1-1-1997

Common Law, and Privacy in Computer-Mediated Environments

Stephen D. Cooper
Marshall University, coopers@marshall.edu

Common Law, and Privacy in Computer-Mediated Environments

Stephen Cooper[1]

Computer-mediated environments pose a special challenge to our legal and cultural protections of privacy. These environments are unprecedented in the way commercially valuable information can be generated in their very use. The ease and low cost with which electronic information can be gathered and disseminated in these environments have led many to advocate regulation protecting privacy interests from commercial encroachment. At the same time, the use of digital communications to support criminal or terrorist activities have led others to advocate regulation allowing law enforcement agencies to eavesdrop or intercept. The cultural history of the Internet as a self-regulating, almost anarchical, environment provides an interesting background to this issue. Many writers have looked to statutory law for a solution to the issues of control over, and commercial or governmental use of information about individuals. This article contends that the current discussions have overlooked the potential of common law and market forces to satisfactorily balance the conflicting interests.

The evolution of computer-mediated environments (CME) has placed increasing pressure on our legal protection of privacy. As electronic databases gradually merge into what some scholars have termed the digital library (Fox, Akscyn, Furuta, & Leggett, 1995; Kantor, 1994) and electronic searching tools grow more sophisticated (Rao, Pedersen, Hearst, Mackinlay, Card, Masinter, Halvarsen, & Robertson, 1995), and as the commercial goal of "information at your fingertips" gets closer to fulfillment (Gates, 1995b), many fear the complete erosion of individuals' control of information about themselves. There are good reasons to wonder if loss of privacy may well be a negative externality of the digital library. As computer-mediated environments overcome time and space as barriers to information access, they also erode time and space as *de facto* enforcers of privacy interests.

Our legal recognition of a right to privacy dates to the Yellow Journalism era in the late nineteenth century. Then, the concern was over intrusive reporters and the public disclosure of information considered to be private; the call was for common law recognition of a privacy right. Now, the concern is over the accumulation of and control over electronic data describing individuals, data which have ever-increasing value in the commercial marketplace. Some call now for legislation or regulation to control the acquisition and distribution of such information.

---

1. Stephen Cooper (M. C.I.S., Rutgers University) is a doctoral student in the School of Communication, Information and Library Studies, Rutgers University, 4 Huntington Street, New Brunswick, NJ 08901, and Manager of Television Production at Brookdale Community College, Lincroft, NJ. *An earlier version of this paper was chosen as Best Graduate Student Paper at the Inaugural Conference of the New Jersey Communication Association, Montclair State University, April 26, 1997. The author has many people to thank including Milton Mueller of Rutgers University, Susan Rosenberg of Brookdale Community College, and the Editor and anonymous reviewers of The New Jersey Journal of Communication.*

This paper will argue, contrary to much conventional wisdom, that statutory protection is not necessarily the best option open to us, and that the privacy torts of our common law can be applied to computer-mediated environments. The paper reviews the historical and social roots of our privacy rights, briefly outlines the privacy protections which have evolved in our common law, describes some of the ways CMEs confound statutory law, and outlines how our common law and free market may respond to those stresses (*1).

The Origins of the Idea of Privacy

Prior to industrialization and urbanization, privacy in the form of solitude was simply a feature of daily life (Hixson, 1987). Spatial isolation and very limited means of mediating communication made privacy readily available. Changes in social structures and communication media in the second half of the nineteenth century threatened what had, up to that time, been a given.

Greater population density in urban areas increased the frequency of unwanted social contact. The rise of the mass market newspaper (the "Penny Press") and the professionalization of news reporting furthered both the appetite for information and the mechanism by which it could be commoditized, thus threatening the individual's control over personal information (Cooper, 1995). In a parallel to our own time, commercial pressures within the mass media industry (then, newspapers; now, television) led to the "Yellow Journalism" style, characterized by what at the time were shockingly personal disclosures (Dicken-Garcia, 1989, pp. 185-186).

Concern over the intrusiveness of the press had reached so high a state by the end of the nineteenth century that a pair of young lawyers published an article advocating legal recognition of a privacy right in the *Harvard Law Review.* In their essay, "The Right to Privacy," Samuel D. Warren and Louis D. Brandeis argued for common law recognition of a fundamental "right of the individual to be let alone" (1890, p. 205). Just as the common law had gradually extended its protection from harm to persons and tangible property to harm to ideas and intellectual property, they argued that the law should also recognize the individual's ownership of an "inviolate personality" (Cooper, 1995, pp. 104-1 06; Warren & Brandeis, 1890, p. 205).

