REGULATION OF COMPUTING AND INFORMATION TECHNOLOGY

FLOOD CONTROL ON THE INFORMATION OCEAN: LIVING WITH ANONYMITY, DIGITAL CASH, AND DISTRIBUTED DATABASES

*A. Michael Froomkin**

Table of Contents

 Associate Professor, University of Miami School of Law. B.A. 1982, Yale College; M.Phil. 1984, Cambridge University; J.D. 1987, Yale Law School. Internet: froomkin@law.miami.edu. I received significant advice, comments, suggestions, and in several cases careful readings of earlier drafts, from Phil Agre, Caroline Bradley, Mary Coombs, Hal Finney, Oscar H. Gandy, Jr., Lucky Green, Patrick Gudridge, Richard Field, Trotter Hardy, Lili Levi, Mark Lemley, Tim May, Marcel van der Peijl, David Post, Peggy Radin, Steve Schnably, Bill Stewart, Peter Swire, Stephen F. Williams, and Eugene Volokh. I also benefited from the ideas posted by members of the cyberia-l, cypherpunks, and e-cash mailing lists. SueAnn Campbell and Nora de la Garza provided library support. Rosalia Lliraldi provided secretarial assistance. Portions of this paper, particularly in Part II, are a revised version of an electronically published paper, A. Michael Froomkin, *Anonymity and its Enmities*, 1 J. ONLINE L. Article 4 (1995), *available online* http://www.law.cornell.edu/jol/froomkin.html.

I particularly wish to thank Dean Peter Shane and Pam Samuelson for inviting me to participate in the panel entitled "The Regulation of Computing and Information Technology" at the Conference for the Second Century of the University of Pittsburgh School of Law at which an earlier draft of this paper was presented. Unless otherwise stated, this article attempts to reflect legal and technical developments up to January 1, 1996.

INTRODUCTION

Changes in the technology used to create, disseminate, and store information are likely to present some of the most complex challenges to lawyers, policymakers, and citizens throughout the world in the next century. Some of these challenges present broad choices; others present the more constrained, and perhaps more difficult, problem of adopting legal rules to reflect new and not always welcome technological realities. It is important to establish what choices exist, if only to navigate intelligently in the coming policy turbulence. The set of legal and policy options is shaped not just by culture, history, and politics but by the constraints of technology. This article seeks to explore the limits that technology imposes on the legal and policy options available to those concerned about anonymous communication, digital cash, and distributed databases, and the ways in which proposed limits on anonymous communication might reduce personal privacy in unexpected ways.

Anonymity lies at the heart of three interrelated problems arising from computer-aided communications over distributed networks (which I will call "the Internet" for short[1]). First, communicative anonymity is an issue in itself: the Internet makes anonymous communication easy, and this has both good and bad consequences. Legislation to restrict anonymous electronic speech has been introduced in state legislatures and in Congress.[2] Second, the availability of anonymous electronic communication directly affects the ability of governments to regulate electronic transactions over the Internet (both licit and illicit). Third, anonymity may be the primary tool available to citizens to combat the compilation and analysis of personal profile data, although data protection laws also may have some effect also. The existence of profiling databases, whether in corporate or public hands, may severely constrict

1. Actually, "the Internet" is not one thing, but a set of tools. I. Trotter Hardy, *Government Control and Regulations of Networks*, paper presented at Symposium on The Emerging Law of Computer Networks, Austin, TX, May 19, 1995 (on file with author). The Internet provides the best example because it exists today. The analysis will, I hope, scale up to any successor network although there is good reason to believe that it does not scale down to discussions that occur entirely within a forum owned and operated by a single Internet Service Provider such as America OnLine or Compuserve, at least absent common carrier status. *Cf.* Pacific Gas And Elec. Co. v. Public Utils. Comm'n of Calif., 475 U.S. 1 (1986); PruneYard Shopping Ctr. v. Robins, 447 U.S. 74 (1980).

2. *See* 1995 Pa. S.B. 655, 179th Gen. Assem., 1995-96 Reg. Sess. (enacted June 13, 1995) (amending 18 PA. CONST. STAT. § 910(a)(1)). Proposed federal legislation sought to prohibit all anonymous electronic messages intended to "annoy, abuse, threaten, or harass any person . . . who receives the communication." S. 314, 104th Cong., 1st Sess. § 2(a)(1)(B) (1995). A similar proposal was introduced in Connecticut, *see* Larry Lessig, *The Path of Cyberlaw*, 104 YALE L.J. 1743, 1750 n.20 (1995).

the economic and possibly even the political freedoms of the persons profiled; although profiling may not necessarily change the amount of actual data in existence about a person, organizing the data into easily searchable form reduces her effective privacy[3] by permitting "data mining" and correlations that were previously impossible. As U.S. lawyers we are most accustomed to thinking about the problems of data creation, dissemination, and access in certain delimited categories such as the First Amendment, intellectual property rules, the torts of invasion of privacy and defamation, and perhaps in the ambit of a few narrowly defined statutes such as the Privacy Act[4] or the Fair Credit Reporting Act.[5] These categories are valuable, but are collectively inadequate to the regulatory and social challenges posed by the information production, collection, and processing booms now under way.

The policy choices left open in each of these three areas—anonymous electronic speech, anonymous electronic commerce, and the conflict between data profilers and privacy-seekers—varies, and depends critically on the nature and number of the potential targets of regulation. In the course of a description of these new technologies and their possible effects, this Article will make the following arguments and assertions:

Anonymous Electronic Speech. Once Internet access becomes widely deployed it is not realistically possible for any government to monitor the content of every citizen's Internet communications, especially if cryptographic tools are easily obtained.[6] Part II suggests that

3. I use "privacy" in this article to mean "the control of information about oneself." *See, e.g.*, ALAN WESTIN, PRIVACY AND FREEDOM 7 (1970). By using "privacy" in this sense I do not mean to suggest that there is necessarily a "privacy right" to control information about oneself. That is, for the purposes of this article, a question of policy that needs debate. For arguments that if there is a "right" to privacy it means something other than the right to control information about oneself, see, e.g., Judith Jarvis Thompson, *The Right To Privacy*, 4 PHIL. & PUB. AFF. 295 (1975).

