2005

Tattoos on Our Digital Skin: Anonymity, Privacy, and Accountability in Cyberspace

Sam Grey, *University of Victoria*

Hermes: Canadian Undergraduate Philosophy Journal
University of Ottawa/Université d'Ottawa
Volume VI (2005)

Tattoos on our Digital Skin
Anonymity, Privacy, and Accountability in Cyberspace

Sam Grey, Trent University

> *"Once, words were spoken and vanished like vapor in the air; newsprint faded and turned to dust. Today, our pasts are becoming etched like a tattoo into our digital skins."* (Lasica par. 31)

While it may be oddly flattering that Chapters, Amazon or HMV knew you would like the new Johnny Cash compilation album, you may be less than thrilled to discover that they also knew about your prescription drug addiction, your crabs, your bankruptcy, or your having skipped out on the rent one month back in 1993. When you add the possibility of your favourite e-retailer sharing your personal information – for a profit – to the frank probability of their having known it in the first place, what you initially found flattering may begin to appear more offensive and ominous. Simply put, there is information people are not disposed to share, would not consent to disclose to any individual or organization, and would fight to retain or regain sole control over. People value their privacy.

"Although the ideals of individual privacy have not changed over the last 200 years, the reality has" (Borella par. 38). Most people view the 'Net as private space, often a simple extension of the living room or study where they sit at their computer. Unfortunately, the internet is not only a thoroughly public space (Lasica par. 3), but also public in a way not previously known and not yet fully understood. As a result, with the rise of information technology, anonymity has become strongly linked to privacy, and privacy, in turn, to power.

As a concept, privacy (like accountability) can be found at a point along the indistinct continuum between transparency and opacity, prison-cam surveillance and desert-island isolation, 'our' needs and 'their' needs. It is often claimed that privacy and accountability are what actually sit in the scales when we attempt to balance personal freedom with the safety of society as a whole. Accordingly – since all advances in technology bring with them new or newly accentuated risks and rewards – anonymity has been hailed as both the finest benefit and the most dire threat offered by the internet. Privacy is both a means and an end; its value is intrinsic as well as instrumental. The need for privacy is ubiquitous, and modern civilization has demonstrated a fervent desire to protect it through the creation and enforcement of complex laws. In contemporary society, to lose privacy places your reputation, your dignity, your creativity, your autonomy, your freedom, and even your life at risk. It is notoriously difficult to define with any precision, but with respect to the internet perhaps the most salient description of privacy is "the ability to control the flow of information about one's self and the ability

to make meaningful choices about when information is disclosed" (Preston par. 16). Thus substantive privacy is contingent upon the availability, to all persons, of anonymity and pseudoanonymity.[1] Anonymity should be preserved where it protects privacy, and where privacy has won out when tested against other values (Ward Bynum par. 9).

> Personalization violates privacy if the personal information is handled unfairly, and information can be handled unfairly in several ways. It can be collected without consent; it can be used for purchases other than those for which consent was given; and it can be kept secret from the people whom it's about. If the user isn't in ongoing control of the information, that's also unfair. (Jason Catlett, qtd. in Kontzer par. 6)

Current threats to privacy represent the erosion of a longstanding right with the advancement of technology, and key issues in the case for internet anonymity are the capacity and architecture of the internet itself. While technology is ethically neutral[2], the opportunities it presents are acted upon either for good or ill, and its effects are therefore morally measurable. The gathering of information in the internet age happens with greater ease and speed than ever before, as does the manipulation and sharing of that information. What's more, information may be (and normally is) gathered without the knowledge of the individual themselves, through 'cookies,' tracking bugs, spyware, and legitimate software registration processes, which monitor browsing habits and capture personal data from the individual's hard drive. The storage of information is another important concern, since the 'Net allows permanent archiving of data beyond any moratorium or limitation currently known in the 'real' world. Currently, "Government paranoia and control and overly broad security laws compel many internet providers worldwide and virtually all that operate from the USA to maintain and preserve detailed logs of all the internet usage of their customers" ("Online Anonymity" par. 3). Unlike words and actions in 'meatspace,'[3] which wither and vanish into our faulty human memory, what is done in cyberspace endures.