Common Law Protection of Privacy

In the time since the publication of the Warren and Brandeis article, common law has evolved to recognize four distinct privacy torts. Statutory protection has been uneven. A few states have passed privacy laws, but most have extended common law recognition instead (Pember, 1972, pp. 231-232, 267-270). Supreme Court consideration of privacy rights is rather recent (summarizeed in Hixson, 1989, p. 495 ff.), dating to the *Time v. Hill* case decided in 1967 (*2). At this time Federal legislation has taken up privacy concerns in a piecemeal fashion; unlike the privacy torts, Federal statutes have applied to particular types of information, databases, situations, or media.

It is useful to review the common law torts of privacy, as they contain the broadest conception of a right to privacy, and because they provide for direct compensation to the party whose privacy has been injured. Prosser (1960, p. 389 ff.) identified four distinct torts: intrusion, public disclosure, false light, and appropriation.

The tort of *intrusion* originally protected against physical presence in a space thought to condition an expectation of privacy. It was broadened, as technology raised the possibility of less

obvious intrusion, to such situations as wire tapping, covert recording of speech, blood tests, and access to bank records. A necessary ingredient for a successful intrusion tort is a space rightfully expected to be private; a photograph taken in a public place is not considered intrusion.

The *public disclosure of private facts* tort protects against certain kinds of publicity. The tort requires that the disclosure be public, that the facts be private and not public information (and thus, matters of public record are not protected), and that the facts be objectionable or offensive in some way.

The *false light* tort is similar to defamation. This tort allows recovery if remarks are falsely attributed to one, or one's image falsely associated with some activity or object. Again, there is a requirement that the information be in some way objectionable or offensive to contemporary *mores.*

The *appropriation* tort protects against use of some aspect of one's identity without consent. Early cases concerned use of photographic images for advertising purposes, and this tort can be seen as protecting the individual's proprietary interest in his or her identity.

Prosser comments that the evolution of these torts has been a compromise between privacy interests and the First Amendment protection of a free press (1960, p. 410), since so many of the cases involved newspapers or broadcasting. Along the way an important distinction has been drawn between the privacy rights of a public figure, and a private figure. A person can voluntarily waive some degree of protection by running for public office or purposely becoming a celebrity. A person can also involuntarily lose some degree of protection by being involved in a newsworthy event, or generating some kind of record deemed public, such as a criminal conviction.

A number of points are of particular application to computer-mediated environments. First, a public figure, whether voluntary or involuntary, is in general less protected than a private figure. Second, newsgathering has been allowed a degree of latitude concerning privacy interests which other commercial activities have not enjoyed. Third, prevailing notions of the offensiveness or sensitivity of certain information (i.e., the *mores* issue) are important in determining the degree to which the information is privileged.

The Difficulty With Statutory Protection of Privacy

The central problem for protection of privacy is that both technology and the marketplace stress our expectations of privacy, which are, at bottom, cultural norms. Although they were written over a century ago, the words of Warren and Brandeis still seem to frame the problem well: "recent inventions and business methods call attention to the next step which must be taken for the protection of the person" (1890, p. 195).

A recent development is the complexity of the privacy problem in CMEs. Privacy concerns now involve not just journalism, but also law enforcement, national security, counter-terrorism measures, workplace monitoring, product marketing, government record-keeping, personal correspondence, electronic commerce, and digital money. One aspect of the problem is that CMEs complete the erosion of spatial and temporal isolation as controls on information flow; information in electronic form is much easier to access, pool, reproduce, and transport. Moreover, computer-mediated communications, unlike previous media, *create* new and valuable information in their use. The convenience of CMEs, which offers the promise of a world-wide electronic commerce (Kalakota & Whinston, 1996) and ready access to a tremendous quantity of information (Gates, 1995b), also creates the problem of transaction-generated or telecommunica-

tion-generated records which can be used to compile profiles of individuals (National Telecommunications and Information Administration, 1995). The productivity of computer networking in the business world is accompanied by the specter of covert surveillance of workers (Privacy Rights Clearinghouse, 1993). Our excitement about the information riches of the digital library is tempered by the realization of how transparent an intrusion may be.