William A. Parent, *Privacy: A Brief Survey of the Conceptual Landscape*, 11 SANTA CLARA COMP. & HIGH TECH. L.J. 21 (1995), gives a useful survey of the various ways in which the term privacy can be deployed, including: "the right to be let alone," Samuel D. Warren & Louis B. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 205 (1890), "control of personal information about oneself," Charles Fried, *Privacy*, 77 YALE L.J. 475, 483 (1968), "limitation of access to oneself," Ruth Gavison, *Privacy and the Limits of the Law*, 89 YALE L.J. 421, 428 (1980), "having control of [one's] entire realm of intimate decisions," JULIE C. INNESS, PRIVACY, INTIMACY, AND ISOLATION 7 (1992), and Dean Prosser's four privacy torts, William L. Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960).

4. Privacy Act of 1974, 5 U.S.C. § 552a (1977).

5. 15 U.S.C. § 1681 (1995). Several other nations have data protection laws. *See infra* text accompanying note 347.

6. *See* A. Michael Froomkin, *The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709 (1995).

the same is true of monitoring the sending of anonymous communications: So long as the tools to communicate anonymously remain widely available in other countries, there is not much that any single country can do about it. Nations could, however, make it difficult for their own citizens to provide those tools to others, and if essentially all nations connected to the Internet did this independently or as the result of a concerted effort, the result would be to make anonymous electronic communication more difficult and more risky. Whether this would be constitutional in the U.S. is, however, debatable. It is even less likely that all other major industrialized nations would agree to such a policy. If even one nation with extensive Internet connections chooses not regulate the provision of anonymizing technology, the effect is to make anonymous communication possible by all persons connected to the Internet.

Anonymous Digital Cash. Part III describes a number of competing digital cash products. It is too soon to tell which if any of these products will become widely used. Whatever products persist, national governments are likely to be concerned about digital cash because they will fear that it facilitates illicit transactions, and makes money laundering easy. While digital cash enables rapid, electronic, and even international transactions, only anonymous digital cash is likely to raise regulatory hackles since the non-anonymous variety leaves easily audited records. Furthermore, as Part III explains, different types of digital cash have significantly different implications for law and policy regarding anonymous digital commerce. Many types of digital cash do not allow anonymous transactions at all. Others allow the payor, but not the payee, to be anonymous, although digital money laundries might be able to provide two-way anonymity. Only one of the schemes discussed in Part III is designed to allow direct peer-to-peer fund transfers without the intermediation of an entity functioning as a bank, and even that system could be configured to keep records of every transaction.

Until very large amounts of untraceable anonymous currency are in wide circulation, and these funds are widely accepted for physical purchases as well as electronic commerce, the owners of electronic cash will need a means of transferring funds from electronic cash to ordinary cash. In most cases, the owners of significant sums of electronic cash will also want to invest their funds. In either case they will require the services of a financial service provider, such as a bank. Thus, at least in the medium term, governments may be able to control anony-

mous commerce by concentrating on financial service providers. Financial service providers are already highly regulated, and present a relatively easy target for governments seeking to prevent fully anonymous fund transfers. Regulators may also benefit from the reluctance of consumers to bank abroad, even when offered accounts denominated in their home currency. If, however, consumers become more willing to bank abroad, the ability of governments to control anonymous transactions will be reduced further, unless all or almost all governments are able to agree on common rules.

Anonymity as a Privacy-Enhancing Response to Profiling. Part IV suggests that the policy decision to limit anonymous commerce could itself have large costs. Diverse data become more valuable when aggregated. *If*, as tends to be the case today, the aggregations are carried out by small numbers of parties who hold the aggregated data in proprietary databases, e.g., credit bureaus and credit card companies, *then* it may be possible to regulate them to protect the informational privacy of citizens. The existence of these regulatory chokepoints is unlikely to last, however, because modern search techniques make it increasingly attractive to keep data disaggregated, and continuously updated, while making it searchable over distributed networks akin to the Internet. If every data supplier to the network can also become a user of the network's data, the number of parties who would have to be regulated would grow considerably. When one considers that computerized data are highly mobile, and that data can be stored or searched overseas in "data havens," the regulatory possibilities begin to seem more limited. If indeed regulation is unavailing, or unavailable for other reasons, anonymous communications and anonymous commerce may be the primary tool available to most citizens to prevent their personal data from becoming part of profiles over which they have no control, and which may limit at least their economic options. Thus, it is conceivable that an otherwise legitimate regulation on anonymous digital cash may have such extreme effects on the ability of citizens to use the Internet to receive information without having their reading habits recorded as to call into question the regulation's constitutional propriety, not to mention the wisdom, of such regulation.

Given the importance of anonymity to free speech, electronic commerce, and privacy, it is only a small exaggeration to suggest that the debate about anonymity on the Internet is in effect a debate about the degree of political and economic freedom that will be fostered, or toler-

ated, in a modern society.[7] Part I therefore seeks to frame the issue by quickly sketching a few of the moral and social aspects of the debate over anonymity.

I. THE MORAL AND SOCIAL ENVIRONMENT

There is no consensus, nor is there likely to be, as to whether, on balance, anonymity is a good. Anonymity has both valuable and harmful consequences, and different persons weigh these differently. Some, perhaps focussing on anonymity's contribution to many freedoms, argue that anonymity's benefits outweigh any likely harms it may cause, or that the harms (e.g., censorship) associated with trying to ban anonymity are not worth any benefits that could ensue. Others, perhaps focussing on the victims of harmful actions that can be accomplished anonymously, look at anonymity and often see dangerous license. Their conclusion is that at least some forms of anonymity should be banned.

A. Costs of Anonymity

Anonymous communication is a great tool for evading detection of illegal and immoral activity. Conspiracy, electronic hate-mail and hate-speech in general, electronic stalking, libel, general nastiness, disclosure of trade secrets and other valuable intellectual property, all become lower-risk activities if conducted via anonymous communications. These activities are merely low-risk rather than no-risk because it always remains possible to infer the identity of the author of some messages from clues intrinsic to the message itself. For example, by analyzing the manifesto issued by the "unabomber," the FBI concluded that he went to class or "hovered around" a major university in the late 1970's to mid-1980's, most probably Northwestern University, the Chicago Circle campus of the University of Illinois, the University of Utah, Brigham Young University or University of California at Berkeley.[8] Similarly, the leaker of proprietary or classified data can sometimes be identified if the circle of people who had access to the information was small.

