"[76] around the clock to every activity recorded in the database. If implemented, powerful software programs would analyze records representing virtually every aspect of individuals' lives in painstaking detail. Of course, these systems will rely on profiling to distinguish between "normal" and "suspicious" behavior.

The specter of ethnic profiling looms especially large when it comes to eating patterns, which can reveal information about a shopper's origin, life experiences, and current economic status.[77] In the wake of the September 11th terrorist attacks, federal agents reviewed the shopper card records of the men involved to create a profile of ethnic tastes and supermarket shopping patterns associated with terrorism.[78] It's hard to see how this information could improve national security, however, considering that the eating habits of Middle Eastern terrorists are probably quite similar to those of Middle Eastern schoolteachers and factory workers.

Unfortunately, supermarkets are making little effort to shield their customers from law enforcement fishing expeditions through their databanks; in fact quite the reverse is true. A national supermarket chain recently approached privacy consultant Larry Ponemon for recommendations on how to advise shoppers that it had violated the privacy policy associated with its

continued on page 558



The Right to Privacy of Medical Records

Balancing Competing Expectations

by Joel Glover, Esq. & Erin Toll, Esq.[1]

Introduction

Today, the right to privacy of medical records is seldom contested. A recent decision by the United States Supreme Court recognized our "reasonable expectation" that medical records are private.[2] Courts permit tort claims for invasion of privacy where medical record information is disclosed. In addition, new federal regulations promulgated under the Health Insurance Portability and Accountability Act ("HIPAA") are being implemented on the presumption that medical records are private and entitled to protection.

This article examines the development of that right to privacy and the related balancing of expectations in the federal courts and the Colorado courts. Even where privacy rights have been recognized, those rights often fail in the balancing test when compared to society's legitimate interest in monitoring health care information. Finally, this article addresses the information that the HIPAA regulations consider to be private and subject to protection.[3]

The law recognizes our two competing expectations regarding medical records' privacy. First, we each expect our medical records to be private and confidential. Second, we understand that privacy will be regularly invaded as a

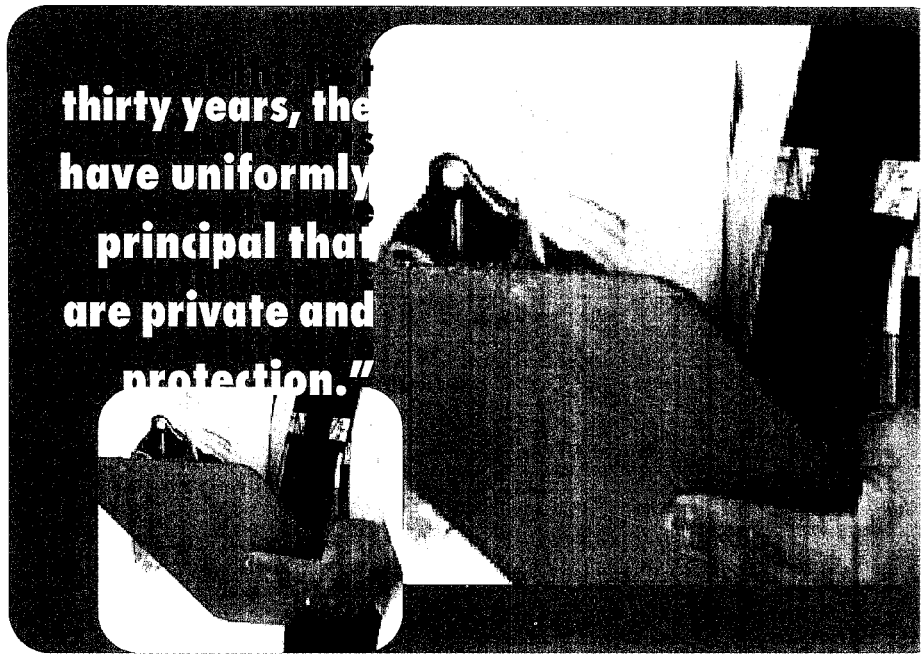
part of the health care system to support national priorities such as the protection of public health, health care research, health care quality monitoring, and the prevention of crime, including health care fraud.

These competing expectations are reflected in the balancing tests established in the federal and state cases and more recently, in the HIPAA regulations. First, medical records are private, consistent with our expectations. Second, our privacy expectation will be invaded as necessary to satisfy society's needs to utilize health care information of the population to promote the public welfare. While HIPAA, at least in part, appears to be based on an attempt to codify case law, even after the HIPAA regulations, a precise understanding of that balancing test can be elusive. As is evident from the case law, it often comes down to a case-by-case approach with the balance typically favoring a limited invasion of our privacy expectations when societal interests outweigh our privacy needs.

I. Development of the right to privacy in medical records.

A. The Whalen[4] *decision - an arguable right to privacy.*

Over the last thirty years, the federal courts have uniformly accepted the principal that medical records are private and entitled to protection. The existence of a right to privacy in medical records can be traced to the United States Supreme Court's decision in *Whalen v. Roe*.[5] In some ways, the *Whalen* decision is an unusual authority to serve as the basis for such an important privacy right. In answering the question before it, the Court ruled that there was no constitutional violation and expressly did not decide whether there was a right to privacy in medical records.[6] Nevertheless, it is repeatedly cited as precedent for that right.



The *Whalen* Court was presented with the question "whether the State of New York may record, in a centralized computer file, the names and addresses of all persons who have obtained, pursuant to a doctor's prescription, certain drugs for which there is both a lawful and an unlawful market."[7] The Court, in an opinion drafted by Justice Stevens, answered the question affirmatively and held that, "neither the immediate nor the threatened impact of the patient-identification requirements in the New York State Controlled Substances Act of 1972 on either the reputation or the independence of patients for whom Schedule II drugs are medically indicated is sufficient to constitute an invasion of any right or liberty protected by the Fourteenth Amendment."[8] However, in rejecting a constitutional violation, the Court created the framework by which future courts would develop the right to privacy in medical records.

In deciding that there was no privacy violation, the Court discussed two different types of individual privacy interests: (1) the interest in avoiding disclosure of personal matters; and (2) the interest in independence in making certain important kinds of decisions.[9] The program did not pose a sufficiently grievous threat to either interest.[10] The Court concluded that any privacy invasions would not be meaningfully distinguishable "from a host of other unpleasant invasions of privacy that are associated with many facets of health care."[11]

> Nevertheless, disclosures of private medical information to doctors, to hospital personnel, to insurance companies, and to public health agencies are often an essential part of modern medical practice even when the disclosure may reflect unfavorably on the character of the patient. Requiring such disclosures to representatives of the State having responsibility for the health of the community, does not automatically amount to an impermissible invasion of privacy.[12]

In essence, the Court balanced the two individual interests against the societal need to protect the public's health and to deter criminal activity. Although *Whalen*

held that the mandatory disclosure of prescriptions and patient identities was not a violation of privacy, the Court also explained that "[t]he right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures."[13] The Court then concluded that "in some circumstances that duty arguably has its roots in the Constitution."[14] Although clearly identified as an issue "not decided" by the Court, subsequent cases nevertheless relied on *Whalen*'s reasoning to develop what has become a generally accepted right to privacy in medical records.

Shortly after *Whalen*, two district courts implicitly adopted Justice Stevens' analysis that the right to privacy in medical records arguably has its roots in the Constitution, although in both cases the right to privacy did not prohibit disclosure. In one of the first district court decisions to rely on *Whalen*, an employer, du Pont, raised the right to privacy argument as a defense to a subpoena seeking employee health information.[15] The employer argued that the medical records of its employees were protected by a constitutional right of privacy and thus could not be disclosed.[16] Relying on *Whalen*, the district court implicitly accepted that a right to privacy in medical records existed.[17] Accordingly, the issue was "not whether a right of privacy exists respecting the information sought, but rather whether the record indicates that such right will be abridged."[18] Although the court upheld the subpoenas over the right to privacy claim, the court echoed Justice Stevens' concern in *Whalen* that unwarranted disclosure of the medical records could violate the Constitution.[19]

Just a year later, in *McKenna v. Fargo*,[20] a district court considered a program in which Jersey City required applicants for its fire department to undergo psychological testing. Even in the absence of public disclosure of the results, the district court determined that the "character and amount of information given to the Government alone is itself an intrusion on the privacy interest in nondisclosure of personal information to government employees recognized in *Whalen*."[21] As a result, the court required Jersey City to "justify the burden imposed on the constitutional right of privacy by the required psychological evaluations."[22] After confirming a right to privacy, the court determined that there was "sufficient support to conclude that the psychological evaluation and hiring procedure taken as a whole [was] useful and effective in identifying applicants whose emotional make-up makes them high risk candidates for the job of fire fighting."[23] As in *Whalen*, the court balanced the individual's privacy interests against society's interest in having a psychologically sound fire department.

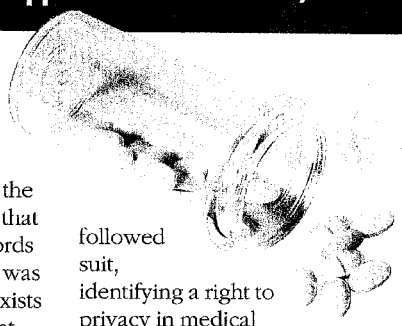
B. The Third Circuit accepts the right to privacy in medical records.

A federal appellate court soon followed suit, identifying a right to privacy in medical records though typically finding in favor of the invasion of that right. In one of the first decisions by a circuit court of appeals upholding a right to privacy in medical records, the Third Circuit Court of Appeals relied on the *Whalen* decision to conclude that there is a protected privacy right "not to have an individual's private affairs made public by the government."[24] The Third Circuit concluded that medical records fall within one of the zones of privacy entitled to protection:

> There can be no question that an employee's medical records, which may contain intimate facts of a personal nature, are well within the ambit of materials entitled to privacy protection. Information about one's body and state of health is a matter which the individual is ordinarily entitled to retain within the "private enclave where he may lead a private life."[25]

As is evident from the quotation, *Westinghouse* was one of the first cases to accept explicitly Justice Stevens' "argument" that medical records may be subject to constitutional protection. While the court noted "there can be no question" of this right, there was also no previous judicial authority that could be cited for that proposition.[26] In the absence of judicial decisions for authority, the Third Circuit relied on a law review article and protections for medical records in the Federal Rules of Civil Procedure and the Freedom of Information Act.[27] Seven years later, relying on its own *Westinghouse* decision, the Third Circuit again recognized the right to privacy in medical records.[28] In 1995, the Third Circuit relied on the *Westinghouse* decision to conclude that records of prescription medications are private.[29] "An individual using prescription drugs has a right to expect that such information will customarily remain private."[30]

the Sixth Circuit Court of Appeals concluded that, "



C. A division among the circuits on the right to privacy in medical records.

Although the Third Circuit adopted Justice Stevens' argument, the Sixth Circuit did not follow suit. Without citation to *Westinghouse* or *Whalen*, the Sixth Circuit Court of Appeals concluded that, "[d]isclosure of plaintiff's medical records does not rise to the level of a breach of a right recognized as 'fundamental' under

the Constitution."[31]

This difference of opinion among the circuits was brought to the United States Supreme Court's attention by a decision of the Fourth Circuit Court of Appeals. In *Ferguson v. City of Charleston,*[32] the Fourth Circuit expressly noted the division among the circuits, as follows:

> Although the Supreme Court addressed a claim to a right of privacy in medical records in *Whalen*, it declined to decide whether such information merits constitutional privacy protection. See *Whalen*, 429 U.S. at 605-06. And, the circuit courts of appeals are divided on this issue.[33]

Although the United States Supreme Court reversed and remanded the Fourth Circuit's decision in *Ferguson*, the Court did not address the division of authority noted among the circuits. Instead, it acknowledged an "expectation of privacy" in medical records, as follows, "[t]he reasonable expectation of privacy enjoyed by the typical patient undergoing diagnostic tests in a hospital is that the results of those tests will not be shared with nonmedical personnel without her consent."[34] The Court did not indicate whether this expectation of privacy was protected by the Constitution, as had been "argued" by Stevens in *Whalen.*

D. No right to privacy in making medical decisions.

The *Westinghouse* line of authority and the *Ferguson* decision focus on the first type of privacy identified in *Whalen,* that is avoiding disclosure of personal matters.[35] The second type of privacy identified in *Whalen* is independence in making certain important kinds of decisions.[36] It has not received much, if any, support from the courts. For example, in *New York State Ophthalmological Society v. Bowen,*[37] the court determined that there was no right to privacy in medical determinations.[38] The plaintiffs were seeking to challenge a federal statute limiting Medicare payments for certain cataract services.[39] Plaintiffs maintained "that the right to privacy protects patients' interest in procuring the treatment of choice" and insisted that "all medical treatment decisions are protected from state interference because they are inherently private and peculiarly 'personal.'"[40] The court concluded that "[t]here is no basis under current privacy case law for extending such stringent protection to every decision bearing, however indirectly, on a person's health and physical well-being."[41]

II. Application of a balancing test to privacy rights in medical records.

Even in the cases where medical records were considered within a zone of privacy, that privacy was nearly always invaded after application of a balancing test to determine whether the "societal interest in disclosure outweighs the privacy interest on the specific facts of the case."[42] According to the Third Circuit, the factors to be considered in deciding whether an intrusion into an individual's privacy is justified are:

> [T]he type of record requested, the information it does or might contain, the potential for harm in any subsequent nonconsensual disclosure, the injury from disclosure to the relationship in which the record was generated, the adequacy of safeguards to prevent unauthorized disclosure, the degree of need for access, and whether there is an express statutory mandate, articulated public policy, or other recognizable public interest militating toward access.[43]

In *Westinghouse,* the court balanced the factors and concluded that complete employee medical records needed to be turned over to the government in response to a subpoena issued under the Occupational Safety and Health Act.[44] The court found that "the interest in occupational safety and health to the employees in the particular plant, employees in other plants, future employees and the public at large is substantial."[45] The court also relied on the security measures that would be taken to protect against the disclosure of the information.[46] Recognizing that there may still be privacy concerns, the Court permitted employees the opportunity to raise a personal claim of privacy.[47]

The Third Circuit has repeatedly utilized these *Westinghouse* factors to conclude that the balance favors invasion of the privacy right in medical records. For example, in *In re: Search Warrant,*[48] the Third Circuit concluded the balance favored disclosure of medical records where the patients were already known through insurance submissions and separate mechanisms existed to guard against disclosure and to maintain the confidentiality of the records.[49] As well, in *Fraternal Order of Police v. Philadelphia,*[50] the Third Circuit again concluded that the balance favored the government's need for the medical records.[51]

> Because the medical information requested is directly related to the interest of the police department in selecting officers who are physically and mentally capable of working in dangerous and highly stressful positions, sometimes over long periods of time, and because police officers have little reasonable expectations that such medical information will not be requested, we hold that questions 18 [physical

does not rise to the level of a breach of a right recognized as "fundamental" under the Constitution."

> defects], 19 [prescription drugs] and 20 [mental or psychiatric condition] do not unconstitutionally impinge upon the applicants' privacy interests.[52]

Finally, in *SEPTA*, the court concluded that the right to privacy in medical records was not absolute.[53] In that case, an employer learned that one employee suffered from an HIV-related illness when the employer reviewed medical records that gave each employee's name and listed the prescription drugs each employee purchased through a prescription drug program.[54] In its review, the court concluded that audits of drug information, in the aggregate, are essential to the public interest.[55] The review of the identity of the employee and his medication was not a violation of the employee's privacy largely because it was unintentional.[56] The employer did not ask for the employee's identity from the drug company.[57]

In concluding that the balance favors disclosure, other courts have relied on the purpose of the disclosure in order to override the privacy rights. For example, in 1985, the District Court for New Jersey concluded that the privacy interests in medical records were not absolute and needed to be balanced against the legitimate interests of the state in securing such information.[58] In *Shoemaker,* jockeys were required to disclose illnesses or conditions for which a particular drug had been prescribed or used.[59] However access to the information was limited.[60] In concluding that the balance favored the interests of the state, the court focused on the purpose, noting that "[s]uch information is gathered with 'rehabilitative' and not 'penal' purposes in mind."[61] Another example is *Patients of Dr. Barbara Solomon v. Board of Physician Quality Assurance.*[62] There, the court acknowledged a privacy interest in medical records but found in favor of the government's interest in reviewing that information.[63] In that case, patients were attempting to keep a regulatory body from reviewing the medical records maintained by their doctor.[64] The court focused on the purpose of the information and the safeguards, as follows:

> Given the Board's mission of identifying physicians who engage in immoral or unprofessional conduct, and the Board's goal of preventing future misconduct, courts in this Circuit would most likely find that the Board's activity furthers a compelling state interest. Moreover, because Maryland's statutory restrictions against disclosure of medical records are adequate to protect the Patients from widespread disclosure, courts in this Circuit would most likely find no constitutional violation.[65]

In *In Re: Subpoena Duces Tecum,*[66] the court considered challenges to four subpoenas issued arising from an investigation into federal health care offenses.[67] The doctor argued that his patients' privacy interests in their medical files outweigh the government's interest in those files.[68] The court rejected the argument because the government has a compelling interest in identifying illegal activity and in deterring future misconduct.[69] That interest outweighs the privacy rights of those whose records were turned over to the government, particularly in light of the protections associated with the subpoena.[70] The subpoena prohibited use of disclosed information except as directly related to receipt of health care, payment for health care, a fraudulent claim related to health care or as authorized by a court.[71]

III. The right to privacy in medical records in Colorado.

Various states, including Colorado, have adopted an approach to privacy based on the federal courts' approach. More than twenty years ago, in a case not specifically related to medical records, the Colorado Supreme Court adopted the *Whalen* privacy analysis, and performed a balancing test to invalidate a state agency's regulation.[72] Several life insurance agents brought suit to enjoin the Colorado Division of Insurance's enforcement of a regulation requiring them to notify a life insurer whose insurance was being replaced of the proposed replacement, even when the insured specifically requested that the transaction remain confidential.[73]

Acknowledging that the United States Constitution does not explicitly mention any right to privacy, the Colorado court, citing several United States Supreme Court cases, found that the right to privacy is implicit in various Constitutional amendments, including the First, Fourth, Fifth, Ninth, and Fourteenth Amendments and the Bill of Rights.[74] The Colorado court adopted the *Whalen* definition of two types of privacy interests: "1) the individual interest in avoiding disclosure of personal matters; and 2) the individual interest in making certain kinds of important decisions."[75] The court found that the insurance regulation clearly invaded the insured's interest in avoiding disclosure of personal matters.[76] The Colorado court enjoined enforcement of the regulation but noted that "a burdensome regulation may be validated by a sufficiently compelling state interest."[77] "A generalized concern for protecting the public from unscrupulous practices or misrepresentations by replacing insurers is outweighed by the insured's request for nondisclosure."[78]

Seven years later, without discussion of the constitutional aspects of the right, the Colorado Supreme Court implicitly recognized a right to privacy regarding medical information.[79] Respondents were recipients of donated blood infected with the AIDS virus.[80] They sought disclosure of the identities of each of the donors whose blood was used and production of all of the donors' records in order to pursue their claims.[81] The blood center asserted that compelling public policy grounds, including the maintenance of the supply of volunteer blood and the privacy interests of volunteer blood donors, prohibited disclosure of the donors' identities.[82]

The court performed a balancing test and determined that the blood donors had a "privacy interest in remaining anonymous and avoiding the embarrassment and potential humiliation of being identified as AIDS carriers."[83] The blood center, and society as a whole, had "an interest in maintaining the availability of an abundant supply of volunteer blood."[84] The petitioners had an interest in pursuing their claims.[85] Therefore, the court tailored a limited discovery procedure designed to provide the respondents with the information without risking the consequences of public disclosure of the donors' identities or infringing upon society's interests in a safe, adequate, voluntary blood supply.[86] While no constitutional authority was cited, the *Belle Bonfils* case indicated that Colorado courts would recognize a right to privacy concerning medical information, but that this right must be balanced by the societal interest in disclosing the information.

Although the Colorado courts have not explicitly applied the *Whalen* analysis to medical information, when considering privacy interests, the courts recognize a right to privacy regarding medical information, and balance the individual's privacy interests with society's interest in obtaining the information.[87] As with the federal cases, the emphasis in Colorado has been on the first interest expressed in *Whalen*, that of avoiding disclosure of personal matters, as opposed to the second interest of independence in making certain kinds of decisions.

IV. Privacy rights in medical records give rise to a tort claim for invasion of privacy.

The *Whalen* and *Westinghouse* decisions address medical records' right of privacy in the context of government actions. However, courts have also recognized that the private sector may be liable for claims for violating privacy with respect to medical records.[88] Even in cases where there was no liability, a court would not rule out the possibility that instances may exist where the collection of highly personal information irrelevant to any legitimate business purpose might constitute an invasion of privacy by unreasonable intrusion.[89]

The state law claim of invasion of privacy generally requires the plaintiff to establish: "1) an intrusion upon her seclusion or solitude or in her private affairs; 2) a public disclosure of embarrassing private facts; 3) publicity which places her in a false light in the public eye; or 4) an appropriation, for the defendant's advantage, of the plaintiff's name or likeness."[90] While medical records often trigger privacy interests, the communications may be considered privileged where the following elements are satisfied: "1) good faith; 2) an interest to be upheld; 3) a statement limited in its scope to this purpose; 4) a proper occasion; and 5) publication in a proper manner and to proper parties only."[91]

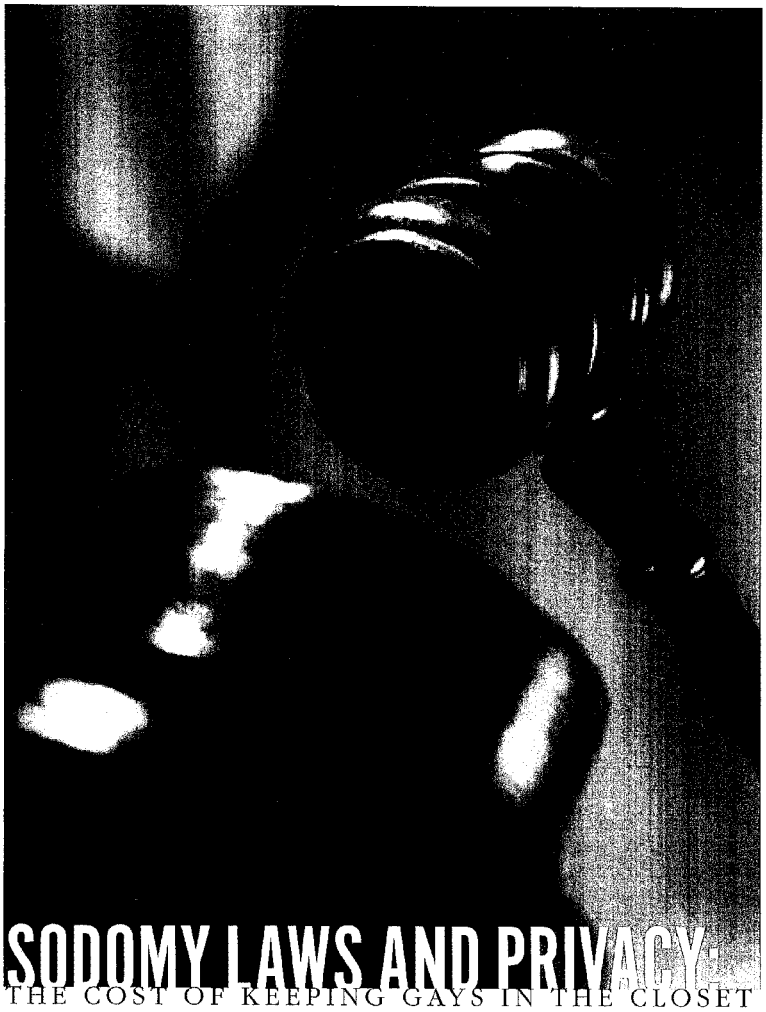
In *Ross*, an employee had complaints about working under fluorescent lights.[92] The employer required her to see the agency's doctor, a psychologist.[93] The employee authorized the doctor to forward a copy of the psychological evaluation to one individual, who then distributed the report to three others at the office.[94] Because there was a reasonable belief that the other individuals needed to review the report, the court ruled that the employer was not liable, even though the situation could "have been handled in a more sensitive way."[95]

Other cases have resulted in the employer's liability for invasion of privacy. For example, in *Levias*, the medical examiner for an employer (United Airlines) received a report from a flight attendant containing details of contemplated gynecological surgery.[96] The medical examiner disclosed most of that information to the flight attendant's male flight supervisor, who had no compelling reason to know it, and to the employee's husband.[97] The flight supervisor repeatedly contacted her to discuss the details of her medical condition and its effect on her employment.[98] The flight attendant had not authorized the medical examiner to disclose any of that information, and she considered it highly personal.[99] The court upheld a damages claim (for compensatory damages but not punitive damages) for the flight attendant, concluding that it was "doubtful that either the flight attendant's supervisors or her husband had a real need to know the disclosed data."[100]

As another example, in Colorado, in a case of first impression, the Colorado Supreme Court recognized a tort claim for invasion of privacy "in the nature of unreasonable publicity given to one's private life," in the context of medical information.[101] The court determined that disclosure of "disgraceful illnesses" are considered private in nature and disclosure of such facts constitutes an invasion of the individual's right of privacy.[102]

Though admittedly based on a different test, the court's recognition of a tort claim for invasion of privacy based on medical records generally appears to track the approach set forth in *Whalen* and *Westinghouse*.

continued on page 553



SODOMY LAWS AND PRIVACY:

THE COST OF KEEPING GAYS IN THE CLOSET

by Michael E. Brewer

Millions of Americans remember certain events of July 1969 as milestones in the national consciousness. On July 20 of that year, Neil Armstrong walked on the moon. One week later, on the streets of Greenwich Village, a typical police raid of a gay bar called the Stonewall Inn sparked an atypical response among the crowd of people who normally would have dispersed quietly after the police arrived.

For three days, crowds rioted through the streets of the Village, spawning a movement which has affected the daily lives of millions of gay, lesbian, bisexual, and transgender Americans. Whether the movement is labeled "Gay Liberation," "Gay Rights," or "Queer Activism," the momentum unleashed that hot July weekend has transformed the landscape of American society, politics, sciences, academia, and theology, and challenged the historical relationship of gay people to the law - especially sodomy laws.

No other group of people has had their private, consensual sexual behavior attacked and scrutinized as much as the gay, lesbian, bisexual and transgender population. For this population, privacy concerns are of utmost importance, because what happens in the bedrooms of this group of citizens has been held up for public scrutiny and condemnation. This scrutiny of private behavior happens legally through the use of sodomy laws. Thus, for this community to be afforded the privacy rights that the rest of the American population enjoys in their bedrooms, sodomy laws must be first understood, and then finally abolished.

In the years since the events at the Stonewall Inn, public support for sodomy laws has waned as people become less tolerant in general of state regulation of adult, consensual sexual behavior. Specifically, social attitudes have moved toward the position that sexual activity between competent, mutually consenting adults should not be the subject of state interference. The bedrooms of gays and straights have become a private realm.

In the evolutionary lineage of laws touching the rights and behaviors of gays, sodomy laws form the starting point. The first American lawmakers imported them into the colonial codes,[1] adopting the prohibition against sodomy rooted in the British common law.[2] Sodomy laws were not invented to regulate

homosexual sex, though people associate sodomy with homosexual sex and homosexuals with sodomites. There are two reasons for this disjunction between origins and common perception. The first is historical. Not until the nineteenth century did homosexuality come to be seen as a condition or identity of a person.[3] The law did not categorize people as homosexual and did not apply laws to gays as a class. However, as society came to recognize gays as an identifiable group, sodomitical acts became more and more identified with homosexuals. The second reason is analytical. Though not applying by definition to acts of a class of people, laws prohibiting sodomy do apply to classes of acts.[4] Therefore, sodomy laws do not analytically relate to any one group.[5]

The legal definition of sodomy often confused courts well into the twentieth century. By 1940, courts applied sodomy statutes "to nearly all sexual activities other than procreative activities between husbands and wives."[6] From the beginning of the nineteenth century to that time, however, confusion about the definition of sodomy caused courts to struggle with how and when to apply sodomy laws.

At common law, copulation by a man with an animal or another male, adult or child, was clearly a sodomitical act. Under common law, however, some jurisdictions required prosecutors to prove that emission of semen had taken place.[7] Appellate courts sometimes reversed trial court decisions for lack of evidence of either seminal emission or penile penetration.[8] Prosecutors responded by urging courts to expand the definition of sodomy. They were not always successful. In some jurisdictions, courts overturned convictions on appeal after finding that fellatio was not an offense at common law or that statutes adopting the common law did not encompass the act of fellatio.[9] They sometimes appealed to legislatures to define the offense more clearly.[10]

Confusion about the nature of the crime was sometimes compounded by Victorian modesty about things sexual. Appellate courts reluctantly dismissed or remanded some cases in which the criminal information failed to set forth facts describing in sufficient detail the circumstances of the crime[11] (in other cases, though, appeals court opinions contain graphic descriptions of the offense).[12] For the sake of propriety, some courts did not require a full description of the act charged in the bill of information.[13]

Some legislatures and courts expanded the scope of sodomy beyond its traditional common law definition. For instance, some courts ruled that anal intercourse by a man with a woman fell within the category of sodomy.[14] In some jurisdictions, a man or a woman who received in the act of fellatio could be found guilty of sodomy.[15] Attempted sodomy came to be a recognizable offense.[16] Late into the twentieth century, courts and theorists found that sodomy between two women was a legal impossibility.[17] As the definition of sodomy became broader over time, the law extended to acts by a male with another male, a female, or an animal. The common, requisite element for a conviction for sodomy, through the first half of this century, was genital sexual activity by a male. Without male sexual misbehavior, no act of sodomy could be performed. Sodomy laws, therefore, have been directed primarily at regulating male sexual behavior. They generally regulate female sexual behavior only insofar as it relates to male behavior. Because sodomy has been associated in the public mind with homosexuality, and because sodomy laws relate primarily to male sexual behavior, criminal sodomy is associated primarily with male homosexuality.

Despite this popular association, however, the historical application of sodomy laws to consensual gay male sex appears to be far less than to other situations regulated by sodomy laws. A survey of 148 appeals court decisions in sodomy cases from 1883 through 1944 reveals few cases involving consensual, adult male-to-male sexual activity.[18] Sodomy involving animals accounts for 9.5% (14) of the cases. The same percentage involves "girls," presumably females under the age of 18. Cases involving adult females account for 8.8% (13). In 20% (30) of the cases, the sex and age of the other party is not identified in the court's opinion. Sex with males age 18 and under occurred in 30% (43) of the cases. Of those, six cases (4% of the total) involve boys age seven or younger. (The youngest identified was three years of age). Sodomy with adult men accounts for 22% (33) of the total number of cases.

The fact that so many of the cases involve non-consensual sex acts is a function of the nature of the acts themselves. Unless a third party witnesses an act of sodomy and reports it, the crime will unlikely be discovered unless one of the actors reports it to authorities or tells another about it. Unlike rape or child sexual abuse, where there is always a perpetrator and a victim, in sodomy cases it is not always correct to refer to the actors as perpetrator and victim. They may be consenting adults. In a minority of the historical cases surveyed, third parties (sometime law enforcement officers) who happened to be at the right place at the right time observed the acts. In almost all cases involving animals, the actor was seen by neighbors performing the act which the

elimination of the nation's way to legally invade the privacy of the bedrooms...

neighbors either reported to authorities or about which they circulated stories which led authorities to an arrest. In a few cases, especially involving female prostitutes, charges were brought after the women testified regarding the nature of the sex acts they had had with a customer. However, in most of the cases surveyed, a male perpetrated an unwanted sexual act on a victim.

These cases illustrate the fact that sodomy laws are rarely enforced in cases of consensual, adult same-sex male sexual activity. They also illustrate, by comparison to appellate decisions of recent years, the contemporary strategy of attacking the validity of sodomy laws on the ground that they violate constitutionally protected rights to privacy. These privacy-based attacks have achieved mixed success. In 1986, the United States Supreme Court found that the Constitution contains no privacy right protecting same-sex sexual activity because such activity has no connection to family, marriage or procreation.[19] Since the Court handed down that decision, several state courts have found that their states' constitutions offer greater privacy protections than does the federal Constitution and declared their states' sodomy laws unconstitutional.[20] Not all states' constitutions are so generous, and not all state privacy-rights cases have succeeded.[21]

One wonders, though, whether the attack is worth the effort. After all, prosecution for sodomy is not regularly used against homosexuals, and sodomy is not analytically identifiable only with homosexuality. So why does the popular mind associate sodomy laws so closely with homosexuality, and why do gays adamantly support attempts to repeal the sodomy laws still on the books?[22]

The answer to these questions rests, at least in part, on the role the very existence of sodomy laws plays in the shaping of gay identity and defining the place of gay people in American society. Janet Halley argues that sodomy laws serve to subordinate gay identity and superordinate heterosexual identity.[23] The laws, she contends, lead to an identification of homosexuality with sodomy and confirms the subordination of gay people.[24] Others suggest that unenforced sodomy laws "create a criminal class," brand "gay men and lesbians as criminals," create a "social hierarchy" that inflicts emotional harm on gay people, and legitimize anti-gay violence.[25]

Richard Posner observes that the main contemporary significance of laws against homosexual sodomy is to make a statement of opposition to homosexuality.[26] He subscribes to the proposition that sodomy laws in fact apply only to homosexual sodomy, and that they would be unconstitutional if applied to heterosexual sodomy.[27] Posner devotes a chapter in his book *"SEX AND REASON"* to the analysis of social policy toward gay people from the point of view of law and economics theory. He places sodomy laws in context with other laws which establish anti-gay policy, such as those forbidding same-sex marriage and limiting career opportunities for gays in the military, government service, and education.[28] From the point of view of law and economics theory, Posner criticizes laws, including sodomy laws, which subordinate gays in society.[29] He questions why society has an interest in subordinating gays.[30] He subjects anti-gay policy to an economic cost-benefit analysis.[31]

Law and economics theory assumes that a person acts rationally to choose economically beneficial modes of action: that people make choices to act in their best interest, and that self-interest is identifiable with economic benefit. "[R]ational man goes where the balance of costs and benefits inclines."[32] Laws promote or hinder the aggregate benefit to society by encouraging or discouraging people from making certain choices rather than others. If a person has no ability to make a rational choice, then that person has no ability to choose an economically efficient form of action, and law, therefore, is ineffective to influence that person's action. The issue of choice in being gay is central, therefore, to a law and economics analysis of the efficiency of laws subordinating gay people.

The question of whether people choose to be homosexual has formed the core of debate over the morality of homosexuality. If being gay is a pure moral choice and society places a value on restraining that choice, then sodomy laws may be analyzed in terms of their efficiency as a counter-incentive to make the choice to be gay. Religious and social conservatives, for example, tend to view homosexuality as a choice, lifestyle, or preference. Their premise is that homosexuality is a social evil, that it is a choice, and therefore, that it can be effectively discouraged through legal disincentives.