Anonymity and the State

> *"With old-fashioned phone wiretapping, the FBI is obliged to obtain a warrant for the phone company to tap a single line, telephone or conversation. Because phone companies are required to do some of the work involved in the tap, including paperwork, they're also given some amount of accountability. [...] The situation is different with [the internet]."* (Weisman par. 18)

In regulatory circles the notion of privacy blurs with that of liberty, making an exact definition virtually impossible; without a precise definition, protection in the legal sense is also impossible. The U.S. Constitution does not contain the word privacy anywhere (Walton par. 3), which underscores the observation that privacy has "a protean capacity to be all things to all lawyers" (Tom Gerety, qtd. in Solove, *Conceptualizing* 1089). Complicating the matter is the role of the state and the posture of the government inhabiting its structures. There is a duality and a tension in the legal fight for anonymity and privacy in cyberspace: in some cases, people seek protection from the government's gathering and use of personal data; in others, they ask that the government intercede to protect them from private actors. The mercurial definition of privacy has combined with a lack of general knowledge about how cyberspace operates; when combined with the duality of the state's regulatory role these factors yield a sort of judicial paralysis, lack of regulatory consensus (both within and between nations), and a reliance on sectorial self-regulation on the internet. In no other area of publishing, surveillance, or communication is this the norm.

In all three of his interrelated conceptions of privacy, Lawrence Lessig stresses the protection of the individual against unwarranted or excessive disruption by the state. His utilitarian definition, "privacy to minimize burden," offers that privacy simply describes our desire to be left untroubled. His second definition, "privacy as dignity," describes a search of persons or possessions by the state as an offence to an individual's dignity. Lessig's third and final conception offers that privacy is "a substantive limit on government's power" (Lessig 149). In all three of these areas, anonymity ameliorates the burden or otherwise protects the individual.

The freedom of individuals to criticize their leaders should not be underestimated, and having individual voices protected by anonymity is key to full, timely, and honest expression. The ability to question or critique the government online is especially important in countries where human rights are only tenuously supported or violently suppressed – a virtual equivalent of China's 'democracy wall'.[4] Political watchdogs such as Amnesty International could not operate without anonymous tips and whistleblowers, since the risk of exposure is a powerful inhibitor in even the most democratic and transparent political systems. There is a long history of political activism and thought under

[1] "Pseudoanonymity,' which includes the use of online personas or game characters, is a variant of anonymity characterized by the use of pseudonyms. Unlike anonymity, pseudoanonymity often involves longer term use of a fictitious identity, including the development of a reputation and personality. See, among others, Froomkin, A. M. "Anonymity and Its Enmities." Journal of Online Law (1995, June): art. 4.

[2] Certainly this point is debatable; however, it may be asserted that until put to use, no technology has a practical ethical character. Even instruments of torture, in the absence of the torturer, are nothing more than their component parts; they are inert.

[3] "meatspace (MEET.spays) n. The flesh-and-blood real world; the opposite of cyberspace" (McFedries par.1).

[4] "Beijing democracy activists were allowed to record news and ideas on a designated wall in the city from December 1978. In line with the party's new policy of 'seeking truth from facts,' the activists were encouraged to criticise the Gang of Four and failed government policies" ("China's Communist Revolution" par. 1). As the Democracy Wall was torn down within five months, "It proved to be a short spring for freedom" (Dobson, par. 1).

the 'anonymous' moniker and pseudonyms, including *Cato's Letters*, *Common Sense* and *The Federalist Papers*, leading to the characterization of anonymity and pseudoanonymity as the cornerstones of free speech (Wallace 2). Further, anonymous informants have had considerable legal and political weight, and journalists and police would find their work seriously hampered by the withdrawal of anonymity for their sources. Witness or source credibility has long been trusted to the writers and officers involved, who are specifically empowered to judge such matters.