An anonymous author suggests that the most serious argument against anonymous speech is that "disclosure advances the search for

7. *See* Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 500-01 (1995) ("In democratic society, information standards reflect specific conceptions of governance. . . . For private interactions and the relationship between citizens, both law and practice set the balance between dignity and free flows of information.").

8. Martin Gottlieb, *Pattern Emerges in Bomber's Tract*, N.Y. TIMES, Aug. 2, 1995, at A1.

truth,"[9] because when propaganda is anonymous it "makes it more difficult to identify the self interest or bias underlying an argument."[10] The author notes, however, that this argument assumes the validity of the metaphor of the marketplace of ideas, and that whether the benefit of increased information from the ban on anonymous speech outweighs the loss of the ideas whose expression the anonymity ban discourages is an empirical question that is unanswerable.[11] Justice Black, the First Amendment absolutist, thought identity disclosure requirements might enhance the freedom of speech, and suggested Congress could require the disclosure of foreign agents "so that hearers and readers may not be deceived by the belief that the information comes from a disinterested source. Such legislation implements rather than detracts from the prized freedoms guaranteed by the First Amendment."[12]

To an economist who treats markets in ideas as more concrete than a metaphor, the desire to control information about oneself can be either a final or an intermediate good. Treating privacy as a final good, however, limits the power of economic analysis, since privacy is no more than one of many elements of consumer preferences that determine her purchases when faced with the purchases that the market has to offer.[13] Judge Posner has suggested that privacy can usefully be analyzed as an intermediate good.[14] Using this simplifying assumption, Posner concluded that personal privacy is generally inefficient, since it allows persons to conceal disreputable facts about themselves.[15] This failure to disclose disreputable facts shifts costs of information acquisition (or the cost of failing to acquire information) on to those who are not the least-cost avoiders. On the other hand, Posner argues that concealment by businesses is generally efficient, since allowing businesses to conceal trade secrets and other forms of intellectual property will tend to spur innovation.[16] Posner's formulation, however, has been criti-

9. Note, *The Constitutional Right to Anonymity: Free Speech, Disclosure and the Devil*, 70 YALE L.J. 1084, 1109 (1961) (collecting cases) [hereinafter *Anonymous Note*].

10. *Id.* at 1111.

11. *Id.* at 1112-13.

12. Viereck v. United States, 318 U.S. 236, 251 (1943) (Black, J., dissenting).

13. Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393, 394 (1978).

14. Richard A. Posner, *Privacy, Secrecy, and Reputation*, 28 BUFF. L. REV. 1 (1979); Posner, *supra* note 13.

15. *See* Posner, *supra* note 13, at 294-97.

16. Posner, *supra* note 13.

cized for neglecting the strategic aspects of the individual's desire to control the release of personal information that is not disreputable.[17]

Anonymous communication also poses particularly stark enforcement problems for libel law and intellectual property law. While it may be true that a signed defamatory message carries more credibility and thus is more damaging than an anonymous one, it does not necessarily follow that an unsigned message is harmless. Most people would probably be upset to discover a series of unsigned posters accusing them of pedophilia tacked to trees or lampposts in their neighborhood. Perhaps aware that some people believe that where there is smoke there must be fire, the victim of such a libel is unlikely to be soothed by the suggestion that anonymous attacks lack credibility.[18] An Internet libel can be spread world-wide, and may be effectively indelible since it may be reproduced, and stored, in countless and untraceable numbers of computers.[19] Anonymity can also be used to reveal a trade secret. For example, on September 9, 1994 an anonymous poster sent source code purporting to be RC4, a proprietary cryptographic algorithm of RSA Data Security, Inc., to the cypherpunks Internet mailing list.[20] In most cases, a public posting will tend to reduce the value of a trade secret.[21]

Sissela Bok has argued that a society in which "everyone can keep secrets impenetrable at will" be they "innocuous . . . [or] lethal plans," noble acts or hateful conspiracies, would be undesirable because "[i]t would force us to disregard the legitimate claims of those persons who might be injured, betrayed, or ignored as the result of secrets inap-

17. *See* KIM LANE SCHEPPELE, LEGAL SECRETS 43-53, 111-26 (1988); *see also* James Boyle, *A Theory of Law and Information: Copyright, Spleens, Blackmail, and Insider Trading*, 80 CAL. L. REV. 1413 (1992) (arguing that most law and economic analysis of markets for information are based on fundamentally contradictory assumptions).

18. *See, e.g.*, New York v. Duryea, 351 N.Y.S.2d 978, 996 (1974) (arguing that people tend to apply an appropriate discount to anonymous writing).

19. *See* Francis Auburn, *Usenet News and the Law*, [1995] 1 WEB J. CURRENT LEGAL ISSUES, *available online URL* http://www.ncl.ac.uk/~nlawwww/articles1/auburn1.html (discussing the failure of the Western Australia Supreme Court in Rindos v. Hardwick (No. 1994 of 1993, judgment delivered 31 March 1994) to understand USENET and measure damages accordingly).

20. *See* RC4 Source Code, *available online* URL http://www.hks.net/cpunks/cpunks-7/1369.html (entry in cypherpunks list archives). A spokesman for RSA Data Security stated that it has been informed by third parties that the code produces output identical to RC4, but has not confirmed this for itself. Telephone interview with Kurt Stammberger, Director of Technologies Marketing, RSA Data Security, Inc. (Nov. 22, 1995) [hereinafter Stammberger Interview].

21. Interestingly, RSA itself suggested that the public posting of the purported RC4 source code did not affect sales of licensed products because clients who want cryptographic products want to purchase them from vendors they can trust to provide a genuine and reliable product. Stammberger Interview, *supra* note 20.

propriately kept."[22] Justice Scalia believes anonymity is generally dishonorable because it eliminates accountability.[23] This damage to society's ability to redress legitimate claims is, I believe, the strongest moral objection to the increase in anonymous interaction. It is also clearly an objection with popular resonance, as a recent Wall Street Journal column critiquing the growth of anonymous communication on the Internet illustrates.[24] Even a more moderate writer, while admitting that anonymity has its place, suggests that "[p]ermitting anonymity for the purpose of removing any vestige of accountability for abusive behavior . . . is not likely to be tolerated in the Networld."[25]

Anonymity has another serious consequence. Digital anonymity exacerbates the trends that are producing a society of strangers. Strangers are people who lack the mutual and continuous monitoring associated with life in a small town.[26] Another way of putting the same point is that strangers are people about whom one has little or no information; in effect strangers engage each other as if they had complete informational privacy. A society of strangers may be one in which trust may be more difficult. "He who stands by what he has allowed to be known about himself, whether consciously or unconsciously, is worthy of trust."[27] People about whom one knows little or nothing are harder to trust; they can be feared.