Being gay, however, is not a choice. Rather, it is a pre-moral condition (such as conservatives generally believe heterosexuality to be). Legitimate scientific research recognizes that people do not choose their sexuality and science has discarded theories that homosexuality is a disease that can be treated or cured.[33] Therefore, using law as a disincentive for being homosexual makes no practical sense. The best the law can do is to discourage homosexual activity, not homosexuality per se. The fact that being gay is not a choice begs the question: what social value (or disvalue) is there to limiting homosexual activity? What are the costs, and what are the benefits?

Posner identifies two results of limiting same-sex sexual activity that some perceive as beneficial.[34] The first is prevention of the spread of AIDS; the second is limiting the exposure of young people to the blandishments of homosexuality which would lure them into a homosexual lifestyle.[35] Posner dismisses them both as perceived and not real benefits, the first being ineffectual (perhaps even if sodomy laws were enforced), the second being based on a false belief that young people convert to homosexuality.[36]

If the benefits of limiting same-sex sexual activities are illusory, why bother to regulate gay sex? Posner

points to a deep-seated anti-gay sentiment in Anglo-American culture, which he associates with the rise of companionate marriage.[37] Posner theorizes that in societies where marriage was not historically companionate, that is, where the function of marriage was primarily political or procreational, as in ancient Greece and Rome, homosexual activity was tolerated or even encouraged. He believes that the origin of American society's traditional abhorrence of same-sex sexual activity relates to the restraint that societies which value companionate marriages place on the sexual activities of males.[38] Such societies place a high value on monogamous sexual activity, and a high disvalue on "any form of nonmarital sexual activity."[39] Posner's theory does not account, however, for the fact that American society does not react as negatively to pre-marital and extra-marital heterosexual activity as it does to gay sex, a fact which suggests that the origins of the "disgust" which drives the traditional American antipathy toward homosexuality lies elsewhere.[40]

Whatever the origin of anti-gay animus may be, Posner recognizes that this animus is simply irrational. He characterizes it as being the "biggest externality: the revulsion that so many people in our society feel at the very idea of . . .sexual deviance . . . . The disgust that homosexual intercourse arouses . . . explains the survival of sodomy laws better than the external effects of such intercourse do."[41]

What are the costs to society, and to gay people, of society's attempts to limit gay sexual activity? Here, Halley's connection of sodomy laws with subordination of gay people is helpful. Although sodomy laws are rarely used to prosecute sexually active gay people, they contribute to and form a locus for the subordination of gay people. Posner points out that gay people incur costs when society punishes people for sexual orientation, or *threatens* to punish.[42] Attitudes supported by the very existence of sodomy laws lead to the subordination of gay people, in turn leading to two high-cost results: a clandestine search for partners, and, when the cost of that search is too high, marriage to members of the opposite sex.[43] Both these situations result from a fear of expression of "gayness" in a society in which gay people are subordinated to heterosexual people.

Subordination also results in the cost of mental distress from the alienation which subordination engenders in gay people and their families and friends, including high rates of suicide among gay youth.[44] In addition, the emotional and economic costs rise from fighting political battles to overcome subordination. Some of those battles take place in arenas traditionally recognized as being "political," while some occur in arenas such as churches and workplaces which are also political, but not usually denominated as such.

These costs to gay people may actually be viewed as benefits by an anti-gay society which seeks to keep gay identity and behavior clandestine, and impel gay people into traditional heterosexual marriage. As Posner points out, the higher the cost of gay activity (sexual or otherwise), the less activity there will be.[45] But the cost to society of achieving those perceived benefits is high: clandestine behavior results in social disruption, unhappy marriages result in family dysfunction and divorce, emotional distress leads to economic inefficiency, and legal battles destabilize private and public equilibria.

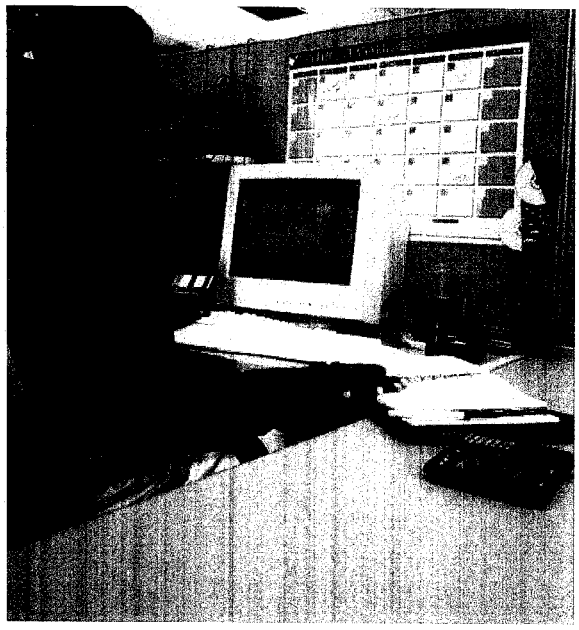
Society has begun to discover that subordination of gay people may be too costly to continue, at least to the degree that it has subordinated them in the past. The post-Stonewall era has witnessed increasing incorporation of openly gay people in society, and a gradual decline of some barriers to their inclusion. Among the signs indicating the change: gay people are finding acceptance or toleration in neighborhoods outside of gay urban ghettos, corporations and government agencies are extending benefits to same-sex partners, and the media portray gay people in a positive light.

Yet states attempt to pass amendments to their constitutions specifically excluding gay people from special legal consideration,[46] heated debates rage in legislatures and Congress over protecting "traditional family values" from "threats" by gay people, and discrimination in workplaces is still common. And sodomy laws remain on the books.

Obviously, society has not concluded that the benefits of eliminating traditional anti-gay structures outweigh the costs of subordinating gay people. But what about the costs of maintaining sodomy laws? As Posner notes, the cost to the taxpayer of retaining criminal penalties for gay sexual behavior is minimal, especially when those penalties are rarely or weakly enforced.[47]

The time has come, indeed is long past, when sane and rational voices should speak out for the elimination of the nation's sodomy laws - the nation's way to legally invade the privacy of the bedrooms of a substantial population should end. Their cost to society is simply too high to allow them to remain silently, but not ineffectively, in our criminal codes. The population of citizens that is affected by these laws deserves the same respect for the privacy of their bedroom as the rest of the population. Regardless of whether courts find that federal or state constitutions guaranty the right of adults to behave as they choose to behave in the privacy of their bedrooms, lawmakers should take responsibility for the social inequities and economic harm they or their predecessors have created. The movement that began publicly on the streets of New York in 1969 has at the beginning of the 21st Century evolved into a force for the recognition of some people's right to pursue happiness in privacy and peace.

Michael Brewer is legal director of the Colorado Legal Initiatives Project, a program of the Gay, Lesbian, Bisexual and Transgender Community Center of Colorado. He is formerly the executive director of the Western Colorado AIDS Project, headquartered in Grand Junction, Colorado. He was graduated with honors from the University of Denver College of Law in 1999.



I'M WATCHING YOU

BY LESLIE E. NUNN, J.D., DANE PATRIDGE, PH.D., & BRIAN MCGUIRE, PH.D.

Over the last several years, an issue has emerged that has challenged employers: whether and how to monitor employee electronic communications, in particular, employee use of e-mail and the Internet. Employers have undertaken such monitoring in an effort to reduce the amount of productivity lost to non-work related activities and to guard against employees accessing inappropriate websites or sending inappropriate e-mails.[1] Employer concern with potential sexual or racial harassment has also motivated many to take action.[2] Major employers, such as The New York Times, Dow Chemical, and Xerox, have recently terminated employees for inappropriate e-mail and Internet use.[3] In addition, the American Management Association reports that over eighty percent of surveyed companies engage in electronic monitoring and/or surveillance of their employees.[4] These employers monitor employee use of the Internet, e-mail, and computer files, as well as video recording employee performance and reviewing employee telephone conversations and voice mail messages.[5] Furthermore, nearly ten percent of companies in the United States have been subpoenaed for employee e-mail in pending cases.[6] There have also been cases where employers have obtained court orders allowing them to search the home computer hard drives of employees.[7]

One consequence of the actions that employers have taken in this area is concern regarding the rights of employees.[8] To what extent, if any, are there limits on the employer's right to monitor employee use of e-mail and the Internet? Most companies have policies concerning e-mail and Internet use, a somewhat smaller percentage provide notification to employees of the monitoring, and relatively few provide training regarding such policies.[9]

In an ironic twist, the United States Court of Appeals for the Ninth Circuit ordered staff members to disable the

software that had been monitoring the e-mail and Internet use of the judges.[10] The United States Judicial Conference's Committee on Automation and Technology, however, was of the opinion that "federal employees - including judges - should continue to be monitored for Internet misuse and should be blocked from such activities as downloading music."[11]

This paper will address the monitoring of employee electronic communication. The following sections will examine the law concerning searches, the issue of employee notice, and recommend policies in this area that would be prudent for employers to adopt.

BACKGROUND: SEARCHES AND THE FOURTH AMENDMENT

Fourth Amendment

The first ten amendments to the Constitution of the United States are referred to as the "Bill of Rights" and are generally understood to codify the most basic of rights that we enjoy as citizens and residents of this country.[12] The right to be free of unreasonable searches is one of the most carefully guarded rights, and is treated in the Fourth Amendment to the Constitution.[13] The Fourth Amendment reads as follows:

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.[14]

What is a "Search"?

The Supreme Court has construed the constitutional protection against unreasonable searches and seizures embodied in the Fourth Amendment "as proscribing only governmental action; it is wholly inapplicable 'to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the government or with the participation or knowledge of any governmental official.'"[15] Within the meaning of the Fourth Amendment, "a 'search' occurs when an expectation of privacy that society is prepared to consider reasonable is infringed."[16] In determining whether a claimed expectation of privacy is proper, the courts apply a two-part test.[17] First, did the individual demonstrate by his conduct that he had an "actual (subjective) expectation of privacy?"[18] Secondly, if so, was that subjective expectation something that society at large would "recognize as reasonable?"[19]

However, this is not to say that the individual's subjective expectation of privacy is dispositive of the issue.[20] The totality of the circumstances must be considered to determine whether an individual has a legitimate expectation of privacy.[21] For example, what can be observed or heard, without the aid of technical enhancement, when the observer is legally present in a place where he has a right to be is not considered an illegal search.[22]

Searches can be performed visually[23] or by more advanced technology, such as through the use of electronic listening devices[24] or thermal imaging devices.[25] It is not the same as a seizure.[26] The term "seizure" describes the actual taking of an item or items found during a search.[27]

Plain View

The law is well settled in that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[28] "The rationale of the plain-view doctrine is that if contraband is left in open view and is observed by a police officer from a lawful vantage point, there has been no invasion of a legitimate expectation of privacy and thus no 'search' within the meaning of the Fourth Amendment . . . ."[29]

Administrative/Regulatory Inspections

As with searches that occur in the criminal context, Fourth Amendment protections also apply "with respect to administrative inspections designed to enforce regulatory schemes."[30] "In closely regulated industries, however, an exception to the warrant requirement has been carved out for searches of premises pursuant to an administrative inspection scheme."[31] For an

administrative or regulatory inspection to be conducted constitutionally without a warrant, three criteria must be met: (1) "there must be a substantial government interest in the regulatory scheme under which the inspection is conducted;"[32] (2) "the warrantless search must be necessary to further the regulatory scheme;"[33] and (3) "in terms of certainty and regularity of its application, the inspection must provide a constitutionally adequate substitute for a warrant."[34] These three requirements combined present a formidable chasm to cross. These requirements for warrantless inspections are normally met only in a few industries; i.e., the liquor,[35] gambling,[36] tavern,[37] meatpacking,[38] wastewater treatment,[39] auto-body repair,[40] and toxin-producing industries.[41]

Search Warrant

The police must have a search warrant before they conduct a search, except in rare and specific situations.[42] As the Fourth Amendment specifically states, a search warrant should be issued only upon a finding of "probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[43] The property to be searched must be described in writing and in specific detail.[44] Likewise, the items being looked for must be described in specific detail in the search warrant.[45]

Exceptions to Warrant Requirement

Normally, searches without a warrant are presumed to be unreasonable.[46] Among the situations where a warrant is not necessary, other than for administrative or regulatory searches of closely regulated industries, are situations where time is clearly of the essence.[47] A warrant is also not necessary when: (a) the person to be searched gives free and voluntary consent to be searched;[48] (b) entry of the subject property is necessary to save a person's life;[49] (c) a search is necessary to prevent the immediate loss or destruction of evidence of a crime;[50] (d) the items are in plain view, as described above;[51] (e) a search is necessary to protect the safety of the law enforcement officer, such as looking for weapons in the driver's area of a car that is stopped because of a traffic violation;[52] and (f) a search occurs incident to arrest.[53]

SEARCHES CONDUCTED BY AN EMPLOYER

Private employers are normally not subject to the same restrictions as law enforcement officers because the Fourth Amendment applies to governmental actors and not private individuals.[54] In a purely commercial setting an employer has a business and monetary interest in what her employees are doing while on the job and while on the business premises. Under general employment law, every employee owes a duty of loyalty to his employer.[55] This duty gives the employer a vital, as well as legal, interest in what is going on in and about her premises.[56] Since the employer is not a criminal investigator, she is given wider latitude in conducting searches of her own business areas.[57]

Employer as an Agent of the Police

When the police conduct a criminal investigation, they cannot coerce or too strongly encourage an employer to search her employee's work place without a search warrant.[58] If the employer does so, she is acting as an agent of the police and the constitutional restrictions are the same as if the police themselves conducted the search.[59] A search warrant is required unless the search fits one of the above referenced exceptions.[60]

A two-part test is used to determine if the employer's actions are subject to constitutional strictures. The first inquiry is whether the law enforcement agency initiated, "'knew of[,]' or 'acquiesced in' the intrusive conduct."[61] The second inquiry is whether the employer who performed the search intended to assist law enforcement efforts, or was merely trying to further her own ends.[62]

That is not the case, however, when the employer conducts a private search of the employee's work area, on her own, and without any contact with the police.[63] In that case, whatever the employer finds is usually held to be admissible in a criminal prosecution of the employee.[64]

Invasion of Privacy

When an employer suspects an employee of misconduct, the employer usually simply fires the employee.[65] If, however, the employer is not trying to assist law enforcement and has as her main purpose the furtherance of her own business ends, the employer is usually permitted to conduct her own search of the employee's work area located on the employer's property.[66] However, this general rule has limitations, one of which is the common law tort of invasion of privacy.[67]

The tort of invasion of privacy has come to symbolize several different causes of action.[68] However, for purposes of this article, we will concentrate on the cause of action entitled "intrusion upon seclusion, which focuses on the manner in which information that a person has kept private has been obtained."[69]

...is usually held to be admissible in a criminal prosecution of the employee.

continued on page 576

continued from page 545
The courts recognize a privacy interest in medical records and then balance that interest against various legitimate purposes associated with disclosing that information.

V. The HIPAA regulations adopt and seek to implement the privacy interests and balancing tests developed in the various cases.

In 1996, Congress enacted the Health Insurance Portability and Accountability Act ("HIPAA").[103] Among other things, HIPAA required Congress to enact new safeguards to protect the security and confidentiality of health care information. Congress failed to do so, requiring the Department of Health and Human Services ("HHS") to promulgate regulations for such protections.[104] In November of 1999, HHS published proposed regulations and, during the comment period, received 52,000 communications from the public.[105] In December 2000, HHS issued the final rule that took effect on April 14, 2001.[106] However, most covered entities have until April 14, 2003 to comply with the final rule's provisions.[107] The HIPAA regulations are intended to establish a set of basic national privacy standards to serve as a floor of ground rules for health care providers, health plans and health care clearinghouses to follow.[108]

In promulgating the regulations, HHS considered the need for privacy of medical records to be great.[109] The HHS recognized a "growing concern" stemming from several trends, "including the growing use of interconnected electronic media for business and personal activities, our increasing ability to know an individual's genetic make-up, and, in health care, the increasing complexity of the system."[110] Unless those public concerns were allayed, the HHS believed we would be "unable to obtain the full benefits of electronic technologies. The absence of national standards for the confidentiality of health information has made the health care industry and the population in general uncomfortable about this primarily financially-driven expansion in the use of electronic data."[111] The HHS focused on one of the same concerns that was recognized by various courts, the consequences of sharing information without the knowledge of the patient involved.[112]

In concluding that "privacy is a fundamental right," HHS looked to judicial authority and, in particular, to the *Whalen* decision.[113] In several aspects, the HIPAA regulations have followed the guidance from the federal courts.[114] In relying on this federal authority, HHS did not specifically address the fact that the judicial authority it cited related to the right to privacy from the perspective of government actors rather than the private sector, which is not subject to the constitutional restrictions.[115]

There are several principles from the federal decisions that are reflected and expanded in the HIPAA regulations. First, the cases generally accept that there is an expectation of privacy in medical records, although the extent to which it reaches a constitutionally protected right may be debated.[116] In promulgating the regulations, HHS characterized privacy as a "fundamental right" and concluded that the "United States Supreme Court has upheld the constitutional protection of personal health information" in *Whalen*.[117] Second, the HIPAA regulations focus on the first type of individual privacy protection identified in *Whalen*, the protection for medical records.[118] The HIPAA regulations do not seek to protect medical decision-making, an interest also largely ignored by the courts.[119] Third, the HIPAA regulations acknowledge that the right to privacy "is not absolute" and must be balanced against legitimate

continued on page 556

continued from page 518
California v. Ciraolo[24], the Court held that an overflight of the defendant's property by a police airplane did not amount to a search, on the unusual ground that the plane was in FAA approved air space. The Court's rationale for this rule was that no expectation of privacy could be reasonable, as "[a]ny member of the public flying in this airspace who glanced down could have seen everything that these officers observed."[25] Here, the individual's fault is not conveying information to a third party, but failing to properly safeguard his property:

> That the area is within the curtilage does not itself bar all police observation. The Fourth Amendment protection of the home has never been extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares. Nor does the mere fact that an individual has taken measures to restrict some views of his activities preclude an officer's observations from a public vantage point where he has a right to be and which renders the activities clearly visible.[26]

In its most recent Fourth Amendment case, *Kyllo v. United States*,[27] the Court held that the use of thermal imaging technology to measure the heat coming off of a dwelling was a search subject to the requirements of the Fourth Amendment. The Court held that because the device provided details about the interior of a home that could not otherwise be obtained without trespassing into the home and because the device had not yet entered into general use, its use constituted a search.[28] The flip-side of this argument appears to be that had the device used by the police

continued on page 574

continued from page 521

II. THE TANGIBLE, THE INTANGIBLE, AND THE PROBLEM OF CONTEXT

The tangible-versus-intangible framework also overvalues security because it embeds the choice between tangible and intangible in a specific factual context, such as the process of boarding an airplane - a context that is itself tangible. As explained below, framing the question in such a context inevitably leads people to guard against the more tangible harms.

In an age pervaded by cost-benefit analysis, there is an urge to reduce all policy decisions to a balance sheet. But we lack a single currency in which to measure the relative value of the privacy and security interests. Attempts to equate a "unit" of privacy to a "unit" of security, for example, are doomed to fail. As we attempt to choose between these two incommensurable goods,[46] we lack a simple, cost-benefit approach to the balancing.

Of course, the mere fact that two goods are incommensurable need not skew the calculus in one direction or the other; it simply makes the choice more difficult. Indeed, incommensurability characterizes most attempts to balance competing goods.[47] Despite our lack of a common "metric" in which to measure those goods, we find ways to make hard decisions.

What does skew the calculus, however, is the perception that breaches of security lead to tangible harms, while intrusions on privacy lead to intangible harms. Proponents of security measures can raise the specter of specific, all too tangible acts of violence. Failures of security can lead to concrete harms that have shaped our collective experience, such as the bombing of the Marine barracks in Beirut, the bombing of the American Airlines flight over Lockerbie, Timothy McVeigh's attack in Oklahoma City, and September 11.

Privacy, in contrast, is often considered a purely abstract value, one that we can sacrifice in a particular instance without risking any real, tangible harm.[48] Many who argue for the preservation of privacy stress its importance for purposes that are themselves abstract, such as personal autonomy,[49] personal and political identity,[50] and freedom of expression and association.[51] Moreover, privacy is a highly subjective concept, one that can vary from person to person.[52]

Comparing tangible and intangible consequences in the context of specific security proposals is likely to overstate the value of the tangible. As Julie Cohen observed in a related context, "Privacy, like other dignity-related goods, has inherently nonmonetizable dimensions. These dimensions may be lost or distorted beyond recognition in the translation to dollars and cents."[53] So a consumer making a decision about a transaction, with consequences defined in monetary terms, will find it difficult to translate the intangible, nonmonetizable dimensions of privacy into that decision making equation.[54] The specific context in which the consumer must decide constrains her decision making calculus.

A similar problem of context frustrates privacy advocates in the debate over privacy and security.[55] Debates over security proposals are often grounded in specific factual contexts in which the privacy implications appear innocuous, while a security breach could lead to grave harm. British Home Secretary David Blunkett colorfully contrasted the danger of terrorist attacks with abstract notions of privacy and liberty: "We can live in a world with airy-fairy civil liberties and believe the best in everybody and then they destroy us."[56] Oracle CEO Larry Ellison expressed a similar sentiment in testimony submitted to a congressional subcommittee considering national ID cards:

> Two hundred years ago, Thomas Jefferson warned us that our liberties were at risk unless we exercised 'eternal vigilance.' Jefferson lived in an age of aristocrats and monarchs. We live in a nuclear age with the threat of terrorists getting their hands on weapons with the capacity to destroy entire cities. Only by giving our intelligence and law enforcement agencies better tools and more latitude to pursue terrorists can we expect to save life and liberty together.[57]

Former National Security Agency general counsel Stewart Baker summed up this perspective:

> We as a people are willing to trade a little less privacy for a little more security. If using more intrusive technology is the only way to prevent horrible crimes, chances are that we'll decide to use the technology, then adjust our sense of what is private and what is not.[58]

Security proposals implicitly summon images of a horrible reprise to the World Trade Center and Pentagon attacks, as well as attacks using biological or nuclear weapons. Juxtaposed against those images are what some characterize as "airy-fairy" notions of privacy.[59] Though they do not explicitly deny that privacy has some value in the abstract, they urge people to sacrifice it in particular cases to prevent "real," tangible harms.[60] With the issue framed in such stark terms, one would be hard pressed to argue that, *in just this one case,* abstract privacy values should not yield to the need to prevent attacks by terrorists with biological and nuclear weapons.[61]

Furthermore, differences in the scale upon which security and privacy benefits are observable exaggerate our perception of privacy benefits as intangible and security benefits as tangible. The example of airport checkpoint searches helps illustrate this point. As I am frisked or scanned, I cannot possibly see the cumulative effect across society of implementing these types of uniform measures. I experience only my search and the searches of a few

continued on page 571

Bruce Kobayashi is Professor of Law, George Mason University School of Law.
Professor Kobayashi received his Ph.D in economics from the University of California, Los Angeles. He is the author of numerous articles on the law and economics of intellectual property, antitrust, regulation, litigation, and procedure. He and Professor Ribstein have published numerous articles on jurisdictional competition and regulation, including recent articles on state regulation of consumer marketing information and state regulation of electronic commerce.

continued from page 531
employers' information may override the interests of a state that has no policy favoring sharing information.[38]

A potential solution to all these problems is allowing the parties to nail down the applicable state law by including a choice-of-law clause in their employment contracts. This can potentially ensure enforcement of the clause against application of state law that protects employees or raiding employers. The Restatement provides that the law designated in the contract is not enforced as to a regulatory issue if:

> (a) the chosen state has no substantial relationship to the parties or the transaction and there is no other reasonable basis for the parties' choice, or
>
> (b) application of the law of the chosen state would be contrary to a fundamental policy of a state which has a materially greater interest than the chosen state in the determination of the particular issue and which, under the rule of § 188, would be the state of the applicable law in the absence of an effective choice of law by the parties.[39]

Since the chosen state is often the employer's headquarters or at least a branch office, the main issues concern, not the relationship with the chosen state,[40] but whether another state has a fundamental policy against enforcement and that state's interests outweigh the chosen state. The cases reach varied results, but a review of 67 restrictive covenant cases involving choice-of-law clauses shows that clauses were enforced in 39 cases, not enforced in 25 cases, and interpreted as inapplicable in three cases. To be sure, further analysis is necessary to determine the marginal effect of the clause - that is, whether the court would have reached the same result under either law. But the courts' tendency to enforce contractual choice suggests that the clauses may have some effect in inducing courts to enforce
restrictive covenants.

This brief review of the law suggests that the parties gain something from these choice-of-law clauses, even if they are frequently not enforced. Where the law of a contractually selected state is fairly similar to that of another state whose law would apply in the absence of contractual choice, but where the law of the two states might go either way with close facts, the court likely will apply the selected law. Thus, a firm may be able to gain predictability by contracting for the application of the law of a state that has experience with these clauses or has enforced the particular clause or clauses in relevant industries.[41] Also, even if the two potentially applicable laws differ significantly, a court may choose to apply the less regulatory statute where the fact situation is arguably not covered by the more regulatory statute.[42]

However, these clauses do not give employers perfect protection. The problem is that states enforce their own "fundamental" policies, while at the same time refusing to apply the laws of states that have weak contacts with the contract. This often means protecting local employers against employers based out of state. Consider, for example, *Application Group, Inc. v. Hunter Group, Inc.*,[43] in which a California state court protected a local employer raiding an employee of a Maryland firm despite a Maryland choice of law clause. Applying the Restatement[44], the court held that California's anti-non-compete policy applies to employment involving performance of "services for California-based customers" even if the employee had no prior contact with California and does not reside in California. The court reasoned:

> In this day and age—with the advent of computer technology and the concomitant ability of many types of employees in many industries to work from their homes, or to 'telecommute' to work from anywhere a telephone link reaches—an employee need not reside in the same city, county, or state in which the employer can be said to physically reside. California employers in such sectors of the economy have a strong and legitimate interest in having broad freedom to choose from a much larger, indeed a 'national,' applicant pool in order to maximize the quality of the product or services they provide,

continued on page 567

---

continued from page 525
in the judicial process because Ms. Lewinsky struck a deal with Mr. Starr and voluntarily turned over the records.

The Tattered Cover, in its case, urged the court to apply the compelling need standard. We argued that the government did not demonstrate a compelling need for the information to make their case, nor did authorities exhaust their other alternatives in gathering information. Only when there is compelling need and there are no other alternatives should First Amendment guarantees be set aside.

continued on page 570

Bruce Kobayashi is Professor of Law, George Mason University School of Law.
Professor Kobayashi received his Ph.D in economics from the University of California, Los Angeles. He is the author of numerous articles on the law and economics of intellectual property, antitrust, regulation, litigation, and procedure. He and Professor Ribstein have published numerous articles on jurisdictional competition and regulation, including recent articles on state regulation of consumer marketing information and state regulation of electronic commerce.

continued from page 531
employers' information may override the interests of a state that has no policy favoring sharing information.[38]

A potential solution to all these problems is allowing the parties to nail down the applicable state law by including a choice-of-law clause in their employment contracts. This can potentially ensure enforcement of the clause against application of state law that protects employees or raiding employers. The Restatement provides that the law designated in the contract is not enforced as to a regulatory issue if:

> (a) the chosen state has no substantial relationship to the parties or the transaction and there is no other reasonable basis for the parties' choice, or
>
> (b) application of the law of the chosen state would be contrary to a fundamental policy of a state which has a materially greater interest than the chosen state in the determination of the particular issue and which, under the rule of § 188, would be the state of the applicable law in the absence of an effective choice of law by the parties.[39]

Since the chosen state is often the employer's headquarters or at least a branch office, the main issues concern, not the relationship with the chosen state,[40] but whether another state has a fundamental policy against enforcement and that state's interests outweigh the chosen state. The cases reach varied results, but a review of 67 restrictive covenant cases involving choice-of-law clauses shows that clauses were enforced in 39 cases, not enforced in 25 cases, and interpreted as inapplicable in three cases. To be sure, further analysis is necessary to determine the marginal effect of the clause - that is, whether the court would have reached the same result under either law. But the courts' tendency to enforce contractual choice suggests that the clauses may have some effect in inducing courts to enforce
restrictive covenants.

This brief review of the law suggests that the parties gain something from these choice-of-law clauses, even if they are frequently not enforced. Where the law of a contractually selected state is fairly similar to that of another state whose law would apply in the absence of contractual choice, but where the law of the two states might go either way with close facts, the court likely will apply the selected law. Thus, a firm may be able to gain predictability by contracting for the application of the law of a state that has experience with these clauses or has enforced the particular clause or clauses in relevant industries.[41] Also, even if the two potentially applicable laws differ significantly, a court may choose to apply the less regulatory statute where the fact situation is arguably not covered by the more regulatory statute.[42]

However, these clauses do not give employers perfect protection. The problem is that states enforce their own "fundamental" policies, while at the same time refusing to apply the laws of states that have weak contacts with the contract. This often means protecting local employers against employers based out of state. Consider, for example, *Application Group, Inc. v. Hunter Group, Inc.*,[43] in which a California state court protected a local employer raiding an employee of a Maryland firm despite a Maryland choice of law clause. Applying the Restatement[44], the court held that California's anti-non-compete policy applies to employment involving performance of "services for California-based customers" even if the employee had no prior contact with California and does not reside in California. The court reasoned:

> In this day and age—with the advent of computer technology and the concomitant ability of many types of employees in many industries to work from their homes, or to 'telecommute' to work from anywhere a telephone link reaches—an employee need not reside in the same city, county, or state in which the employer can be said to physically reside. California employers in such sectors of the economy have a strong and legitimate interest in having broad freedom to choose from a much larger, indeed a 'national,' applicant pool in order to maximize the quality of the product or services they provide,

continued on page 567

---

continued from page 525
in the judicial process because Ms. Lewinsky struck a deal with Mr. Starr and voluntarily turned over the records.

The Tattered Cover, in its case, urged the court to apply the compelling need standard. We argued that the government did not demonstrate a compelling need for the information to make their case, nor did authorities exhaust their other alternatives in gathering information. Only when there is compelling need and there are no other alternatives should First Amendment guarantees be set aside.

continued on page 570

continued from page 553
public uses of that information.[120] However, steps must be taken to ensure that the balancing does not result in unnecessary privacy breaches.[121]

Initially, the HIPAA regulations seek to implement these principles with its definitions. The regulations protect the defined term "protected health information" by generally limiting the use of that information to the individual or with the individual's consent.[122] That key phrase - protected health information - is based on another defined phrase, "individually identifiable health information."[123] In turn, "individually identifiable health information" is defined as a subset of health information, including demographic information collected from an individual that:

> (1) Is created or received by a health care provider, health plan, employer or health care clearinghouse; and
> (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and
>
> > (i) That identifies the individual;
> > (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.[124]

However, health information that does not identify an individual or permit identification of the individual does not meet the definition of "identifiable health information."[125] In order to satisfy this exclusion, numerous identifiers must be removed, including identifiers such as names, dates, numbers, addresses and any unique identifying characteristics.[126]

Similar to the balancing test from judicial decisions, the regulations identify many situations where the "protected health information" may be disclosed, even without consent, so long as it is required by law and the use or disclosure complies with and is limited to the relevant requirements of law.[127] Similar to the federal case law, appropriate disclosures are determined based on their purposes and scope of disclosure.[128] Some examples[129] of permitted disclosures include:

> To a public health authority to prevent or control disease or injury;
>
> To a public health authority authorized by law to receive reports of child abuse or neglect;
>
> To a person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition;
>
> To a social service agency about a victim of abuse, neglect or domestic violence, if required by law and if the individual consents or if there is a belief that disclosure is necessary to prevent serious harm to individuals;
>
> To a health oversight agency for oversight activities authorized by law;
>
> To a law enforcement official's request for the purpose of identifying or locating a suspect, fugitive, material witness or missing person.[130]

This list focuses on many of the purposes identified in the federal case law as appropriate and necessary societal uses of medical records. As noted by Justice Stevens in *Whalen*, disclosures for these types of purposes are those "unpleasant invasions of privacy that are associated with many facets of health care."[131] The HIPAA regulations seek to implement the courts' case-by-case analysis by itemizing those instances where society's needs outweigh the individual's privacy rights. While the regulatory approach provides more specificity, it also lacks the flexibility that would be exercised by a court enforcing the existing case-by-case approach. However, that specificity may provide greater certainty and predictability, which are critical for the entities subject to HIPAA.

Conclusion

The right to privacy in medical records is balanced against society's expected invasions of privacy related to health care. Our expectation of privacy in those records has never been seriously contested. Federal courts have consistently reached that conclusion without the need for precedent. However, those rights often fail in the balancing test against society's interests. The extent to which the privacy expectation rises to a constitutional right has not yet been resolved and may never be resolved. The HIPAA regulations attempt to adopt the balance established by the courts, by protecting medical records and protecting society's legitimate uses of the health care information.

LAND OF THE FREE?

Professor Mell's forthcoming article discusses how the USA Patriot Act erodes traditional protections afforded American citizens against invasion of privacy by the government. by Joseph H. Lusk

The USA Patriot Act ("Act") changes the existing legal landscape by, among other things, amending both the Foreign Intelligence Surveillance Act[2] ("FISA") and the "Wiretap Statute."[3]

Traditionally, Congress and the courts have limited the CIA's investigative authority to non-domestic issues, and its surveillance power to outside the United States.[4] According to Mell, these restrictions were enacted to protect American citizens from the scrutiny of the CIA, because Congress "recognized the potential for abuse by an organization with authority to pursue clandestine surveillance."[5] Mell explains that the Act's FISA amendments diminish the protections traditionally afforded U. S. citizens by allowing the CIA to conduct domestic surveillance.[6]

Additionally, Mell describes how the Act is vague and overbroad.[7] For example, the Act's "crimes of Domestic Terrorism and Harboring a Terrorist" may include "such legitimate activist activity as anti-abortion rights, animal rights, environmentalists, striking union members in vital industries, civil rights protesters, and the G-4 protesters . . . ."[8]

Mell also traces the history of law enforcement surveillance abuse, which led to FISA's enactment.[9] Before FISA, law enforcement, notably the FBI, used a "national security" justification in conducting surveillance that would have otherwise been disallowed.[10] When enacted, FISA created a "scheme of surveillance oversight" which balanced the government's desire to institute surveillance with the target's civil liberties. This scheme protected the subject of a criminal investigation from the government's abuse of its surveillance authority.[11] Similarly, the Wiretap Statute created an oversight scheme in the unique area of wiretapping.[12] Mell explains how the Act's amendments to both FISA and the Wiretap Statute allow for potential abuses the original acts sought to prohibit.[13]

In addition to the potential for abuse in the FISA and Wiretap Statute amendments, the Act also enhances the CIA-FBI information sharing partnership. This same type of agreement resulted in the compilation of intelligence dossiers on citizens involved in legitimate protests during the 1970s.[14] The CIA-FBI partnership, coupled with the Act's loosened restrictions on gaining information obtained in CIA-conducted surveillance, has the potential to intrude on Americans' political activity, business relationships, and personal lives.[15]

Thus, Mell concludes that the Act generally removes critical "checks and balances on governmental action" which "could have the effect of diminishing the already waning protection afforded by the Fourth Amendment."[16]

Patricia Mell is professor of law at Michigan State University-Detroit College of Law in East Lansing, Michigan, where she teaches courses in criminal law, corporate law, rights in art, and white-collar crime.