Securing the Channel

One aspect of the privacy issue is the matter of protecting messages against interception. The obvious legislative step has already been taken, but the problem created by CMEs is much more difficult than that of earlier media. The Electronic Communications Privacy Act of 1986, Public Law 99-508, made it illegal to intercept or disclose the content of electronic communications ("Excerpts From ..., " not dated), and provided for both civil and criminal penalties against anyone not under color of law doing so. The Act defines content as "any information concerning the substance, purport, or meaning," and electronic communication as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo-electronic, or photo-optical system." In short, this statute extends wiretapping laws into the province of CMEs.

However well-intended, this will not bring the issue to closure. CMEs have made the task of balancing state interests (law enforcement, national security) against individual interests (privacy, anonymity) far more complex than that, as the debate over encryption shows. While one might have expected that statutory controls over earlier electronic media could readily be adapted to CMEs, two factors have made such a transition problematic. One is cultural: many users of CME's have made it clear they place a very high value on privacy and anonymity, strongly oppose government interception of content for any reason, and advocate the general availability of robust encryption technology to private citizens (e.g., "G7 Threat Alert," 1996; Hughes, 1993; Levy, 1996; May, not dated; "Sidebars," 1996). It seems reasonable to see this cultural value as a legacy of the Internet's origins among academics and computer hackers (Hoffman & Novak, 1994), groups in which authority is questioned and personal autonomy cherished.

The problem is not simply that individual desire and preference are in conflict with law enforcement interests, however. Another factor is that the development of viable electronic commerce requires robust security of transactions (Matonis, 1995; "Netbill Overview," 1995). As advocates of deregulating encryption put it, "technological progress has moved encryption from the realm of national security into the commercial sphere" (Simons & Snyder, 1996). Both individuals and corporate entities share concerns about access to information about their transactions. Developing a form of digital money (Camp, Sirbu, & Tygar, not dated; McClellan, 1995), that is, a secure way to settle transactions over the network, is a critical facet of the encryption issue. In short, surveillance of digital communications, whether by law enforcement authorities (Galkin, 1996) or by employers (Privacy Rights Clearinghouse, 1993), is a bugaboo to many CME users.

The story of the Clipper chip, a proposed hardware encryption device which would have allowed court-approved eavesdropping, illustrates the complexity of this issue. Proponents argued for legislation requiring use of the Clipper chip in digital transmissions, as a technological way to balance privacy needs and law enforcement needs (Denning, 1994). Opposition to the Clipper chip was quite heated, for the reasons outlined above. The Clipper chip was intended to

enable government authorities to eavesdrop on digital communications, when given permission by a court, but to secure the transmissions against any other interception. The Clinton administration's enthusiasm for the Clipper chip waned after a researcher discovered a way to circumvent the need for the encryption keys, which were to have been available only to government authorities (Cranor, 1995). Technology moves much faster than legislation; if the Clipper chip had been mandated, it would have been obsolete before the law could be implemented, and in fact might have created even more severe problems. Once the encryption algorithm had been "cracked," it no longer could protect transmissions against third-party interception.

It is not obvious that technology alone can resolve the encryption controversy to all parties' satisfaction. What does seem clear, however, is that the volatile mix of technology, business practice, and cultural values will continue to make a legislative solution elusive.

The Dilemma of Electronic Dossiers

The relative ease and low cost of assembling data scattered across different databases into revealing profiles of individuals have prompted concerns of a different nature. One journalist was able to construct profiles of a number of prominent Californians, including "financial, legal, marital, and residential histories," using only legally accessible information obtained from online commercial and government sources (Piller, 1993). If anything, we can expect this to be easier in the future:

> A likely byproduct of greater user-friendliness in computer technology is erosion of the gatekeeper's role: more people will be able to access more data on their own. A likely byproduct of market competition among database services is lower pricing: the financial commitment to such inquiry will be smaller. A likely byproduct of networking is greater convenience: records that had formerly been scattered across many discrete databases will be pooled (Cooper, 1995, p. 112).

The privacy concerns about such business practices have been used to argue for general availability of robust encryption (Chaum, 1992; Gilmore, 1991), but this misses the heart of the matter. The real issue here is the ease with which a great number of scattered bits of information -- most revealed voluntarily, some generated incidentally in the course of our daily lives, none of which would give us much pause -- can be assembled by a third party into a profile of ourselves which we might find overly revealing (Katsh, 1989, pp. 195-196). A new problem for privacy protection is that no intrusion into private space is required; the data are simply "out there" for the compiling.