The lack of regulatory consensus on privacy and anonymity presents serious problems for the issue of legal jurisdiction. The definition of criminal activity may be profoundly different at the posting and downloading terminals of internet communication, and individuals may be charged at either end, making action within the law of your home state or country no guarantee of immunity in another. If the individual cannot be protected in such instances, the only alternative to effective anonymity is complete silence.

"Increasingly, there is a two-way information flow between the private and public sectors. In other words, not only is the government supplying information to the private sector, but the private sector is assisting the government in generating information about individuals" (Solove, *Access* 1151). Even ignoring the democratic issues of the consent of the governed and 'checks and balances,' simple accuracy is a major hurdle to the characterization of such private-public interplay as an acceptable practice. The Privacy Foundation discovered numerous serious errors in sample personal data that a single private firm, ChoicePoint, Inc., provides to thirty-five separate federal agencies (and countless private sector companies). One such report, erroneously detailing theft and drug offences, cost a Florida woman her job; similar errors resulted in the 2000 Presidential Election debacle in Florida, wherein many of the 8,000 people eliminated from the voter registry by virtue of their felony record were not ex-felons (Solove, *Access* 1152). While the average citizen can expect legal protection from the most extreme fallout of privacy violations – credit card, or even identity theft – currently, there is no central government database and therefore no way for individuals to request, view, and challenge (or correct) their own personal data. There is also an emotional and social price to be paid for escalating government and private sector surveillance, namely: "the powerlessness, vulnerability, and dehumanization created by the assembly of dossiers of personal information where individuals lack any meaningful form of participation in the collection and use of their information" (Solove, *Privacy and Power* 1393).

Anonymity and the Market

> *"You're profiting from my seduction... how is that good for me?"* (Gibson par. 19)

Along with political democracy, attacks on electronic anonymity violate the (supposedly) intrinsic democracy of the market. E-commerce is driving both

sides of the debate over accountability and anonymity: websites began to sport 'secure' status when consumer protection became of paramount importance, while at the same time, quietly collecting information on consumers became a growth industry in itself (Rowland par. 2). The harvesting of personal data through internet technology allows companies to circumvent the customary market mechanisms, permitting practices that range across the ethical and legal spectrum. Targeted marketing in the form of e-mail, pop-up and banner ads, and the Windows Passport and XP Messenger programs quickly draw people's ire, yet it remains a legal 'grey area'. A common observation is that such advertising is radically different from the norms of broadcast and print media, which are accepted by virtue of their static – and therefore perfectly equitable – message: every reader or listener receives the same advertisement or announcement, and a company must gauge profitability and probability in undertaking an ad campaign. In contrast, targeted advertising utilizes personal information to identify likely consumers and dispatches a more intrusive, tailored – and therefore inequitable – message.

> When I read billboards while driving my car down the freeway, I encounter the same billboards as everyone else. The signage is not 'per driver'. When I flip through the pages of a magazine, I encounter the same ads as everyone else. The magazine knows nothing about me, and I don't want it to. (Gibson par. 15)

A related practice with the misleadingly innocuous moniker of 'dynamic pricing,' however, has landed companies as robust as Amazon.com in more serious trouble. Also known as price discrimination, the practice allows companies to merge the rewards of variable-pricing (i.e. auction) and stable markets, producing an ingenious, legally tolerable[5] advantage for themselves. The bottom line is that customers are charged what their personal information, held in databases, calculates is the maximum they would be willing to pay.[6] Overwhelmingly negative customer and media reaction to the Amazon.com episode indicated that while dynamic pricing may be a subject for legal debate, it is widely perceived as unethical.[7] *Junkbusters'* Jason Catlett captured the essence of the issue when he noted: "Just because something is legal doesn't mean it's a good idea. And any product manager who's making decisions on the use of personal information based strictly on whether they're breaking the law or not is being very short-

[5] "the [Federal Trade Commission] ultimately determined Amazon had been deceptive, but did not take enforcement action" (Kontzer par. 2).