Professor Mell earned her bachelor's degree with honors from Wellesley College in 1975 and her JD from Case Western Reserve University in 1978. While in law school, she was on the Moot Court Board and was advisor to the Jessup Moot Court Team.

From 1978-1983, Professor Mell was an assistant attorney general for the state of Ohio, working as a trial attorney in the Consumer Frauds and Crimes Section and in the Charitable Foundations Section. In 1983, she joined the Ohio secretary of state's office, where she was chief administrator and legal counsel for the Corporations Section as well as legal advisor to the Uniform Commercial Code Section.

Professor Mell began her teaching career at Capital University Law School. She subsequently taught at the University of Toledo College of Law and Widener University School of Law. She joined the MSU-Detroit College of Law faculty in 1992 and served as associate dean from 1998-2001. She is the author of several scholarly articles focusing on privacy and computers.

Joe is a recent graduate of the University of Denver College of Law and plans to sit for the Colorado Bar Examination in July, 2002. Joe works as a Senior Law Clerk with Merrill Lynch, Pierce, Fenner & Smith Incorporated.

continued from page 539
card.[79] On his own initiative, a company employee had provided "huge swaths" of customer data to law enforcement to aid in the investigation of the terrorist attacks.[80] Ponemon says that such breaches are increasingly common, with a variety of industries routinely "breaking their privacy policies" and sharing customer data with law enforcement "to analyze suspicious activity."[81]

Can government agents be trusted with this data?

By capturing the fundamental profile of each household... supermarket databases provide the government with a close and surreptitious look into the lives and habits of individuals.[82]
- Christine Anthony, Researcher

While government agencies may want to add shopper card information to the ever-widening number of databases they can access for information about citizens, would such information be safe in their hands? Considering tales of corruption, fraud, and shady dealings around the country, the answer may well be "no."

Abuse of data

Law enforcement officials, who clamor for databases on citizens to keep the public safe from crime, are not above abusing the data to commit their own crimes. Data abuse by government officials appears to be widespread. Just a few recent cases include a DEA agent caught selling sensitive records from several different government databases and officials in Las Vegas selling confidential court records.[83]

More than 90 state police employees have been accused of misusing Michigan's Law Enforcement Information Network, including a state trooper who used it to keep tabs on her ex-husband's new girlfriend,[84] and another who obtained the home address of an 18-year-old woman in order to hound her for a date.[85] The abuse reaches as far back as 1983 when the database was used to harass a union representative.[86]

The California Department of Motor Vehicles (DMV) has had a particularly hard time keeping its database secure. Scores of DMV employees have abused their access to sensitive information on the system to help criminals commit identity theft and other crimes.[87] Even after firing 80 employees in a yearlong crackdown, the agency acknowledged in late 2000 that it still has "a very large employee fraud problem."[88]

California DMV and Safeway

The California DMV has been involved in some shady dealings with supermarkets, as well. A few years back Safeway (the nation's 3rd largest grocery chain) sent someone to two rival grocery stores to copy the license plate numbers from 1,000 cars in the other stores' parking lots. For $5,000, the DMV sold Safeway the home address of every individual parked at the competition's lot.[89]

Amazingly, a 1990 California state law allows the DMV to release drivers' residential addresses (but not their names) to anyone who can demonstrate a "legitimate business reason" to request the data.[90] The Safeway transaction was apparently "business as usual" and only came to light when an audit revealed that the DMV failed to obtain a written statement from Safeway promising not to use the information for direct marketing purposes.[91] Had the DMV filled out the paperwork correctly, the transaction would have gone undetected.

Perhaps more disturbing, when Safeway's actions came to light the company made no effort to apologize to the people whose privacy it had violated. Safeway spokeswoman Debra Lambert justified the company's behavior and dismissed privacy concerns saying, "It's only addresses. We keep the data to ourselves. It is never divulged outside of the company."[92]

Somehow I suspect the fact that the company keeps those records to themselves would be scant reassurance to the 1,000 shoppers who had chosen not to do business with Safeway in the first place. Since Safeway aggressively collects data on its own customers through its "Safeway Club Card," shoppers in rival parking lots may have been intentionally trying to keep their shopping habits out of Safeway's reach. It is unconscionable that a government agency would circumvent the desire of its citizens to avoid a particular business by selling their confidential records to marketers, and even more appalling that Safeway seems to place no moral or ethical limits on their data collection practices.

SECTION 3: TECHNOLOGY IS PAVING THE WAY FOR DATA COLLECTION ON AN ENORMOUS SCALE

Cards will become inextricably linked with identity

The ability to match names, addresses, purchasing behavior, and lifestyles all together into one record allows companies to build detailed pictures of people's lives.[93] Grocery card records are already being linked with data from a variety of outside sources. For example, more than 700,000 British shoppers have linked their Tesco grocery cards with the natural gas supplied to their homes,[94] thus necessitating the use of a valid name and home address to obtain the card. Of even greater concern are the links being formed between marketing databases and government identification documents.

As supermarket purchase records become increasingly useful informational commodities for law enforcement, government bureaus, and other entities, the accuracy of the data collected will become an important issue. Though it is currently possible to obtain a supermarket card using anonymous or fictitious information at many supermarkets around the country, this loophole could easily close. With "document fraud" being the new buzzword in law enforcement and legislative circles since September 11th (carrying with it a maximum 15-year prison sentence[95]), it is not hard to envision a day when providing

false information on a private contract or card application could be punishable as "fraud."

Supermarkets may begin tightening up their card application procedures to include identity verification. Though customers may balk, the process could be streamlined and made transparent by offering the option of scanning a government-issued ID card instead of a loyalty card. Not only would this reduce the number of cards in a shopper's wallet, it would simplify the collection of food purchase records for inclusion in government databases.

Such a scheme is not far-fetched. Virginia Congressmen Jim Moran (D-VA) and Tom Davis (R-VA) recently introduced legislation that would require all state driver's licenses and ID cards to contain an embedded computer chip capable of accepting "data or software written to the license or card by non-governmental devices."[96] The mandatory "smart chips"[97] would carry bank and debit card data so that citizens could use their ID cards "for a variety of commercial applications."[98] Barring protests from citizens, the state of New Mexico plans to issue a "smart card" driver's license containing a computer memory chip, a portion of which will be set aside for use by credit card issuers and other commercial service providers.[99]

Supermarket "loyalty" cards would be an obvious application for the high-tech smart cards. As Alan Glass, Senior Vice President of Electronic Commerce at MasterCard International, points out, "A senior citizen could have securely protected medical information, supermarket loyalty programs, social club membership and access, discount programs, a municipal transportation pass, and a library card all stored on a single chip."[100]

To complete the total identity picture, the biometrics industry hopes that security concerns will "advance the day when mass commercial applications of biometrics become routine."[101] Accordingly, supermarkets have begun testing out biometric identification systems on U.S. shoppers. Fingerprint payment technology is already in place at a Thriftway grocery store in Washington,[102] and Kroger, the nation's largest supermarket chain, is testing a fingerprint payment system in Texas.[103] The eventual endpoint of the identification-for-food trend may require transmitting one's shopper ID number through a subdermal computer chip implant, such as the Verichip produced by Applied Digital Solutions.[104] A Florida family recently had these chips surgically embedded in a procedure publicized on national television.[105]

Linking government and private sector databases would provide both with nearly omniscient powers of observation over the consumer-citizen. Such a potent concentration of power and knowledge in so few hands could hardly be expected to operate in the interest of privacy and freedom. Sadly, it may be all too easy to convince shoppers that conducting their commercial transactions by means of a government identity document would be more convenient, or that it might somehow promote national security.

Technologies to monitor shoppers' movements

The trade publications for the loyalty marketing industry offer a unique window of insight into the marketers' long-range goals. The writings of marketing strategists reveal a pervasive, industry-wide mentality that will stop at nothing short of omniscient knowledge of consumers' every move — a goal that can only be achieved through total surveillance. As evidence of this mindset, here are a few of the invasive retail surveillance technologies in use today as described on the companies' websites and in related publications.

The ceiling-mounted store cameras originally installed to prevent shoplifting have been turned to a new use — spying on the average shopper. A market research company called Envirosell uses time-lapse surveillance cameras to record detailed information about consumers as they shop. Unlike stationary camera surveillance, which only records what occurs in a given area, Envirosell's technology singles out *individual shoppers*, identified by body mass or body temperature, and "passes" them from camera to camera to record their movements during the entire shopping trip.[106] The surveillance is so complete that if a shopper lingers for more than a few moments in one spot, a wall-mounted camera may zoom in to peer closely at the individual's face.[107]

Apparently, Envirosell feels it is necessary to collect "hundreds of hours of video tape"[108] in this manner, since customer behaviors such as reading labels are "easier to observe on tape, where they may be repeatedly watched frame by frame, than live."[109] The system also employs unobtrusive on-site researchers called "trackers" to follow shoppers around the store, listening in on and recording their conversations.[110] Envirosell has even stooped to closely scrutinizing the moment-by-moment behavior of customers seated at fast food restaurants and groups interacting in sit-down restaurants, without their knowledge or consent.[111]

A "Frequently Asked Questions" (FAQ) page on Envirosell's website is filled with reassurances apparently designed to soothe the skittish retail executive. It explains, for example, that "according to Federal law, in-store filming in public areas does not constitute an invasion of the privacy of customers or employees,"[112] and asserts that video surveillance is employed by "virtually every retail chain in this country."[113] The FAQ page also offers revealing insight into the company's attitude towards shoppers. Asked, "Do customers know they're being watched?" the website explains that "most shoppers are so intent on the shopping process that they notice very little of what goes on around them. . . . However, when they do notice [the cameras] most people assume that they are for security purposes."[114]

Apparently, Envirosell has no shortage of clients. Fred Meyer, CVS, Trader Joe's, and Wal-Mart are among

the nearly 50 major retailers that have used Envirosell's surveillance system to spy on their customers.[115]

Envirosell is just one of many companies eager to deploy its espionage systems in retail environments. Brickstream Corporation uses in-store video technology and image analysis software to track where customers go and what they do in retail stores and banks.[116] A press release issued by Brickstream and partner company Retek Inc. once boasted, "This solution is transparent to the customer yet yields a wealth of information and customer insight for the retailer," [117] implying that shoppers will have no knowledge of being watched. Point Grey Research markets the Censys3D video surveillance system, which literally draws a line on a time lapse video indicating the exact movements of each person who enters the environment.[118]

Not content to rely on mere surveillance cameras, IBM has developed a thermal tracking system it calls "Footprints" to monitor shoppers.[119] The system uses sensors mounted throughout the store that pick up body heat.[120] The sensors are so precise that they can distinguish between individuals in a group and track the exact path of an individual shopper through the store.[121] It is suggested that the thermal technology be coupled with existing video cameras so that human observers can record sex, age and approximate income group data as well.[122]

A company called ShopperTrak has developed a "traffic counter [that] utilizes an on-board video sensor and multiple high-speed microprocessors to unobtrusively track shoppers' movements."[123] The system, which "literally watches shoppers from overhead," has already been implemented at 6,000 retail locations worldwide and is touted as "discreet" on the company's website.[124]

Another company, KartSaver Inc., mounts tracking devices to shopping carts that communicate via infrared signals to receivers mounted in the store's ceiling.[125] This allows the store to track "the traffic patterns and shopping habits"[126] of individual consumers as they walk around the supermarket. In the covert fashion typical of these companies, KartSaver once boasted in a press release that "most consumers will never even know that the product is being employed."[127]

Hy-Vee Food Stores, one of America's 15 largest grocery chains, recently contracted to have a similar infrared cart-tracking network installed in its Kansas City stores.[128] Klever Marketing, which developed and installed the system, equipped Hy-Vee shopping carts with tracking devices and video screens to better "guide [shoppers'] movements and influence their purchasing decisions."[129]

Klever Marketing suggests that its technology could be linked with frequent shopper card records, since knowing a shopper's complete purchase history, along with his or her precise location in the store, would better enable the supermarket to target the shopper with promotional messages.[130] "I think we have just touched the tip of the iceberg," said a senior Hy-Vee executive.[131] "[This] will be a standard part of our business within the next three to five years."[132] Then, ominously, he added, "I'm not sure any of us know what all the final uses will be."[133]

Semcor Inc., a Microsoft strategic partner in the business of using "geographic information systems"[134] to "track and monitor the movements of vehicles, equipment, wildlife and virtually anything else that moves,"[135] also suggests "inserting mini radio transmitters into shopping carts in your supermarket"[136] to keep track of shoppers.

Bridge Technology, an Arizona corporation, is just one of the many companies that hope to link loyalty cards to wireless communications, global positioning systems (GPS), and Internet technologies to record transactions and collect data from remote and mobile locations on a real-time basis.[137] This technology would enable supermarket cards not only to record what people buy, but where they travel as well.

Even the floor people walk on can be used to surreptitiously gather data on them.[138] Semcor's website advises the use of pressure sensitive floor pads to keep tabs on people as they visit museums, galleries, and zoos.[139] Pressure sensitive flooring may be just the beginning. Students at MIT's Media Lab have developed a system of floor sensors that can identify each place a person has moved within a room over time and exactly where they are at any given moment.[140]

While a shopper may be upset to learn how extensively her local retailer observes customers, imagine her horror at discovering that her favorite boutique is not a store at all, but a carefully designed clandestine consumer research laboratory. One such "store" now exists.[141] The Once Famous boutique in Minneapolis is a 1,800-foot storefront that presents itself to shoppers as a trendy home furnishings store.[142] What shoppers don't know is that the decorative items are merely props to lure them inside the store where they serve as unsuspecting - and unpaid - research subjects.[143] A complex network of cameras and microphones carefully concealed throughout the boutique is used to observe and record each shopper's response to specific items offered for sale.[144] These reactions are later written up and sold to clients of the parent company, who pay anywhere from $15,000 to $100,000 or more for researchers to observe subjects handling their products.[145]

Considering how determined marketers seem to be to watch customers' every move, it may not be long before another Applied Digital Solutions product—the "Digital Angel Monitor," a GPS system that can be worn as a wristwatch to allow anyone to "find a person, animal or object anywhere in the world . . . anytime"[146]—is recommended as the perfect device for collecting consumer data 24 hours a day.

Auto-ID: Tracking everything, everywhere

In 5-10 years, whole new ways of doing things will emerge and gradually become commonplace.

Expect big changes.[147]
- MIT's Auto-ID Center

Supermarket cards and retail surveillance devices are merely the opening volley of the marketers' war against consumers. If consumers fail to oppose these practices now, our long-term prospects may look like something from a dystopian science fiction novel.

A new consumer goods tracking system called Auto-ID is poised to enter all of our lives, with profound implications for consumer privacy. Auto-ID couples radio frequency (RF) identification technology with highly miniaturized computers that enable products to be identified and tracked at any point along the supply chain.[148]

The system could be applied to almost any physical item, from ballpoint pens to toothpaste, which would carry their own unique information in the form of an embedded chip.[149] The chip sends out an identification signal allowing it to communicate with reader devices and other products embedded with similar chips.[150]

Analysts envision a time when the system will be used to identify and track every item produced on the planet.[151]

A number for every Item on the planet

Auto-ID employs a numbering scheme called ePC (for "electronic product code"), which can provide a unique ID for any physical object in the world.[152] The ePC is intended to replace the UPC bar code used on products today.[153]

Unlike the bar code, however, the ePC goes beyond identifying product categories — it actually assigns a unique number to every single item that rolls off a manufacturing line.[154] For example, each pack of cigarettes, individual can of soda, light bulb or package of razor blades produced would be uniquely identifiable through its own ePC number.[155]

Once assigned, this number is transmitted by a radio frequency ID tag (RFID) in or on the product.[156] These tiny tags, predicted by some to cost less than 1 cent each by 2004,[157] are "somewhere between the size of a grain of sand and a speck of dust."[158] They are to be built directly into food, clothes, drugs, or auto-parts during the manufacturing process.[159]

Receiver or reader devices are used to pick up the signal transmitted by the RFID tag. Proponents envision a pervasive global network of millions of receivers along the entire supply chain — in airports, seaports, highways, distribution centers, warehouses, retail stores, and in the home.[160] This would allow for seamless, continuous identification and tracking of physical items as they move from one place to another,[161] enabling companies to determine the whereabouts of all their products at all times.[162]

Steven Van Fleet, an executive at International Paper, looks forward to the prospect. "We'll put a radio frequency ID tag on everything that moves in the North American supply chain," he enthused recently.[163]

The ultimate goal is for Auto-ID to create a "physically linked world" [164] in which every item on the planet is numbered, identified, catalogued, and tracked. And the technology exists to make this a reality. Described as "a political rather than a technological problem," creating a global system "would . . . involve negotiation between, and consensus among, different countries."[165] Supporters are aiming for worldwide acceptance of the technologies needed to build the infrastructure within the next few years.[166]

The implications of Auto-ID

Theft will be drastically reduced because items will report when they are stolen, their smart tags also serving as a homing device toward their exact location.[167]
- MIT's Auto-ID Center

Since the Auto-ID Center was founded at the Massachusetts Institute of Technology (MIT) in 1999, it has moved forward at remarkable speed. The center has attracted funding from some of the largest consumer goods manufacturers in the world, and even counts the Department of Defense among its sponsors.[168] In a mid-2001 pilot test with Gillette, Philip Morris, Procter & Gamble, and Wal-Mart, the center wired the entire city of Tulsa, Oklahoma with radio-frequency equipment to verify its ability to track Auto-ID equipped packages.[169]

Though many Auto-ID proponents appear focused on inventory and supply chain efficiency, others are developing financial and consumer applications that, if adopted, will have chilling effects on consumers' ability to escape the oppressive surveillance of manufacturers, retailers, and marketers. Of course, government and law enforcement will be quick to use the technology to keep tabs on citizens, as well.

The European Central Bank is quietly working to embed RFID tags in the fibers of Euro bank notes by 2005.[170] These tags would allow money to carry its own history by recording information about where it has been, thus giving governments and law enforcement agencies a means to literally "follow the money" in every transaction.[171] If and when RFID devices are embedded in banknotes, the anonymity that cash affords in consumer transactions will be eliminated.

Hitachi Europe wants to supply the tags. The company has developed a smart tag chip that — at just 0.3mm square and as thin as a human hair — can easily fit inside of a banknote.[172] Mass-production of the new chip will start within a year. [173]

Consumer marketing applications will decimate privacy

Radio frequency is another technology that supermarkets are already using in a number of places throughout the store. We now envision a day where consumers will walk into a store, select products whose packages are embedded with small radio frequency UPC codes, and exit the store without ever going through a checkout line or signing their name on a dotted line.[174]
- Jackie Snyder, Manager of Electronic Payments for Supervalu (Supermarkets), Inc., and Chair, Food

Marketing Institute Electronic Payments Committee

Auto-ID would expand marketers' ability to monitor individuals' behavior to undreamt of extremes. With corporate sponsors like Wal-Mart, Target, the Food Marketing Institute, Home Depot, and British supermarket chain Tesco, as well as some of the world's largest consumer goods manufacturers including Proctor and Gamble, Phillip Morris, and Coca Cola[175] it may not be long before Auto-ID-based surveillance tags begin appearing in every store-bought item in a consumer's home.

According to a video tour of the "Home of the Future" and "Store of the Future" sponsored by Proctor and Gamble, applications could include shopping carts that automatically bill consumer's accounts (cards would no longer be needed to link purchases to individuals), refrigerators that report their contents to the supermarket for re-ordering, and interactive televisions that select commercials based on the contents of a home's refrigerator.[176]

Now that shopper cards have whetted their appetite for data, marketers are no longer content to know who buys what, when, where, and how. As incredible as it may seem, they are now planning ways to monitor consumers' use of products within their very homes. Auto-ID tags coupled with indoor receivers installed in shelves, floors, and doorways,[177] could provide a degree of omniscience about consumer behavior that staggers the imagination.

Consider the following statements by John Stermer, Senior Vice President of eBusiness Market Development at ACNielsen:

[After bar codes] [t]he next 'big thing' [was] [f]requent shopper cards. While these did a better job of linking consumers and their purchases, loyalty cards were severely limited...consider the usage, consumer demographic, psychographic and economic blind spots of tracking data.... [S]omething more integrated and holistic was needed to provide a ubiquitous understanding of on- and off-line consumer purchase behavior, attitudes and product usage. The answer: RFID (radio frequency identification) technology.... In an industry first, RFID enables the linking of all this product information with a specific consumer identified by key demographic and psychographic markers....Where once we collected purchase information, now we can correlate multiple points of consumer product purchase with consumption specifics such as the how, when and who of product use.[178]

Marketers aren't the only ones who want to watch what you do in your home. Enter again the health surveillance connection. Some have suggested that pill bottles in medicine cabinets be tagged with Auto-ID devices to allow doctors to remotely monitor patient compliance with prescriptions.[179]

While developers claim that Auto-ID technology will create "order and balance" in a chaotic world,[180] even the center's executive director, Kevin Ashton, acknowledges there's a "Brave New World" feel to the technology.[181] He admits, for example, that people might balk at the thought of police using Auto-ID to scan the contents of a car's trunk without needing to open it.[182] The Center's co-director, Sanjay E. Sarma, has already begun planning strategies to counter the public backlash he expects the system will encounter.[183]

Customers are dehumanized

[T]he consumer is therefore constantly constructed as an exterior object to be captured, studied, reduced and targeted by the operator, in other words, as the enemy of the intelligent machine.[184]
- John Goss, Marketing the New Marketing

What does all of this say about the marketing industry and its attitudes? In their frenzy to manipulate others, marketers have lost their awareness of their fellow human beings as equals, deserving of dignity and respect. Viewed through the distorted lens of loyalty marketing, customers cease to be people; they are transformed into rather stupid domestic animals or laboratory specimens, becoming inventory units to be studied, manipulated, controlled, and exploited to maximize their contribution to the bottom line. Any *feelings* the customer may express about this treatment are dispassionately observed and duly recorded to become fodder for even more analysis, which is then used to inform the next, more thorough iteration of persuasion and control.

While we may be "valued customers," our value is no more than that of chattel, since our true value — our *humanity* — is disregarded. Shopper cards play a key role in fostering this dehumanization in the minds of retailers and marketers. Once consumers are systematically numbered and recorded in the database, the supermarket can finally treat them like any other item in their inventory control system — as impersonal units to be numbered, cataloged, and tracked.

SECTION 4: WORKING TOWARD A SOLUTION

A national organization to oppose supermarket surveillance cards

When I first realized the long term implications of allowing our food purchases to be monitored and recorded, I created a website that grew into CASPIAN, Consumers Against Supermarket Privacy Invasion and Numbering (www.nocards.org). CASPIAN's mission is to educate consumers, condemn marketing practices that invade customers' privacy, and encourage privacy-conscious shopping habits across the retail spectrum. Today, CASPIAN's membership base spans the U.S.A. and our efforts have been featured by numerous media outlets including Kiplinger's Personal Finance magazine, Extra!, the Boston Globe, the Seattle Times, the major television networks, PBS, and local

radio, TV, and newspapers around the country.[185]

CASPIAN believes that individual consumers are ultimately responsible for protecting their own privacy, so we encourage shoppers to become informed, inform others, and "vote with their feet."[186] We also encourage peaceful protests against card programs and other intrusive retail surveillance schemes. We do not advocate legislative solutions to the card problem, having observed a disturbing trend in the past for "data protection laws" to put the data to be protected squarely into the hands of the government.[187]

A common sentiment expressed by new CASPIAN members is, "Thank goodness I found you; I thought I was the only person to feel this way!"[188] And indeed one of CASPIAN's key roles is to encourage privacy-conscious shoppers with the knowledge that they are not alone. Regrettably, many supermarket chains demoralize card opponents by pretending ignorance of the movement to oppose cards and failing to acknowledge the large volume of anti-card complaints they receive.[189]

Arguments against using "fake" or traded cards

Unfortunately, many shoppers think they have found a clever way to bypass the surveillance schemes at their local supermarkets by filling out shopper card applications under false names or trading their grocery cards with others.[190] Though the shopper may think he or she is pulling the wool over the supermarkets' eyes, these tactics actually play right into the marketers' hands.

In a brilliant counter-move, stores not only permit these practices, but may openly encourage them as a way to lull card opponents into participating in the system rather than fighting it. Stores know that the fake name "loophole" removes dissenters from the ranks of the opposition and adds them instead to the army of shoppers standing in line with cards — where they continue to pour money into the store's coffers. The anti-shopper-card movement loses some of its strongest potential allies this way, because shoppers who sign up under fake names or trade cards with others believe they've found "the solution" and no longer have to fight.

Though the choice of where to shop may feel like a decision that only affects the consumer, it is a two-way street. Money that leaves the shopper's wallet winds up in someone else's. By continuing to shop at card stores, consumers contribute their hard-earned grocery money to fund the retail surveillance agenda. They pay for publicists to fight people like me. They pay the salaries of the Catalina Marketing executives who create and peddle these schemes.[191] And they pay for psychologists to analyze the remaining holdouts to find ways to overcome their resistance.

Boycott cards now while there are still alternatives

[One] customer issue is the inertia of the typical consumer. While a segment will always be active and vigilant, the majority will pay less attention to encroachments on their right to privacy.[192]
- Frank Franzak, et al., Journal of Consumer Marketing

Find out just what any people will quietly submit to and you have found out the exact measure of injustice and wrong which will be imposed upon them, and these will continue till they are resisted with either words or blows, or both. The limits of tyrants are prescribed by the endurance of those whom they oppress.[193]
- Fredrick Douglass, Two Speeches

It is surprising that so many people cooperate with the retail surveillance agenda, considering how easy it is to resist. For most shoppers, resisting simply means driving a few extra minutes to a card-free supermarket and paying by cash instead of using a credit card. If everyone who opposed cards decided to shop elsewhere for even a few months, the card stores would soon feel the financial effects and the card programs would crumble.

The time to shop elsewhere is now, while alternatives are plentiful. Two of the nation's largest card-free grocery chains are currently test marketing cards (Albertson's in Dallas/Ft. Worth[194] and Winn-Dixie in Florida and Georgia[195]). If shoppers do not stand firm in boycotting these trials, eventually both chains may implement cards nationwide, leaving towns and cities all over the country stranded with few or no card-free shopping options left.

The longer consumers postpone taking action on the problem, the harder it will be to solve in the future. Eventually, the implementation of fingerprint readers in the supermarket coupled with Auto-ID technology may make the problem so enormous that few will have the strength to resist.

The tide is turning

The good news is that consumers appear to be growing wary of card-based surveillance. Stop & Shop's Curt Avallone revealed that acceptance levels for Stop & Shop's card have dropped from a high of 50% eight years ago to just 40% today.[196] He admits that "people are disappointed in the card and what we've been doing with it"[197] and acknowledges that privacy concerns have become a sticky issue for the company.[198]

American consumers may be poised to take back the ground they have lost. When Albertsons began test-marketing its card program in Texas last year, it was met with fierce opposition by CASPIAN-led shoppers who joined together in a boycott and mounted a peaceful protest against the store.[199] Virtually all of the major media in Dallas (television, newspaper, and radio) discussed the privacy implications of the card and informed shoppers of the movement to oppose it. The media coverage and boycott corresponded with a drop in Albertson's market share in the region.[200] Through continued pressure, CASPIAN hopes to encourage Albertsons to reconsider its plans to introduce the card

elsewhere.

A number of other supermarket chains have dismantled their card programs over the years in response to consumer concerns.[201] These include Raley's (rated America's #1 supermarket chain by Consumer Reports[202]), Wild Oats (the nation's third largest natural food chain by sales[203]), and the H.E.B. Grocery Company of San Antonio (recently called the "most impressive"[204] of U.S. grocery retailers).

Even Britain's fourth largest grocery retailer, Safeway (now unrelated to the U.S. chain of the same name), abandoned its card program in 2000 because of its enormous cost. When the chain re-channeled the approximately $70 million it had been spending annually on cards into lower overall prices,[205] its market share rose 5%.[206] "People don't think [the cards] give value. [But] they'll never get tired of great deals," explained Safeway's chief executive Carlos Criado-Perez.[207]

A message of hope

Though danger is on the horizon, consumers need not feel hopeless, outnumbered, or discouraged. The good news is that the corporations are dependent on their customers, not the other way around. As soon as large numbers of consumers begin to withhold their shopping dollars from stores that engage in shopper surveillance, stores will scramble to regain those dollars through more responsible practices. We must each make the decision to stop funding the beast.

SECTION 5: CONCLUSION

It's not too late to turn back

We all want progress . . . [but] if you're on the wrong road, progress means doing an about-turn and walking back to the right road; and in that case, the man who turns back soonest is the most progressive man... We are on the wrong road. And if that is so, we must go back. Going back is the quickest way on. [208]
- C.S. Lewis, Mere Christianity

Of the many reasons to oppose cards, the future is perhaps the most important. Should our children grow up trained to report their every move, activity, and purchase — even the contents of their every meal — to marketers and government officials? As a nation we must think twice about creating a society where everything we do is monitored, scrutinized, and observed by others. I believe that most Americans feel strongly enough about privacy and freedom to reject the surveillance model of society — and are uncomfortable with the direction we are headed.

The promoters of retail surveillance technology might better spend their time asking more fundamental questions about the societal implications of their work, rather than asking themselves how to convince the public to tolerate the all-encompassing surveillance their systems are likely to spawn.

Even today, supermarket cards have begun to serve a conditioning function to ease the public's concerns over other forms of intrusive registration and surveillance. Consumers' use of grocery cards and, by extension, their implied acceptance of the cards' data collection function, are pointed to as justification whenever more invasive schemes are proposed.

A recent UN report cited "the increasing data collection by the private sector" as possibly the most important factor influencing the public's willingness to surrender data to government entities.[209] The report mentions Catalina Marketing, which has collected billions of rows of data on American shoppers, saying, "the widespread public awareness of private sector profiling may act to actually reduce privacy and confidentiality concerns among the public, if they believe that all information about them is already known."[210]

Among other things, supermarket cards have been used to justify National ID.[211] Alan Simpson, Former Senate Majority Whip, testifying on National ID said, "Every time we try to do something in this area, it's filled with emotion, fear, guilt, and racism. You have to do something, and that something is not any more intrusive than what you get when you go into the [grocery] store and slide your [discount] card."[212]

Instead of using supermarket cards as justification for even more invasive surveillance, we need to remember that surveilling the food habits of millions of human beings is in and of itself tremendously invasive. The fact that large numbers of Americans scan a supermarket card on a regular basis does not detract from this reality.

The future is up to us

While surveillance should not be tolerated in any area of our lives, its application to something as physically intimate and essential for survival as food is particularly repugnant. As long as shoppers continue to allow their eating habits to be recorded, the danger will always remain that laws or political maneuvering will override their stores' privacy policies or ethical standards. The data that supermarkets have quietly collected for nearly a decade has become a tempting target for busybodies of all stripes.

There will always be those who believe the potential societal benefits of surveillance schemes outweigh the risks of abuse. However, though there is ample evidence that the supposed security "benefits" of mass surveillance are quite doubtful,[213] the risks of unchecked government control are very real and not to be discounted.[214] As the police and other agents of the state increasingly tap the power of the retail sector's growing arsenal of sophisticated surveillance technologies, we may soon find ourselves in the totalitarian nightmare described by George Orwell in *1984*. It is up to each of us to ensure that comprehensive, all-knowing surveillance systems are returned to the scrap heap of history's bad ideas before it is too late to turn back.

Even though most citizens are unaware of Auto-ID and plans for omniscient police and UN databases, virtually everyone has heard of the lowly supermarket card. And here,

finally, is one useful purpose cards can serve: as a wake up call to the public. Americans must take a second look at the cards in their wallets and on their key chains, recognizing that they represent only the most visible component of a massive push toward global surveillance being driven by the retail sector. Cards are just one symptom of an advancing disease that, left unchecked, will almost certainly prove fatal to privacy — and may ultimately threaten freedom itself.

Katherine Albrecht is the founder and director of Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN), a national grass-roots consumer group dedicated to fighting supermarket "loyalty" or frequent shopper cards. CASPIAN's efforts are dedicated to educating consumers, condemning marketing practices that invade customers' privacy, and encouraging privacy-conscious shopping habits across the retail spectrum. Formed in 1999, CASPIAN has since reached millions of American consumers with its pro-privacy message.

Katherine Albrecht holds a Master's degree in Education from Harvard University and a Bachelor's degree in International Marketing.

Appendix 1: Grocery Card Programs

This chart lists the card status of a number of chains owned by the ten largest grocery retailers based on 2001 sales

RANKING BY 2000 SALES[215]	COMPANY	CARD STATUS	PROGRAM NAME
1) $51b	THE KROGER COMPANY		
	• Kroger, Hilander, Owen's, Pay Less, Dillons, Gerbes	CARD	Plus Card
	• City Market	CARD	Value Card
	• King Soopers	CARD	SooperCard
	• Ralph's	CARD	Club Card
	• Fry's	CARD	VIP Card
	• Smith's	CARD	Fresh Values Rewards Card
	• Food 4 Less	NO CARD	Food 4 Less is a "no-frills" grocery store where shoppers bag their own groceries.
	• Fred Meyer	NO CARD	Kroger customer service representatives say that Fred Meyer may get a card program in late 2002.
	• Quality Food Centers (QFC)	CARD	Advantage Card
2) $38b	ALBERTSON'S INC.		
	• Albertson's	TESTING CARD	"Preferred Savings Card" introduced in Dallas/Ft. Worth, Texas November 2001
	• Acme	CARD	Super Card
	• Jewel	CARD	Preferred Card
3) $34b	SAFEWAY INC.		
	• Safeway	CARD	Club Card
	• Dominick's	CARD	Fresh Values Card
	• Pavilions	CARD	ValuePlus Card
	• Randall's	CARD	Remarkable Card
	• Tom Thumb	CARD	Rewards Card
	• Vons	CARD	VonsClub Card
4) $23b	AHOLD USA, INC.		
	• Bi-Lo, Giant, Tops	CARD	Bonuscard / Bonus Card
	• Stop & Shop	CARD	Stop & Shop Card
5) $20b	WAL-MART SUPERCENTERS	NO CARD	
6) $18b	SAM'S CLUB	MEMBER CARD	Membership card tracks purchases but there is no "two-tiered" pricing
7) $18b	COSTCO WHOLESALE GROUP	MEMBER CARD	Membership card tracks purchases but there is no "two-tiered" pricing
8) $15b	DELHAIZE AMERICA		
	• Food Lion	CARD	MVP Card
	• Kash n' Karry	CARD	Preferred Customer Club
	• Hannaford (Shop 'n Save)	NO CARD	
9) $15b	PUBLIX SUPER MARKETS, INC.	NO CARD	
10) $13b	WINN-DIXIE STORES, INC.	TESTING CARD	"Customer Reward Card" introduced in Florida and SE Georgia March 2002

continued from page 533
about being American. I do believe, however, that we can utilize many modern technologies in government and business as long as we fully appreciate and evaluate the larger stakes. There has been too much blind criticism and too much jerking of the knees on this subject. Government has a stake in both efficiency and privacy. We have large problems that need to be managed by modern technologies. But, government also has a stake in maintaining privacy. Meaningful privacy guarantees are necessary to ensure public confidence in government. After all, privacy is the foundation of the secret ballot, search and seizure protection, doctor-patient and lawyer-client privilege, and our whole concept of being a free and independent American.