Anonymous communication can thus be viewed as one part of a more general debate over the extent to which individuals should control the dissemination of information about themselves. The problem is more complex than the loss of some imagined rural idyll. Urbanization itself does not necessarily breed mistrust. Georg Simmel suggested that in many cases "external facts" about people and goods suffice to create interpersonal confidence which therefore "no longer needs any properly

22. SISSELA BOK, SECRETS: ON THE ETHICS OF CONCEALMENT AND REVELATION 16, 28 (1982).

23. *See infra* text at note 46.

24. WALL ST. J., Jan. 26, 1995, at B1, *available online URL* http://www.clas.ufl.edu/~avi/NII/wsj_no-anon.html.

25. Anne Wells Branscomb, *Anonymity, Autonomy, and Accountability: Challenges to The First Amendment in Cyberspaces*, 104 YALE L.J. 1639, 1675 (1995); *cf.* George P. Long, III, Comment, *Who Are You?: Identity and Anonymity in Cyberspace*, 55 U. PITT. L. REV. 1205 (1994) ("if law enforcement authorities are precluded from obtaining the identities of anonymous users, illegal activities will proliferate").

26. On traditional rural ideas of the personal relationships required as a prerequisite to a commercial relationship, see Anne-Mari Sellerberg, *On Modern Confidence*, 25 ACTA SOCIOLOGICA 39 (1982).

27. NIKLAS LUHMANN, TRUST AND POWER 39 (Howard Davis et al. trans., 1979).

personal knowledge."[28] Certainly, the prevalence of trust is valuable:[29] "Trust is not the sole foundation of the world; but a . . . fairly complex society . . . could not be established without trust."[30] Anonymity, like other forms of personal control over information, threatens to make access to those "external facts" on which people rely more difficult. Unwillingness to trust strangers leads to the growth of social institutions designed to compensate for, or eliminate, anonymity—walled and monitored communities, credit checks, lie detectors, drug tests and on-the-job monitoring.[31] "Surveillance is the cost of [] privacy."[32] The reinterpretation of Fourth Amendment privacy rights via so-called regulatory searches in recent decisions such as *National Treasury Employees Union v. Von Raab*,[33] and *Vernonia School District 47J v. Acton*,[34] may be in part a response to perceived social consequences of privacy.[35]

---

28. GEORG SIMMEL, THE SOCIOLOGY OF GEORG SIMMEL 319 (Kurt H. Wolff trans. & ed., 1964); *see also* Georg Simmel, *The Sociology of Secrecy and of Secret Societies*, 11 AM. J. SOC. 441 (1906).

29. See Carol M. Rose, *Trust in the Mirror of Betrayal*, 75 B.U. L. REV. 531 (1995), for delightful examples.

30. LUHMANN, *supra* note 27, at 94; *see also* FRANCIS FUKUYAMA, TRUST: THE SOCIAL VIRTUES & THE CREATION OF PROSPERITY (1995). Jon Elster defines trustworthiness as the ability to make credible promises. JON ELSTER, THE CEMENT OF SOCIETY 274-75 (1989).

31. *See* STEVEN L. NOCK, THE COSTS OF PRIVACY (1993).

32. *Id.* at 1.

33. 489 U.S. 656 (1989); *see also* Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602, 634 (1989) (finding drug and alcohol tests mandated by Federal Railroad Administration regulations reasonable under the Fourth Amendment); Marshall v. Barlow's, Inc., 429 U.S. 1347, 1347 (1977) (granting stay of injunction against further warrantless searches of workplaces permitted under the Occupational Safety and Health Act of 1970, Pub L. No. 91-596, 84 Stat. 1590 (codified as amended in scattered sections of 5 U.S.C., 15 U.S.C., 18 U.S.C., 29 U.S.C., and 42 U.S.C. (1988 & Supp. V 1993))). *But see* Camara v. Municipal Court, 387 U.S. 523, 540 (1967) (finding that the defendant had a constitutional right to deny a housing inspector entry into a leasehold without a warrant in a non-emergency situation).

34. 115 S. Ct. 2386 (1995) (upholding suspicionless mandatory drug testing of all student athletes in high school). The case is shocking not for the authoritarian principle of law it reiterates, that in the absence of a "clear" 18th century "practice" to guide Fourth Amendment analysis of the reasonableness of a warrantless "administrative" search, the reasonableness "is judged by balancing its intrusion . . . against its promotion of legitimate governmental interests." *Id.* at 2390 (quoting Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602, 619 (1989)), but for how the test was applied: Justice Scalia concluded that because student athletes have a lower expectation of privacy given the nature of the high school locker room, and because by volunteering for sports they "subject themselves to a degree of regulation even higher than that imposed on students generally," *id.* at 2392-93, their privacy interest could be overbalanced by a school district's "perhaps compelling," *id.*, desire to deter drug use in school by making examples of what it perceived to be student leaders, despite an absence of any particularized suspicion that those students used drugs.

35. The result in *Vernonia* seems at least partly influenced by the District Court's finding that the school was "in a state of rebellion" that "was being fueled by alcohol and drug abuse as well as by the student's misperceptions about the drug culture." *Id.* at 2395. Justice Scalia described this as

A similar impulse may motivate legislative initiatives such as Megan's Law.[36]

The objection to communicative anonymity with the most popular resonance may blend all these concerns. The combination of communicative anonymity with a powerful, global, poorly understood new medium seems to threaten people because the Internet allows strangers to reach into the same homes that are being turned into fortresses against strangers, and to allow those strangers to interact with its inhabitants (especially its children) without any risk of being held accountable for their communications. It may be that the idea of the home as a secure fortress is an illusion,[37] but it is a powerful hope.