Why such data profiles should be so valuable to commercial interests is a point worth considering. The concerns have been aired, but the potential benefits to consumers have been given short shrift. Data mining to support target marketing is one reason for the interest in customer profiles. When firms can target products with less marketing cost, there is potential benefit to both the organization (reduced costs, expanded markets) and the consumer (lower pricing, more specialized products, better need satisfaction). In addition, some firms use such profiles to reduce the risk of dealing with clients unknown to them. A bank, for instance, uses a credit history to justify extending a mortgage to a person with whom it has never done business before. In an increasingly mobile and anonymous society, such use of electronic data can provide benefit to

consumers even as it raises questions about their loss of control over information about themselves (Kling, Ackerman, & Allen, 1994). Simply prohibiting such profiles altogether has the unintended consequence of preventing certain market benefits. As Varian (1996a) points out, the real concern is how best to guarantee that people can retain their property rights in information about themselves.

In sum, the mix of business practice, social priorities, technological development, and personal autonomy is quite complex. Some believe encryption technology will, in the end, decisively restore control to the individual (Chaum, 1992), whatever the trade-off in law enforcement interests. Others worry that the march of technology-enabled disclosure is inexorable. It does seem, however, that the power of market forces to enforce privacy interests tends to be overlooked. We should note that Lotus Development was forced to abandon plans to market a database of household demographics in the face of public outcry (Kling, Ackerman, & Allen, 1994). In similar fashion, Lexis-Nexis was driven to disable features of their P-TRAK database when faced with Internet-fueled protests (Weber, 1996).

How Common Law and the Marketplace Can Protect Privacy

A number of difficulties with statutory protection have been noted above. The pace of technological evolution is so rapid, the range of communication technologies so broad, the economic consequences of delaying policy decisions so costly, and the positions so polarized that a legislative approach may at best be ineffective, and at worst, outright damaging. CMEs differ from prior media in speed, geographic reach, and cost structure. While our first response to the awareness of a social problem is often, "there oughta be a law!" it is doubtful at this point that the political process can produce an intelligent, comprehensive statute which adequately addresses the needs of all the stakeholders. Clearly, statute or regulation runs a significant risk of unintended consequences, such as inhibiting development of information services or products, or preventing cost savings in marketing (*3).

While it may be rhetorically attractive to advocate a decisive legislative or regulatory fix, it is not a given that individuals' privacy interests will be well served in the political arena, given the fluidity of both the technologies supporting computer-mediated environments and our behaviors in those environments. There are a number of reasons to expect a better solution to emerge from common law than from regulation:

- Common law is "bottom-up" (case-driven) rather than "top down" (legislation-driven)
- It diffuses enforcement power among a variety of courts, rather than concentrating it within an agency
- It may thus be better at avoiding or mitigating unintended consequences
- It provides direct compensation to victims.

To be sure, common law has its own set of problems in addressing privacy concerns. For it to operate, the injured party must file suit; this requires the resources to take legal action, and the awareness that one has been victimized. As noted above, we generate data about ourselves when we engage in such routine activities as shopping or renewing our car registration, and it possible that many people could become complacent about the commercial use of that data, even after

they become aware of the data's existence. Another criticism of common law is that damage awards can be inconsistent, across jurisdictions and jurists. Still, there is little to suggest that we are, as a ·society, averse to filing tort actions, including class action suits. Moreover, a single damage award in a privacy case can profoundly impact industry practice.

The major privacy concerns regarding computer-mediated environments can be grouped into three broad categories, which map readily onto the privacy torts in this way:

- Issues of workplace surveillance and monitoring of digital communications are essentially questions of intrusion and expectation of privacy
- Issues of transaction-generated data and access to electronic records are essentially questions of disclosure
- Issues of electronic profiles are essentially false light questions when made public, and appropriation questions when sold on the market (*4).

In addition, we should not overlook the extent to which the information market regulates itself. Information service providers will be keenly aware of barriers to adoption of their services, one of which is clients' perception that using the service generates information about themselves which they cannot control. While not endorsing self-regulation as a complete solution to the problem of telecommunications-related personal information (TRPI), the National Telecommunications and Information Administration has recognized that in a competitive market, "privacy is one of the terms on which businesses struggle for customers and where consumers can walk away from transactions that do not provide adequate privacy protection" (NTIA, 1995). Control over transaction-generated information can very well be a contractual matter between providers
and their customers, and not a statutory question. In short, there are a number of forces in the marketplace which also can protect privacy interests, including the rational choices of consumers and producers, the libertarian bent of cyber-culture, encryption technologies, and the scrutiny of a "watchdog" press.