Richard D. Lamm is Director of the Center for Public Policy & Contemporary Issues at the University of Denver. He is one of the new breed of policy analysts who argues that the challenge of the 21st Century is to meet new public needs by reconceptualizing much of what government does and how it does it. Lamm maintains we cannot retire the baby boomers under our current social systems, nor provide health care without rethinking the goals of medicine.

Lamm has always been in the forefront of political change. As a first year legislator, he drafted and succeeded in passing the nation's first liberalized abortion law. He was an early leader of the environmental movement. Reacting to the high cost of campaigning, he walked the state in his campaign for Governor of Colorado. Lamm was elected to three terms as Colorado's top elected official, and in serving as Governor from January 1975 and retiring in January 1987, he was the longest-serving Governor in Colorado's history to that date.

Lamm was selected as one of Time Magazine's "200 Young Leaders of America" in 1974, and won the Christian Science Monitor "Peace 2020" essay in 1985. In 1992, he was honored by the Denver Post and Historic Denver, Inc. as one of the "Colorado 100" - people who made significant contributions to Colorado and made lasting impressions on the state's history. He was Chairman of the Pew Health Professions Commission, and a public member of the Accreditation Council for Graduate Medical Education.

During 1996, Lamm appeared on virtually every national news program, including *Larry King Live* and *Inside Politics* (CNN), *Today* (NBC), *Meet the Press* (NBC), ABC's *Good Morning America*, *Lehrer NewsHour* (PBS), and CBS's *Face the Nation*. His editorials have appeared in the *San Francisco Chronicle*, *New York Times*, *Christian Science Monitor*, *Newsday*, *Boston Globe*, *Los Angeles Times*, and *Chicago Tribune*, as well as in a number of academic and medical journals. While Governor, Lamm wrote or co-authored six books: *A California Conspiracy*, with Arnold Grossman (St. Martin's Press, 1988); *Megatraumas: America in the Year 2000* (Houghton Mifflin Company, 1985); *The Immigration Time Bomb: The Fragmenting of America*, with Gary Imhoff (Dutton and Company, 1985); *1988*, with Arnie Grossman (St. Martin's Press, 1985); *Pioneers & Politicians*, with Duane A. Smith (Pruett Publishing Company, 1984); and *The Angry West*, with Michael McCarthy (Houghton Mifflin Company, 1982).

The Center for Public Policy & Contemporary Issues advances the University of Denver's commitment to the study and discussion of American society's most critical issues. Research produced by the Center is targeted at influential policy makers nationwide. The Center contributes to the national policy dialogue through an active program of conferences, seminars, courses, forums, and several monograph series. It also grants degrees in public policy through its Public Affairs Program, an interdisciplinary, honors-based program designed to create analytical skills that can be applied to public policy questions through courses involving virtually every major social issue.

continued from page 555

as well as the reach of their 'market.'[45]

In short, the court insisted on the ability of California employers to compete for employees nationwide irrespective of the costs incurred by non-California employers from abrogation of their non-competition agreements.

There are strong arguments for enforcing contracts choosing the law applicable to non-competition agreements. First, such agreements are likely to reflect the contracting parties' mutual interests. Second, enforcement allows firms to escape inefficient restrictions on contracting, particularly where states otherwise would be able to reach far outside their borders, as in *Hunter*. Third, enforcing agreements notifies parties what law will be applied to their contract, and therefore how to draft the contract, price its provisions and behave in accordance with the applicable law. Fourth, these contracts allow firms to impose the same rules with regard to all employees, even if they live in states with different rules on enforcement of non-competes. This may be significant where the firm must design company-wide rules and contracts relating to information dissemination, incentives, and basic structure of its employment relationships.[46] For example, a firm may want to make its compensation contracts contingent on compliance with the non-compete in order to discipline potential abuse of corporate information.

The problem with enforcing contractual choice is that it can allow an end-run around efficient state regulation. If state regulation of non-competes reduces externalities such as the efficiency of free-flowing information, it follows that these externalities will impede efficient contractual choice just as they do efficient non-competes.[47]

One way to accommodate arguments for and against enforcement is to enforce contractual choice of law except where a state whose law would apply in the absence of a choice of law clause specifically legislates against enforcement of the non-compete. This restriction has two components. First, it limits the reach of state restrictions on contractual choice. This focuses attention on the terms of the default choice-of-law rule. In contrast to the current multi-factor test, this rule should be designed to be as precise and predictable as possible. Predictability would maximize the parties' ability to exit from oppressive laws by avoiding regulating states, and would let the parties shape their conduct and contract with reference to the applicable law.[48] These considerations would, for example, usually preclude application of the law of a raiding employer's state where the firm is raiding employees of an out-of-state firm, as in *Hunter*.[49]

Second, the applicable state should be able to restrict contractual choice only by explicit legislative policy. This again reflects the need to facilitate contracting with reference to the applicable law. It also helps ensure popular support for any restrictions on contractual choice by making the restriction salient and thereby inviting active competition among interest groups.[50] This is not feasible where courts decide choice of law disputes *ex post* in specific cases.[51] This approach contrasts with the current emphasis on "fundamental policy" and a state's "interests," which make it uncertain which states' regulation will be applied to trump contractually selected law. The vagueness of these tests sometimes allows states to have it both ways, applying their laws to enforce contracts of local firms against out-of-state firms, as well as to trump contracts of out-of-state firms in favor of local firms.

Efficient enforcement of contractual choice of law consistent with the recommended rule may follow from the combined influence of several related contractual devices and legal rules. First, since results like that in *Hunter* are likely to be reached only by state courts in states with self-serving policies regarding non-competition agreements, the parties may be able to minimize these results through choice-of-forum or arbitration clauses that choose more contract-friendly adjudicators or jurisdictions. For example, in the *Hunter* situation, the parties might agree to have the case tried in Maryland. Although the employee may seek to avoid the effect of this clause by suing in California, a California state court may have some incentive to avoid having to decide the tricky choice-of-law issue by enforcing the choice-of-forum clause.[52] The Federal Arbitration Act may ensure enforcement of the arbitration clause if the transaction involves interstate commerce.[53]

Second, to the extent that courts do not enforce *ex ante* choice of forum clauses, the parties have significant leeway to ensure enforcement of their chosen law by choosing to litigate in a hospitable forum. For example, the employer can sue in the contractually selected state or in federal court to enforce the choice-of-law clause or to get a declaratory judgment that the contract is enforceable. Although federal courts apply local state law in diversity cases,[54] they may tend more than state courts to enforce contractual choice of law in marginal cases because they lack state judges' incentives to back the prerogatives of the local legislature.[55] In fact, a survey of approximately 20 years of decisions under the Restatement provisions quoted above showed that federal courts were approximately twice as likely to enforce contractual choice as state courts.[56] As one might expect, most cases involving enforcement of contractual choice of law have been decided in federal court.[57]

To be sure, the employee can play the same game and sue in a non-enforcing court to invalidate the agreement. Indeed, both games played out in *Hunter*, with the wronged employer suing and getting a judgment in Maryland, and the competing new employer suing in California.[58] The former employer was able to stay the California action pending completion of the Maryland action.[59] The California court noted that it was not determining the full

faith and credit effect of any judgment Hunter might obtain in Maryland.[60] Although the employer will not always succeed in this game, the prospect of competing judgments may be enough to persuade courts to enforce choice of forum clauses and eliminate any uncertainty about the forum.[61]

Third, even if the parties cannot control the forum, they may be able to structure their contracts to avoid application of regulating states' laws, or avoid contacts with those states that might justify application of those states' laws. In *Hunter*, for example, the raided employer could avoid subjecting its own activities to California law by not stationing employees with non-competes in California, instead working there through independent contractors.

Although none of these approaches helped Hunter avoid application of California law to the California firm that raided its employees, *Hunter* should be seen as an extreme case where Hunter was specifically concerned about being raided by the California firm. The application of California law there meant that the parties were at least treated symmetrically — that is, Hunter could not hide behind Maryland law while raiding the California firm under California law. Thus, the decision effectively preserves the viability of California law, which otherwise would have been threatened by one-sided application of the California regulation. Moreover, the quote from the opinion above makes clear that the court was specifically concerned about "virtual" or knowledge-based firms with no fixed location.[62] The court held that under its rule "it is plainly not sufficient simply to be employed by a California-based employer such as AGI, or to be treated as a California employee for tax and other legal purposes, if the employee is to perform services exclusively 'beyond the borders of California.'"[63]

In sum, this discussion raises two general points. First, the existence of an externality or spillover problem with state regulation is based on the same factors that give rise to jurisdictional choice. Second, jurisdictional choice supports enforcement of contracts from an interstate perspective even if these contracts do not seem to be enforceable from an intrastate perspective.

III. PROTECTING EMPLOYEES' PRIVACY

This Part discusses the issues regarding privacy of employees' information. As discussed in Part I, above, the employers' need for this information is a function of the inherent characteristics of the firm — namely, the team production problem, which triggers a need for monitoring. As discussed in subpart A, this need for information may collide with employees' desire for and expectation of privacy. As discussed in subpart B, these problems theoretically may be resolved by contracts between employers and employees, although these contracts may not always be enforced. Subpart C shows that, as with privacy of employers' information, contracting is a viable solution from an interstate perspective.

A. GENERAL POLICY CONSIDERATIONS

Employees have an interest in protecting against employers' intrusions on their private space. Conversely, employers have a legitimate interest in monitoring employees, including preventing abuse of employers' confidential information and detecting crimes and other wrongs committed by employees. Enforcing contracts regarding these matters increases social wealth by encouraging efficient employment arrangements.

Arguments concerning the employee's privacy draw on the economic theories of privacy and information costs. Protecting employees' privacy increases employers' information costs, thereby making the employment market less efficient and increasing agency costs.[64] This may both reduce social wealth and redistribute wealth from "good" to "bad" employees. Among other effects, the inability to monitor may decrease employers' ability to protect against employee abuse of trade secrets, thereby increasing the firm's need to rely on non-competition agreements.

On the other hand, protecting employees' privacy to some extent may be efficient. Employees may derive utility from protecting their personal space.[65] This protection may enable them to better realize their private preferences, such as sexual orientation, or to avoid misinterpretation of isolated bits of information, such as out of context statements.[66] If legal protection is inadequate, employees may have to invest in self-protection, which would force greater expenditures on reputation than would be the case under an efficient legal rule.[67] Even if

Larry Ribstein

I am currently Foundation Professor of Law, George Mason University School of Law. Effective in May I will be the Richard W. and Marie L. Corman Professor of Law, University of Illinois College of Law. I am the author or co-author of six books and more than 80 articles on corporations, securities law, partnerships, conflict of laws, professional responsibility, bankruptcy, constitutional law and other topics. My interest in privacy law stems from my work on contractual choice of law. See especially my written articles with Professor Bruce Kobayashi: A Recipe for Cookies: State Regulation of Consumer Marketing Information, Federalism Project Roundtable Paper Series, No. 1, May 2001, available at http://www.federalismproject.org/conlaw/ecommerce/cookies.pdf, and State Regulation of Electronic Commerce, George Mason Law & Economics Working Paper 01-31, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=294466, forthcoming Emory Law Journal.

the particular basis for employee utility cannot be identified, the test arguably should be subjective rather than objective.[68]

B. ENFORCING CONTRACTS: INTRASTATE PERSPECTIVE

As with non-competition agreements and protecting against abuse of trade secrets, enforcing contracts can lead to the optimal rules for particular situations. Employers arguably would not seek excessively to invade employees' privacy because they will have to pay employees to succumb to this surveillance. Employers seemingly would have little interest in generating irrelevant or inaccurate information about employees. The courts have, in fact, enforced employer surveillance where it has a business purpose.[69]

An initial contracting issue regarding employer surveillance concerns the appropriate default rule.[70] In the consumer information context, a default rule favoring privacy may be appropriate because the merchant arguably has a better idea than the consumer of the value of the information.[71] However, in the employment context the default rule arguably should favor surveillance because the employee has a better idea of the negative information that the employer might discover. The default rule, of course, would not be expected to prefer unlimited surveillance because this would impose high costs on employees without enough benefit for employers to justify sufficient wage adjustments to cover these costs. This supports the general requirement of surveillance being reasonably related to the employer's business purpose.[72]

But it is not feasible to design a default rule that adequately covers all situations because such a rule would have to be too narrow or too broad. A default rule based on a legitimate business purpose might cover all employers and employees but is too broad to provide adequate guidance in specific situations. Thus, the parties will need to rely on specific contracts.

Nevertheless, there is significant recent authority against enforcement of contracts. *Cramer v. Consolidated Freightways, Inc.*[73] held that a collective bargaining agreement that arguably allowed video surveillance behind two-way bathroom mirrors could not supersede what the court deemed to be the mandatory provisions of state privacy law. The judge who wrote the en banc decision expressed a concern in his panel dissent about Orwellian intrusions.[74] This makes little sense assuming that the employees consented to the intrusion in the collective bargaining agreement, as a dissenter to the en banc decision argued.[75] Moreover, the Orwellian argument suggests the implementation of a federal policy, which is inappropriate in the context of purportedly interpreting a state restriction on intrusions. In any event, this case indicates that, as with non-competition agreements, employers apparently cannot rely on contracts with employees, at least viewed from the intrastate perspective.

C. ENFORCING CONTRACTS: INTERSTATE PERSPECTIVE

The interstate perspective on employee privacy contracts differs from that in the non-competition setting because employee privacy agreements are more likely to be anchored in a single state. The non-compete context involves the competing interests of states where raiding and raided firms are located. With respect to employee privacy, on the other hand, the primary interests are focused in a single state, where the employee whose interests are at stake is located. Thus, there are less likely to be regulatory spillovers in this context. In other words, the employers' ability to select jurisdictions in which they locate may be enough to internalize regulatory costs and benefits in regulating jurisdictions. At the same time, employers' ability to choose the applicable jurisdiction is likely to be more limited. Under the Restatement, courts are unlikely to enforce the contractual choice of a jurisdiction other than where the invaded employee works to trump the "fundamental" regulatory policy of the state of employment.

Despite these considerations, employee privacy has a real interstate dimension. Multi-state employers are likely to want to choose a single policy for monitoring employees. The problem is even more serious for "virtual" companies like those in *Hunter*, where employees live and work in several states and the employers' privacy policies relate to, for example, networked computers.

Although default choice of law rules raise fewer problems in this context than in the non-compete context, choice-of-law clauses may be useful to enable employers to avoid oppressive states without having to avoid hiring in those states. Again, these clauses should be enforceable unless the "default" state specifically legislates against them. However, the *Consolidated Freightways* case indicates that contractual choice may not always be enforceable. The court refused to enforce the employer's effective choice of federal labor law against a supposed state mandatory privacy rule.

As with non-competes, employers may be able to enforce jurisdictional choice by choosing the forum in which they litigate. To be sure, courts with strong pro-privacy policies may be unwilling to enforce contractual choice of forum. But an employer may be able to choose *ex post* to litigate the enforceability of the contract in a state in which it does substantial business.

IV. CONCLUDING REMARKS

Traditional economic theories of the firm intersect with modern concerns about privacy. The firm is about ensuring the free flow of information, while privacy policies attempt to intersect these flows. These competing concerns generally should be resolved by contracts. In some cases state regulation is appropriate. Jurisdictional choice in our federal system serves to discipline excessive state regulation.

continued from page 555

The government argued that the information sought was only a business record, that they could not care less what the suspect read, and that it could be used to establish a state of mind. They contended that a book purchase is no different than a hardware purchase record when it comes to a criminal investigation. I fundamentally disagree.

Entering books into evidence that are found at a crime scene is one thing. Seeking out who bought what from a bookstore is another. Purchasing, borrowing or "reading a book is not a crime."[4] To edge closer to using a customer's book purchase records as an acceptable way of determining criminal behavior is disquieting at best, and downright frightening at worst. Whether as a reporter seeking information, an iconoclast harmlessly pushing the envelope of societal acceptance, or even someone potentially contemplating illegal behavior, reading is not a crime.

The Tattered Cover is appreciative of the thoughtful consideration Judge Phillips gave to his decision. While we are in disagreement with part of that decision, we could not agree more with the chilling effect that he addressed when speech is thwarted. Judge Philips stated: "It is clear that the First Amendment of the Constitution protects the right to receive information and ideas, regardless of social worth, and to receive such information without government intrusion or observation." [5] He went on to quote the late Supreme Court Justice Douglas on the necessity for such protection:

> Once the government can demand of a publisher the names of the purchasers of his publications, the free press as we know it disappears. Then the spectre of a government agent will look over the shoulder of everyone who reads. The purchase of a book or pamphlet today may result in a subpoena tomorrow. Fear of criticism goes with every person into the bookstall. The subtle, imponderable pressures of the orthodox lay hold. Some will fear to read what is unpopular, what the powers-that-be dislike. When the light of publicity may reach any student, any teacher, inquiry will be discouraged. The books and pamphlets that are critical of the administration, that preach an unpopular policy in domestic or foreign affairs, that are in disrepute in the orthodox school of thought will be suspect and subject to investigation. The press and its readers will pay a heavy price in harassment. But that will be minor in comparison with the menace of the shadow which government will cast over literature that does not follow the dominant party line. If the lady from Toledo can be required to disclose what she read yesterday and what she will read tomorrow, fear will take the place of freedom in the libraries, bookstores, and homes of the land. Through the harassment of hearings, investigation, reports, and subpoenas government will hold a club over speech and over the press.[6]

When they heard about this case, hundreds of our customers took the time to call or write to us in support of our stand, underscoring this message and raising their own concerns about privacy and the chilling effect on the First Amendment of requiring bookstores to turn over to the police information regarding the purchases of customers.

continued from page 525

When the trial court held that officers could seize the record of the purchase that was delivered in the mailer, but denied them the right to confiscate other records of the same customer, the Tattered Cover appealed.

In its decision, the Colorado Supreme Court explained "how the First Amendment and Article II, Section 10 of the Colorado Constitution safeguard the right of the public to buy and read books anonymously, free from governmental intrusion."[5] Accordingly, the court developed a test for whether law enforcement officials may seek to seize the book purchase records of an innocent, third-party bookstore in order to gather evidence against a customer. The test requires the government to demonstrate a compelling need for the information sought. "The court must then balance the law enforcement officials' need for the bookstore record against the harm caused to constitutional interests by execution of the search warrant."[6] The court also held that "an innocent, third-party bookstore must be afforded an opportunity for a hearing prior to the execution of any search warrant that seeks to obtain its customers' book-purchasing records."[7] In this hearing, the court is to apply the test created by the Colorado Supreme Court.

In applying this test to the Tattered Cover search warrant, the court looked at the government's three justifications for wanting the record of the suspect's purchase: (1) to prove that the suspect had the necessary mens rea to be prosecuted for the manufacture of methamphetamine, (2) to prove that the suspect lived in the bedroom where the meth lab and books were found and (3) to connect the suspect to the crime. Analyzing each one separately, the court held that the government showed no sufficiently compelling interest to outweigh the potential chilling effect on the right to buy books anonymously.

continued from page 555

The government argued that the information sought was only a business record, that they could not care less what the suspect read, and that it could be used to establish a state of mind. They contended that a book purchase is no different than a hardware purchase record when it comes to a criminal investigation. I fundamentally disagree.

Entering books into evidence that are found at a crime scene is one thing. Seeking out who bought what from a bookstore is another. Purchasing, borrowing or "reading a book is not a crime."[4] To edge closer to using a customer's book purchase records as an acceptable way of determining criminal behavior is disquieting at best, and downright frightening at worst. Whether as a reporter seeking information, an iconoclast harmlessly pushing the envelope of societal acceptance, or even someone potentially contemplating illegal behavior, reading is not a crime.

The Tattered Cover is appreciative of the thoughtful consideration Judge Phillips gave to his decision. While we are in disagreement with part of that decision, we could not agree more with the chilling effect that he addressed when speech is thwarted. Judge Philips stated: "It is clear that the First Amendment of the Constitution protects the right to receive information and ideas, regardless of social worth, and to receive such information without government intrusion or observation." [5] He went on to quote the late Supreme Court Justice Douglas on the necessity for such protection:

> Once the government can demand of a publisher the names of the purchasers of his publications, the free press as we know it disappears. Then the spectre of a government agent will look over the shoulder of everyone who reads. The purchase of a book or pamphlet today may result in a subpoena tomorrow. Fear of criticism goes with every person into the bookstall. The subtle, imponderable pressures of the orthodox lay hold. Some will fear to read what is unpopular, what the powers-that-be dislike. When the light of publicity may reach any student, any teacher, inquiry will be discouraged. The books and pamphlets that are critical of the administration, that preach an unpopular policy in domestic or foreign affairs, that are in disrepute in the orthodox school of thought will be suspect and subject to investigation. The press and its readers will pay a heavy price in harassment. But that will be minor in comparison with the menace of the shadow which government will cast over literature that does not follow the dominant party line. If the lady from Toledo can be required to disclose what she read yesterday and what she will read tomorrow, fear will take the place of freedom in the libraries, bookstores, and homes of the land. Through the harassment of hearings, investigation, reports, and subpoenas government will hold a club over speech and over the press.[6]

When they heard about this case, hundreds of our customers took the time to call or write to us in support of our stand, underscoring this message and raising their own concerns about privacy and the chilling effect on the First Amendment of requiring bookstores to turn over to the police information regarding the purchases of customers.

continued from page 525

When the trial court held that officers could seize the record of the purchase that was delivered in the mailer, but denied them the right to confiscate other records of the same customer, the Tattered Cover appealed.

In its decision, the Colorado Supreme Court explained "how the First Amendment and Article II, Section 10 of the Colorado Constitution safeguard the right of the public to buy and read books anonymously, free from governmental intrusion."[5] Accordingly, the court developed a test for whether law enforcement officials may seek to seize the book purchase records of an innocent, third-party bookstore in order to gather evidence against a customer. The test requires the government to demonstrate a compelling need for the information sought. "The court must then balance the law enforcement officials' need for the bookstore record against the harm caused to constitutional interests by execution of the search warrant."[6] The court also held that "an innocent, third-party bookstore must be afforded an opportunity for a hearing prior to the execution of any search warrant that seeks to obtain its customers' book-purchasing records."[7] In this hearing, the court is to apply the test created by the Colorado Supreme Court.

In applying this test to the Tattered Cover search warrant, the court looked at the government's three justifications for wanting the record of the suspect's purchase: (1) to prove that the suspect had the necessary mens rea to be prosecuted for the manufacture of methamphetamine, (2) to prove that the suspect lived in the bedroom where the meth lab and books were found and (3) to connect the suspect to the crime. Analyzing each one separately, the court held that the government showed no sufficiently compelling interest to outweigh the potential chilling effect on the right to buy books anonymously.

continued from page 554
people before and after me. A single individual cannot appreciate the full effect of widespread personal searches of everyday American travelers.

In contrast, the security benefits that appear to flow from the searches seem quite tangible. I board the plane with the knowledge that I pose no risk, and the belief that those around me pose no risk either, since they all endured the same scrutiny as I did. Then, after the flight goes smoothly, the safe landing reinforces the notion that security measures increase my safety. Of course, the many things that I failed to perceive are precisely the things that would undermine my confidence in security measures. For example, I may not have realized that the metal detector through which my fellow passengers and I passed had been inadvertently unplugged.[62] I may not have noticed one of my fellow passengers boarding the plane despite the fact that his driver's license did not match the name on his ticket.[63] Nor might I understand that such oversights are inevitable in passenger checks and baggage scans, because the "signal rate" - the frequency with which terrorists or impostors appear at the gate or weapons appear in the baggage - is so low.[64] Instead, I see only the safe result, which confirms my perception that security measures produce tangible benefits, or more specifically, that they avert tangible harms.

The distortion of individual perception in favor of security is obviously heightened in the wake of September 11. In today's climate, with physical and emotional scars from terrorist attacks still present on the landscape and in our lives, the perceived tangible benefits of security measures are magnified in the eyes of many. For that reason, we should not be surprised at the surface appeal of suggesting that we sacrifice "a little " privacy to preserve the tangible benefits of security. An important task for privacy advocates is to focus attention on how even seemingly limited intrusions on privacy can have consequences that reach far beyond the limited context in which they are proposed.

III. REVEALING THE TANGIBLE AS INTANGIBLE

Finally, I suggest that the tangible-versus-intangible framework is misleading. Measures alleged to yield tangible security benefits in fact serve many intangible purposes. Admittedly, in the wake of September 11, it is difficult to imagine a more tangible concern than the destructive effects of a terrorist attack. Many responses to these attacks, however, are not merely aimed at preventing such tangible harms. Instead, they serve in large measure to preserve merely the *perception* of security - the intangible notion that our government can, in fact, protect us from terrorism.

Jeffrey Rosen's investigation of Britain's experience with terrorism and video surveillance illustrates how security measures can serve predominantly intangible concerns.[65] In the wake of two IRA bombings in London's financial district, the government responded by installing surveillance cameras at the city's entry points.[66] Fear of terrorism continued, and the cameras - closed circuit TV, or "CCTV" - multiplied beyond anyone's expectations, both in London and throughout Britain.[67] Under Prime Minister John Major, the government devoted "more than three-quarters of its crime-prevention budget to encourage local authorities to install CCTV."[68] "[B]y 1998, 440 city centers" had surveillance camera networks.[69] Rosen's report estimates that "there are 2.5 million surveillance cameras in Britain," and that 300 different cameras photograph the average Briton every day.[70]

How many terrorists has Britain caught using this pervasive surveillance network? None.[71] "Although the cameras in Britain were initially justified as a way of combating terrorism, they soon came to serve a very different function. The cameras are designed not to produce arrests but to make people feel that they are being watched at all times."[72] And the people monitoring the cameras are most likely to focus on unconventional behavior in public, young men (especially if they are dark skinned), and attractive young women.[73] Cameras in London are most productive tracking "car thieves and traffic offenders. 'The technology here is geared up to terrorism,'" said London's press officer.[74] "'The fact that we're getting ordinary people - burglars stealing cars - as a result of it is sort of a bonus.'"[75] But there is no evidence that the cameras have prevented terrorism or other serious crime.[76]

The national ID card debate offers another timely illustration of the intangible nature of security concerns. Despite all best intentions, a national ID card will not prevent terrorism. Most countries have national ID cards or ID numbers,[77] and yet terrorism is a problem across the globe. September 11 hijacker Khalid Al-Midhar was on the INS's "watch list" of potential terrorists for nearly a year before the attacks, yet he boarded one of the hijacked flights using a ticket he bought in his own name.[78] Seven of the hijackers obtained fraudulent IDs from the State of Virginia.[79] Even more disturbingly, the INS recently notified a Florida flight school that it had approved student visas for Mohamet Atta and Marwan Alshehhi - six months *after* Atta and Alshehhi carried out the September 11 attacks, and in the midst of one of the most important and publicized law enforcement investigations in history.[80] Moreover, at Boston's Logan Airport, from which one of the September 11 flights originated, a man recently passed through two airport security checkpoints despite the fact that the name on his government-issued ID did not match the name on his ticket.[81]

Nonetheless, in the wake of the attacks, the American public threw its support behind a national ID card. Seventy percent of respondents to a Pew Research Center poll supported a "must carry" card - a card that the government would require us to carry on our person at all times and "show a police officer on request."[82] Perhaps most disturbingly, 49% of respondents to a CNN/USA Today/Gallup poll supported a

special national ID card that only Arab-Americans would be required to carry.[83]

Now, did the public suddenly review empirical evidence suggesting that national ID cards prevent terrorism? Certainly not. This was a reflexive response to the perception of vulnerability. The public needed to believe that there was something the government could do to prevent this type of attack. In the wake of September 11, fear and self-delusion are empowered to drive the debate over security proposals. Larry Ellison claims that people need not give up their privacy, only their "illusions" of privacy.[84] In the privacy-versus-security debate, however, privacy advocates often find themselves opposing efforts to preserve the mere illusion of security.

It is not enough, however, to point out the intangible nature of the security interest. That alone is unlikely to change the debate, precisely because people want, at some level, to believe that government can protect them against foreign threats. Government, too, has an essential interest in preserving this perception.

Accordingly, privacy advocates must also identify the tangible effects of preserving privacy against government intrusion. Speaking to a class at Harvard's John F. Kennedy School of Government in the fall of 2000, Simson Garfinkel said that privacy advocates need to show "where the bodies are buried."[85] I take him to mean that privacy advocates will make relatively little progress until they can show specific, tangible harms flowing from intrusions on privacy. His comment recognizes the tangible-versus-intangible perception that privacy advocates often confront.

Garfinkel's point finds support in the patchwork of privacy laws on the books today. In the few areas where we have found metaphorical "buried bodies," Congress has offered a healthy measure of privacy protection, albeit in the most narrow of circumstances. For example, Congress passed the Driver's Privacy Protection Act in the wake of the 1989 stalking and murder of actress Rebecca Schaeffer by a deranged fan who found her address through the department of motor vehicles.[86] Similarly, Congress passed the Video Privacy Protection Act after Judge Robert Bork's confirmation hearings, during which a *Washington Times* reporter shamelessly obtained copies of Judge Bork's video store rental records.[87]

Privacy advocates, then, must emphasize the tangible consequences of what some would dismiss as intangible aspects of privacy - those related to autonomy, to freedom of association and expression, and to personal and political identity. Joanna Malamud Smith notes that systematic deprivation of privacy by government is a hallmark of oppressive, totalitarian regimes.[88] Describing abuses in Nazi-occupied France, cold war East Germany, and the Soviet Union, Smith observes that:

> Constantly spying and then confronting people with what are often petty transgressions is a way of maintaining social control and unnerving and disempowering opposition . . . . [E]ven when one shakes real pursuers, it is often hard to rid oneself of the feeling of being watched - which is why surveillance is an extremely powerful way to control people.[89]

Smith quotes a memoir of a woman who lived under Stalinism: "'An existence like this leaves its mark. We all became slightly unbalanced mentally - not exactly ill, but not normal either: suspicious, mendacious, confused and inhibited in our speech . . . .'"[90] Such campaigns are nothing less than state-run terrorism.[91] Viewed from this perspective, privacy seems less an intangible abstraction than it does an instrumental value that produces tangible effects essential to a free citizenry.

Nor are deliberate assaults on privacy confined to totalitarian states. Smith also notes that the U.S. government has spied on dissenters such as Emma Goldman, the Wobblies, Malcolm X, and Martin Luther King, Jr.[92] Smith recounts the FBI's attempts to force King to commit suicide by sending him and his wife videotapes of King's sexual infidelities.[93] "Along with the videos, King received an anonymous letter. Knowing that he had attempted suicide as a twelve-year-old child, the writer, an FBI agent, encouraged King to end his life."[94] J. Edgar Hoover used the FBI's surveillance capabilities for his personal gain. One Hoover biographer tells the story of a magazine publisher who was planning an exposé on Hoover and the FBI.[95] "Hoover struck first, viciously. Favored newspaper contacts all over the country received a plain brown envelope with no return address. Inside was a packet of photographs showing the publisher's wife engaged in fellatio with her black chauffeur."[96] Thus, invasions of privacy empower the invader to control information and quell dissent.

IV. CONCLUSION

Today, police in Washington, D.C. are building a centralized network of surveillance cameras that will blanket the District of Columbia.[97] This unprecedented initiative operates within the cryptically named "Synchronized Operations Command Complex" (the "SOCC").[98] In the SOCC's Joint Operation Command Center, fifty workers monitor a wall of video screens hooked up to surveillance cameras.[99] The network already includes 200 cameras in public schools.[100] The SOCC will soon add another 200 in subways and parks.[101] It will also link the video from surveillance cameras that monitor intersections for drivers who run red lights, and from private cameras in banks, retail stores, hotels, and apartment buildings.[102] According to the director of the project, "I don't think there's really a limit on the

feeds it can take. We're trying to build . . . the capability to tap into not only video but databases and systems across the region."[103]

> A man living under a similar surveillance network in Britain observed: I am gay and I might want to kiss my boyfriend in Victoria Square at 2 in the morning. I would not kiss my boyfriend now. I am aware that it has altered the way I might behave. Something like that might be regarded as an offense against public decency.[104]

Despite this, the man maintains that "the benefits of the cameras outweighed the costs, because 'thousands of people *feel* safer.'"[105] As William Safire asks: "Is this the kind of world we want?"[106]

Policymakers are now deciding the fate of the D.C. video surveillance network, in addition to countless other security measures. If they accept uncritically the tangible-versus-intangible framework, their decision may be foreordained. The framework suggests a simple question: Which is more costly - the destruction from a terrorist attack on our capitol, or the discomfort that a commuter, tourist, or student might feel when passing innocently before a surveillance camera?

This essay has tried to illuminate what really lies on either side of the scale. First, the framework's short-term temporal focus necessarily excludes the future uses of such a surveillance network. Even today, the project is considering linking not only surveillance cameras, but also "databases and systems across the region."[107] The potential uses of centralized video surveillance and databases are unlimited, as are the long-term privacy intrusions of such expanded uses.

Second, the factual context in which the question is posed necessarily suggests the answer. We are left to imagine a known terrorist riding the Metro or walking across the Capitol Mall en route to his target. Even if one understands as a conceptual matter that the privacy consequences of pervasive surveillance will be widespread, it is difficult to measure such seemingly intangible harms against the prospect of another devastating terrorist attack. To accept the limited context in which the framework places the issue is to determine the outcome of the decision.

Finally, even if the surveillance system employed facial recognition technology that was 100% accurate - an extremely unlikely possibility[108] - it could not prevent terrorist attacks. Only two of the nineteen September 11 hijackers were on the terrorist watch list; the rest were unknown to intelligence or law enforcement officials before the attacks.[109] To catch even those two with facial recognition technology, the government would have needed not only their names, but also digital images of their faces. Like the pervasive surveillance network in Britain, centralized surveillance in D.C. would be better suited to making people *feel* safe rather than actually stopping terrorists.

So the question that policymakers must in fact decide is far more complex than the tangible-versus-intangible framework would suggest. The security side of the scale is much less substantial than many would suspect, because it is both empirically suspect and comprised in large part of mere *perceptions* of security. Similarly, the privacy side is weightier than the framework would admit, because it includes the long-term effects that unintended consequences will have on privacy, and because it considers the effect that security measures will have on the entire community, rather than on a single individual passing a checkpoint. Moreover, the privacy side of the scale holds far more than mere abstractions. Instead, intrusions on privacy can change behavior, control information, and deter political and cultural dissent. This more comprehensive way of approaching the security-versus-privacy debate makes decision-makers far more likely to protect privacy.

In an important address to the nation, President Bush warned, "Freedom and fear are at war."[110] In that context, Bush equated freedom with America, and fear with the Taliban and Al Qaeda. In the aftermath of September 11, however, privacy values are safeguarding our freedom, while some security proposals seek mainly to alleviate our fear. Freedom and fear are indeed at war. Let us not sacrifice the former by indulging the latter.