B. Advantages of Anonymity

Ironically, the same anonymity that is blamed for undermining the accountability necessary for the security of the home/fortress may turn

---

"an immediate crisis of greater proportions than existed in *Skinner*" *id.* where the showing of drug use by railroad employees was based on national data, rather than data particularized to a single railroad. *Id.* Nevertheless, while it may not have been particularized, the danger in *Skinner* affected railway safety, a field in which accidents can kill hundreds; it is difficult to see a "crisis of greater proportions" in a rebellious classroom.

36. N.J.S.A. 2C:7-1 (1996).

37. There is no doubt, for example, that the home is permeable to sense-enhanced searches by the police and possibly others. *See, e.g.*, Florida v. Riley, 488 U.S. 445, 451-52 (1989) (plurality opinion) (holding valid a warrantless aerial surveillance of a greenhouse from four hundred feet); California v. Ciraolo, 476 U.S. 207, 215 (1986) (holding valid a warrantless aerial surveillance of a yard enclosed by a 10-foot fence). *Cf.* Jeff Cole, *Eyes in the Skies: New Satellite Imaging Could Soon Transform The Face of the Earth*, WALL ST. J., Nov. 30, 1995, at A1 (describing new generation of ultra-high-quality satellite images offered for sale).

The government can use satellites to spy in the home's windows. Lisa J. Steele, Comment, *The View from on High: Satellite Remote Sensing Technology and the Fourth Amendment*, 6 HIGH TECH. L.J. 317, 327-33 (1991) (discussing warrantless searches by satellite and the applicable constitutional implications). It may use heat-detection gear to monitor heat emanations from the home. *See* United States v. Pinson, 24 F.3d 1056, 1059 (8th Cir.) (holding that a warrantless use of infrared sensing devices did not violate the Fourth Amendment because any defendant's subjective expectation of privacy in heat emanating from her house is not one that society is prepared to recognize as objectively reasonable), *cert. denied*, 115 S. Ct. 664 (1994); *but see* State v. Young, 867 P.2d 593 (Wash 1994) (holding that warrantless use of infrared thermal detection device violates state constitution); United States v. Cusamano, 67 F.3d 1497 (10th Cir. 1995) (holding that warrantless use of thermal imager upon home violates Fourth Amendment).

Given the wide range sense-enhanced searches outside the reasonable expectation of privacy for Fourth Amendment purposes, see Scott E. Sundby, *"Everyman's" Fourth Amendment: Privacy or Mutual Trust Between Government and Citizen?*, 94 COLUM. L. REV. 1751, 1758-63 (1994) (explaining how the Supreme Court has used increasing permeability of home to enhanced intrusion as a reason to find no reasonable expectation of privacy for Fourth Amendment analysis), one can reasonably ask what sort of intrusions other than a simple Peeping Tom is actionable as common law trespass or invasion of privacy. Of course, unofficial invasions of privacy can be statutory offenses.

out to be the tool that the inhabitants of that home need to level the playing field against corporations and governments that might seek to use new data processing and data collection tools in ways that constrain the citizen's transactional or political freedom. Larger and faster database processing techniques combined with the ever-increasing quantity of personal data available on individuals makes it possible for both governments and private organizations to construct personal profiles based on transactions, demographics, and even reading habits of most citizens. Since most people lack the ability to contract for privacy on affordable terms, their main line of defense against being profiled is likely to be anonymous communication and anonymous transactions.[38]

Anonymous communication may be particularly deserving of protection for its own sake. Not everyone is so courageous as to wish to be known for everything they say,[39] and some timorous speech deserves encouragement. Corporate whistle-blowers, even junior professors, may fear losing their jobs. People criticizing a religious cult or other movement from which they might fear retaliation may fear losing their lives. In some countries, even this one in some times and places, it is unsafe to be heard to criticize the government. Persons who wish to criticize a repressive government[40] or foment a revolution against it may find anonymity invaluable. Indeed, given the ability to broadcast messages widely using the Internet, anonymous e-mail may become the modern replacement of the anonymous handbill.

Communicative anonymity encourages people to post requests for information to public bulletin boards about matters they may find too personal to discuss if there were any chance that the message might be traced back to its origin. In addition to the obvious psychological benefits to people who thus find themselves enabled to communicate, there may be external benefits to the entire community. To pick just one example, public health is enhanced by the provision of information regarding communicable diseases, but many people would feel uncomfortable asking signed questions about sexually transmitted diseases, and might be especially cautious about being identified as a potential sufferer of AIDS. This caution may be particularly reasonable as data-

38. *See infra* Part IV.

39. "[A]ctual instances of the deterrent impact of disclosure laws are legion." *Anonymous Note*, *supra* note 9, at 1107.

40. *Cf.* Dirk Johnson, *Chinese in U.S. Lament Bush Victory*, N.Y. TIMES, Jan. 27, 1990, § 1, at 10 (describing fears of Chinese students in U.S. that protests against the Beijing government would lead to persecution if they returned home and retaliation against their families).

collection technology improves: any post to a public newsgroup or bulletin board is liable to be archived and searchable, perhaps for all eternity.

Anonymous communication, whether traceable or not, fosters the development of digital personae, which may be experienced as liberating by some.[41] The option of creating such personae is likely to increase and enhance the quantity, if not inevitably the quality, of speech. In addition to increasing the quantity of speech, anonymous communication may also enhance the quality of speech and debate.[42] Communications that give no hint of the age, sex, race, or national origin of the writer must be judged solely on their content as there is literally nothing else to go by. This makes bigotry and stereotyping very difficult, and also should tend to encourage discussions that concentrate on the merits of the speech rather than the presumed qualities of the speakers.[43]

In the U.S., anonymous speech may be guaranteed by the First Amendment or whatever right to privacy exists in the Constitution. In the U.S., anonymous speech also benefits from its association with well-remembered incidents in which political actors holding unpopular views that many now accept benefitted from the ability to hide their identity. The *Federalist Papers*, the nation's most influential political tracts, were published pseudonymously under the name "Publius." More recently, the Supreme Court held the guarantee of free speech in the Constitution protects a right of anonymous association and that a state therefore lacked the power to compel a local chapter of the NAACP to disclose the names of its members.[44] In so doing, the Court protected the NAACP members from danger at the hands of bigots who would have had access to their identities if the state had prevailed. Anonymity basks in the glow of association with good causes.

---

41. For a celebration of such "digital personalities," see Curtis E.A. Karnow, *The Encrypted Self: Fleshing Out the Rights of Electronic Personalities*, 13 J. COMPUTER & INFO. L. 1 (1994).