[6] Amazon.com themselves describe it somewhat differently: "From time to time, we test and re-evaluate various aspects of our Web site to determine which characteristics drive customer purchases and satisfaction... Price is one aspect we may test, and, accordingly, that means that some customers may pay a different price for select items" (Rosencrance par. 13).

[7] One analyst with ActivMedia Research called Amazon's pricing experiment "a bone-head move" (Harry Wolhandler, qtd. in Weiss par. 7).

sighted" (qtd. in Kontzer par. 12).

Anonymity and Freedom of Expression

> *"There are two sides that it boils down to: 'The validity of concepts and ideas expressed are based upon the poster's identity' [and] 'The validity of concepts and ideas expressed are not related to the poster's identity'."* (David Hayes, qtd. in Detweiler sec. 3.1)

In situations where honesty is either desirable or quite necessary, a reasonable assurance of anonymity is critical. Such situations arise electronically in business, legal, and social spheres; and are manifested in marketing surveys, anonymous tips, feedback forms, certain academic reviews, and the personal and organizational web pages of countless critics and advocates. Without a means by which honest expression and feedback may be secured, market, state, and society all stand to suffer. The privacy issue involved is usually heroically termed 'free speech,' and hailed as the protected right to freely and anonymously voice opinions. Anonymity allows ideas to be judged on their own merit, rather than by virtue of their authorship – indeed, there are cases where anonymity is the only reasonable guarantee of fair judgement, without the influence of personal grudges or biases against race, class, gender, or social status. Following behind the initial desire for equity in assessment is the related concern over recrimination after opinions have been aired. Addressing critics of anonymity on the internet, Karl Barrus observed that "[i]n an ideal world we would all be sitting around engaging in Socratic dialogues, freely exchanging our opinions in an effort to learn. But in an ideal world nobody will threaten you for your thoughts, or ridicule you" (Karl Barrus, qtd. in Detweiler sec. 3.1). Retaliation may itself be anonymous and intended to annoy, or it may come in the form of a serious physical or legal threat. In 2001, the ACLU challenged a State Superior Court Judge's attempt to uncover an online detractor's identity through the court system, noting that "legal intimidation tactics have increased toward those who voice their opinions on the Web" (McDonald par. 5). In 2000 alone, America Online dealt with almost five hundred such subpoenas (McDonald par. 5).

> Many seem to question the value of anonymity. But who are they to say what risks another individual should take? [...] Some say that anonymous posters are "cowards" and should stand up and be counted. Perhaps that is one point of view but what right do these detractors have to exercise such censorship? (David Clunie, qtd. in Detweiler sec. 3.1)

Finally, a discussion of anonymity and individual expression cannot be undertaken without raising the spectre of censorship. If a free trade in ideas benefits society and is fostered by anonymity, as is often claimed, banning anonymity is censorship. And as John Gilmore has commented, "The Internet interprets censorship as damage, and routes around it" (qtd. in Barnes par. 60).

Anonymity, Community & Individuality

> *"The distinction between the public and private spheres of human life is a critical facet of contemporary moral, political, and legal thought. [...] Much recent scholarship has invoked privacy as an important component of individual autonomy and as something essential to the ability of individuals to lead complete and fulfilling lives."* ("The Right to Privacy" par. 1)

Despite a media focus on the issues of regulation and state power, at the end of the day there is more to the issues of internet anonymity and privacy than such straightforward legal and political matters. It is certainly subjective, but the need for privacy is, at the basic level, universal. Each person has a personal identity and a social identity, equivalent to person and persona, which play an important part in determining who you are and want to be, as well as where and how to belong. In this sphere, selective anonymity or pseudoanonymity plays a critical role in supporting individual creativity, artistic expression, and autonomy. People feel they have a right not only to a personal space – either physical or virtual – and a right to role-play within that space. To assume an alternative identity:

> can be playful and life affirming, one way of feeling closer to others and to yourself. [...] Ironically, when we temporarily cast aside our day-to-day roles, and try on other artificial ones, we force ourselves to be spontaneous -- no longer able to fall back on habit -- and hence by deliberately trying not to be ourselves, we may find ourselves and also may reveal more about ourselves to others than we ever intended. Perhaps we reveal ourselves the most when most we seek to disguise. (Seltzer par. 17)

Without anonymity, certain communities would cease to function effectively or cease to function altogether; this holds true for 'real world' and virtual communities alike. A basic internet search on the term "anonymous" yields droves of examples, from the well-respected Alcoholics Anonymous to the more frivolous social support groups (including recovery groups for people addicted to surfing the 'Net). Anonymity is a factor in the coalescence of legitimate support groups, and each community's fragility is proportional to the threat of social, legal, or economic consequences from without. Anonymity is also a strong factor in the provision and recording of counselling sessions, both of which are becoming more frequent online. Individuals commonly seek medical, financial, and legal advice over the internet; the interaction should allow anonymity in order to attract as many individuals in need as possible, and foster an atmosphere of trust in the exchange. Related data records should only be disclosed in ethically defensible ways, similar to the legal provisions currently in place for therapists who wish to protect their 'real world' patients' identities. There are, of course, many shorter-term or less formal instances in which an individual may value privacy online, including seeking information on sensitive topics such as homosexuality or

abortion, or merely having the opportunity to ask 'stupid' questions without fear of ridicule. In these cases, anonymity is no less valuable.

While critics seem certain that anonymity will result in the social equivalent of the 'Diners' Dilemma' [8] or the 'Tragedy of the Commons,' aggravating free riding, exploitation, and general disrespect, studies designed specifically to address the unique atmosphere of cyberspace have not been as confident. Two major studies found that "[...] despite the increases in the expression of extreme and controversial ideas, one more positive attribute of anonymity in this medium was a reduction in the 'stultifying effects of hierarchy'. [...] The advantage is that social posturing and sycophancy decline" (Rowland par. 15).

Conclusion

> *"The value of, and right to, privacy will continue to compete with other values in our global society within the virtual community."* (White par. 22)

When carefully assessed, calls for banning internet anonymity are not proportionate to the actual threats posed by software, or architectural features that may protect an individual's identity. Contrary to techno-fearmongering, "there is no safety in activity that is unlawful. Anonymity should not be considered a secure shield because, ultimately, any data may be intercepted" (Walton par. 14). Illegal and offensive behaviours were not unknown in society before an internet connection became a household norm, and so do not in themselves constitute a sufficient argument for disallowing anonymous use of the 'Net. "It is akin to closing down the highway system because a few people speed" (Rigby par. 15). Taken as a whole, the potential risks presented by banning online anonymity far outweigh the harms such a ban is meant to curb. There is a regulatory and social challenge, without question, but there are viable options (such as traceable pseudoanonymity [9] and trusted third parties (Bynum par. 10), which offer the social and ethical benefits of both privacy and accountability. David R. Johnson acknowledges this, in an article otherwise favouring the banning of anonymity, when he notes that: "Now that we know what's at stake, it's time for the sysops

[8] The March 1994 edition of *Scientific American* carried an article called "The Dynamics of Social Dilemmas," "a study of cooperation featuring the example of a group that has agreed to split the meal check evenly and then must decide, individually, whether to order lobster or hot dog" (Johnson par. 1).

[9] 'Traceable pseudoanonymity' refers to a condition wherein the real-world identity of an individual can be traced, if required, though not necessarily by an equivalent ('ordinary') individual. See, among others, Froomkin, A. M. "Anonymity and Its Enmities." Journal of Online Law (1995, June): art. 4.

[10] Any time you interact with others without producing (authentic) identification you're operating somewhere within the precincts of anonymity. Cash transactions, conversations on the city bus, shot-down propositions in the local pub – in most mundane situations we have the freedom to reveal our identities or to keep them to ourselves.

who control key policies [...] to build in the structures that hold the greatest potential for altruism, collaboration and responsibility" (Johnson par. 6).