The author is a Climenko/Thayer Lecturer on Law at Harvard Law School. Before joining Harvard, he taught as an Adjunct Professor at Boston College Law School, and practiced in the litigation department of the Boston law firm Bingham Dana. The ideas in Part I of this essay are drawn substantially from the author's forthcoming article, Reasonable Expectations and the Erosion of Privacy, 39 SAN DIEGO L. REV. (forthcoming 2002). The author is grateful for the comments of Richard Sobel, and for the extensive contributions of Lawrence Friedman. The author also thanks Tanya Thiessen and the Denver University Law Review for organizing this important Symposium.

continued from page 553
been in regular public use at the time that it was used to scan Kyllo's home, Kyllo's failure to take precautions against the device would be proof of his lack of a reasonable expectation of privacy in the heat coming off his house. Just as Ciraolo's case would have come out very differently 100 years ago (when airplanes were unknown) than today, so Kyllo's case might come out very differently 10 years from now when the use of thermal imaging technology becomes better known to the public.

This leads me back to my original thesis. What all of these cases demonstrate is that if an individual has allowed private actors to look into areas that would otherwise be private, he has invited the government in as well. Even if others were invited in for a narrow and specific purpose, the individual has run the risk that her trust will be abused. Similarly, even if one has behaved passively, not conveying or showing information to anyone, but simply failing to take precautions against intrusions by others, she has likely lost an expectation of privacy in the area she has carelessly exposed. Furthermore, precautions that might be sufficient to protect an expectation of privacy in one era — for example, protecting the four sides but not the roof of a shed from public view — will be deemed insufficient in another.

This is why I argue that privacy vis-à-vis private actors is crucial in defining the contours of Fourth Amendment law. In recent years, technological changes have made surveillance easier, cheaper, and much more pervasive. For example, a recent report indicated that more than one third of the United States work force is subject to workplace monitoring of their web use and e-mails.[29] Microsoft, which makes the vast majority of the operating systems in the world, placed code in its Windows XP operating system that records the titles of DVDs watched on an individual's computer and transmits this information back to the company "in a way that allows the company to match individuals with their music and movie choices."[30] Night vision goggles, long-distance microphones, and personal tracking devices can all be purchased by members of the public on the Internet for under $1,000.[31] While it was once possible to defeat nosy neighbors, prying employers, or avaricious marketers simply by shutting the door and keeping your voice down, such precautions are simply insufficient today.

As these examples illustrate and as many have written, much of this new surveillance technology has been adopted not by the government,[32] but by the so-called Little Brothers — advertisers, employers and other private snoops, who many argue pose a greater threat to privacy than is posed by government's Big Brother.[33] What has been less understood, however, is that the more power the Little Brothers gain, the more power Big Brother gains. Every time a Little Brother gains access to an area previously forbidden to him, it becomes easier for Big Brother to later claim that a defendant's reasonable expectation of privacy has been lost.

Thus, those of us interested in the amount of government intervention into our private lives should be deeply concerned with the extent to which others are allowed in. If we allow our employers to read our e-mails, we cannot very well complain when the government does so as well. If we allow our software companies to learn what movies we are watching, we cannot complain when the government does so as well. Yet we cannot do anything to eliminate the technologies that are making privacy more fleeting; technological fixes — encryption, wiretap blocking, etc. — will only lead to new and different technological responses by those who would invade our privacy. What is needed is a legal response, one that makes actionable the use of technology by private actors to obtain information that an individual has taken steps to keep private.

If it is a violation of statute for private actors to gain access to information in which an individual has a reasonable expectation of privacy, if those whose privacy has been invaded can bring a private cause of action akin to trespass against those who have invaded their privacy, then privacy can be preserved even in the face of technological change. Just as the possibility that private actors might break into your house and rifle through your things does not allow the government to freely break in and snoop around, so the tortious privacy invasion of a third party will not give the government carte blanche to snoop. So long as third party privacy invasions violate no laws, however, they will only embolden those in government who seek greater access to private information and will make it more difficult for any of us to claim that we should be protected from government attempts to get at this information

The current war against terrorism has energized civil liberties groups to respond to governmental attempts to extend surveillance of citizens and non-citizens alike. Of course, these attempts to control the worst excesses of government are laudable. But if civil libertarians wait until the government acts to invade privacy, they will have lost the battle before it has even begun.

Sam Kamin is an assistant professor of law at the University of Denver where he teaches Criminal Law, Criminal Procedure, and the Death Penalty. He is currently completing a book on the death penalty decisions of the California Supreme Court.

continued from page 516
monitoring policy, the employee consents to the employer's monitoring of the content of all electronic communications sent, received, or stored by the system;

5. When using the electronic communications system, employees should always keep in mind that others may view their communications, therefore employees should use discretion when sending e-mail and making Web visits;

6. Employees are not authorized to use any computer password unless the password is revealed to the employer;

7. Personal use of the employer's electronic communications system is not permitted;

8. The following are impermissible uses of the system: transmission of sexually oriented or ethnically derogatory materials, unauthorized distribution of trade secrets or confidential information, and unauthorized copying of copyrighted material;

9. Any violation of the policy may subject the employee to discipline, up through and including termination;

A different electronic monitoring policy should be put in place by employers with less concern about potential abuse and a philosophy that their corporate mission will benefit from a workforce who can communicate freely by e-mail or over the Internet. This type of policy would guarantee the privacy of certain communications while preserving the employer's ability to police the system and to punish abusers. A policy embodying this approach might include the following elements:

1. The types of personal uses that are permissible and impermissible;

2. The amount of personal time allowed;

3. The time of day that personal use is permitted;

4. That permissible, personal e-mail and Internet use will not be monitored absent justification for doing so;

5. The security measures that will be taken to protect the privacy of personal e-mail and Internet use;

6. An explanation of the type of monitoring technology used to prevent impermissible personal use;

7. How frequently employees will be monitored;

8. The consequences of violating the policy.

There is one caveat for an employer who opts for this "privacy-as-a-benefit" approach. A failure to honor the policy might open the employer to liability for tortiously intruding upon the private space created by the employer or for breach of an implied contract.

Regardless of the type of policy the employer decides to adopt, a document retention/destruction policy should accompany any electronic monitoring policy. The former policy should be designed to assist the employer in managing the enormous quantity of information stored in its computer systems. At the same time, this policy should reduce the cost of responding to "electronic discovery" and reduce the risk that a "smoking-gun" e-mail will remain stored on the employer's system. The policy should address the following:

1. Classifications of data compatible with search capabilities;

2. Segregation of privileged communications and trade secrets;

3. The period for data retention, bearing in mind the type of data in question and any applicable legal requirements;

4. Strict limits on the retention of personal e-mail;

5. Application of the policy to all corporate computers (e.g., local, network, and back-up storage) and to computers of employees leaving the company.

Document destruction, no matter how well intentioned, almost inevitably will spur allegations of bad faith when litigation does arise. To deter such allegations, the policy should be developed and implemented long before litigation is on the horizon. In addition, the employer should maintain all documents bearing upon the creation and implementation of the policy. Finally, the policy should be consistently enforced, and suspended and reviewed when litigation is imminent.

Conclusion

The American workforce continues to use a growing array of communications tools to the benefit of employers. Some of these tools, like e-mail and the Internet, contemporaneously create unprecedented risks for employers. The existing statutory regime and accompanying judicial construction impose few limits on workplace surveillance of e-mail and Internet use. Nonetheless, employers should avoid the temptation of spying on their employees without notice. Surreptitious monitoring has no deterrent value and breeds resentment and discomfort upon discovery. Instead, each employer should give notice to its workforce of the method and scope of electronic monitoring by promulgating a policy tailored for the employer's particular workplace.

continued from page 552
Just as the Fourth Amendment protects peoples' reasonable expectations of privacy from governmental intrusion, so to does this common law tort protect the private individual from the prying eyes, ears, and senses of others, both public and private.

In order to "prevail on a claim of intrusion of seclusion as a violation of one's privacy, a plaintiff must show that another has intentionally intruded, physically or otherwise, upon the plaintiff's seclusion or solitude, and that such intrusion would be considered offensive by a reasonable person."[70] In the employer/employee context, the protection afforded an employee from intrusion by his employer is determined by balancing the employee's reasonable expectation of privacy in the area against the reasonableness of that expectation.[71]

Searching a Terminated Employee's Work Area

When an employee's working relationship with the employer is terminated, either voluntarily or involuntarily, the employer has a major business interest at stake. Is the employee wrongfully taking some of the employer's property with them as they leave (such as customer and supplier lists, equipment, trade secrets, supplies, etc.)? This is particularly alarming to the company owner when the employee's parting has been a less than happy scene. Therefore, the employer's interest in what is in the terminated employee's workspace is a legitimate one.[72]

Other People Having Access to the Employee's Office

When others have access to the office of the employee being searched, it would be difficult for that employee to restrict access by other people to his work area. If the employee cannot keep others out of his area, he cannot reasonably expect to have privacy in his work area.[73] This issue was, perhaps, carried to extended lengths when, in 1992, a Florida federal court in *Pottinger v. City of Miami*,[74] held that a homeless person had a subjective expectation of privacy regarding their property, including their bedroll and other personal belongings, when they slept in public areas.[75] However, the court did deny that there was an expectation of privacy to sleep and eat in public, and, therefore, the city may arrest them for these activities without violating their privacy rights.[76] Accordingly, others having access to an area greatly diminishes the ability of anyone working in that area to claim a valid privacy interest.[77] If there is no reasonable expectation of privacy, then without any other prohibition, the search can validly take place.[78]

Shared Offices With Other Workers

New Jersey considered the issue of workers sharing a common work space and found that, from an objective viewpoint, a worker sharing locked work space cannot reasonably have an expectation of privacy where other workmen have access to the same work space.[79]

This view is shared by most state and federal courts, which have addressed the issue in the Fourth Amendment context.[80] In fact, the United States Supreme Court says that, "what a person knowingly exposes to the public" is not subject to constitutional protection.[81] Again, as stated above, what can be perceived with ones own unaided senses, when lawfully in a place where they have a right to be present, is not an illegal search.[82]

In the employer/employee context, if an employee is insensitive to his surroundings and who might be present to observe or overhear, that employee should not be able to later claim that it was improper for someone to see or overhear what he did or said. Accordingly, even if the employee had a subjective expectation of privacy in his office space, the employee's expectation would not be reasonably grounded.

Locked Desk or Computer

If an employee has the only key to his desk and keeps it locked, that situation is essentially the same as where the employee has the only password to the company provided computer, which he uses. Again, we must look to the circumstances of the work environment. In *United States v. Speights*,[83] the court reviewed a case involving a police officer that kept an illegal sawed-off shotgun in his personally assigned locked locker in the police station dressing room.[84] In this case, the court noted that the police department did not have any regulation or notice that the police lockers were subject to unannounced searches at any time.[85] While the lockers were infrequently checked for cleanliness, these checks had occurred only three or four times in the preceding twelve years.[86] The police officers were permitted to keep personal items in their lockers and were allowed to use their own personal padlock to secure the contents of their assigned locker.[87] There was no requirement that an extra key to that padlock be given to the police chief or any other supervisor.[88] Under these specific circumstances, the court held that the officer did have a reasonable expectation of privacy and the warrantless search was violative of his constitutional rights.[89]

The same logic incorporated by the court in *Speights* would apply in a non-governmental situation. For example, in *K-Mart Corp. Store No. 7441 v. Trotti*,[90] the court stated that where "the employee purchases and uses his own lock on the lockers, with the employer's knowledge, the [jury] is justified in concluding that the employee manifested, and the employer recognized, an expectation that the locker and its contents would be free from intrusion and interference."[91]

On the other hand, a warrantless search of a deputy sheriff's locker was upheld where the locks given the deputies had both keys and combinations, but the commander kept a master key and the combinations to all locks.[92] While the deputies could change the keys and combinations at will, copies of the new keys and new combinations had to be given to the commander.[93]

Would the approach adopted in the

above-cited cases also apply to a computer? If the employee is permitted to have his own password, and that password is not required to be given to his supervisor, then the employee could reasonably expect privacy as to what he kept on the company owned computer that he was using (assuming this employee is the only person assigned to use that computer).

Sending the Computer Out for Repair

What protection would an employee have when he sends out his company-owned computer to be repaired? What if management temporarily took the computer to install new software or modify the configuration? What expectation of privacy would the employee have at that time?

The Supreme Court of Kentucky, in *Deemer v. Commonwealth*,[94] addressed an analogous situation. Film was taken to a commercial developer to be processed.[95] As the processing company developed the film, the photos clearly depicted a crime taking place.[96] Police were notified and the culprit was prosecuted.[97] The defendant filed a motion to suppress the photos because he had been taking film to that location for five years and never experienced interference before.[98] Apparently, he argued that the processing company acted as his agent in the developing process.[99] The court, noting that the defendant lost any expectation of privacy when he delivered the film for processing, rejected this argument.[100] The rolls of film here were delivered to a commercial entity whose responsibility was to visually examine the prints in the development process.[101] The defendant, the court stated, knew or should have known this.[102]

In like circumstances, an employee could not reasonably complain that a computer technician observed improper materials on his company-owned computer when the technician was updating, reconfiguring, or otherwise working on the computer. While it might be said that in *Deemer*, the employee initiated the action that led to the viewing of the photos,[103] this would not be true when a company technician comes to the employee's computer (if the work was done at the behest of the employer and not the employee). Nevertheless, the employee should reasonably anticipate that the employer could, at any time, install improvements to the company-owned computer.

Employers Following the Electronic Trail

Unlike many other forms of communication, it is difficult, if not impossible, to totally erase from a computer hard drive the communications sent out from that computer.[104] Recently, software has been developed which enables an employer to see what has been done on a computer in the past.[105] Software, like *Investigator*, is now commercially available to read a hard drive, thereby telling of the nefarious deeds done by the employee.[106] The computer itself incriminates the worker.[107]

That an employer may, from time-to-time, conduct a random search of an employee's possessions on the job, could arguably give the employer the right to review e-mails from one employee to another or otherwise see what an employee has done on the company-owned computer in the ordinary course of business.[108] For instance, if an employee is not at work due to illness, it may be necessary for the employer to review what messages were sent by that employee (to ensure the continuity of workflow until the worker is able to return to the job). While federal law might not prohibit this action, some state laws may nevertheless still consider this as offensive and illegal.[109] Part of the issue may be the manner in which the employer views employee's thoughts and actions. Viewing what went out electronically in e-mail or hearing voice-mail messages left for the employee can sometimes be treated differently than monitoring a telephonic (or actual) conversation between workers.

For example, Wal-Mart Stores learned this in *Desilets v. Wal-Mart Stores, Inc.*,[110] when the company was held liable for eavesdropping on employees in violation of the Omnibus Crime Control and Safe Streets Act of 1968.[111] Title III of this act prohibits interception, disclosure, and intentional use of private conversations,[112] and Wal-Mart recorded conversations between its workers.[113]

EMPLOYEE MALFEASANCES AND EMPLOYER RESPONSES

Harassment, Discrimination, and other "No-No's"

Employees' use of the Internet or company intranet to send harassing, sexually suggestive, or racially motivated messages can be very costly for a company that does not prevent or stop it.[114] For example, Chevron paid out $2.2 million dollars to settle claims for failing to prevent the circulation of an e-mail message describing 25 reasons why beer is better than women.[115] Accordingly, companies have a duty to stop and also prevent improper messaging because failing to do so can result in hefty penalties for the company.[116]

Employers Terminating Employees

Recently, there have been a number of employers disciplining and terminating employees for improper use of the Internet.[117] For example, the New York Times fired over twenty employees and Xerox Corporation fired forty for unauthorized use of the Internet.[118] These employees were terminated for sending offensive e-mail messages and/or viewing Internet pornographic materials at work.[119]

Lawsuits by Employees

Where employees have brought lawsuits against their employers or former employers, the legal foundations have been based on the following theories: the tort of invasion of privacy, discrimination statutes, Fourth Amendment protections regarding search and seizure, First Amendment guarantee

The damage to the company is obvious.

Necessary work is not getting done, yet the employee is still being compensated.

of freedom of speech, Electronic Communications Privacy Act of 1986, Omnibus Crime Control and Safe Streets Act of 1968, and familiar torts such as defamation, negligence, and intentional infliction of emotional distress.[120] The success that these employees meet in the judicial system is varied. Perhaps most importantly, the policy of the employer (in effect at the time of the communication) prohibiting such conduct was a major factor on the outcome of the cases.[121] Other important factors are circumstances of the communication, the intent and attempt of the employee to keep the communication privileged and away from the employer's knowledge, and the means used for the communication itself (telephone or email).

Theft of Time

A safer course of action for the company to take when discharging employees for unauthorized use of the internet, telephone, and other communications means is to discharge the employee for not working during the time she was improperly using the Internet, telephone, or other communication.

The damage to the company is obvious. Necessary work is not getting done, yet the employee is still being compensated. Furthermore, useless e-mails sent to a large number of employees can overtax the company servers, thereby causing a meltdown of the internal communications system.[122] The company may have to pay overtime in order for the employee to accomplish what he should have been doing during regular work hours. The list could go on, but these grounds would be considered sufficient for a court to uphold a firing of an employee for improper usage of the Internet or intranet.

Employers' Policies

One hurdle that a company must overcome to have its "monitoring of employee's conduct" held proper is the various federal and state statutes requiring a person's consent before his conversations can be monitored or recorded.[123] The employer should give advance notice to all employees that conversations, e-mails, and use of the Internet will be monitored. In order to better protect itself, the company should have each employee sign a consent form allowing the company to monitor the employee's use of the Internet, telephone, and other company assets. "Notification and consent negate an expectation of privacy and usually protects companies from liability under such federal statutes as Title III of the Omnibus Crime Control and Safe Streets Act of 1968 and the Federal Electronic Communications Privacy Act of 1986, governing interstate communications, as well as common law invasion of privacy charges."[124]

Union Organizing Activities

One exception to the right of an employer to prohibit employees' use of the Internet for other than company purposes is the right of a union to use the company's Internet.[125] Federal labor laws (National Labor Relations Act, and others) protect the union and its members' right to use certain company facilities to discuss matters considered within the union's purview.[126]

CONCLUSION

As held by the United States Supreme Court in *O'Conner v. Ortega*,[127] "employees' expectations of privacy in their offices, desks, and file cabinets... may be reduced by virtue of actual office practices and procedures, or by legitimate regulation."[128] The Court went on to state that, "offices may be so open to fellow employees or the public that no expectation of privacy is reasonable. Given the great variety of work environments . . . the question whether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis."[129]

While it is hoped that employers will always make the correct decisions regarding the monitoring of employees, the complexity of laws related to protecting the privacy of individuals often causes confusion on behalf of companies conducting employee searches. This study examined some of the complexities involved and some possible alternatives in addressing those complexities.

Footnotes

Job Insecurity pg. 513 - Philip L. Gordon

[1] A recent study by the Privacy Foundation determined that 14 million workers worldwide are subject to workplace surveillance of their e-mail and Internet use. *See* Andrew Schulman, *The Extent of Systematic Monitoring of Employee E-mail and Internet Use* (July 9, 2001), *available at* http://www.privacyfoundation.org/workplace/technology/extent.asp.

[2] *See* Neil A. Lewis, *Rebels in Black Robes Recoil at Surveillance of Computers*, N.Y. TIMES, Aug. 8, 2001, at A1.

[3] *See* Alex Kozinski, *Privacy on Trial*, WALL ST. J., Sept. 4, 2001, at A22; *Greenfield at Large*, CNN.COM (Sept. 6, 2001), *available at* http://www.cnn.com/TRANSCRIPTS/0109/06/gal.00.html.

[4] When enacted, the Federal Wiretap Act was Title III of the Omnibus Crime Control and Safe Streets Act of 1968. Pub. L. No. 90-351, 82 Stat. 212 (1968) (codified as amended at 18 U.S.C. §§ 2510-2520 (2002)).

[5] For sources addressing the effect on businesses of workplace Internet use, see Gary Krakow, *Battling 'Cyber-Slackers' at Work* (Dec. 8, 2000), *available at* http://www.msnbc.com/news/500581.asp; *Results of Vault Survey of Internet Use in the Workplace, available at* http:// www.vault.com/suveys/internetuse2000/index2000.jsp.

[6] Employers with operations in countries other than the United States may not have the same freedom to establish the rules of the game for electronic monitoring. The European Union, for example, has placed strict limits on workplace monitoring. *See*, Article 29 - Data Protection Working Party, Opinion 8/2001, On The Processing Of Personal Data In The Employment Context, § 12 at 28. The law governing workplace monitoring in countries other than the United States is beyond the scope of this Article.

[7] *See generally* Olmstead v. United States, 277 U.S. 438 (1928) (upholding federal conviction based upon use of evidence obtained through wiretaps conducted by federal officials in violation of state law).

[8] 389 U.S. 347 (1967).

[9] *See* Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

[10] *See* Senate Report on the Electronic Communications Privacy Act of 1986, S. REP. NO. 99-541, at 2 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3556.

[11] Electronic Communications Privacy Act of 1986 ("ECPA"), Pub. L. No. 99-508, Title I, §101(a)(6)(c), 100 Stat. 1848, 1848-1849 (codified at 18 U.S.C. § 2510(12)).

[12] *See* Senate Report on the Electronic Communications Privacy Act of 1986, *supra* note 10, at 12, 14.

[13] Electronic Communications Privacy Act of 1986, *supra* note 11 (identifying Title II of the ECPA as the Stored Wire and Electronic Communications and Transactional Records Access [Act]).

[14] 18 U.S.C. § 2701(a)(1) (2002). Even a personal computer can qualify as a "facility" under the Stored Communications Act. *See* In re DoubleClick, Inc. Privacy Litigation, 154 F. Supp. 2d. 497, 509 (S.D.N.Y. 2001) (holding implicitly that a personal computer could be a facility); Chance v. Avenue A, Inc., 165 F. Supp. 2d. 1153, 1160-61 (W.D. Wash. 2001) (holding that plaintiffs had proved that a personal computer was a "facility").

[15] *See* 18. U.S.C. § 2702(a)(1) (2002).

[16] 36 F.3d 457 (5th Cir. 1994).

[17] *See* Steve Jackson Games v. United States Secret Serv., 36 F.3d 457, 458 (5th Cir. 1994).

[18] *See id.* at 461-62.

[19] *See id.* at 462.

[20] *See* 18 U.S.C. § 2701(c)(1) (2002).

[21] *See* 18 U.S.C. § 2510(17)(A) (2002) (defining "electronic storage"); *In re* Toys R Us, Inc., Privacy Litig., 2001 U.S. Dist. LEXIS 16947, at*10-11 (N.D. Cal. Oct. 9, 2001) (holding that "cookies placed on hard drives are not in 'electronic storage'").

[22] *See*, e.g., Wesley College v. Pitts, 974 F. Supp. 375, 385 (D. Del. 1997) (following *Steve Jackson Games*); United States v. Reyes, 922 F. Supp. 818, 836 (S.D.N.Y. 1996 (same).

[23] 236 F.3d 1035 (9th Cir. 2001).

[24] *See* Konop v. Hawaiian Airlines, Inc., 236 F.3d 1035, 1046 (9th Cir. 2001).

[25] *See* id. at 1041.

[26] *See id.* at 1040-41.

[27] *See id.* at 1048.

[28] 155 F.3d 1051 (9th Cir. 1998).

[29] *See* United States v. Smith, 155 F.3d 1051, 1059 (9th Cir. 1998).

[30] *See Konop*, 236 F.3d at 1043-44.

[31] *See* Konop v. Hawaiian Airlines Inc., 262 F.3d 972 (9th Cir. 2001).

[32] *See id.*

[33] *See, Steve Jackson Games*, 36 F.3d at 462-63. *Compare* The Federal Wiretap Act, 18 U.S.C. § 2516 (2002), *with* The Stored Communications Act, 18 U.S.C. § 2703 (2002) (a comparison which illustrates the more stringent requirements of the Federal Wiretap Act).

[34] *Smith*, 155 F.3d at 1059.

[35] *See* 18 U.S.C. § 1708 (2002).

[36] *See Steve Jackson Games*, 36 F.3d at 462.

[37] Even "real-time" interceptions are not actionable under the Federal Wiretap Act if the employer intercepts with the employee's consent, obtained, for example, through the distribution of a monitoring policy. *See* 18 U.S.C. § 2511(2)(d) (providing that it is not unlawful to intercept a communication with the consent of one of the parties to the communication). Employers should note that in some states, such as California and Maryland, an interception is unlawful unless both parties to the communication consent. *See* CAL. PENAL CODE § 631(a) (West 2002); MD. CODE ANN., CTS. & JUD. PROC. § 10-402(c)(3) (Bender 2001).

[38] Electronic Communications Privacy Act of 1986, *supra* note 11, at § 101(a)(D).

[39] *See* Senate Report on the Electronic Communications Privacy Act of 1986, *supra* note 10, at 12.

[40] *See, e.g.*, United States v. Smith, 978 F.2d 171, 173 (5th Cir. 1992); Askin v. McNulty, 47 F.3d 100, 101 (4th Cir. 1995); United States v. Carr, 805 F. Supp. 1266, 1267 (E.D.N.C. 1992).

[41] *See Smith*, 978 F.2d at 181; *Askin*, 47 F.3d at 106; *Carr*, 805 F. Supp. at 1276.
[42] Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified as amended at 18 U.S.C. §§ 2510-2511 (2002)).
[43] H.R. REP. NO. 103-827, at (I)*10 (1994), *reprinted in* 1994 U.S.C.C.A.N. 3489, 3490 (extending the protections of the Federal Wiretap Act to communications over cordless telephones and to certain data communications transmitted by radio).
[44] Uniting And Strengthening America Act By Providing Appropriate Tools Required to Intercept And Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, § 209, 115 Stat. 272, 283.
[45] *See* 18 U.S.C. § 2511(2)(d) (2002) (providing that it is not unlawful to intercept a communication with the consent of one of the parties to the communication).

Little Brothers are Watching You pg. 517 - Sam Kamin

[1] The phrase "Little Brothers" has become almost a term of art in the area of privacy law. When authors write about "Little Brothers" they refer to non-governmental entities snooping in areas that many would consider private. *See, e.g.*, Wendy R. Leibowitz, *Personal Privacy and High Tech: Little Brothers Are Watching You*, NAT'L L.J., Apr. 7, 1997, at B16; Thomas L. Friedman, *Foreign Affairs; Little Brother*, N.Y. TIMES, Sept. 26, 1999, Sec. 4 at 17; Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1396 (2001) ("Commentators have adapted the Big Brother metaphor to describe the threat to privacy caused by private sector databases, often referring to private sector entities as 'Little Brothers.'"). Rather than claiming to have coined a novel metaphor for the analysis of privacy concerns, I am merely using the phrase "Little Brothers" in this well-established sense.
[2] Assistant Professor, University of Denver College of Law. A summer research stipend from the College of Law made this work possible.
[3] *See, e.g.*, Burdeau v. McDowell, 256 U.S. 465, 475 (1921) (explaining that the provisions of the Bill of Rights regulate official conduct, not private conduct).
[4] *See, e.g.*, U.S. v. Koenig, 856 F.2d 843, 849 (7th Cir. 1988) ("Although the DEA may have known of Federal Express's security search policy, it is clear that Federal Express acted for its own private, business purposes."). Throughout this essay I attempt to use the word "search" only in its constitutional sense. As I discuss more fully below, unless a government actor intrudes on the reasonable expectation of privacy of an individual, no search, in a constitutional sense, has occurred.
[5] U.S. v. Ramirez, 810 F.2d 1338, 1342 (5th Cir. 1987) (holding that at least so long as "[t]he manager was neither compensated for nor instructed by the [government] to seize and search the personal property in the room" his search of the hotel room did not constitute state action).
6 Coolidge v. New Hampshire, 403 U.S. 443, 487 (1971) (finding that the crucial inquiry is whether the person conducting the search, at the time in question, was acting at the direction or encouragement of law enforcement).
[7] *Id.* at 487-90.
[8] 389 U.S. 347 (1967).
[9] *Id.* at 361 (Harlan, J., concurring).
[10] *Id.* Prior to *Katz*, the Court applied a more textual interpretation of the Fourth Amendment, focusing on whether the area in question was one that the language of the Constitution seemed intended to protect. So, for example, in the 1928 case of Olmstead v. United States, 227 U.S. 438, 464 (1928), the Supreme Court held that no search occurred when police tapped the defendant's telephone, because the Fourth Amendment contemplated only physical searches of tangible things:

> The [Fourth] [A]mendment itself shows that the search is to be of material things - the person, the house, his papers or his effects. The description of the warrant necessary to make the proceeding lawful is that it must specify the place to be searched and the person or things to be seized. . . .[t]he amendment does not forbid what was done here. There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses or offices of the defendants.

[11] *Katz*, at 351.
[12] *Id.* at 361 (Harlan J., concurring) ("My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'").
[13] 486 U.S. 35 (1988).
[14] *Id.* at 40-41. ("Accordingly, having deposited their garbage 'in an area particularly suited for public inspection and, in a manner of speaking, public consumption, for the express purpose of having strangers take it,' respondents could have had no reasonable expectation of privacy in the inculpatory items that they discarded.") (quoting United States v. Reicherter, 647 F.2d 397, 399 (3rd Cir., 1981)).
[15] *Id.* at 41.
[16] *Id.* at 40.
[17] *Id.* ("Moreover, respondents placed their refuse at the curb for the express purpose of conveying it to a third party, the trash collector, who might himself have sorted through respondents' trash or permitted others, such as the police, to do so."). Furthermore, as we saw above, no search occurs when private actors conduct a search and turn over the contents to law enforcement.
[18] 442 U.S. 735 (1979).
[19] *Id.* at 743.
[20] *Id.*
[21] 425 U.S. 435 (1976).
[22] *Id.* at 443. Note that Colorado law is currently contrary to both *Smith* and *Miller*. *See, e.g.*, People v. Corr, 682 P.2d 20, 27-28 (Colo.1984)(holding that the Colorado state constitution provides a reasonable expectation of privacy in the numbers dialed from a home telephone); Charnes v. DiGiacomo, 612 P.2d 1117, 1119-21 (1980)(finding that the Colorado state constitution provides a reasonable expectation of privacy in bank records).
[23] A similar line of reasoning applies to the use of hidden microphones by undercover government agents. Federal courts have consistently held that no search occurs when a government agent wears a wire in a conversation with an unaware suspect. The rationale for these cases is that an individual who chooses to share her secrets with others runs the risk that her confidences will be exploited. *See, e.g.*, United States v. White, 401 U.S. 745, 752 (1971) ("[O]ne contemplating illegal activities must realize and risk that his companions may be reporting to the police. . . Given the

possibility or probability that one of his colleagues is cooperating with the police, it is only speculation to assert that the defendant's utterances would be substantially different or his sense of security any less if he also thought it possible that the suspected colleague is wired for sound."); Hoffa v. United States, 385 U.S. 293, 302 (1966) ("Neither this Court nor any member of it has ever expressed the view that the Fourth Amendment protects a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it.").

[24] 476 U.S. 207 (1986).

[25] *Id.* at 213-14.

[26] *Id.* at 213. Of course, the defendant was not merely asking law enforcement officials to avert their eyes. *See id.* at 212. He was asking them not to fly over his property looking down on it for evidence of crimes. *See id.* However, the Court has discarded the line between looking for evidence and stumbling across it. *See, e.g.*, Horton v. California, 496 U.S. 128, 138 (1990) ("The fact that an officer is interested in an item of evidence and fully expects to find it in the course of a search should not invalidate its seizure if the search is confined in area and duration by the terms of a warrant or a valid exception to the warrant requirement.").

[27] 533 U.S. 27 (2001).

[28] *See id.* at 34 ("We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area,' constitutes a search - at least where (as here) the technology in question is not in general public use." (quoting Silverman v. United States, 365 U.S. 505, 512 (1961))).

[29] *See* Andrew Schulman, *The Extent of Systematic Monitoring of Employee E-mail and Internet Use*, Privacy Foundation Report ("Fourteen million employees - just over one-third of the online workforce in the United States - have their Internet or e-mail use under continuous surveillance at work."), *available at* http://www.privacyfoundation.org/workplace/technology/extent.asp (July 9, 2001).

[30] Editorial, *Technology's Threats to Privacy*, N.Y.TIMES, February 24, 2002, § 4, at 12. Similarly, TiVo, a maker of digital video recorders, has been accused of gathering information on the viewing habits of its subscribers, in apparent violation of its privacy policy. *See* David Martin, *TiVo's Data Collection and Privacy Practices*, Privacy Foundation: Privacy Watch Report, *available at* http://www.privacyfoundation.org/privacywatch/report.asp?id=62&action=0 (posted March 26, 2001); *see also* Janet Kornblum, *Privacy Organization Hits Recorder Maker*, USA TODAY, February 8, 2002, *available at* http://www.usatoday.com/life/cyber/tech/2001-03-26-ebrief.htm (updated February 8, 2002).

[31] *See, e.g.*, http://www.spyshops.com/index1.html (listing each of these items) (last visited March 17, 2002).

[32] There are many exceptions, of course. For example, the government's Carnivore system, which would allow the government to intercept and read virtually all e-mails sent in the country, has received widespread coverage and criticisms. *Compare* http://www.fbi.gov/hq/lab/carnivore/carnivore2.htm (describing the Carnivore system on the FBI website) (last visited March 17, 2002), *with* http://www.epic.org/privacy/carnivore/default.html (providing criticisms of the Carnivore program, known as "The Carnivore FOIA Litigation") (updated August 9, 2001).

[33] *See, e.g.*, Professor Dorothy Glancy, *At the Intersection of Visible and Invisible Worlds: United States Privacy Law and the Internet*, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 357, 377 (2000) ("The focus of primary concerns about government invasions of privacy, such as those associated with Watergate, seem to [be] shifting toward enhanced concern about invasions of privacy by the private sector, such as those associated with disclosures of credit card numbers from Internet sites."); Honorable Ben F. Overton & Katherine E. Giddings, *The Right of Privacy in Florida in the Age of Technology and the Twenty-First Century: A Need for Protection from Private and Commercial Intrusion*, 25 FLA. ST. U. L. REV. 25, 27 (1997) ("It is no longer simply intrusion by the government of which we should be wary; it is intrusion by various commercial entities looking to profit from the use of private information as well.").

Security vs. Privacy pg. 519 - Shaun B. Spencer

* The author is a Climenko/Thayer Lecturer on Law at Harvard Law School. Before joining Harvard, he taught as an Adjunct Professor at Boston College Law School, and practiced in the litigation department of the Boston law firm Bingham Dana. The ideas in Part I of this essay are drawn substantially from the author's forthcoming article, Reasonable Expectations and the Erosion of Privacy, 39 SAN DIEGO L. REV. (forthcoming 2002). The author is grateful for the comments of Richard Sobel, and for the extensive contributions of Lawrence Friedman. The author also thanks Tanya Thiessen and the Denver University Law Review for organizing this important Symposium.

** President George W. Bush, Address on Terrorism Before a Joint Meeting of Congress (Sept. 20, 2001), *reprinted in A Nation Challenged*, N.Y. TIMES, Sept. 21, 2001, at B4.

[1] For a more expansive examination of secondary uses, unintended consequences, and incremental encroachment on the expectation-driven conception of privacy, see Spencer, *supra* note *, §§ I.C & II.C.

[2] *See* Spencer, *supra* note *, § II.C.1.

[3] In 1946, the Board was replaced by the Social Security Administration. The Official Website of the Social Security Administration, *Brief History, at* http://www.ssa.gov/history/history6.html.

[4] *See* SIMSON GARFINKEL, DATABASE NATION: THE DEATH OF PRIVACY IN THE 21ST CENTURY 18 (2000).