While there has been much support for government intervention regarding privacy (e.g., Gates, 1995a; Shapiro, 1997; Varian, 1996b, pp. 15-16), and concern about possible collateral damage to privacy interests from indirectly related legislation (e.g., Electronic Privacy Information Center, 1995), less attention has been given LO the ways the common law of privacy may be able to react to technological and market challenges. This paper has argued the contrary position that regulation may well be inferior to common law in several respects. Legislation runs a significant risk of unintended negative consequences, particularly by inhibiting potential market efficiencies. Legislation can also produce a false sense of security, and incline us to overlook action we can voluntarily take, as individuals, to protect our privacy interests. By contrast, extending the common law torts into computer-mediated environments makes good use of existing legal, economic, and cultural antecedents, and creates a legal context better able to cope with rapidly evolving technologies and uses of these environments.

Endnotes

(*l) Many of the sources used here were obtained from the Internet; URL's and e-mail addresses were current at the time of writing.

(*2) Hixson (1989), Pember (1972). and Cooper (1995) contain more detail on the essential privacy cases than space permits here.

(*3) For a full discussion of the idea of regulatory failure, see Mitchell and Simmons (1994).

(*4) One legal scholar expects a new tort to evolve, which allows recovery against such electronic profiles (Smolla, 1992. pp. 149-150).

References

Camp, L. J., Sirbu, M., & Tygar, *1.* D. (not dated). *Token and notational money in electronic commerce* [Online]. Available: http://www.cs.cmu.edu/afs/cs.cmu.edu/user/jeanc/www/ usenix.html.

Chaum, *D.* (1992, August). Achieving electronic privacy. *Scientific American* [Online], 96-101. Available: http://www.digicash.com/publish/sciam.html.

Cooper, S. (1995). Privacy and the news media. *The New Jersey Journal of Communication. 3*(2), 103-117.

Cranor, L. F. (1995. May). Digital liberties: Free speech and privacy under attack in cyberspace. *Crossroads* [Online]. Available: http://www.acm.org/crossroads/xrdsl-4/cyberbate.html.

Denning, D. E. (1994). *Encryption and law enforcement* [Online]. Available: gopher://gopher. cpsr. org: 70 /00/ cpsr/privacy/crypto/denning_ encryprion~law _enforcement_ feb_ 94.txt.

Dicken-Garcia, H. (l989). *Journalistic standards in nineteenth-century America.* Madison, WI: University of Wisconsin Press.

Electronic Privacy Information Center (1995). *Overview of 104th Congress electronic privacy And civil liberties legislation* [Online]. Available: ftp://cpsr.org/cpsr/privacy/epic/ 104th_congress_bills/EPIC_Legislative_Update_3.26.txt.

Excerpts from the Electronic Communications Privacy Act of 1986 (not dated) [Online]. Available: http://userfs.cec.wustl.edu/~csl42/articles/PRIVACY/electronic_privacy_ act-excerpts.

Fox, E. A., Akscyn, R. M., Furuta. R. K., & Leggett, J. J. (1995). April CACM introduction: Digital networks. *Communications of the ACM* [Online], *38(4).* Available: http://www .acm.org/ pubs/cacm/previous/CACM apr95 _intro.html.

G7 Threat Alert From International Net-Coalition (1996, August 8). CRTNET[Online], *1484.* Available E-mail: LISTSERV@PSUVM.PSU.EDU Message: Get INDEX CRTNET.

Galkin, W. S. (1996, January 29). Electronic privacy rights and police power. *The Computer Law Observer* [Online], *16.* Available: http://userfs.cec.wustl.edu/~cs142/articles/ PRIVACY/ computer_law_observer_16.

Gates, B. (1995a). *The privacy issue: Who should know what about whom?* [Online]. Available: http://nytsyn.com/live/Gates/256_091395_103311_2582.html.

Gates, B. (1995b). *The road ahead.* New York. NY: Viking.

Gilmore, J. (1991). *The private and open society* [Online]. Available: http://userfs.cec. wustl.edu/ ~csl42/articles/PRIVACY/private_ open_ society-gilmore.

Hixson, R. F. (1987). *Privacy in a public society.* New York, NY: Oxford University Press.