It is pointless to deny reality... anonymous interaction and expression is a fundamental part of 'meatspace' society and therefore already exists[10]; further, it is fervently protected. Anonymity is both a simple by-product of the fallible human memory and part of a history of free speech in print and broadcast media. It is therefore incumbent upon advocates of the banning of anonymity to demonstrate that anonymity in 'real world' forms should be protected while that in cyberspace should not. In a 1995 decision that still holds precedent, the U.S. Supreme Court declared anonymity part of "an honourable tradition of advocacy and of dissent. Anonymity is a shield from the tyranny of the majority" (Wallace 3).

In every instance where privacy and liberty intersect, the case for anonymity becomes highly charged. In a society that equates information with power, harvesting and utilizing personal data without permission can easily be viewed as theft, racketeering, and ultimately the denial of individual autonomy. In *Time Magazine*'s point/counterpoint on the issue of anonymity, privacy, and accountability, Jamais Cascio summed up the case for the protection of anonymous internet use: "At its core, this is a question of choice. I wish to be able to choose what I reveal about myself. Protecting anonymity on the 'Net is one of the few remaining ways of retaining that freedom to choose" (qtd. in *Time* TD14).

Sources

Barnes, Douglas. "The Coming Jurisdictional Swamp of Global Networking (Or, How I Learned to Stop Worrying and Love Anonymity)." *Legal Issues and Policy: Cyberspace and the Law Archive*. 16 November 1994. Electronic Frontier Foundation. 10 December 2003. <http://www.eff.org/legal/Jurisdiction_and_sovereignty/anon_juris.article>.

Borella, Michael S. "Computer Privacy vs. First and Fourth Amendment Rights." *Legal Issues and Policy: Cyberspace and the Law Archive*. 13 March 2003. Electronic Frontier Foundation. 10 December 2003. <http://www.eff.org/Privacy/comp_privacy_4th_amend.paper>.

Bynum, Terrell Ward. "Anonymity on the Internet and Ethical Accountability." *On the Emerging Global Information Ethics*. Autumn 1997. The Research Centre on Computing and Society. 30 November 2003. <http://www.southernct.edu/organizations/rccs/resources/research/global_info/bynum_anonymity.html>.

"China's Communist Revolution: A Glossary." *My Century (BBC World Service)*. 1999. BBC Online Network. 1 December 2003. <http://news.bbc.co.uk/hi/english/static/special_report/1999/09/99/china_50/democ.htm>.

Detweiler, L. "Anonymity on the Internet FAQ (1 of 4)." *What is the value or use of anonymity?* 9 May 1993. Electronic Frontier Foundation (EFF). 2 December 2003. <http://www.eff.org/Privacy/Anonymity/net_anonymity.faq>.

Dobson, William J. "Dissidence in cyberspace worries Beijing." *San Jose Mercury News*. 28 June 1998. Southeast Asia Discussion List <SEASIA-L@LIST.MSU.EDU>. <http://www.hartford-hwp.com/archives/55/428.html>.

"Does anonymity on the Internet protect users privacy or merely avoid accountability? Two opposing views on the philosophy of privacy." Hiding Behind a Screen Name (Point/Counterpoint). *Time*. 23 September 1996: TD14-TD14.

Gibson, Steve. "The Ethics of Anonymous Surveillance for Profit." *OptOut*. 6 October 2003. Gibson Research Corporation. 8 December 2003. <http://www.grc.com/oo/ethics.htm>.

Johnson, David R. "The Unscrupulous Diner's Dilemma and Anonymity in Cyberspace ." *Anonymity*. 4 March 1994. Electronic Frontier Foundation (EFF). 2 December 2003. <http://www.eff.org/Misc/Publications/David_Johnson/anonymity_online_johnson.article>.

Kontzer, Tony. "One on One with Junkbuster's Jason Catlett". *Information Week*. 20 August 2001. TechWeb Business Technology Network. 1 December 2003. <http://www.informationweek.com/story/IWK20010817S0024>.