[5] *See* H.R. Rep. No. 106-996(1) (2000), 2000 WL 1604000, at *23 ("The SSN was created in 1935 for the sole purpose of tracking workers' earnings so that Social Security benefits could be calculated upon retirement or disability . . . Because a unique SSN is assigned to each individual, the number is commonly used as a personal identifier, although it was never intended for this purpose."); *accord* Charlotte Twight, *Constitutional Counterrevolution*, IDEAS ON LIBERTY, Oct. 2000, at 20.

[6] Executive Order 9397 (3 CFR (1943-1948 Comp.) 283-284), *cited in* The Official Website of the Social Security Administration, *Social Security Number Chronology, at* http://www.ssa.gov/history/ssn/ssnchron.html.

[7] U.S. Department of Health & Human Services, National Committee on Vital Health Statistics, *Unique Health Identifier for Individuals: A White Paper* § III.A.1 (July 2, 1998), *available at* http://www.epic.org/privacy/medical/hhs-id-798.html (visited Apr. 28, 2001).

8 *See* Flavio L. Komuves, *We've Got Your Number: An Overview of Legislation and Decisions to Control the Use of Social Security Numbers as Personal Identifiers*, 16 J. MARSHALL J. COMPUTER & INFO. L. 529, 535 (1998).

9 The history of identification systems throughout the world provides evidence of 'function creep' - application to additional purposes not announced, or perhaps even intended, at the commencement of the scheme. Uses of the Social Security Number in the U.S.A., the Social Insurance Number in Canada, the Tax File Number in Australia, the SOFI number in The Netherlands, and the Austrian Social Security Number have been extended progressively to include taxation, unemployment support, pensioner benefits, and in some cases health and higher education.

Simon G. Davies, *Touching Big Brother: How biometric technology will fuse flesh and machine*, 7:4 INFO. TECH. & PEOPLE *6 (1994), *available at* http://www.privacy.org/pi/reports/biometric.html.

[10] *See* Electronic Privacy Information Center, *EPIC Files FOIA Suit for Profiling Records*, 9.02 EPIC ALERT § 3 (Jan. 29, 2002), *available at* http://www.epic.org/alert/EPIC_Alert_9.02.html (the Electronic Privacy Information Center is investigating "news reports that ChoicePoint, a profiling company, routinely sells personal information to federal law enforcement agencies.").

[11] *See, e.g.*, Stephanie Stoughton, *Poll: Firms Relaxed Privacy Rules*, BOSTON GLOBE, Oct. 8, 2001, at C4 (fifty-nine percent of "airlines, hotel chains, travel agencies, rental car companies, and other travel-related firms" surveyed said they "relaxed" their own privacy policies to aid law enforcement officials in the wake of September 11).

[12] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (Oct. 26, 2001).

[13] 18 U.S.C. § 2703(c)(2) (1994), *as amended by* USA Patriot Act § 210 (Oct. 26, 2001). Government agencies can simply use an administrative subpoena, grand jury subpoena, or trial subpoena to demand information from an electronic communication service provider. *See id.* The information can include when and for how long the Internet user surfed the net, the user's unique Internet Protocol address, and the credit card or bank account number with which the user pays for the Internet service. *See id.*

[14] *See generally* Spencer, *supra* note *, § II.C.2.

[15] *See* Declan McCullagh, *Xenu Do, But Not on Slashdot*, WIRED NEWS, Mar. 17, 2001, *at* http://www.wired.com/news/print/0,1294,42486,00.html (a General Accounting Office report explained that the GAO had successfully hacked into sensitive IRS databases in March 2001, and "demonstrated that unauthorized individuals, both internal and external to IRS, could have viewed and modified electronically filed taxpayer data on IRS computers.").

[16] *See* Mark E. Budnitz, *Privacy Protection for Consumer Transactions in Electronic Commerce: Why Self-Regulation is Inadequate*, 49 S.C. L. REV. 847, 854 (1998); Charles Piller, *Web Mishap: Kids' Psychological Files Posted*, L.A. TIMES, Nov. 7, 2001, at A1-1, *available at* http://pqasb.pqarchiver.com/latimes/.

[17] *See* Federal Trade Commission, *Eli Lilly Settles FTC Charges Concerning Security Breach* (Jan. 18, 2002), *available at* http://www.ftc.gov/opa/2002/01/elililly.htm; *In the Matter of Eli Lilly & Co.*, File No. 012-3214, FTC, Proposed Agreement Containing Consent Order, *available at* http://www.ftc.gov/os/2002/01/lillyagree.pdf.

[18] Brian McWilliams, *Congressional Committee Web Site Exposed Internal Database*, NEWSBYTES, Mar. 6, 2002, *at* http://www.newsbytes.com/cgi-bin/udt/im.display.printable?client.id=newsbytes&story.id=175010.

[19] *See generally* ABUSE OF POWER: THE NEW NIXON TAPES (Stanley I. Kutler ed., 1997); Editorial, *Politics and the IRS*, WALL ST. J., Jan. 9, 1997, at A12 (quoting Nixon in 1971 as saying he intended to select an IRS Commissioner who "is a ruthless son of a bitch, that he will do what he's told, that every income tax return I want to see I see, that he will go after our enemies and not go after our friends."); CURT GENTRY, J. EDGAR HOOVER: THE MAN AND THE SECRETS (1991); Orr Kelley, *The Secret Files of J. Edgar Hoover*, U.S. NEWS & WORLD REP., Dec. 19, 1983, at 45.

[20] Privacy International, *Identity Cards: Frequently Asked Questions*, § 13 (Aug. 24, 1996), *at* http://www.privacy.org/pi/activities/idcard/idcard_faq.html:

> Some privacy advocates in the UK argue against ID cards on the basis of evidence from various security threat models in use throughout the private sector. In these models, it is generally assumed that at any one time, one per cent of staff will be willing to sell or trade confidential information for personal gain. In many European countries, up to one per cent of bank staff are dismissed each year, often because of theft.

[21] Electronic Privacy Information Center, *Your Papers, Please: From the State Drivers License to a National Identification System*, at 7 n.23 (Feb. 2002), *available at* http://www.epic.org/privacy/id_cards/yourpapersplease.pdf (citing *Legislators Order DMV Audit*, ORANGE COUNTY REG., Feb. 27, 2001).

[22] Brooke A. Masters, *Va. Notary Gets 33 Months for ID Fraud; Woman Exploited State Law to Help Thousands of Illegal Immigrants*, WASH. POST, Nov. 17, 2001, at B1.

[23] *See id.*

[24] *Id.*

[25] *See* United States General Accounting Office, *National Crime Information Center: Legislation Needed to Deter Misuse of Criminal Justice Information*, GAO/T-GGD-93-41 (1993) (statement of Laurie E. Ekstrand, Associate Director, Administration of Justice Issues, General Government Division).

[26] *Id.* at 2.

[27] *Id.* at 3.

[28] *Id.* at 16-17.

[29] *See id.* at 16.

[30] *See id.*

[31] *See* United States General Accounting Office, *National Crime Information Center: Legislation Needed to Deter Misuse of Criminal Justice Information*, GAO/T-GGD-93-41, at 25, 29, 30 (1993) (statement of Laurie E. Ekstrand, Associate Director, Administration of Justice Issues, General Government Division).

[32] For a complete discussion of the expectation-driven conception of privacy, see Spencer, *supra* note *, § I.

[33] *See id.; see also* Kyllo v. United States, 533 U.S. 27, at 33, 39 (2001) (law enforcement use of thermal imaging device to scan heat radiating from defendant's home violated reasonable expectation of privacy because thermal imaging technology was not in general use); Katz v. United States, 389 U.S. 347, 361 (1967) (proof of warrantless search in violation of Fourth Amendment requires not only subjective expectation of privacy, but an expectation of privacy "that society is prepared to recognize as 'reasonable'"); RESTATEMENT (SECOND) OF TORTS: INVASION OF PRIVACY § 652B(1) (1977) (intrusion on seclusion not actionable unless intrusion "would be highly offensive to a reasonable person"); RESTATEMENT (SECOND) OF TORTS: INVASION OF PRIVACY § 652D(1)(A) & cmt. c (disclosure of private facts not actionable unless disclosure "would be highly offensive to a reasonable person," with offensiveness judged "relative to the customs of the time and place, to the occupation of the plaintiff and to the habits of his neighbors and fellow citizens"); Frederick Schauer, The Social Construction of Privacy, at 10 (Mar. 20, 2000) (unpublished manuscript, discussion draft, *available at* http://www.ksg.harvard.edu/presspol/publications/pdfs/schauer1.PDF) (actionable harm flowing from privacy torts is "a function of going beyond what most of the people in the society have come to expect, so if those expectations change, then so too does the conception of harm that is based upon them").

[34] *See* Spencer, *supra* note *, § I.B.

[35] *See* Spencer, *supra* note *, § I.C.3.

[36] For a complete discussion of incremental encroachment, see Spencer, *supra* note *, §§ I.C.1 & I.C.2 (explaining how the imprecision embedded in societal expectations, as well as society's internalization of privacy intrusions, facilitates the incremental erosion of privacy).

[37] *See, e.g.*, Alan M. Dershowitz, *Why Fear National ID Cards?*, N.Y. TIMES, Oct. 13, 2001, at A23 (advocating an optional national ID card with a digitally encoded fingerprint as an "effective tool for preventing terrorism"). Dershowitz suggested that Americans already have a minimal expectation of privacy in a variety of areas essential to our society: "American taxpayers, voters and drivers long ago gave up any right of anonymity without loss of our right to engage in lawful conduct within zones of privacy." *Id.*

[38] Dershowitz does note that we should set criteria for when officials could ask to see the card, and that the card should contain only limited information about the person that it identifies. *See id.* The problem, however, is that the best intentions at the outset will inevitably fall to the irresistible temptation to use the card for additional purposes and to include additional information.

[39] For example, the American Association of Motor Vehicle Administrators (AAMVA), which has proposed uniform standards for driver's licenses, "supports and encourages the access by [state motor vehicle administrators] to other databases, such as SSA, INS and Vital Statistics to confirm identity, residency, citizenship and address verification." Electronic Privacy Information Center, *Your Papers, Please: From the State Drivers License to a National Identification System*, at 8 n.28 (Feb. 2002) [hereinafter *Your Papers, Please*], *available at* http://www.epic.org/privacy/id_cards/yourpapersplease.pdf, quoting AAMVA Special Task Force on Identification Security Report to the AAMVA Board at 8 ("AAMVA Task Force Report").

[40] *See* Spencer, *supra* note *, Conclusion.

[41] *See Your Papers, Please, supra* note 39, at 5-6.

[42] *Id.* at 1.

[43] *See id.* at 5.

[44] *See id.* at 6; *see also* Jennifer Lee, *Welcome to the Database Lounge*, N.Y. TIMES, Mar. 21, 2002, at G1 (describing a Boston bar using a license scanning machine to build a database of information about its patrons).

[45] *See* American Association of Motor Vehicle Administrators, *Uniform Identification Practices Working Group* § G, *available at* http://www.aamva.org/drivers/drvDL&CuniformIdentificationWG.asp (stating that one task of the working group is to promote the use of AAMVA's "Uniform Identification Practices model program" to "various potential customers, such as: . . . Insurance companies; Banks; Travel Industry; Car rental agencies; Retailers; Others").

[46] *See generally* Cass R. Sunstein, *Incommensurability and Valuation in Law*, 92 MICH. L. REV. 779 (1994) (discussing incommensurability and different kinds of valuation).

[47] *See id.* at 798-99.

[48] *See* Alan M. Dershowitz, *Why Fear National ID Cards?*, N.Y. TIMES, Oct. 13, 2001, at A23 (suggesting that we trade "a little less anonymity for a lot more security"); *cf.* Jane Black, *Don't Make Privacy the Next Victim of Terror*, BUSINESSWEEK ONLINE (Oct. 4, 2001), *at* http://www.businessweek.com/bwdaily/dnflash/oct2001/nf2001104_7412.htm (quoting Oracle CEO Larry Ellison in a television appearance on KPIX in San Francisco, where he said, "The privacy you're concerned about is largely an illusion. All you have to give up is your illusions, not any of your privacy.").

[49] *See, e.g.*, Joseph Kupfer, *Privacy, Autonomy, and Self-Concept*, 24 AM. PHIL. Q. 81, 82-85 (1987) (arguing that autonomy depends upon the "concept of oneself as a purposeful, self-determining, responsible agent," which concept in turn depends upon privacy to facilitate self-determination, self-examination, and the perception of the self as worthy of acting autonomously); Hyman Gross, *Privacy and Autonomy*, in PRIVACY: NOMOS XIII 169, at 181 (J. Roland Pennock & John W. Chapman eds., 1971) (criticizing Griswold v. Connecticut for using the term "privacy" to obscure the individual's right to autonomous determination, and arguing that intrusions on privacy offend autonomy).

[50] *See* Richard Sobel, *The Degradation of Political Identity Under a National Identification System*, 8 B.U. J. SCI. & TECH. L. 37, 40 (2002).

[51] *See* McIntyre v. Ohio Elections Comm'n, 514 U.S. 334 (1995); NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449 (1958).

[52] *See, e.g.*, Ronald F. Wright, *The Civil and Criminal Methodologies of the Fourth Amendment*, 93 YALE L.J. 1127 (1984). Wright argues that courts trying to balance privacy against law enforcement needs may underestimate privacy, in part because "a privacy claim is highly subjective . . . A judge cannot actually know how different persons in different contexts perceive an invasion of privacy, yet it is something that he or she must know in order to arrive at an 'objective' value for privacy. Hence, every effort to place an objective value on privacy interests risks error." *Id.* at 1142-43 (footnotes omitted).

[53] Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1398 (2000) (arguing that a "privacy-as-choice" model in the marketplace rests on the flawed assumption that "data privacy can be valued using market measures").

[54] *See id.*

[55] *See generally* Wright, *supra* note 52, at 1142-44 (arguing that balancing privacy against law enforcement in the Fourth Amendment context consistently undervalues privacy interests).

[56] Michael Clarke, *Blunkett Defiant Over Crackdown on the Enemy Within*, DAILY MAIL (London), Nov. 13, 2001, at 19.

[57] *National ID Cards: Life, Liberty and the Pursuit of Terrorists, Before the United States House of Representatives, Subcomm. on Gov't Efficiency, Fin. Mgmt., Comm. on Gov't Reform*, Federal Document Clearing House, 107th Cong., 2001 WL 1468660 (2001) (statement of Larry Ellison, Founder, CEO Oracle Corp.).

[58] David Streitfeld & Charles Piller, *Big Brother Finds Ally in Once-Wary High Tech*, L.A. TIMES, Jan. 19, 2002, at A1.

[59] Clarke, *supra* note 56.

[60] *See* Ellison's statement, *supra* note 57; Streitfeld & Piller, *supra* note 58.

[61] *Cf.* Ronald F. Wright, *The Civil and Criminal Methodologies of the Fourth Amendment*, 93 YALE L.J. 1127, 1143-44 (1984) (arguing that, because of the exclusionary rule, Fourth Amendment challenges generally arrive in the highly unfavorable context of a defendant who appears quite guilty).

[62] *See* Mac Daniel, *Loose Plug Disrupts Logan - Again*, BOSTON GLOBE, Mar. 21, 2002, at B4. On ten occasions between November 2001 and March 21, 2002, the discovery of unplugged metal detectors required the evacuation of major American commercial airports. *See id.* After a National Guard member noticed the unplugged metal detector in Boston's Logan Airport, a security staffer tried to plug it back in without notifying authorities. *See id.* The National Guard member, however, "reported the incident, and the terminal was evacuated." *Id.*

[63] *See* Mac Daniel, *Lapses at Logan Fail to Catch Ticket Mix-Up; Wrong Identification Doesn't Prevent Man From Boarding Plane*, BOSTON GLOBE,

Mar. 19, 2002, at B1. After Delta Airlines ticket agents issued the same ticket to two passengers with similar names, the passenger whose name did not match the ticket passed through two security checkpoints where guards compared his license to the name on the ticket. When a Delta scanning machine at the gate rejected his boarding pass, a Delta flight attendant commented to a colleague, "This guy's already on the plane." *Id.* Nevertheless, they let the passenger board. *See id.* The mix-up finally surfaced when the second passenger found someone already sitting in his seat, and a flight attendant discovered that two tickets had been issued in the same passenger's name. *See id.*

[64] *See* Malcolm Gladwell, *Safety in the Skies: How Far Can Airline Security Go?*, THE NEW YORKER, Oct. 1, 2001, at 50, 52-53. Gladwell explains that as the "signal rate" declines, so does detection accuracy. *Id.* at 53. "In the wake of the September attacks, some commentators called for increased training for X-ray security operators. Yet the problem is not just a lack of expertise; it is the paucity of signals." *Id.*

[65] *See* Jeffrey Rosen, *A Watchful State,* N.Y. TIMES MAGAZINE, Oct. 7, 2001, at 38.

[66] *See id.* at 41.

[67] *Id.*

[68] *Id.*

[69] *Id.*

[70] *Id.*

[71] *See id.* at 42.

[72] *Id.*

[73] *See id.*

[74] *Id.*

[75] *Id.*

[76] *See id.*

[77] *See* Julia Scheeres, *ID Cards Are de Rigueur Worldwide*, WIRED NEWS, Sept. 25, 2001, *at* http://www.wired.com/news/print/0,1294,47073,00.html.

[78] Mike France et al., *Privacy in an Age of Terror*, BUSINESSWEEK ONLINE, Nov. 5, 2001, *at* http://www.businessweek.com:/print/magazine/content/01_45/b3756001.htm?mainwindow.

[79] *See* Brooke A. Masters, *Va. Notary Gets 33 Months for ID Fraud; Woman Exploited State Law to Help Thousands of Illegal Immigrants,* WASH. POST, Nov. 17, 2001, at B1.

[80] *See* Dan Eggen & Mary Beth Sheridan, *Terrorist Pilots' Student Visas Arrive; Officials Blame 'Antiquated' System for Delay of Paperwork,* WASH. POST, Mar. 13, 2002, at A1. The INS actually approved the visas before the September 11 attacks, but did not issue notice of approval until March 2002. *See id.*

[81] *See* Mac Daniel, *Lapses at Logan Fail to Catch Ticket Mix-Up; Wrong Identification Doesn't Prevent Man From Boarding Plane*, BOSTON GLOBE, Mar. 19, 2002, at B1.

[82] Pew Research Center for the People & the Press, *American Psyche Reeling from Terror Attacks,* Sept. 19, 2001, *available at* http://people-press.org/reports/print.php3?ReportID=3.

[83] USA Today/CNN/Gallup Poll Results, Sept. 16, 2001, *available at* http://www.usatoday.com/news/nation/2001/09/16/terrorism-poll2.htm (citing Question 23).

[84] Jane Black, *Don't Make Privacy the Next Victim of Terror,* BUSINESSWEEK ONLINE (Oct. 4, 2001), *at* http://www.businessweek.com/print/bwdaily/dnflash/oct2001/nf2001104_7412.htm (quoting Oracle CEO Larry Ellison in a television appearance on KPIX in San Francisco, where he said, "The privacy you're concerned about is largely an illusion. All you have to give up is your illusions, not any of your privacy.").

[85] Lecture from Simson Garfinkel to Prof. Nolan Bowie's Fall 2000 Harvard University, JFK School of Government class on *Information, Media Regulation, and Public Policy* (unpublished notes, on file with author). For a similar sentiment, see Stephen Keating, *The Exxon Valdez of Privacy,* PRIVACY FOUND. (Feb. 27, 2002), *at* http://www.privacyfoundation.org/commentary/tipsheet.asp (arguing that privacy advocates need "a made-for-TV disaster, cast with distraught victims, dissembling corporate mouthpieces, a chorus of outraged elected officials and a media horde to amplify it all".).

[86] Jennifer Lee, *Welcome to the Database Lounge,* N.Y. TIMES, Mar. 21, 2002, at G1.

[87] *See* SIMSON GARFINKEL, DATABASE NATION: THE DEATH OF PRIVACY IN THE 21ST CENTURY 72 (2000).

[88] *See* JANNA MALAMUD SMITH, PRIVATE MATTERS: IN DEFENSE OF THE PERSONAL LIFE 27-32 (1997).

[89] *Id.* at 29.

[90] *Id.* at 30 (quoting NADEZHDA MANDELSTAM, HOPE AGAINST HOPE: A MEMOIR 89 (1970)).

[91] *See* Smith, *supra* note 88, at 32 ("Terrorists of all sorts destroy privacy both by corrupting it into secrecy and by using hostile surveillance to undo its useful sanctuary.").

[92] *See id.* at 31.

[93] *See id.*

[94] *Id.*

[95] *See* CURT GENTRY, J. EDGAR HOOVER: THE MAN AND THE SECRETS 388 (1991).

[96] *Id.*

[97] *See* William Safire, *The Great Unwatched,* N.Y. TIMES, Feb. 18, 2002, at A15; Spencer S. Hsu, *D.C. Forms Network of Surveillance; Police System of Hundreds of Video Links Raises Issues of Rights, Privacy,* WASH. POST, Feb. 17, 2002, at C1.

[98] Safire, *supra* note 97.

[99] *See id.*

[100] *See id.*

[101] *See id.*

[102] *See id.*

[103] Spencer S. Hsu, *D.C. Forms Network of Surveillance; Police System of Hundreds of Video Links Raises Issues of Rights, Privacy,* WASH. POST, Feb. 17, 2002, at C1.

[104] Jeffrey Rosen, *A Watchful State,* N.Y. TIMES MAGAZINE, Oct. 7, 2001, at 38.

[105] *Id.* (emphasis added).

[106] Safire, *supra* note 97.

[107] Hsu, *supra* note 103.

[108] The goal of the new generation of face-recognition systems is to limit the number of false-positive matches to a tiny fraction, no more than one per 1,000 passengers screened . . . [and] to get the number of "correct positives" — fugitives who actually are caught by face-recognition technology — up in the range of 80 percent.

Jeffrey Leib, *Airport Eyeing Face-ID System; Test Program Would Screen DIA Workers,* DENVER POST, Dec. 3, 2001, at A1. "Biometric experts ... say the [facial recognition] technology is easily foiled if the subject looks down or coughs while passing the camera, or has dark skin tone, wears a hat, or simply gets a fresh haircut or a shave." Dana Hawkins et al., *Tech vs. Terrorists,* U.S. NEWS & WORLD REP., Oct. 8, 2001, at 56.

[109] *See* Lowell Bergman & Don Van Natta, Jr., *Agents Pursue German Leads on Terror Trail,* N.Y. TIMES, Sept. 25, 2001, at A1.

[110] President George W. Bush, Address on Terrorism Before a Joint Meeting of Congress (Sept. 20, 2001), reprinted in *A Nation Challenged,* N.Y. TIMES, Sept. 21, 2001, at B4.

Judging a Book pg. 522 - Joyce Meskis

[1] For an explanation of some of the legal concepts and the outcome of the Colorado Supreme Court case, see the following case summary. *Tattered Cover v. Thornton: The Right to Buy Books Anonymously,* by Corey Ann Finn.

[2] *See In re* Grand Jury Subpeona to Kramerbooks & Afterwards, 26 Media L. Rep. (BNA) 1599 (D.D.C. 1998) (concerning independent counsel Kenneth Starr's effort to obtain records of books purchased by former White House intern Monica Lewinsky).

[3] *In re* Grand Jury Subpeona to Kramerbooks & Afterwords, Inc., 26 Media L. Rep. (BNA) at 1601 (D.D.C. 1998).

[4] Judith Krug, Executive Director of the Freedom to Read Foundation of the American Library Association.

[5] Tattered Cover v. Thornton (Case No. 00 CV 1761) at 2 (October 28, 2000) (citing Stanley v. Georgia, 394 U.S. 557, 564 (1969)).

[6] *Id.* at 2-3 (quoting United States v. Rumely, 345 41, 57-58 (1953) (Douglas, J., concurring)).

Tattered Cover v. Thornton pg. 525 - Corey Ann Finn

[1] 44 P3d 1044 (Colo. 2002).

[2] *Tattered Cover,* 44 P.3d at 1048.

[3] *Id.*

[4] *Id.* at 1049.

[5] *Id.* at 1051.

[6] *Id.* at 1059.

[7] *Id.* at 1061.

Privacy and Firms pg. 526 - Bruce Kobayashi & Larry Ribstein

[1] *See, e.g.*, Richard A. Posner, *Privacy, in* THE NEW PALGRAVE DICTIONARY OF ECONOMICS AND THE LAW, P. Newman, ed. 103 (1998); George J. Stigler, *An Introduction to Privacy in Economics and Politics,* 9 J. LEGAL STUD. 623 (1980); Jack Hirshleifer, *Privacy, Its Origin, Function, and Future,* 9 J. LEGAL STUD. 649 (1980); Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy,* 84 GEO. L. J. 2381 (1996).

[2] *See* Frank H. Easterbrook, *Insider Trading, Secret Agents, Evidentiary Privileges, and the Production of Information,* 1981 SUP. CT. REV. 309, 339-353 (1981) (discussing Snepp v. U.S., 444 U.S. 507 (1980)).

[3] *See infra* Section I.

[4] See Edmund W. Kitch, *The Law and Economics of Rights in Valuable Information,* 9 J. LEGAL STUD. 683, 685 (1980).

[5] R. H. Coase, *The Nature of the Firm,* 4 ECONOMICA 386 (1937).

[6] *See* Oliver E. Williamson, THE ECONOMIC INSTITUTIONS OF CAPITALISM (1985); Armen A. Alchian & Susan Woodward, *Reflections on the Theory of the Firm,* 143 JOURNAL OF INSTITUTIONAL AND THEORETICAL ECONOMICS 110, 111 (1987).

[7] *See* Armen A. Alchian & Harold Demsetz, *Production, Information Costs, and Economic Organization,* 62 AM. ECON. REV. 777 (1972).

[8] *See* Benjamin Klein, et al., *Vertical Integration, Appropriable Rents, and the Competitive Contracting Process,* 21 J. L. & ECON. 297 (1978); Williamson, *supra* note 6, at 47-49.

[9] *See, e.g.,* Kitch, *supra* note 4, at 690 (discussing difficulties detecting theft of information).

[10] Alchian and Woodward, *supra* note 6, at 115-17.

[11] For discussions of limitations on intra-firm information transfer in the absence of effective means to prevent inter-firm information transfers, see Robert M. Sherwood, INTELLECTUAL PROPERTY IN DEVELOPING COUNTRIES AND JUDICIAL SYSTEMS AND ECONOMIC DEVELOPMENT, Chapter 5, (Westview Press 1980), *available at* http://www.kreative.net/ipbenefits/iped (last visited February 28, 2002); David D. Friedman, et al., *Some Economics of Trade Secret Law,* 5 J. ECON. PERSP. 61, 67 (1991) *available at* http://davidfriedman.com/Academic/Trade/_Secrets/Trade_Secrets.html (last visited February 28, 2002).

[12] One example would be the misappropriation of a firm's information to engage in stock trading. *See* Easterbrook, *supra* note 2, at 314-39; Larry E. Ribstein, *Federalism and Insider Trading,* 6 SUP. CT. ECON. REV. 123 (1998).

[13] *See* Richard A. Epstein, *International News Service v. Associated Press: Custom and Law as Sources of Property Rights in News,* 78 VA. L. REV. 85 (1992) (discussing misappropriation of hot news in INS v. AP, 248 U.S. 215 (1918)); *see also* Kitch, *supra* note 4, at 684-85 (discussing transfer of business information though mobility of employees); Sherwood, *supra* note 11 (discussing "predatory hiring" and unrestricted employee mobility as primary ways in which valuable business information is transferred to third parties in developing countries); *infra* Section II.

[14] *See generally* Alchian & Demsetz, *supra* note 7.

[15] This assumes that the seller of information is unable to use speculative mechanisms to appropriate a normal return from the disclosure of his information. *See* Jack Hirshleifer, *The Private and Social Value of Information and the Reward to Inventive Activity,* 61 AM. ECON. REV. 561 (1971).

[16] *See* George A. Akerlof, *The Market for 'Lemons': Qualitative Uncertainty and the Market Mechanism,* 84 Q. J. ECON. 488 (1970).

[17] *See, e.g.,* ProCD, Inc. v. Zeidenberg, 86 F.3d 1447 (7th Cir. 1996); *see also* Bruce H. Kobayashi & Larry E. Ribstein, *Uniformity, Choice of Law, and Software Sales,* 8 GEO. MASON L. REV. 261 (1999).

[18] *See generally* Jennifer Arlen, *The Potentially Perverse Effects of Corporate Criminal Liability,* 23 J. LEGAL STUD. 833 (1994) (discussing effects of

corporate criminal liability on a corporation's incentive to engage detection and monitoring of their agents); Daniel R. Fischel & Alan O. Sykes, *Corporate Crime,* 25 J. LEGAL STUD. 319 (1996) (discussing and criticizing the recent increase in application of vicarious corporate criminal liability for the wrongdoings of their employees); Bruce H. Kobayashi, *Antitrust, Agency and Amnesty: An Economic Analysis of the Criminal Enforcement of the Antitrust Laws Against Corporations,* GEO. WASH. L. REV. (forthcoming 2002) (discussing antitrust leniency policy for corporate monitoring and self detection); Jeffrey S. Parker, *Rules Without . . . : Some Critical Reflections on the Federal Corporate Sentencing Guidelines,* 71 WASH. U. L.Q. 397, 404-10 (1993) (discussing corporate criminal liability and the U.S. Sentencing Guidelines).

[19] *See* Epstein, *supra* note 13 (discussing relative advantages of bottom-up and top down approaches to lawmaking); *see also* Larry E. Ribstein & Bruce H. Kobayashi, *An Economic Analysis of Uniform State Laws,* 25 J. LEGAL STUD. 131 (1996) (discussing benefits of a decentralized state law approach); Kobayashi and Ribstein, *supra* note 17; Larry E. Ribstein & Bruce H. Kobayashi, *State Regulation of Electronic Commerce,* EMORY L. J. (forthcoming 2002) (hereinafter *State Regulation*).

[20] *See infra* text accompanying note 45 and note 60.

[21] *Id.* Note that the law of the state of incorporation, which firms can freely choose, provides the basic fiduciary duty rules governing managers. We see no reason why incentive and compensation arrangements should be treated differently for corporate employees than for corporate managers.

[22] *See* Ronald J. Gilson, *The Legal Infrastructure of High Technology Industrial Districts: Silicon Valley, Route 128, and Covenants Not to Compete,* 74 N.Y.U. L. REV. 575 (1999). That is, the scope of protection given to confidential business information is limited by the same use/creation tradeoff that is present during the productions of patentable inventions and copyrightable works. *See generally,* Easterbrook, *supra* note 2 (discussing general applicability of use/creation tradeoff to a broad set of legal cases); William M. Landes & Richard A. Posner, *An Economic Analysis of Copyright Law,* 18 J. LEGAL STUD. 325 (1989) (discussing limitations on the scope of copyright law); Paul H. Rubin & Peter Shedd, *Human Capital and Covenants Not to Compete,* 10 J. LEGAL STUD. 93 (1981) (finding that enforcement is consistent with the efficiency of balancing the costs and benefits of these restrictions).

[23] *See* Sherwood, *supra* note 11 (noting exit of human capital and suppression of information production from countries in which valuable business information is not effectively protected); *see also* Easterbrook, *supra* note 2 (discussing *ex ante* effects of enforcing restrictive employment contracts); Kitch, *supra* note 4, at 699-700 (same).

[24] *See, e.g.,* Gilson, *supra* note 22; Kitch, *supra* note 4, at 690-91. *But see* Friedman, et al., *supra* note 11 (discussing trade secret law as generally consistent with economic efficiency).

[25] Insider trading, of course, is a separate problem. *See supra* note 12.

[26] *See* Eric A. Posner & George G. Triantis, *Covenants Not to Compete from an Incomplete Contracts Perspective, available at* http://papers.ssrn.com/paper.taf?abstract_id=285805 (September 2001).

[27] *See* Rubin & Shedd, *supra* note 22; Kitch, *supra* note 4.

[28] *See* Kitch, *supra* note 4, at 685.

[29] California Business and Professions Code, §16600.

[30] *See* Posner & Triantis, *supra* note 26.

[31] *See* Gilson, *supra* note 22, at 577-79.

[32] *See* Kitch, *supra* note 4, at 685-88.

[33] *See* Stewart E. Sterk, *Restraints on Alienation of Human Capital,* 79 VA. L. REV. 383, 454-56 (1993).

[34] *See* Epstein, *supra* note 13, at 106 (suggesting that creation of quasi-property right to hot-news allowed the Associated Press to enforce existing customs that evolved between competing news gathering organizations).

[35] *See* Gilson, *supra* note 22, at 627-28.

[36] RESTATEMENT (SECOND) OF CONFLICTS § 188 (1971).

[37] *Id.* § 6.

[38] This result is particularly likely under a "comparative impairment" approach to choice of law, which looks to which state's interests would be most impaired by not enforcing the state's law. *See* William F. Baxter, *Choice of Law and the Federal System,* 16 STAN. L. REV. 1, 17-18 (1963); Erin A. O'Hara & Larry E. Ribstein, *From Politics to Efficiency in Choice of Law,* 67 U. CHI. L. REV. 1151, 1172-74 (2000).

[39] RESTATEMENT (SECOND) OF CONFLICTS § 187(2) (1971).

[40] This controls under U.C.C. §§ 1-105 (2000). *See* DeSantis v. Wackenhut Corp., 793 S.W.2d 670, 677 (Tex. 1990) (describing this as a "party autonomy" approach).

[41] *See* Overholt Crop Ins. Serv. Co. v. Travis, 941 F.2d 1361 (8th Cir. 1991) (upholding a choice of law stipulation contained in a non-competition agreement).

[42] *See, e.g.,* Int'l. Bus. Machines Corp. v. Bajorek, 191 F.3d 1033 (9th Cir. 1999) (denying application of California anti-non-compete statute to denial of stock options and holding that chosen New York law trumps California law).

[43] 61 Cal. App. 4th 881 (Cal. Ct. App. 1998).

[44] RESTATEMENT (SECOND) OF CONFLICTS § 6 (1971).

[45] *Hunter,* 61 Cal. App. 4th at 901.

[46] It has been said that applying the law of the employer's state provides necessary predictability. *See* DeSantis v. Wackenhut Corp., 793 S.W.2d 670, 680 (Tex. 1990) (noting the problems companies may face if forced to abide by various state laws concerning employment contracts). To be sure, that may be a second-best solution if courts refuse to enforce contractual choice of law. But enforcing contractual choice gets the same result across employees without sacrificing the other advantages of contractual choice.

[47] To be sure, the parties may choose the law of a regulating state in order to obtain some of that state's other advantages if they are required to pick a single law for the entire contract rather than being permitted to choose the law specifically governing the restrictive covenant. For example, the parties might choose a state that is generally expert in employment matters even if the state does not enforce all non-competes. However, enforceability of a restrictive covenant may dominate the parties' choice of the applicable law.

[48] *See* O'Hara & Ribstein, *supra* note 38 at 1191.