42. Or, it may not. *See supra* text at note 10.

43. There is probably a great deal more to be said on this subject. One need only to consider the enormous weight that our "identity-conscious society and legal world," Clark Freshman, *Were Patricia Williams and Ronald Dworkin Separated at Birth?*, 95 COLUM. L. REV. 1568, 1576 (1995) (book review), places on factors such as race, *see* Christopher A. Ford, *Administering Identity: The Determination of "Race" in Race-Conscious Law*, 82 CAL. L. REV. 1231 (1994), to imagine the effects.

44. NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449 (1958).

C. *Legislating Accountability*

Dissenting in *McIntyre v. Ohio Elections Commission*,[45] Justice Scalia summed up the case against anonymity. Anonymity, he wrote, is generally dishonorable: "It facilitates wrong by eliminating accountability, which is ordinarily the very purpose of the anonymity."[46] To create legal protection for anonymous communication absent a reason to expect "threats, harassment, or reprisals," he argued, is "a distortion of the past that will lead to a coarsening of the future."[47]

The specter of a cheap and potentially ubiquitous means of avoiding accountability for one's speech or one's possibly illicit purchases is worrying to many, and seems to be leading to increasing attempts to regulate anonymous communication, and anonymous digital cash. Pennsylvania, for example, has just passed a statute making it a crime to possess, program, or use a device which can be used to "conceal or to assist another to conceal . . . the origin or destination of any telecommunication."[48] In other cultures with a more authoritarian tradition, anonymous speech may seem even more threatening to the established order; in some places the idea of anonymous communication may also conjure up unhappy images of secret informers and malicious denunciations.

In a legal culture that tends to glorify the First Amendment as the bedrock of our freedoms, it may seem odd to suggest the possibility of controls on information creation, dissemination, or storage. And in an age where the political rhetoric, if not always the policy, is increasingly that of *laissez-fair* capitalism it may seem strange to suggest that governments might impose curbs on technologies that increase transactional freedom. The instinct that says all such controls are bad may indeed be a healthy one, although it is not the instinct that animates all current U.S., much less foreign, law,[49] and definitely not the instinct

---

45. 115 S. Ct. 1511 (1995).

46. *Id.* at 1537 (Scalia, J., dissenting). On the link between identity and accountability see, e.g., Sally Engle Merry, *Manipulating Anonymity: Streetwalkers' Strategies for Safety in the City*, 45 ETHNOS 157, 158 (1980) (stating that prostitutes seek to reduce their risks by "finding out as much as possible about the identities of those they encounter while hiding clues to their own identity").

47. 115 S. Ct. at 1537. There is some irony in Justice Scalia being so concerned that every private harm have a private remedy, when he so firmly rejects the idea that public harms necessitate a remedy. *See, e.g.*, Webster v. Doe , 486 U.S. 592, 661-71 (1988) (Scalia, J., dissenting).

48. Pa. S.B. 655, *supra* note 2.

49. U.S. examples include the copyright law, 17 U.S.C. § 102 *et seq.* and the International Traffic in Arms Regulations. *See* 22 C.F.R. § 121.1 (XIII)(b)(1) (1994).

that animates some notorious current policy proposals.[50] The instinct is complicated, although by no means invalidated, by the global reach of the information ocean now lapping at our doorstep.[51] Our ability to police ourselves is eroded by pools and rivers of foreign data outside our shores, and by our interconnection with networks in other countries that may operate by different rules. Similarly, foreign governments with repressive tendencies may find their restrictive information policies undercut by the extraterritorial consequences of our practices.

II. FREE SPEECH NOW: THE ANONYMOUS MESSAGE IN THE IMPREGNABLE BOTTLE

The Internet we have today is a tool for communication, one undergoing rapid growth.[52] At present the Internet is primarily an elite tool, but it seems reasonable to suppose that access to the Internet will become almost as ubiquitous as access to the telephone network within a few years.[53] Some of the transformative effects of this explosion in

50. *See supra* note 2 (proposals to censor the Internet).

51. I owe the metaphor of an information ocean to Rishab A. Ghosh. *See* E-mail to Michael Froomkin (Jan. 11, 1995) (on file with author) (quoting from his article in *Asian Age* magazine of Jan. 2, 1995).

52. *See* gopher://ncic.merti.edu:7043/11/statistics/nsfnet/history/hosts for a recent count of computers connected to the Internet. Today's Internet is an amalgam of many government and academic networks. An increasing number of commercial and nonprofit information service providers have joined these networks, including Dow Jones, Telebase, Dialog, CARL, the National Library of Medicine, and RLIN. Benard Aboba, *How the Internet Came to Be, in* THE ONLINE USER'S ENCYCLOPEDIA (1993), *available online URL* gopher://gopher.isoc.org:70/00/Internet/history/how.Internet.came.to.be. The relationship between the Internet and commercial consumer information providers such as America OnLine (AOL), CompuServe and Prodigy continues to evolve. At their inception these services provided no Internet connectivity. They then began to offer limited gateways for the exchange of electronic mail. Now they are expanding their gateways to allow their users to gain access to the World Wide Web, and sometimes to other Internet services as well. The number of subscribers is also growing rapidly. Subscriber growth is estimated at 25% or more per year. During the first three months of 1995, U.S.-based PC online services added more than 1 million subscribers. Testimony of William. W. Burrington, Assistant General Counsel and Director of Government Affairs, America OnLine, Inc before the Senate Subcommittee on Terrorism, Technology, and Government Information 6 (May 11, 1995), *available online* LEXIS library Nexis, Curnws File [hereinafter Burrington Testimony]. However, the commercial access provided by large national ISPs is primarily one-way, and it is unclear to what extent commercial ISPs desire to allow persons outside their service to have Web or FTP access to information generated by subscribers. Market pressures, notably the desire of users to have their Web pages widely read, appear to be promoting this development.

53. More than 93% of U.S. households had telephones in 1990. Warren G. Lavey, *Universal Telecommunications Infrastructure for Information Services*, 42 FED. COMM. L.J. 151 (1990) (citing FCC News No. 723: Preliminary Domestic Information from Statistics of Communications Common Carriers Released by FCC, at Table 9 (1989)). Thirty percent of U.S. households have a computer. DAVID BENDER, THE MICROSOFT ANTITRUST WARS, PRACTICING LAW INSTITUTE, PATENTS, COPY-

Internet connectivity, particularly within the United States, are already becoming visible.