Lasica, J.D. "The Net Never Forgets." *21st: The culture of technology and technology of culture*. 25 November 1998. Salon.com. 9 December 2003. <http://archive.salon.com/21st/feature/1998/11/25feature.html>.

Lessig. Lawrence. *Code and Other Laws of Cyberspace*. New York: Basic, 1999.

"Online Anonymity." *Digital Insurrection*. 8 October 2003. PirateDen.com. 3 December 2003. <http://www.digitalinsurrection.com/anonymity.php>.

McDonald, Tim. "ACLU Defends Internet Anonymity." *News Factor Technology News*. 27 February 2001. NewsFactor Network. 2 December 2003. <http://www.newsfactor.com/perl/story/7782.html>.

McFedries, Paul. "meatspace." *The Word Spy*. 14 November 1996. Paul McFedries and Logophilia Limited. 15 November 2003. <http://www.wordspy.com/words/meatspace.asp>.

Preston, Ethan. "Finding Fences in Cyberspace: Privacy and Open Access on the Internet." *Journal of Technology, Law and Policy* 3 (6.1): 85 pars. <http://grove.ufl.edu/~techlaw/vol6/issue1/preston.html>.

Rigby, Karina. "Anonymity on the Internet." paper presented at MIT 6.805/STS085: *Ethics and Law on the Electronic Frontier*. Fall 1995. 30 November 2003. <http://swissnet.ai.mit.edu/6095/student-papers/fall95-papers/rigby-anonymity.html>.

"The Right to Privacy." *Social Philosophy & Policy* 17(2): 3 pars. Social Philosophy & Policy Centre. Summer 2000. 2 December 2003. <http://www.bgsu.edu/offices/sppc/privacy.htm>.

Rosencrance, Linda. "Customer outrage prompts Amazon to change price-testing policy." *Computerworld*. 13 September 2000. International Data Group. 8 December 2003. <http://www.computerworld.com/industrytopics/retail/story/0,10801,50153,00.html>.

Rowland, Diane. "Anonymity. Privacy and Cyberspace." Paper presented at the 15th BILETA Conference: *Electronic Datasets and Access to Legal Information*. 14 April 2000. University of Warwick. 30 November 2003. <http://www.bileta.ac.uk/00papers/rowland.html>.

Seltzer, Richard. "Anonymity for fun and deception: the other side of 'community'." *The Way of the Web* (chapter 7). 1995. The B&R Samizdat Express. 30 November 2003. <http://www.samizdat.com/anon.html>.

Solove, Daniel J. "Access and Aggregation: Public Records, Privacy and the Constitution." *Minnesota Law Review* 86(6): 1137-1218.

—. "Conceptualizing Privacy." *California Law Review* 90: 1087-1156.

—. "Privacy and Power: Computer Databases and Metaphors for Information Privacy." *Stanford Law Review* 53: 1393-1462.

Wallace, Jonathan D. "Nameless in Cyberspace: Anonymity on the Internet." *Cato Institute Briefing Paper* 54 (8 December 1999): 1-8.

Walton, Timothy. "The Constitutional Basis for Privacy." *Internet Attorney*. 2000. 5 December 2003. <http://www.netatty.com/privacy/privacy.html>.

Weisman, Robyn. "It's Official: FBI's Carnivore No More." *NewsFactor Technology News*. 14 February 2001. NewsFactor Network. 2 December 2003. <http://www.newsfactor.com/perl/story/7505.html>.

Weiss, Todd R. "Amazon apologizes for price-testing program that angered customers." *Computerworld*. 28 September 2000. 8 December 2003. <http://www.computerworld.com/industrytopics/retail/story/0,10801,51392,00.html>.

White, Victoria A. "Ethical Implications of Privacy in Electronic Mail." paper presented at *Proceedings of Technical Conference on Telecommunications R&D*. 25 October 1994. University of Massachusetts (Lowell). 28 November 2003. <http://www.eclectechs.com/priv.html>.