[49] *See supra* text accompanying note 43. Note, however, that the predictability problem presented in the *Hunter* case was mitigated to some extent by the fact that the party relying on the choice-of-law clause was specifically aware of the possibility of recruitment by California employers and of the possible application of California law, and had structured its employment practices to minimize the possibility of being subject to the California law. *See infra* text following note 58.

[50] *See generally* Gary S. Becker, *A Theory of Competition Among Pressure Groups for Political Influence,* 98 Q. J. ECON. 371 (1983) (outlining an

economic approach to political behavior, choices and influence).
[51] *See* O'Hara & Ribstein, *supra* note 38 at 1153.
[52] *See* Hulcher Serv., Inc. v. R.J. Corman R.R. Co., 543 S.E.2d 461, 465 (Ga. Ct. App. 2001) (noting that "[g]enerally, Georgia will follow a forum selection clause in an employment contract" but noting that the present case involved a law-selection clause); *see also* Ribstein & Kobayashi, *State Regulation, supra* note 19.
[53] *See* 9 U.S.C. § 2. For cases applying the FAA to claims arising under mandatory federal laws, see Circuit City Stores, Inc. v. Adams, 532 U.S. 105 (2001), *on remand,* 279 F.3d 889 (9th Cir. 2002) (holding arbitration clause unconscionable under California state law); Gilmer v. Interstate/Johnson Lane Corp., 500 U.S. 20 (1991) (subjecting a claim under the ADEA to compulsory arbitration pursuant to an arbitration agreement in a securities registration application); Rodriguez de Quijas v. Shearson/Am. Express Inc., 490 U.S. 477 (1989) (holding a pre-dispute agreement to arbitrate claims under the Securities Act of 1933 as enforceable).
[54] *See* Klaxon Co. v. Stentor Electric Mfg. Co., 313 U.S. 487 (1941).
[55] *See* Larry E. Ribstein, *Choosing Law by Contract,* 18 J. CORP. L. 245, 284-86 (1993) (applying an 'interest group' hypothesis to account for differences in results of state and federal court litigation concerning choice of law provisions).
[56] *Id.* at 285.
[57] *See id.* The count was 151 of 216 cases in the Restatement survey and 473 of 663 in the larger survey. The survey of restrictive covenant cases involving contractual choice of law showed that federal courts were slightly more likely to enforce than state courts - about 30% of federal decisions held the clauses unenforceable as compared with about 37% of state decisions. The larger number of federal cases might also reflect party preference for the quality of adjudication in federal court, together with the accessibility of federal court due to the size of the dispute and its multi-state character. *See id.* at 285 n.212.
[58] *See Hunter,* 61 Cal. App. 4th at 881.
[59] *Id.* at 77.
[60] *Id.* at 90 n.22.
[61] *See* Michael Whincop & Mary Keyes, *The Recognition Scene: Game Theoretic Issues in the Recognition of Foreign Judgments,* 23 MELB. U. L. REV. 416 (1999) (analyzing conflicts of law questions using game theory).
[62] *See supra* text accompanying note 44.
[63] *Hunter,* 61 Cal. App. 4th at 905.
[64] *See generally* Richard A. Posner, OVERCOMING LAW 531-551, Harvard Univ. Press (1995); Stigler, *supra* note 1, at 628-29.
[65] *See* Jeffrey Rosen, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 123-24, 207 (2000).
[66] *See id.* at 46-48, 200-01.
[67] *See* Murphy, *supra* note 1, at 2397 (discussing avoidance of such costs as a "dynamic benefit" from protecting privacy).
[68] *See id.* at 2386.
[69] *See* Spencer R. Wood, *The Legal Risks of Monitoring Employee Conduct,* 89 ILL. B.J. 134 (2001) (collecting cases for proposition that business purpose justifies employer surveillance).
[70] *See* Murphy, *supra* note 1, at 2410-11 (discussing the general importance of setting the optimal default rule); *see also* Ribstein & Kobayashi, *State Regulation, supra* note 19.
[71] *See* Murphy, *supra* note 1, at 2414.
[72] *See* Wood, *supra* note 69, at 135.
[73] 255 F. 3d 683 (2001), *cert. denied,* 122 S.Ct. 806 (2002).
[74] Cramer v. Consolidated Freightways, Inc., 209 F. 3d 1122, 1135-36 (9th Cir. 2000) (Fisher, J., dissenting), *rev'd en banc,* 255 F. 3d 683 (9th Cir. 2001).
[75] 255 F. 3d at 698-704 (O'Scannlain, dissenting).

Privacy and Public Policy pg. 532 - Richard D. Lamm

[1] *See generally* WILLIAM E. NELSON, AMERICANIZATION OF THE COMMON LAW: THE IMPACT OF LEGAL CHANGE ON MASSACHUSETTS SOCIETY, 1760-1830 36-45 (1975).
[2] *Id.* at 37.
[3] Leviticus 19:17 (King James) ("Thou shalt not hate thy brother in thine heart: thou shalt in any wise rebuke thy neighbour, and not suffer sin upon him.").
[4] *See* NELSON, *supra* note 1, at 36-38.
[5] *See* ROBERT L. CORD, SEPARATION OF CHURCH AND STATE: HISTORICAL FACT AND CURRENT FICTION 4 (1988).
[6] *See id.*
[7] *See* HENDRIK HARTOG, PUBLIC PROPERTY AND PRIVATE POWER: THE CORPORATION OF THE CITY OF NEW YORK IN AMERICAN LAW, 1730-1860 62 (1983).
[8] *See* CORD, *supra* note 5, at 4.
[9] Ronald P. Corbett, Jr. & Gary T. Marx, *Emerging Technofallacies in the Electronic Monitoring Movement,* in SMART SENTENCING: THE EMERGENCE OF INTERMEDIATE SANCTIONS 85, 86 (James M. Byrne et al. eds., 1992).

Supermarket Cards pg. 534 - Katherine Albrecht

[1] *See* CASPIAN website, *available at* http://www.nocards.org.
[2] Paraphrased from Rick Barlow, *Frequency Marketing in the 21st Century* (1999), *available at* http://www.medill.northwestern.edu/imc/studentwork/pubs/directions/winter00/frequency.pdf.
[3] Barry Janoff, *Private Practice,* PROGRESSIVE GROCER, 79-84 (Jan. 2000), *available at* http://proquest.umi.com/qp...Fmt+3&Deli=1&Mtd=1&Idx=77&Sid+1&RQT'=309.
[4] *See* Sidebar in Appendix.
[5] Robert O'Harrow, Jr., *Consumers Trade Privacy for Lower Prices,* THE WASH. POST, Dec. 31, 1998, at A1, *available at* http://www.washingtonpost.com/wp-srv/washtech/daily/dec98/privacy31.htm.
[6] ACNielsen found that 70% of U.S. households held at least one card in 1999, double the number of households that participated in a card program

in 1996. AC Nielsen, *ACNielsen Study Finds 70 Percent of all U.S. Households Participate in Frequent Shopper Programs* (Apr. 17, 2000), *available at* http://acnielsen.com/news/american/us/2000/20000417.htm.

[7] Archer Daniels Midland Company, *Andreas Leaves Chairmanship after 28 Years* (Jan. 25, 1999), *available at* http://www.admworld.com/oldworld/news/docs/94.htm.

[8] A 1999 AC Nielsen study reported that "100 percent of U.S. households shopped in the grocery channel (including grocery stores with supercenters)." ACNielsen, *ACNielsen Study Finds U.S. Consumers Making Fewer Trips to the Grocery Store* (May 7, 2000), *available at* http://acnielsen.com/news/american/us/2000/20000507.htm.

[9] Anonymous, *Chain Derides Loyalty Card 'Benefits'*, GROCER, June 5, 1999, at 5, *available at* http://proquest.umi.com/pq...mt+4&DELI+1&Mtd+1&Idx=107&Sid=1&RQT=309.

[10] The author did a price comparison on Chase & Sanborn coffee at Shaw's Supermarket. With the card, the item was $0.99, and without card the item was $2.29. This item was also available at a competing, card-free chain for $0.99. These prices were observed on January 12, 2002 in Nashua, New Hampshire. Further details are available from the author.

[11] *See* John Vanderlippe, *Kroger "Card Savings" Exposed as a Sham* (May 2000), *available at* http://www.nocards.org/savings/krogerads.shtml.

[12] Ann M. Raider, *Programs Make Results Out of Research*, MARKETING NEWS, June 21, 1999, at 14, *available at* http://proquest.umi.com/pq...mt+4&DELI+1&Mtd+1&Idx=107&Sid=1&RQT=309.

[13] Curt Avallone, Vice President of Marketing and New Technology, Royal Ahold Stop & Shop, Technology in the Supermarket, Speech at the MIT Media Lab Counter Intelligence (CIT) Luncheon Series (Jan. 22, 2002) (videotape available at CIT). CIT's website is available at http://www.media.mit.edu/ci/resources/events.html. Reference to Mr. Avallone's speech is available at http://www.media.mit.edu/ci/events/luncheonprevious.html. Copy available at University of Denver Law Review office.

[14] Carl Messineo, *Supermarket Sales Carry High Price*, THE COMMON DENOMINATOR, Feb. 8, 1999, at 2, *available at* http://www.thecommondenominator.com/cl020899.html.

[15] *Id.*

[16] For example, John Moritz, Albertson's Marketing Manager in Dallas-Forth Worth, wrote the following in a personal e-mail communication sent to numerous shoppers: "Before we decided to launch the [Albertson's Preferred Savings] card, we conducted extensive consumer research with thousands of Dallas-Fort Worth customers. From this research, Albertson's learned that the majority of our shoppers said they wanted an enhanced savings program." (Dec. 2001).

[17] For a detailed description on one approach to the re-identification process, see Institut d'Investigació en Intelligència Artificial, *On the Re-identification of Individuals Described By Means of Non-Common Variables: A First Approach*, presented at the Work Session on Statistical Data Confidentiality, Statistical Commission and Economic Commission for Europe, Conference of European Statisticians (March 14-16, 2001), *available at* http://www.unece.org/stats/documents/2001/03/confidentiality/17.e.pdf. For an account of planned abuse of this technique by interactive television marketers, see David Burke, *Don't Talk to the Press! White Dot Infiltrates ITV Industry Trade Body, Part One: Privacy at the Yale Club*, *available at* http://whitedot.org/issue/iss_story.asp?slug=privacyattheyaleclub.

[18] Salvador Ochoa, et al., *Reidentification of Individuals in Chicago's Homicide Database: A Technical and Legal Study*, *available at* http://web.mit.edu/sem083/www/assignments/reidentification.html.

[19] John L. Micek, *U.S. Document Sharing Raises Privacy Concerns*, E-COMMERCE TIMES (Apr. 23, 2001), *available at* http://www.ecommercetimes.com/perl/printer/9158.

[20] *Census Bureau Blurs Data to Keep Names Confidential*, INTERACTIVE PRIVACY (Feb. 14, 2001), *available at* http://interactiveprivacy.com/emailstory.asp?id=498.

[21] Ochoa, *supra* note 18.

[22] The author estimates that about one third of grocery chains with card programs required a customer's driver's license and/or social security number on the shopper card application in as late as 1999. *See* CASPIAN's website, *available at* http://www.nocards.org/list/supermarketlist (listing supermarket reports on card requirement details for programs around the country). This trend was reversed in June 2000 with the passage of California legislation. *See* CAL.CIV.CODE.§ 1749.64 (2002) (making it illegal for grocery stores to require identification or social security numbers for supermarket cards). However, some markets still require shoppers to provide their social security number to obtain a card. *See* Dick's Supermarket card application, *available at* http://www.dickssupermarket.com/SavingsClubCard/SavingsClub.

[23] *Supermarkets to Woo "Cocooning" Customers Using Data Strategies According to AccuData America*, AccuData America Press Release (Oct. 31, 2001), *formerly available at* http://biz.yahoo.com/bw/011031/312269_1.html, *now cached at* http://www.google.com/search?q=cache:ARrSpnHIzPoC:biz.yahoo.com/bw/011031/312269_1.html+penetration+profile&hl=en&ie=ISO-8859-1.

[24] *Id.*

[25] *Id.*

[26] *See* Katie Fairbank, *Travelocity Inadvertently Posted Customer Data Online "Human Error" Cited*, THE DALLAS MORNING NEWS, Jan. 24, 2001, at 1D.

[27] *See* Michelle Delio, *Are Crackers Behind AOL Spree?*, WIRED NEWS (Feb. 27, 2002), *available at* http://www.wired.com/news/business/0,1294,50697,00.html.

[28] *Id.*

[29] *See* Linda Rosencrance, *Web Privacy Organization Seeks to Block Toysmart Sale*, COMPUTERWORLD (July 6, 2000), *available at* http://www.computerworld.com/storyba/0,4125,NAV47_STO46729,00.html.

[30] *See* Aaron Pressman, *Voter.com to Sell Membership List*, THE INDUSTRY STANDARD (Mar. 15, 2001), *available at* http://www.thestandard.com/article/display/0,1151,22894,00.html.

[31] *See* Associated Press, *Amazon's Privacy Policy Altered*, WIRED NEWS (Sept. 1, 2000), *available at* http://www.wired.com/news/print/0,1294,38572,00.html.

[32] *See* Troy Wolverton, *Watchdogs Rap eBay Policy Changes*, CNET NEWS.COM (Feb. 26, 2002), *available at* http://news.com.com/2100-1017-845911.html.

[33] *See* Michelle Delio, *Yahoo's 'Opt-Out' Angers Users*, WIRED NEWS (Apr. 2, 2002), *available at* http://www.wired.com/news/privacy/0,1848,51461,00.html.

[34] *See* Dana Hawkins, *Gospel of privacy guru: Be wary; assume the worst*, U.S. NEWS & WORLD REPORT, June 25, 2001, at 71.

[35] *Privacy special report: Selling is getting personal*, CONSUMER REPORTS, Nov. 2000, at 16.

[36] *See* Jennifer Vogel, *When Cards Come Collecting: How Safeway's New Discount Cards Can Be Used Against You,* SEATTLE WKLY., (Sept. 24-30, 1998), *available at* http://www.seattleweekly.com/features/9838/features-vogel.shtml.
[37] *Id.*
[38] MICHAEL S. HYATT, INVASION OF PRIVACY: HOW TO PROTECT YOURSELF IN THE DIGITAL AGE 134 (2001).
[39] *Loyalty Cards Can Open You Up to Criminals,* THEBOSTONCHANNEL.COM, (July 30, 2001), *available at* http://www.thebostonchannel.com/buyerbeware/895259/detail.html.
[40] The author was a guest on KRLD's Marty Griffin radio program when a tape of this incident was aired.
[41] *See* Katie Fairbank, *Grocery Shoppers Sick of Being Carded: Many Resent Trading Information for Savings; Stores Tout Benefits,* DALLAS MORNING NEWS, Dec. 19, 2001, at 1A. The author has details beyond what was printed in this source since she appeared on KRLD's Marty Griffin radio program where a tape of the incident was aired. For more information, contact the author at CASPIAN'S website, *available at* http://www.nocards.org.
[42] *See id.*
[43] *See* Avallone, *supra* note 13.
[44] *See* Sarah B. Scalet, *Checking Out Your Shopping Cart,* CIO MAG. (July 1, 2001) *available at* http://www.cio.com/archive/070101/tl_privacy.html.
[45] *See* Avallone, *supra* note 13.
[46] Boots Insurance website *at* http://www.bootsinsurance.com (visited May 1, 2002).
[47] Boots website *at* http://www.wellbeing.com/Advantagecard/index.jsp (visited May 1, 2002).
[48] Boots website *at* http://www.wellbeing.com/help/adcard_donor.jsp (visited May 1, 2002).
[49] Gemplus Website, *at* http://www.gemplus.com/app/loyalty/boots.htm (visited Apr. 30, 2002) (translation of the website from Chinese into English on file with Denver University Law Review).
[50] *See* SLMsoft.com website, *at* http://www.slmsoft.com/slm/PGE?type=page&pid=0_smart cards.
[51] *See* Michael Y. Park, *Lawyers See Fat Payoffs in Junk Food Lawsuits,* FOX NEWS (Jan. 23, 2002), *at* http://www.foxnews.com/story/0,2933,43735,00.html.
[52] *See* WESTERN GOVERNORS' ASSOCIATION, HEALTH PASSPORT: FREQUENTLY ASKED QUESTIONS, *available at* http://www.westgov.org/wga/initiatives/hpp/faq-fin.htm (visited Mar. 24, 2002).
[53] *See id.*
[54] *See* Press Release, Western Governors' Association, *Health-based Smart Card Demonstration to Expand* (Jan. 25, 1999), *available at* http://www.westgov.org/wga/press/pr1-31-0.htm.
[55] *See* CASPIAN, *supra* note 1.
[56] *See* Press Release, *Friends of the Earth: Supermarket Loyalty Cards to Track GM Food Threat* (Jan. 25, 1999), *available at* http://www.foe.co.uk/pubsinfo/infoteam/pressrel/1999/19990125154458.html (visited Mar. 24, 2002).
[57] *See id.*
[58] SCOTTISH OFFICE, EATING FOR HEALTH: A DIET ACTION PLAN FOR SCOTLAND, *available at* http://www.scotland.gov.uk/library/documents/diet-04.htm.
[59] *Id.*
[60] *See* WORLD HEALTH ORGANIZATION, NUTRITION, *available at* http://www.who.int/nut/aim.htm (including obesity and diet-related diseases within its definition of malnutrition) (emphasis added) (visited Mar. 24, 2002).
[61] *Id.*
[62] *See* William Matthews, *Digging Digital Gold,* FED. COMPUTER WK. (Feb. 7, 2000), *available at* http://www.fcw.com/fcw/articles/2000/0207/tech-datamining-02-07-00.asp.
[63] *See id.*
[64] *Id.*
[65] *See id.*
[66] *See id.*
[67] *See id.*
[68] David Cay Johnston, *New DM tools for the IRS to Sniff Out Tax Cheats,* DSSTAR (Jan. 11, 2000), *available at* http://www.tgc.com/dsstar/00/0111/101240.html (visited Mar. 24, 2002).
[69] *See id.*
[70] Simon Davies, *Big Browser will Watch your Every Move,* THE INDEPENDENT (June 18, 2000), *available at* http://www.independent.co.uk/story.jsp?story=40531.
[71] *See 'Birthday Boy' Gets Special Greeting from Selective Service,* THE RECORD, Aug. 5, 1984, at A22.
[72] *See id.* Farrell's apparently rented its database to a direct-mail broker, but never authorized its release to a government agency. *See id.*
[73] See Robert O'Harrow, Jr., *Bargains at a Price: Shoppers' Privacy; Cards Let Supermarkets Collect Data,* WASH. POST, Dec. 31, 1998, at A01.
[74] *Clinton Backs Tech War on Terror,* BBC NEWS (April 8, 2002), *available at* http://news.bbc.co.uk/hi/english/sci/tech/newsid_1912000/1912895.stm.
[75] David Cleden, *Targeting Criminals Through IT,* POLICE MAG. (Sept. 2001), *available at* http://www.polfed.org/magazine/09_2001_it.htm (visited June 11, 2002).
[76] *Id.*
[77] O'Harrow, *supra* note 5 (quoting Louis Grivetti, Professor of Nutrition at the University of California at Davis).
[78] Scripps Howard News Service, *Washington Calling: Immigration reform? Feds Check Grocery Cards,* NAPLES DAILY NEWS, Perspective (Oct. 7, 2001), *available at* http://www.naplesnews.com/01/10/perspective/d69387a.htm.
[79] D. Ian Hopper, *FTC Backs off Privacy Regs,* ASSOCIATED PRESS ONLINE (Oct. 3, 2001), *available at* http://www.wired.come/news/privacy/0,1848,47262,00.html.
[80] *Id.*
[81] *Id.*
[82] Christine Anthony, *Grocery Store Frequent Shopper Cards: A Window Into Your Home,* 4 B.U.J. SCI. & TECH. L. 4 (Sept. 30, 1998), *available at*

http://www.bu.edu/law/scitech/volume4/4jst107.pdf.
[83] Kevin Poulsen, *Accused DEA Data-Thief Skips Bail,* THE REGISTER (Dec. 2, 2002), *available at* http://www.theregister.co.uk/conten/55/24028.html.
[84] M.L. Elrick, *Information Network: Cops Abuse Database, Three Privacy Suits Say,* DETROIT FREE PRESS (Dec. 25, 2001), *available at* http://www.freep.com/news/mich/lein25_20011225.htm.
[85] M. L. Elrick, *Network Abuse Toppled Woman's Trust of Police,* DETROIT FREE PRESS (July 31, 2001), *available at* http://www.detroitfreepress.com/news/mich/amber31_20010731.htm.
[86] Elrick, *supra* note 85.
[87] Kimberly Kindy, *DMV's Mass License Fraud Persists,* ORANGE COUNTY REGISTER (Oct. 1, 2000), *available at* http://www.ocregister.com/news/features/dmv/dmv01001cci.shtml.
[88] *Id.*
[89] Greg Lucas, *DMV Information Sold Illegally, State Audit Finds Agency Also Reaped Profits by Overcharging Clients,* SAN FRANCISCO CHRON., (July 3, 1997), at A19, *available at* http://www.dui.com/oldwhatsnew/DMV/dmv.info.sold.html.
[90] *Id.*
[91] *Id.*
[92] *Id.*
[93] Martin Evans, *Food Retailing Loyalty Scheme— and the Orwellian Millennium.* BRIT. FOOD J., Vol. 101 No. 2, 1999, at 136.
[94] *TXU Summary Annual Report 2000, available at* http://www.txu.com/investres/invarch/00txuar/company/company_report2.html (last visited June 9, 2002). Through its clubcard program, "Tesco, the UK's largest grocery chain, now offers award points for using TXU energy, which may be 'spent' in its stores." *Id.*
[95] Associated Press, *Woman Sentenced in Identification Fraud* (Jan. 26, 2002), *available at* http://college4.nytimes.com/guests/articles/2002/01/26/898759.xml.
[96] Driver's License Modernization Act of 2002, H.R. 4633, 107th Cong. § 3(a).
[97] *Increased Identification Standards Legislation Introduced by Virginia Congressmen,* AAMVA WK. IN REV. (Am. Ass'n of Motor Vehicle Adm'rs, Arlington, Va.), May 6, 2002, *available at* http://www.aamva.org/weekinreview/20020503.asp.
[98] *Id.*
[99] *New Mexico to Test Smart Card Driver's License,* CardTechnology.com (Mar. 2002), *available at* http://www.eventshome.com/Manual/manualpage.asp?eventId=7145&type=6&manualId=2614&parented=5358&parented=7405&parnentId=11869&parented=11897.
[100] *Oversight Hearing Regarding: Electronic Commerce: The Marketplace of the 21st Century Before the House Committee on Commerce,* 105th Cong. (1998) (statement of Alan Glass, Senior Vice President-Electronic Commerce, MasterCard International), *available at* http://www.mastercard.com/au/about/press/980430a.html.
[101] John E. Siedlarz, *Two Initiatives that will Launch Mass Rollouts of Civilian Uses of Biometrics are a Major Milestone in the Progress of our Industry,* BIOMETRICS ADVOC. REP. (Int'l Biometric Indus. Ass'n, Wash., D.C.), May 17, 2002, *available at* http://www.ibia.org/newslett.htm.
[102] Jane Hadley, *The Latest Way to Pay is at Our Fingertips,* SEATTLE POST-INTELLIGENCER (Apr. 27, 2002), *available at* http://seattlepi.nwsource.com/local/68217_thumb27.shtml.
[103] Press Release, Biometric Access Corporation, *Biometric Access Corporation's SecureTouch-n-Pay Brings Enhanced Transaction Processing to Kroger Stores* (Apr. 11, 2002), *available at* http://biz.yahoo.com/bw/020411/110184_1.html.
[104] Applied Digital Solutions Website, *at* http://www.adsx.com.
[105] *Fla. Family Takes Computer Chip Trip,* CBSNEWS.COM (May 10, 2002), *available at* http://www.cbsnews.com/stories/2002/05/10/tech/main508641.shtml.
[106] Stephanie Simon, *Shopping with Big Brother: The Latest Trend in Market Research is Using Surveillance Devices Such as Hidden Microphones to Spy on Shoppers,* L.A. TIMES (May 1, 2002), *available at* http://www.latimes.com/templates/misc/printstory.jsp?slug=la-050102spy.
[107] *Id.*
[108] Methodology Page on Envirosell's Website, *at* http://www.envirosell.com/method.html (last visited May 1, 2002).
[109] *Id.*
[110] *Id.*
[111] Craig Childress, *Table Tent Cards Finally are Getting Some Respect,* NATION'S RESTAURANT NEWS, Oct. 14, 1996, at 70.
[112] FAQ Page on Envirosell's Website, *at* http://www.envirosell.com/faqs.html (last visited May 1, 2002).
[113] *Id.*
[114] *Id.*
[115] Client List on Envirosell's Website, *at* http://www.envirosell.com/clients/clients_r.html.
[116] *Brickstream Builds Video-Based Retail Customer Intelligence,* COLLOQUY (Jan. 24, 2002), *available at* http://www.colloquy.com/cont_breaking.com/global.asp?file=partners_overview.asp.
[117] *Id.*
[118] Point Grey's website illustrates the invasiveness of these technologies through a video on its website at http://www.ptgrey.com/products/censys3d/index.htm.
[119] *Supermarkets Check You Out,* BEYOND 2000 (June 13, 2000), *available at* http://beyond2000.com/news/story_475.html.
[120] *Id.*
[121] *Id.*
[122] *Id.*
[123] Press Release, ShopperTrak RCT, *ShopperTrak and RCT Systems Merge to Form World's Leading Retail Intelligence Company: ShopperTrak RCT Will Provide Retailers with the Tools Necessary to Make Effective Business Decisions* (Dec. 19, 2001), *available at* http://biz.yahoo.com/bw/011219/192420_1.html.
[124] ShopperTrak Website, *at* http://www.shppertrak.com/orbit.htm.
[125] *Shopping Carts to Track Customer Movements, available at* http://www.nocards.org/news/supermarketnews_tech.shtml (Aug. 8, 2000).
[126] *Id.*

[127] *Id.*
[128] Press Release, Klever Marketing, Inc., *Hy-Vee and Klever Marketing Pair Up to Deploy Wireless Retail Network* (Apr. 25, 2001), *available at* http://www.kleverkart.com/pr04252001_1.html.
[129] *Id.*
[130] *Klever-KardSM -Future Enhancement, available at* http://kleverkart.com/retailer_kleverkard.html.
[131] Dan Alaimo, *Hy-Vee Shopping Carts Going Wireless,* SUPERMARKET NEWS (May 14, 2001), *available at* http://www.kleverkart.com/sn05142001.pdf.
[132] *Id.*
[133] *Id.*
[134] *Semcor Information Systems and Services, Geographic Information Systems, Tracking, available at* http://corpweb.semcor.com/gis/solutions/type/route/tracking.html.
[135] *Id.*
[136] *Id.*
[137] Bridge Technology Website, *at* http://www.bridgetech.net/tranz-system-toc.htm.
[138] Jorge Martinez & Winslow Burleson, *Floor Scale, available at* http://www.media.mit.edu/ci/projects/floorscale.html.
[139] *Semcor, supra* note 134.
[140] Martinez & Burleson, *supra* note 138.
[141] Simon, *supra* note 106.
[142] *Id.*
[143] *Id.*
[144] *Id.*
[145] *Id.*
[146] Applied Digital Solutions Website, *at* http://www.adsx.com.
[147] *Auto-ID Center: Questions, available at* http://www.autoidcenter.org/questions19.asp.
[148] Greg Jacobson, *Technology Revolution Underway,* CHAIN DRUG REV. (Oct. 22, 2001), *available at* http://www.chaindrugreview.com/articles/tech_revolution.html.
[149] Auto Center Joins UK Group, MIT TECH TALK (Jan. 24, 2001), *available at* http://web.mit.edu/newsoffice/tt/2001/jan24/auto.html.
[150] *Introduction to Auto-ID, available at* http://www.autoidcenter.org/technology.asp.
[151] *The Electronic Product Code (ePC), available at* http://www.eretailnews.com/Features/0105epc1.htm.
[152] Steve Traiman, *Tag, You're It! The ePC Tag Could Revolutionize the Retail Supply Chain,* RETAIL SYSTEMS RESELLER (Nov. 2001), *available at* http://www.retailsystemsreseller.com/archive/Nov01/Nov01_5.shtml.
[153] *See ePC, supra* note 151.
[154] *Id.*
[155] Traiman, *supra* note 152.
[156] Margie Semilof, *Bar Codes in a Chip,* INTERNETWEEK.COM (Nov. 19, 2001), *available at* http://www.internetweek.com/newslead01/lead111901.htm.
[157] Lisa Roner, *T2T -The Next Wave of the Internet Revolution,* EYEFORPHARMA, *available at* http://www.eyeforpharma.com/index.asp?news=2822 (n.d.).
[158] Semilof, *supra* note 156.
[159] Robin Cover, *Auto-ID Center Uses Physical Markup Language in Radio Frequency Identification (RF ID) Tag Technology,* THE XML COVER PAGES (Nov. 21, 2001), *available at* http://xml.coverpages.org/ni2001-11-21-c.html.
[160] Cheryl Rosen & Mathew G. Nelson, *The Fast Track: Radio-frequency Devices Promise to Make it Easier to Monitor the Flow of Inventory Across the Supply Chain,* INFORMATION WEEK (June 18, 2001), *available at* http://www.informationweek.com/shared/printableArticle?doc_id=IWK20010618S0001; *see also* Charles W. Schmidt, *The Networked Physical World, available at* http://www.rand.org/scitech/stpi/ourfuture/Internet/sec4_networked.html (last visited Apr. 5, 2002); Indrani Rajkhowa, *Shopping Gets Smarter,* COMPUTERSTODAY (June 16-30, 2001), *available at* http://www.india-today.com/ctoday/20010616/marvels.html.
[161] Cover, *supra* note 159.
[162] Charles W. Schmidt, *The Networked Physical World, available at* http://www.rand.org/scitech/stpi/ourfuture/Internet/sec4_networked.html.
[163] Lori Valigra, *Smart Tags: Shopping Will Never Be the Same,* CHRISTIAN SCIENCE MONITOR (Mar. 29, 2001), *available at* http://www.csmonitor.com/durable/2001/03/29/fp13s1-csm.shtml.
[164] M.K. Shankar, *Algorithm Ensures Unique Object ID,* NIKKEI ELECTRONICS ASIA (Apr. 2001), *available at* http://www.nikkeibp.asiabiztech.com/nea/200104/inet_127161.html.
[165] *Id.*
[166] *Id.*
[167] Auto-ID Center, *Applications, available at* http://www.autoidcenter.org/technology_applications.asp.
[168] Auto-ID Center, *Sponsor Companies, available at* http://www.autoidcenter.org/sponsors_companies.asp.
[169] Cheryl Rosen & Mathew G. Nelson, *The Fast Track: Radio-frequency Devices Promise to Make it Easier to Monitor the Flow of Inventory Across the Supply Chain,* INFORMATIONWEEK (June 18, 2001), *available at* http://www.informationweek.com/shared/printableArticle?doc_id=IWK20010618S0001.
[170] Junko Yoshida, *Euro Bank Notes to Embed RFID Chips by 2005,* EETIMES (Dec. 19, 2001), *available at* http://www.eetimes.com/story/OEG20011219S0016.
[171] *Id.*
[172] George Cole, *The Little Label with an Explosion of Applications,* FIN. TIMES (Jan. 15, 2002), *available at* http://news.ft.com/ft/gx.cgi/ftc?pagename=View&c=Article&cid=FT30414MGWC.
[173] *Id.*
[174] Testimony before the U.S. House of Representatives, Tuesday September 19th, 2000. Subcommittee on Domestic and International Monetary

Policy, Committee on Banking and Financial Services, Washington, DC., *available at* http://commdocs.house.gov/committees/bank/hba66988.000/hba66988_0.HTM#68.

[175] *Id.*; Auto-ID website Auto-ID Center, *Sponsor Companies, available at* http://www.autoidcenter.org/sponsors_companies.asp.

[176] Kayte VanScoy, *Can the Internet Hot-Wire P&G?: They Know What You Eat,* ZIFF DAVIS SMART BUSINESS (Jan. 1, 2001), *available at* http://www.smartbusinessmag.com/article/0,3668,a=13216,00.asp.

[177] Cover, *supra* note 159.

[178] John Stermer, *Radio Frequency ID: A New Era for Marketers?,* CONSUMER INSIGHT MAGAZINE (Winter 2001), *available at* http://acnielsen.com/pubs/ci/2001/q4/features/radio.htm.

[179] Schmidt, *supra* note 162.

[180] Auto-ID Center, *available at* http://www.autoidcenter.org/applications.asp.

[181] VanScoy, *supra* note 176.

[182] David Orenstein, *Raising the Bar,* BUSINESS 2.0 (Aug. 2000), *available at* http://www.business2.com/articles/mag/0,1640,13975[3,FF.html.

[183] Indrani Rajkhowa, *Shopping Gets Smarter,* COMPUTERSTODAY (June 16-30, 2001), *available at* http://www.india-today.com/ctoday/20010616/marvels.html.

[184] John Goss, *Marketing the New Marketing: The Strategic Discourse of Geodemographic Information Systems, in* GROUND TRUTH: THE SOCIAL IMPLICATIONS OF GEOGRAPHIC INFORMATION SYSTEMS 130, 163 (John Pickles, ed., 1995).

[185] *See* CASPIAN's Media Mentions page for a more complete listing, *available at* http://www.nocards.org/press/mediamentions.shtml.

[186] *See* Welcome to CASPIAN, *available at* http://www.nocards.org/welcome/index.shtml (explaining CASPIAN's purpose and philosophy).

[187] *See, e.g.*, CLAIRE WOLFE & AARON ZELMAN, THE STATE VS. THE PEOPLE: THE RISE OF THE AMERICAN POLICE STATE 77-80 (2001).

[188] *See, e.g., What Savings? CASPIAN Shoppers Discuss Kroger "Card Savings," available at* www.nocards.org/savings/savingsletterskroger.shtml (explaining that shoppers frequently send CASPIAN a large volume of copies of letters and emails they have written to grocery chains, along with the replies they receive).

[189] *Id.*

[190] *See* Katherine Albrecht, *Food for Thought, 10 Reasons Not to Use a Fake Card, available at* http://www.nocards.org/essays/nofakes.shtml (explaining why using a fake card is not a good long-term solution to the shopper card program).

[191] *See, e.g.*, Julia Lane, *Attitudes of Respondents Toward Data Confidentiality,* presented at the Work Session on Statistical Data Confidentiality, Statistical Commission and Economic Commission for Europe, Conference of European Statisticians, Mar. 14-16, 2001, *available at* http://www.unece.org/stats/documents/2001/03/confidentiality/crp.3.e.pdf (explaining Prof. Julia Lane's findings).

[192] Frank Franzak et al., *Online Relationships and the Consumer's Right to Privacy,* 18 J. OF CONSUMER MARKETING 631, 640 (2001).

[193] Frederick Douglass, West India Emancipation (Aug. 4, 1857) & Dred Scott (May 1857), *in* TWO SPEECHES BY FREDERICK DOUGLASS, at 22, *available at* http://memory.loc.gov/ammem/doughtml/dougFolder3.html.