Internet communication is capable of becoming a radically democratizing tool. The Internet offers rapid and (relatively) cheap one-to-one communication both nationally and internationally. It also provides means for citizens who have a common interest to find other like-minded persons to communicate with.[54] The autobiographical *bildungsroman* featuring an adolescent who believes he is the only sane, intelligent, or gay person (as the case may be) in a small town, and has no one to talk with, soon may be a thing of the past.

Perhaps more importantly, the Internet promises to democratize one-to-many communication. On the World Wide Web, to take the currently most popular example, everyone is a potential publisher, and the potential readership (and listenership and viewership, since the Internet increasingly transports audio and video) grows every day. The elite nature of the contemporary Internet makes it too soon to call it a truly democratic medium. Nevertheless, as Owen Fiss himself has noted, one can reasonably hope that his warning that radical critics of the status quo find it difficult to obtain access to mass media will soon seem passé.[55] The Internet is already becoming a significant tool of political debate and political organization,[56] and has the potential to en-

---

RIGHTS, TRADEMARKS, AND LITERARY PROPERTY COURSE HANDBOOK SERIES (No. G4-3942) June 22-23, 1995 (*available online* WESTLAW tp-all database).

Currently the Internet reaches more than 90 countries; at least 160 have e-mail connectivity. Burrington Testimony, *supra* note 52, at 7.

The Clinton Administration has stated that it intends to make widespread access a cornerstone of its National Information Infrastructure policy. "Because information means empowerment, the government has a duty to ensure that all Americans have access to the resources of the Information age . . . [the NII will attempt to] Extend the 'universal service' concept to ensure that information resources are available to all at affordable prices." The National Information Infrastructure: Agenda for Action, 58 Fed. Reg. 49,025, 49,027-28 (1993).

54. *See* Eugene Volokh, *Cheap Speech and What It Will Do*, 104 YALE L.J. 1805 (1995). Consider too Karl Marx's remark that, "A relatively thinly populated country, with well-developed means of communication, has a denser population than a more numerously populated country, with a badly-developed means of communication." KARL MARX, CAPITAL (*quoted in* MARK POSTER, THE MODE OF INFORMATION 1 (1990)).

55. *Compare* Owen Fiss, *Silence on the Street Corner*, 26 SUFFOLK U. L. REV. 1, 3 (1992) (cautioning that radical dissent is becoming relegated to the "last desperate forum"—the street corner) *with* Owen Fiss, *In Search of a New Paradigm*, 104 YALE L.J. 1613 (1995); *see also* Jerry Berman & Daniel J. Weitzner, *Abundance and User Control: Renewing the Democratic Heart of the First Amendment in the Age of Interactive Media*, 104 YALE L.J. 1619, 1623 (1995); Volokh, *supra* note 54, at 1833-36.

56. *See, e.g., available online URL* http://dgsys.com/~cgriffin/net_gde.html (detailing how to use the net for political organizing and opposition research); MIT's Political Participation Project, *available online URL* http://www.ai.mit.edu/projects/ppp/home.html; Mark S. Bonchek, *Grass-*

hance representative democracy.[57] Indeed, as group formation on a national scale becomes easier and less costly, some positive critiques of pluralism may lose some (but not all) of their force.[58]

It is yet not evident whether the Internet will be a communicative tool that will be a net benefit to democratic government or society, or even one that is truly democratic.[59] The democratization of publishing means that much more will be published, which may lead to the ultimate in narrowcasting as readers try to keep their virtual heads above a rising tide of data.[60] Talking only to the like-minded has an anti-democratic, or at least anti-communitarian, component. If the Internet becomes the town square, or the shopping mall of the future, it may be one in which millions are shouting on the same street corner while passers-by are able to tune in or out at will. Many speakers may find themselves drowned out in the cacophony, although this will be due to a decision by the listener and not, as today, a function of the limited number of speakers with access to mass media.[61] It should be noted, however, that tools exist which tend to mitigate the drowning-out effect. For example, search tools on the World Wide Web may lead readers to materials they would otherwise never find. Similarly, Bob's decision to include a hypertext link to Alice's web page functions as free

---

roots in Cyberspace: Using Computer Networks to Facilitate Political Participation (Working Paper 95-2.2: Presented at the 53rd Annual Meeting of the Midwest Political Science Association in Chicago, IL on April 6, 1995), *available online URL* http://www.ai.mit.edu/projects/ppp/pubs/95-2-2.html.

57. *See* Cass Sunstein, *The First Amendment in Cyberspace*, 104 YALE L.J. 1757, 1783 (1995).

58. *E.g.*, MANCUR OLSON, THE LOGIC OF COLLECTIVE ACTION (1971). For a quick summary of some positive critiques of pluralism, see A. Michael Froomkin, *Climbing the Most Dangerous Branch: Legisprudence and the New Legal Process*, 66 TEX. L. REV. 1071 (1988) (book review).

59. Statistics on Internet usage vary. A recent study found that 34% of users are female, but that females account for only 23% of measurable usage. Donna L. Hoffman & Thomas P. Novak, *Measuring the Internet: Preliminary Results of the Commerce/Nielsen Internet Demographics Survey*, http://www2000.ogsm.vanderbilt.edu/novak/CN.prelim.results.oct30.html. The most commonly quoted statistic before this study suggested that fewer than 20% of the users of the Internet in 1994 were female. *See, e.g.*, Cabinet Office (OPSS) Press Office, Cyberspace is for Women Too, *available online URL* http://www.coi.gov.uk/coi/depts/GCO/coi8119a.ok (quoting UK Science Minister John Horam) (OPSS 185/95, June 21, 1995); Males Predominate on Internet, But Women are Making Headway, *available online URL* http://www.dgsys.com/~editors/woman.html (citing Georgia Institute of Technology Survey showing 82% of Internet users are male). Presumably, most users of the Internet are at least wealthy enough to have use of a computer, not to mention some basic literacy, which also makes the user community less representative of the population as a whole.

60. *See* Vartan Gregorian, *A Place Elsewhere: Reading the Age of the Computer*, BULL. AM. ACAD. ARTS & SCI. 56 (Jan. 1996); Sunstein, *supra* note 57, at 1787; Volokh, *supra* note 54, at 1835.