Hixson, R. F. (1989). *Mass media and the Constitution.* New York, NY: Garland.

Hoffman, D. L., & Novak, T. P. (1994). Commercializing the information superhighway: Are we

in for a smooth ride? *The Owen Manager* [Online], *15*(2), 2-7. Available: http:/www2000 .ogsm.vanderbilt.edu/smooth. ride. html.
Hughes, E. (1993). *A cypherpunk's manifesto* [Online]. Available: ftp://furmint.nectar.cs.emu .edu/security/cypheressay /cypherpunk-manifesto.
Kalakota, R., & Whinston, A. B. (1996). *Frontiers of electronic commerce.* Reading. MA: Addison-Wesley.
Kantor. P. B. (1994). Information retrieval techniques. In M. E. Williams (Ed.). *Annual Review of Information Science and Technology.* Vol. 29. Medford. NJ: Learned Information.
Karsh. M. E. (1989). *The electronic media and the transformation of law.* New York. NY: Oxford University Press.
Kling, R. Ackerman, M. S. & Allen, J. P. (1994). *Information entrepreneuralism, information technologies, and the continuing vulnerability of privacy* [Online]. Available: http://www-swiss.ai.mit.edu/6095/articles/kling-privacy.txt.
Levy, S. (1996). *Crypto rebels* [Online]. Available: http://hotwired.com/wired/1.21fearures/ crypto.rebels.html.
Matonis. J. W. (1995). *Digital cash and monetary freedom* [Online]. Available: http://www.isoc .org/in95prc/HMP/PAPER/136/html/paper.html.
May, T. C. (not dated). *The crypto anarchist manifesto* [Online]. Available: http://www. quadralay.com/www/Crypt/Crypto-Anarchist/crypto-anarchist .html.
McClellan. D. (1995). *Desktop counterfeiting* [Online]. Available: http://web.mit.edu/ afs/athena/org/t/techreview/www/articles/feb95/mcclellan.html.
Mitchell, W. C., & Simmons, R. T. (1994). *Beyond Politics.* Boulder, CO: Westview Press.
National Telecommunications and Information Administration (1995). *Privacy and the NII* [Online]. Available: http://www.ntia.doc.gov/ntiahome/privwhitepaper.html
Netbill Overview [Online] (1995). Available: http://www.ini.cmu.edu/NETBILL/ publications/CompCon.html#RTFToC4.
Pember, D. R. (1972). *Privacy and the press.* Seattle, WA: University of Washington Press.
Piller, C. (1993, July). Privacy in peril: How computers are making private life a thing of the past. *Macworld, 10(1),* 124-130.
Privacy Rights Clearinghouse (1993). *Privacy Rights Clearinghouse fact sheer # 7* [Online]. Available: http://gopher.vortex.com/ privacy/prc.work-7.Z
Prosser, W. L. (1960). Privacy. *California UJW Review, 48*(3), 383-423.
Rao, R., Pedersen, J. 0., Hearst, M. A., Mackinlay, J. D., Card, S. K., Masinter, L. Halvarsen, P., & Robertson, G. G. (1995). Rich interaction in the digital library. *Communications of the ACM, 38*(4), 29-39.
Shapiro. A. L. (1997, June 23). Privacy for sale: Peddling data on the internet. *The Nation* [Online]. Available: http://www.thenation.com/issue/970623/0623shap.htm.
Sidebars to the Wired Crypto Rebels Article [Online] (1996). Available: http://www.hotwired .com/wired/1.2/features/crypto.rebels.sidebars.html.
Simons. B., & Snyder, J. B. (1996, April 5). ACM/IEEE letter on crypto. *Privacy Forum Digest* [Online], 5(8). Available: http://gopher.vortex.com/privacy/priv.05.08.Z.
Smolla, R. A. (1992), *Free speech in an open society.* New York, NY: Knopf.
Varian, H. (1996a, December 6). *Economic aspects of personal privacy* [Online]. Available: http://www.sims.berkeley.edu/~hal/Papers/privacy.html.
Varian, H. (1996b, September 15). *Economic issues facing the internet* [Online]. Available: ftp://alfred.sims. berkeley.edu/pub/Papers/econ-issues-internet.html.

Warren, S.D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review, 4*(5). 193-220.

Weber, T. E. (1996, September 19). New Lexis database of names sparks outcry on privacy. *The Wall Street Journal*, p. B7.