[194] Albertsons press release, *Albertson's, Inc. Announces a Better way to Save, available at* http://www1.albertsons.com/corporate/default_news.asp?Action=Continue&ContentId=1070.

[195] *Winn-Dixie to Reward Loyal Customers,* NEWSTREAM.COM (March 2002), *available at* http://www.newstream.com/us/story_pub.shtml?story_id=5277&user_ip=208.3.160.71.

[196] *See* Avallone, *supra* note 13.

[197] *Id.*

[198] *Id.*

[199] *See* http://www.nocards.org/protest/IrvingAlbertsons/ (displaying photographs of the protest).

[200] Maria Halkias, *Wal-Mart Gains in Dallas Fort-Worth Grocery Market,* DALLAS MORN. NEWS, Feb. 26, 2002, at 1D.

[201] David Pringle, *Retailers Scrap High-Tech Ideas for Marketing — Safeway of Britain Finds Loyalty-Card Generated Useless Data,* WALL ST. J., June 19, 2000, at A9C.

[202] Raley's Inc., HOOVER'S ONLINE, *available at* http://www.hoovers.com/co/capsule/6/0,2163,40386,00.html (profiling Raley's Inc.).

[203] Wild Oats Markets, Inc., HOOVER'S ONLINE, *available at* http://www.hoovers.com/co/capsule/7/0,2163,41717,00.html (profiling Wild Oats Markets, Inc.).

[204] ANDREW SETH & GEOFFREY RANDALL, THE GROCERS: THE RISE AND RISE OF THE SUPERMARKET CHAINS 193 (2d ed. 2001).

[205] Esther Addley, *CardTricks,* GUARDIAN UNLIMITED (May 11, 2000), *available at* http://www.guardian.co.uk/Archive/Article/0,4273,4016830,00.html.

[206] *Safeway Sales Rise,* BBC NEWS (July 11, 2000), *available at* http://news.bbc.co.uk/hi/english/business/newsid_829000/829080.stm.

[207] Addley, *supra* note 205.

[208] C.S. LEWIS, MERE CHRISTIANITY 36 (1st paperback prtg. 1960).

[209] Lane, *supra* note 191.

[210] *Id.* at 2.

[211] *See, e.g.*, Brian Krebs, *Congress Reopens Debate On National ID Card,* NEWSBYTES (Nov. 16, 2001), *available at* http://www.newsbytes.com/news/01/172252.html.

[212] *Id.*

[213] *See, e.g.*,Lisa Greene, *Face Scans Match Few Suspects,* ST. PETERSBURG TIMES (Feb. 16, 2001), *available at* http://www.sptimes.com/News/021601/TampaBay/Face_scans_match_few_.shtml.

[214] *See, e.g.*, R.J. RUMMEL, DEATH BY GOVERNMENT (New Jersey: Transaction Publishers, 1994).

[215] Figures represent billions of dollars and have been rounded to the nearest billion. Sales figures are from the Food Marketing Institute. Current figures *available online at* http://www.fmi.org/facts_figs/faq/top_retailers.htm.

Right to Privacy of Medical Records pg. 540 - Joel Glover & Erin Toll

[1]Joel Glover, Esq. is a partner with the law firm Rothgerber Johnson & Lyons LLP practicing insurance and health care law. Erin Toll, Esq. is the Director of Consumer Affairs, Compliance, at the Colorado Division of Insurance. The views and opinions reflected herein are solely those of the authors and do not reflect the views or opinions of their respective organizations, firms or clients.

[2] Ferguson v. City of Charleston, 532 U.S. 67, 78 (2001).

[3] 5 U.S.C. § 552a (2000). Another federal law, the Gramm-Leach-Bliley Act, Pub. L. No. 106-102 (GLBA), signed by President Clinton on Nov. 12, 1999, also addresses privacy issues. While the GLBA's prohibitions apply to medical records, its main focus is on regulating the disclosure of non-public financial information by "financial institutions" defined in GLBA (i.e., the banking, insurance and securities industries). Accordingly, an analysis of the GLBA is outside the scope of this article.
[4] Whalen v. Roe, 429 U.S. 589 (1977).
[5] *Id.*
[6] *Id.* at 601-06.
[7] *Id.* at 591.
[8] *Id.* at 603-04.
[9] *Id.* at 599-600.
[10] *Id.* at 601.
[11] *Id.* at 602.
[12] *Id.*
[13] *Id.* at 605.
[14] *Id.*
[15] E.I. du Pont de Nemours & Co. v. Finklea, 442 F. Supp. 821, 824 (S.D.W.V. 1977).
[16] *Id.* The court assumed "without deciding, that du Pont, in its status as an employer, has standing to raise the 'right of privacy' issue." *Id.*
[17] *Id.* at 824-25.
[18] *Id.*
[19] *Id.* at 825-26.
[20] 451 F. Supp. 1355 (D.N.J. 1978).
[21] *Id.* at 1381.
[22] *Id.*
[23] *Id.*
[24] United States v. Westinghouse Elec. Corp., 638 F.2d 570, 577 (3d Cir. 1980) (citation omitted).
[25] *Id.* at 577.
[26] *Id.*
[27] *Id.* at 577. Medical records have been held to constitute "records" subject to the protections under the Privacy Act (5 U.S.C. § 552a (2000)) where they discussed medical history, clinical observations and suggested therapies. Williams v. Dep't of Veterans Affairs, 104 F.3d 670 (4th Cir 1997).
[28] *In re* Search Warrant, 810 F.2d 67, 71-72 (3d Cir. 1987).
[29] Doe v. S.E. Pa. Transp. Auth., 72 F.3d 1133, 1138 (3d Cir. 1995).
[30] *Id.*
[31] Jarvis v. Wellman, 52 F. 3d 125, 126 (6th Cir. 1995).
[32] 186 F.3d 469 (4th Cir. 1999).
[33] *Ferguson,* 186 F.3d at 482.
[34] Ferguson v. City of Charleston, 532 U.S. 67, 78 (2001). To support this proposition, the Court cited to the "Brief for American Medical Association et al. as *Amici Curiae* 11; Brief for American Public Health Association et al. as *Amici Curiae* 6, 17-19." *Id.*
[35] Whalen v. Roe, 429 U.S. 589, 599-600 (1977).
[36] *Whalen,* 429 U.S. at 599-600.
[37] 854 F.2d 1379 (D.C. Cir. 1988).
[38] *Bowen,* 854 F.2d at 1389.
[39] *Id.* at 1383.
[40] *Id.*
[41] *Id.* at 1389.
[42] United States v. Westinghouse Elec. Corp., 638 F.2d 570, 578 (3d Cir. 1980).
[43] *Westinghouse,* 638 F.2d at 578.
[44] *Id.* at 578-80.
[45] *Id.* at 579.
[46] *Id.* at 580.
[47] *Id.* at 581.
[48] 810 F.2d 67 (3d Cir. 1987).
[49] In re *Search Warrant,* 810 F.2d at 72-73.
[50] 812 F.2d 105 (3d Cir. 1987).
[51] *Fraternal Order of Police,* 812 F.2d at 114.
[52] *Id.*
[53] Doe v. Southeastern Pennsylvania Transp. Auth., 72 F.3d 1133, 1138 (3d Cir. 1995).
[54] *SEPTA,* 72 F.3d at 1138-39.
[55] *Id.* at 1143.
[56] *Id.* at 1138.
[57] *Id.* at 1140-1141.
[58] Shoemaker v. Handel, 608 F. Supp. 1151, 1159 (D.N.J. 1985).
[59] *Shoemaker,* 608 F. Supp. at 1160.
[60] *Id.*
[61] *Id.* at 1161.
[62] 85 F. Supp. 2d 545 (D. Md. 1999).
[63] *Board of Physician Quality Assurance,* 85 F. Supp. 2d at 548.

[64] *Id.* at 546.
[65] *Id.* at 548.
[66] 228 F.3d 341 (4th Cir. 2000).
[67] *Id.* at 344.
[68] *Id.* at 351.
[69] *Id.* The Fourth Circuit panel in *In Re: Subpoena Duces Tecum* did not discuss the purported division among the circuits on the right to privacy in medical records noted in the Fourth Circuit's decision in *Ferguson*.
[70] *Id.*
[71] *Id.*
[72] Augustin v. Barnes, 626 P.2d 625, 629-30 (Colo. 1981).
[73] *Id.* at 629.
[74] *Id.* at 629-30.
[75] *Id.* at 630.
[76] *Id.*
[77] *Id.*
[78] Augustin v. Barnes, 626 P.2d 625, 630 (Colo. 1981).
[79] Belle Bonfils Memorial Blood Center v. District Court, 763 P.2d 1003, 1012 (Colo. 1988).
[80] *Id.* at 1004.
[81] *Id.* at 1005.
[82] *Id.* at 1012.
[83] *Id.*
[84] *Id.*
[85] Belle Bonfils Memorial Blood Center v. District Court, 763 P.2d 1003, 1012 (Colo. 1988).
[86] *Id.* at 1014.
[87] Indeed, the existence of an individual right of privacy that is balanced by societal interests is also evident in Colorado statutes and agency regulations. *See, e.g.* COLO. REV. STAT. §§ 24-72-204(3)(a)(I), (open records laws prohibit inspection of medical or mental health data); COLO. REV. STAT. 10-3-1104.5(1) and (4)(b) ("The general assembly declares that a balance must be maintained between the need for information by those conducting the business of insurance and the public's need for fairness in practices for testing for the human immunodeficiency virus, including the need to minimize intrusion into an individual's privacy and the need to limit disclosure of the results of such testing."); COLO. REV. STAT. 10-3-1104.7(1)(c) and (3)(a) ("To protect individual privacy and to preserve individual autonomy with regard to the individual's genetic information, it is appropriate to limit the use and availability of genetic information.") 3 Colo. Code Regs. § 702-6, Regulation 6-4-1 (licensees shall not disclose nonpublic personal health information without authorization except where performing certain insurance functions, including the detection of insurance fraud, misrepresentation and criminal activity).
[88] *See, e.g.,* Ross v. Trumbull County Child Support Enforcement Agency, 2001 Ohio App. LEXIS 495 (Ohio App. 2001) (citing *Levias v. United Airlines,* 27 Ohio App. 3d 222, 500 N.E.2d 370 (1985)).
[89] Tureen v. Equifax, Inc., 571 F.2d 411, 416-417 (8th Cir. 1978) (The court rejected any liability for the alleged tort "[b]ecause there may be a legitimate purpose for the collection and even the disclosure, in certain circumstances, of an individual's past insurance history.")
[90] 98 A.L.R. 3d 561 (citing 62 Am Jur 2d, Privacy § 1; Restatement of Torts 2d §§ 652B-652E).
[91] *Ross,* 2001 Ohio App. LEXIS 495, at 13 (citing *Hahn v. Kotten,* 43 Ohio St. 2d 237, 244, 331 N.E.2d 713 (1975)).
[92] *Id.* at 2-4.
[93] *Id.*
[94] *Id.*
[95] *Id* at 16.
[96] *Levias,* 500 N.E.2d at 373.
[97] *Id.*
[98] *Id.*
[99] *Id.* at 374.
[100] *Id.* at 375-76.
[101] Robert C. Ozer, P.C. v. Borquez, 940 P.2d 371, 379 (Colo. 1997).
[102] *Id.* at 377.
[103] *See generally* Health Insurance Portability & Accountability Act of 1996, Pub. L. No. 104-191, § 110 Stat. 1936 (1996).
[104] *See generally id.*
[105] *See* Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82462, 82464 (proposed Dec. 28, 2000) (to be codified at 45 C.F.R. pts. 160 and 164).
[106] *See id.*
[107] *HHS Fact Sheet,* July 6, 2001, *available at* http://www.hhs.gov/news/press/2001pres/ 01fsprivacy.html.
[108] *See* Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82462, 82464 (proposed Dec. 28, 2000) (to be codified at 45 C.F.R. pts. 160 and 164).
[109] *See id.* at 82465.
[110] *Id.*
[111] *Id.* at 82466.
[112] *See id.* at 82466-67.
[113] *Id.* at 82464.
[114] Admittedly, the HIPAA regulations are complex and a comprehensive analysis of those regulations and compliance therewith would require much more extensive and detailed coverage. That level of analysis is beyond the scope of this article, which focuses on the extent to which medical records are private rather than on how to comply with HIPAA.

[115] *See* Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82462, 82465.
[116] *See generally* Health Insurance Portability & Accountability Act of 1996, Pub. L. No. 104-191, § 110 Stat. 1936 (1996).
[117] Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82462, 82464.
[118] *See generally* Health Insurance Portability & Accountability Act of 1996, Pub. L. No. 104-191, § 110 Stat. 1936 (1996).
[119] *Id.*
[120] *Id.*
[121] Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82462, 82467.
[122] 45 C.F.R. § 164.502.
[123] *Id.*
[124] 45 C.F.R. § 164.501.
[125] 45 C.F.R. § 164.514.
[126] *Id.*
[127] 45 C.F.R. § 164.512.
[128] *Id.*
[129] Other examples include to persons subject to the Food and Drug Adminsitration and to an employer, each under certain circumstances, and for judicial and administrative proceedings. 45 C.F.R. § 164.512.
[130] 45 C.F.R. § 164.512.
[131] *Whalen*, 429 U.S. at 602.

Sodomy Laws and Privacy pg. 546 - Michael E. Brewer

[1] *See* THE BOOK OF THE GENERAL LAWES AND LIBERTYES CONCERNING THE INHABITANTS OF THE MASSACHUSETTS (Harvard University Press, 1929). Along with adultery, murder, and lying with a beast, the crime of a man lying with another man is a capital offense.
[2] *See* 2 WILLIAM BLACKSTONE, COMMENTARIES 215 (1866).
[3] *See* JOHN DE'MILIO & ESTELLE B. FREEDMAN, INTIMATE MATTERS : A HISTORY OF SEXUALITY IN AMERICA 122 (Harper & Row, 1988).
[4] Janet E. Halley, *Reasoning About Sodomy: Act and Identity in and after* Bowers v. Hardwick, 79 VA. L. REV. 1721, 1722 (1993).
[5] Contemporary examples of the identification of homosexuality and sodomy are common and sometimes tragically comic. A Queens Borough school board refused to allow teachers to mention the existence of same-sex parents because it did not want to promote acceptance of sodomy. Campaign buttons distributed in Oregon in opposition to a gay rights amendment to the state constitution declared, "Sodomy is not a special right." Sen. Strom Thurmond, when reminded that gays and lesbians were employed as congressional staffers, responded that "Sodomy is against the law. Why shouldn't they be arrested?" *Id.* at 1736-37.
[6] Lawrence R. Murphy, *Defining the Crime Against Nature: Sodomy in the United States Appeals Courts*, 1810-1940, 19 J. HOMOSEXUALITY 49, 62 (1990).
[7] *See* People v. Hodgkin, 53 N.W. 794, 795 (Mich. 1892).
[8] *See Hodgkin*, 53 N.W. 794. The court reversed the conviction because there was no finding of emission by the lower court.
[9] *See* Prindle v. State, 21 S.W. 360 (Tex. Crim. App. 1893); Mitchell v. State, 95 S.W. 500 (Tex. Crim. App. 1906) (citing *Wharton* in finding that fellatio is not a crime at common law); *see also* Kinnan v. State, 125 N.W. 594, 595 (Neb. 1910); Munoz v. State, 281 S.W. 857 (Tex. Crim. App. 1926) (finding that fellatio is not a crime defined by statutes adopting the common law).
[10] *See* Fennel v. State, 32 Tex. 378 (Tex. 1869).
[11] *See* People v. Boyle, 48 P. 800 (Cal. 1887).
[12] *See* State v. Smith, 38 S.W. 717, 717-18 (Mo. 1897) (describing the actions of a police officer convicted of taking a 16-year-old boy to a lumber yard and initiating sexual contact).
[13] *See* State v. Murry, 66 So. 963, 963-64 (La. 1914) (declining to detail the actions of defendant, convicted of perpetrating the act of buggery on a 12 year-old boy).
[14] *See* James v. State, 134 S.W. 699 (Tex. Crim. App. 1911).
[15] *See* State v. Guerin, 152 P. 747, 748 (Mont. 1915).
[16] *See Guerin*, 152 P. at 748.
[17] *See* Thompson v. Aldredge, 200 S.E. 799, 800 (Ga. 1939) (citing GA. CODE ANN. § 26-5901 (1933) (current version at GA. CODE ANN. § 16-6-2 (2001) (defining sodomy as "the carnal knowledge and connection against the order of nature, by man with man, or in the same unnatural manner with woman."), and 1 FRANCIS WHARTON, CRIMINAL LAW § 754 (11th ed. 1912) ("[T]he crime of sodomy proper cannot be accomplished between two women, though the crime of bestiality may be.")).
[18] For this paper, 148 appeals court cases from 26 states were retrieved in searches in the *Centennial Digest* (to 1919), LEXIS, and WESTLAW. The three states with the largest number of cases found are California (34), Texas (22), and Missouri (7). The chronological distribution of the cases is: 1880-89 (*5*), 1890-99 (*18*), 1910-19 (*25*), 1930-39 (*24*), 1900-09 (*28*), 1920-29 (*23*), 1940-44 (*27*). In his article on sodomy appeals from 1810 to 1940, Lawrence Murphy identified 226 sodomy appeals prior to 1950 in the *Centennial Digest*. His research yielded this chronological distribution:
1800-59 (*2*), 1870-79 (*3*), 1890-99 (*15*), 1910-19 (*33*), 1930-39 (*32*), 1860-69 (*4*), 1880-89 (*5*), 1900-09 (*23*), 1920-29 (*40*), and 1940-49 (*68*).
Murphy, *supra* note 6, at 63, n. 3.
[19] *See* Bowers v. Hardwick, 487 U.S. 186, 190-91 (1986).
[20] *See, e.g.*, Powell v. State, 510 S.E.2d 18, 24 (Ga. 1998) (concluding that "unforced sexual behavior conducted in private between adults . . . is at the heart of the Georgia Constitution's protection of the right to privacy."); Commonwealth v. Wasson, 842 S.W.2d 487, 493 (Ky. 1992) (stating that "[d]eviate sexual intercourse conducted in private by consenting adults is not beyond the protections of . . . the Kentucky Constitution . . ."); Campbell v. Sundquist, 926 S.W.2d 250, 262 (Tenn. Ct. App. 1996) (holding the "Homosexual Practices Act, T.C.A. § 39-13-510 . . . unconstitutional" because " . . . our citizens' fundamental right of privacy . . . encompasses the right of the plaintiffs to engage in consensual, private, non-commercial, sexual conduct . . .").
[21] The supreme courts of Louisiana and Minnesota have declined to invalidate their states' sodomy laws on the theory that those laws violate a

constitutionally guaranteed right to privacy. *See* State v. Smith, 766 So. 2d 501, 510 (La. 2000) and State v. Gray, 413 N.W.2d 107, 114 (Minn. 1987).
[22] As of 1993, twenty-eight states and the District of Columbia had repealed their sodomy laws, seventeen states prohibited sodomy regardless of the sex of the parties, and five states prohibited same-sex sodomy without proscribing cross-sex sodomy. *See* Halley, *supra* note 4, at 1732.
[23] *See* Halley, *supra* note 4, at 1722.
[24] *Id.* at 1722.
[25] Christopher R. Leslie, *Creating Criminals: The Injuries Inflicted by "Unenforced" Sodomy Laws,* 35 HARV. C.R.-C.L. L. REV. 103, 110-128 (2000).
[26] *See* RICHARD A. POSNER, SEX AND REASON 291 (1992).
[27] *See id.*
28 *See generally* POSNER, *supra* note 26.
[29] *See id.*
[30] *See id.*
[31] *See id.*
[32] *Id.* at 88.
[33] *See* Richard C. Friedman & Jennifer I. Downey, *Homosexuality,* 331 NEW. ENG. J. MED. 923, 928 (1994).
[34] *See* POSNER, *supra* note 26, at 299.
[35] *See id.*
[36] *See id.*
[37] *See id.* at 157.
[38] *See id.* at 157-58.
[39] *Id.*
[40] Discussion of where they do lie is beyond the scope of this article. It is worth mentioning in this context, though, that some socio-biological theories relate anti-gay sentiment to the inherent drive of the species to reproduce, which, in theory, is inimical to the non-reproductive sex of gay people. However, these theories do not account for the demonstrable variations of acceptance of same-sex activity in different cultures, and Posner does not rely on them. An area which Posner does not explore in regard to anti-gay feeling is Judeo-Christian mores and literature, from which Anglo-American culture draws heavily. *See* DANIEL A. HELMINIAK, WHAT THE BIBLE REALLY SAYS ABOUT HOMOSEXUALITY (1994).
[41] POSNER, *supra* note 26, at 201-02.
[42] *See id.* at 207.
[43] *See id.* at 117, 207.
[44] *See* Freidman & Downey, *supra* note 33.
[45] *See* POSNER, *supra* note 26, at 207.
[46] Colorado attempted to do this in 1992 when it passed "Amendment 2" to its constitution.
[47] *See* POSNER, *supra* note 26, at 207.

I'm Watching You pg. 550 - Leslie E. Nunn, Dane Patridge, & Brian McGuire

[1] Gregory Weaver, *A Click Too Far,* INDIANAPOLIS STAR, June 12, 2000, at E01.
[2] Ann Carrns, *Prying Times: Those Bawdy E-Mails Were Good for a Laugh—Until the Ax Fell,* WALL ST. J., Feb. 4, 2000, at A1.
[3] *Id.*; Bill Wallace & Jamie Fenton, *Is Your PC Watching You? New Desktop Snoopware Products Let Anyone—Boss, Business Partner, or Spouse—Track Your PC Habits,* PC WORLD, Dec. 1, 2000, at 59, *available at* http://www.pcworld.com/news/article/0,aid,32863,00.asp.
[4] American Management Association, *2001 Workplace Monitoring & Surveillance: Policies and Practices, available at* http://www.amanet.org/research/pdfs/emsfu_short.pdf (last visited Feb. 27, 2002).
[5] *Id.*
[6] *Id.*
[7] Michael J. McCarthy, *Data Raid: In Airline's Suit, PC Becomes Legal Pawn, Raising Privacy Issues,* WALL ST. J., May 24, 2000, at A1.
[8] *See* Michael J. McCarthy, *Thinking Out Loud: You Assumed 'Erase' Wiped Out That Rant Against the Boss? Nope,* WALL ST. J., March 7, 2000, at A1.
[9] American Management Association, *supra* note 4.
[10] Jerry Crimmins, *Even Federal Judges Come Under Surveillance When Online,* CHI. DAILY L. BULL., Aug. 14, 2001, at 1.
[11] *Id.* The entire United States Judicial Conference was scheduled to consider the recommendations of the Committee on Automation and Technology on September 11, 2001. *Id.*
[12] *See* 16A AM. JUR. 2d *Constitutional Law* § 399 (1998).
[13] *See* Terry v. Ohio, 392 U.S. 1, 8-9 (1968).
[14] U.S. CONST. amend. IV.
[15] United States v. Jacobsen, 466 U.S. 109, 113-14 (1984)(quoting Walter v. United States, 447 U.S. 649, 662 (1980)(Blackmun, J., dissenting)).
[16] *Jacobsen,* 466 U.S. at 113.
[17] *See, e.g.*, Dawson v. State, 868 S.W.2d 363, 367 (Tex. App. 1993)(citing Crosby v. State, 750 S.W.2d 768, 773 (Tex. Crim. App. 1987)).
[18] *Id.* (quoting *Crosby,* 750 S.W.2d at 773).
[19] *Id.* (quoting *Crosby,* 750 S.W.2d at 773).
[20] *See* United States v. Mankani, 738 F.2d 538, 542 (2d Cir. 1984).
[21] *See Mankani,* 738 F.2d at 542-43.
[22] *Id.* at 543.
[23] *See* Mapp v. Ohio, 367 U.S. 643, 645 (1961).
[24] *See* Katz v. United States, 389 U.S. 347, 353 (1967).
[25] *See* Kyllo v. United States, 533 U.S. 27, 29-30 (2001).
[26] *See* United States v. Jacobsen, 466 U.S. 109, 113 (1984).
[27] *See Jacobsen,* 466 U.S. at 113.
[28] California v. Ciraolo, 476 U.S. 207, 213 (1986)(quoting *Katz,* 389 U.S. at 351).
[29] Minnesota v. Dickerson, 508 U.S. 366, 375 (1993).
[30] State v. Bromell, 596 A.2d 1105, 1108 (N.J. Super. Ct. Law Div. 1991).

[31] Shoemaker v. Handel, 795 F.2d 1136, 1142 (3d Cir. 1986).
[32] *Bromell*, 596 A.2d at 1108.
[33] *Id.*
[34] *Id.*
[35] *Id.* (citing Colonnade Catering Corp. v. United States, 397 U.S. 72, 76-77 (1970); State v. Rednor, 497 A.2d 544, 546-47 (N.J. Super. Ct. App. Div. 1985)).
[36] *Id.* (citing State v. Turcotte, 571 A.2d 305, 309-10 (N.J. Super. Ct. App. Div. 1990)).
[37] *Id.* (citing State v. Williams, 417 A.2d 1046, 1049, 1051 (N.J. 1980)).
[38] *Bromell*, 596 A.2d at 1108 (citing State v. Bonaccurso, 545 A.2d 853, 857 (N.J. Super. Ct. Law Div. 1988)).
[39] *Id.* (citing *In re* State Dep't of Envtl. Prot., 426 A.2d 534, 539 (N.J. Super. Ct. App. Div. 1981)).
[40] *Id.* at 1109-12.
[41] *Id.* at 1108 (citing Donovan v. Dewey, 452 U.S. 594, 606 (1980); *In re* State Dep't of Envtl. Prot., 426 A.2d at 539).
[42] Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973)(quoting Katz v. United States, 389 U.S. 347, 357 (1967)).
[43] U.S. CONST. amend. IV.
[44] State v. Thein, 957 P.2d 1261, 1264 (Wash. Ct. App. 1998), *rev'd on other grounds*, 977 P.2d 582 (Wash. 1999).
[45] United States v. Vitek Supply Corp., 144 F.3d 476, 480 (7th Cir. 1998).
[46] *Bustamonte*, 412 U.S. at 219 (1973)(quoting *Katz*, 389 U.S. at 357).
[47] *See* Warden, Md. Penitentiary v. Hayden, 387 U.S. 294, 298 (1967) (quoting McDonald v. United States, 335 U.S. 451, 456 (1948)).
[48] *Bustamonte*, 412 U.S. 218, 222 (quoting Bumper v. North Carolina, 391 U.S. 543, 548 (1968)).
[49] Colburn v. State, 966 S.W.2d 511, 519 (Tex. Crim. App. 1998).
[50] Preston v. United States, 376 U.S. 364, 367 (1964).
[51] *See supra* notes 28-29 and accompanying text.
[52] State v. Chapman, 596 N.E.2d 612, 614 (Ohio Ct. App. 1992)(quoting Michigan v. Long, 463 U.S. 1032, 1049 (1983)).
[53] United States v. Edwards, 415 U.S. 800, 802-03 (1974).
[54] *See* United States v. Jacobsen, 466 U.S. 109, 113 (1984).
[55] Food Lion, Inc. v. Capital Cities/ABC, Inc., 194 F.3d 505, 515 (1999).
[56] *See* Lochenmyer v. Didrickson, 636 N.E.2d 93, 98 (Ill. App. Ct. 1994).
[57] *See* Stoker v. State, 788 S.W.2d 1, 11 (Tex. Crim. App. 1989).
[58] United States v. Garlock, 19 F.3d 441, 443 (8th Cir. 1994)(citing Fidelity Fin. Corp. v. Federal Home Loan Bank, 792 F.2d 1432, 1435 (9th Cir. 1986)).
[59] *Garlock*, 19 F.3d at 443.
[60] *See id.*
[61] United States v. Bazan, 807 F.2d 1200, 1203 (5th Cir. 1986).
[62] *Id.* (quoting United States v. Miller, 683 F.2d 652, 657 (9th Cir. 1982)).
[63] *Garlock*, 19 F.3d at 442-43.
[64] Stoker v. State, 788 S.W.2d 1, 11 (Tex. Crim. App. 1989)(quoting Walter v. United States, 447 U.S. 649, 656 (1980)).
[65] United States v. Kahan, 350 F. Supp. 784, 791 (S.D.N.Y. 1972).
[66] Dawson v. State, 868 S.W.2d 363, 369 (Tex. App. 1993)(quoting *Bazan*, 805 F.2d at 1203).
[67] *See, e.g.*, Purelli v. State Farm Fire & Cas. Co., 698 So.2d 618, 620 (Fla. Dist. Ct. App. 1997).
[68] *See* 62A AM. JUR. 2D *Privacy* § 38 (1990). Specifically, "(1) [u]nreasonable intrusion upon the seclusion of another; (2) [a]ppropriation of the other's name or likeness; (3) [u]nreasonable publicity given to the other's private life; [and] (4)[p]ublicity that unreasonably places the other in false light before the public." *Id.*
[69] Doe v. High-Tech Inst., Inc., 972 P.2d 1060, 1065 (Colo. Ct. App. 1998)(emphasis added). Aside from the common law cause of action for "intrusion upon seclusion," several states have sought to codify this prong of the invasion of privacy tort. *See* Munson v. Milwaukee Bd. of Sch. Dirs., 969 F.2d 266, 271 (7th Cir. 1992)(quoting WIS. STAT. ANN. § 895.50(2)(a) (West 1991)); Ritchie v. Walker Mfg. Co., 963 F.2d 1119,1123 (8th Cir. 1992)(quoting NEB. REV. STAT. § 20-203 (1988)).
[70] *High-Tech Inst., Inc.*, 972 P.2d at 1065 (citing RESTATEMENT (SECOND) OF TORTS § 625B (1981)).
[71] *Id.* at 1068.
[72] *See* Sheppard v. Beerman, 822 F. Supp. 931, 939-41 (E.D.N.Y. 1993)(holding that "the relationship between a judge and law clerk is *sui generis*" and that it is reasonable for a judge to search the files and desk of a former law clerk).
[73] *See, e.g.*, State v. Charles, 602 So. 2d 15, 17-19 (La. Ct. App. 1992), *amended by* State v. Charles, 607 So. 2d 566 (La. 1992)(holding that a defendant who was visiting his cousin's house and staying in a den that was a "highly trafficked area" and had no area set aside for his specific use, had a "severely diminished" expectation of privacy).
[74] 810 F. Supp. 1551 (S.D. Fla. 1992).
[75] *Pottinger*, 810 F. Supp. at 1571.
[76] *Id.* at 1573-76.
[77] *See supra* notes 73-76 and accompanying text.
[78] *See supra* notes 67-71 and accompanying text.
[79] State v. Brown, 660 A.2d 1221, 1225 (N.J. Super. Ct. App. Div. 1995).
[80] *See, e.g.*, United States v. Concepcion, 942 F.2d 1170, 1171-72 (7th Cir. 1991)(holding that there is no expectation of privacy in a mailbox at an apartment because the mailboxes were in a common area shared with five other tenants).
[81] *Katz*, 389 U.S. at 351.
[82] *See supra* notes 28-29 and accompanying text.
[83] 557 F.2d 362 (3d Cir. 1977).
[84] *Speights*, 577 F.2d at 362-64.
[85] *Id.* at 363.

[86] *Id.*
[87] *Id.*
[88] *Id.*
[89] *Id.* at 363-65.
[90] 677 S.W.2d 632 (Tex. App. 1984).
[91] *Trotti*, 677 S.W.2d at 637.
[92] Shaffer v. Field, 339 F. Supp. 997, 1003 (C.D. Cal. 1972), *aff'd*, 484 F.2d 1196 (9th Cir. 1973).
[93] *Shaffer*, 339 F. Supp. at 1003.
[94] 920 S.W.2d 48 (Ky. 1996).
[95] *Deemer*, 920 S.W.2d at 49.
[96] *Id.*
[97] *Id.*
[98] *Id.* at 49-50.
[99] *See id.*
[100] *Id.* at 50.
[101] *Deemer*, 920 S.W.2d at 50.
[102] *Id.*
[103] *See supra* text accompanying notes 94-102.
[104] McCarthy, *supra* note 8.
[105] *Id.*
[106] *Id.* Investigator software is manufactured by WinWhatWhere Corp. of Kennewick, Washington. *Id.*
[107] *See supra* text accompanying notes 105-06.
[108] *See* Simpson v. Commonwealth, Unemployment Comp. Bd., 450 A.2d 305, 310 (Pa. Commw. Ct. 1982).
[109] Mary-Kathryn Zachary, *Technology and Employment Law*, SUPERVISION, Mar. 1, 2000, *available at* 2000 WL 7872876. The federal Electronic Communications Privacy Act of 1986, which forbids the interception of electronic communications, "does not appear to apply to e-mail, which is not intercepted, but electronically stored." *Id.*
[110] 171 F.3d 711 (1st Cir. 1999).
[111] *Desilets*, 171 F.3d. at 713.
[112] Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §2520(a) (2000).
[113] *Desilets*, 171 F.3d. at 713.
[114] Nancy Flynn, THE EPOLICY HANDBOOK (2001), *available at* http://www.epolicyinstitute.com/disaster/stories.html.
[115] *Id.*
[116] *See id.*
[117] *See* Maura Kelly, *Your Boss May be Monitoring Your e-mail* (Dec. 8, 1999), *available at* http://www.salon.com/tech/feature/1999/12/08/email_monitoring.
[118] *Id.*
[119] *Id.*
[120] Zachary, *supra* note 109.
[121] *Id.*
[122] *See* Rutrell Yasin, *Web Slackers Put on Notice* (Oct. 15, 1999), *available at* http://www.internetweek.com/lead/lead101599.htm
[123] Zachary, *supra* note 109.
[124] *Id.*
[125] *See* Deborah Joseph, *Unions and the Internet* (Sept. 1999), available at http://www.laborresearch.org/tua/internet3.html.
[126] *Id.*
[127] 480 U.S. 709 (1987).
[128] *O'Conner*, 480 U.S. at 717.
[129] *Id.* at 710.

Land of the Free? pg. 557 - Joseph H. Lusk

[1] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).
[2] Foreign Intelligence Surveillance Act of 1971, 50 U.S.C. §§ 1801-1863 (2002).
[3] Part of the Omnibus Safe Streets Act of 1968, 18 U.S.C. 2510-2520 (2000); *see* Patricia Mell, *Big Brother at the Door: Balancing National Security with Privacy under the USA Patriot Act*, 79 DEN. U. L. REV. (forthcoming 2002) (manuscript at 46-48, on file with the Denver University Law Review).
[4] Mell, *supra* note 3 (manuscript at 28-29).
5 *Id.* (manuscript at 28).
6 *Id.* (manuscript at 27).
7 *Id.* (manuscript at 31).
8 *Id.* (manuscript at 30-31).
9 *See id.* (manuscript at 31-33).
10 *See id.* (manuscript at 32-33).
11 *Id.* (manuscript at 33).
12 *See id.* (manuscript at 43-44).
13 See *id.* (manuscript at 45-46).
14 *See d.* (manuscript at 36-38). After these abuses, President Reagan resurrected the CIA-FBI partnership by executive order. *Id.* (manuscript at 36).
15 See *id.* (manuscript at 37).
16 *Id.* (manuscript at 47).