61. *See* Volokh, *supra* note 54, at 1834.

advertising for Alice, which may garner her readers she would not otherwise have. Such links may function as a primitive set of reputation credentials which would bring some speakers more listeners. Interestingly, both of these examples require some action on the part of the reader; the author/publisher need do nothing more than announce the existence of the resource to the appropriate indexing services.[62]

Any proposal to regulate Internet anonymity in the United States faces two large hurdles: the Constitution and the technological constraints imposed by the international nature of the Internet. At present, however, Internet anonymity relies on a small number of unpaid volunteers who operate the anonymous remailers that make Internet anonymity possible. If many governments impose regulations banning or restricting their activities, access to Internet anonymity could become much more difficult.

A. How the Internet Enables Anonymous Communication

Thanks in large part to the easy availability of powerful cryptographic tools, the Internet provides the ability to send anonymous electronic messages at will. As described in more detail below, the anonymously remailed e-mail cannot, if properly implemented, be traced to its sender. In addition, two or more persons can communicate without knowing each other's identity, while preserving the 'untraceable' nature of their communications. As detailed below, the availability of strong cryptography vastly enhances communicative privacy and anonymity.

Currently the Internet makes it easy to send an anonymous message. Although no tangible goods can be exchanged, this communicative anonymity allows users to engage in political speech without fear of retribution, to engage in whistle-blowing while greatly reducing the risk of detection, and to seek advice about embarrassing personal problems without fear of discovery—things that are hard to do by telephone in this age of caller ID.[63]

---

62. For an example of a service that helps web author/publishers list their works on multiple indices, see Submit It!, *available online URL* http://www.submit-it.com/.

63. On Caller ID, see Robert Asa Crook, *Sorry, Wrong Number: The Effect of Telephone Technology on Privacy Rights*, 26 WAKE FOREST L. REV. 669 (1991); Consuelo Lauda Kertz & Lisa Boardman Burnette, *Telemarketing Tug-of-War: Balancing Telephone Information Technology and the First Amendment with Consumer Protection and Privacy*, 43 SYRACUSE L. REV. 1029 (1992); Glenn C. Smith, *We've Got Your Number! (Is it Constitutional to Give it Out?): Caller Identification Technology and the Right to Informational Privacy*, 37 UCLA L. REV. 145 (1989); Steven P. Oates, *Caller ID: Privacy Protector or Privacy Invader?*, 1992 U. ILL. L. REV. 219; *cf.*

The traditional anonymous leaflet required a printing and distribution strategy that avoided linking the leaflet with the author. If the leaflet risked attracting the attention of someone armed with modern forensic techniques, great pains were required to avoid identifying marks such as distinctive paper or fingerprints. In contrast, on the Internet communications are all digital; the only identifying marks they carry are information inserted by the sender, the sender's software, or by any intermediaries who may have relayed the message while it was in transit. Ordinarily, an e-mail message, for example, arrives with the sender's return address and routing information describing the path it took to get from sender to receiver; were it not for that information, or perhaps for internal clues in the message itself ("hi mom!"), there would be nothing about the message to disclose the sender's identity.

Enter the anonymous remailer. Remailers vary, but all serious[64] remailing programs share the common feature that they delete all the identifying information about incoming e-mails, substitute a predefined header identifying the remailer as the sender or using a cute tag such as nobody@nowhere.[65] By employing easily automated cryptographic precautions widely available on the Internet,[66] and routing a message through a series of remailers, a user can ensure three things conducive to high-security anonymity: (1) none of the remailer operators will be able to read the text of the message because it has been multiply encrypted in a fashion that requires the participation of each operator in turn before the message can be read;[67] (2) neither the recipient nor any

---

Smith v. Maryland, 442 U.S. 735, 745-46 (1979) (no expectation of privacy in telephone numbers dialed because this information is available to the telephone company).

64. Some intentionally insecure remailers are intended to let the sender have a little fun. These typically insert clues in the detailed headers (which are rarely displayed by commercial e-mail packages unless the user specifically instructs the software to show them) that reveal the origin of the message. A particularly cheerful example of this was a World Wide Web page called, "Why Send E-Mail when You Can Send FakeMail?," *available online URL* http://www.netcreations.com/fakemail, which, among other things, sent my mother birthday greetings from various real and fictitious dignitaries. The system ran until the owner shut it down because of "a few really nasty, harmful, hateful messages" sent via the service. *Id.*

65. A list of remailers and their features, as well as current information about their recent performance statistics, can be found at the University of California at Berkeley *available online URL* http://www.cs.berkeley.edu/~ralph/remailer-list.html.

66. Public-key encryption technology is widely available on the Internet. Pretty Good Privacy (PGP) is available online by FTP from many sites including *available online URL* ftp://net-dist.mit.edu/pub/, *available online* URL ftp://ftp.ox.ac.uk/pub/crypto/pgp, or a German server: *available online URL* ftp://ftp.informatik.uni-hamburg.de:/pub/virus/crypt/pgp. For a good description of the technical and political workings of PGP, see SIMSON GARFINKEL, PGP: PRETTY GOOD PRIVACY (1995).

67. *See infra* text following note 75.

remailer operators in the chain (other than the first in line) can identify the sender of the text without the cooperation of every prior remailer's operator; (3) therefore it is impossible for the recipient of the message to connect the sender to the text unless every single remailer in the chain both keeps a log of its message traffic and is willing to share this information with the recipient (or is compelled to do so by a court or other authority). Since some remailer operators refuse to keep logs as a matter of principle, there is a good chance that the necessary information does not exist. Even if logs exist, it could be prohibitively expensive to compel all the operators to divulge their logs when remailers are located in different countries.[68]

Any electronic communication, even live two-way 'chat' communication, can theoretically be made anonymous.[69] In current practice, anonymous remailer technology applies to e-mail, and hence is used for communication to individuals, mailing lists, and 'newsgroup' discussions. E-mail offers the simplest case, and although e-mail remailer technology may not yet be as user-friendly as it could be, it is available to anyone who knows where to look—and can even be found on an easy-to-use World Wide Web page.[70]

It is useful to distinguish between four types of communication in which the sender's physical (or "real") identity is at least partly hidden: (1) *traceable anonymity,* (2) *untraceable anonymity*, (3) *untraceable pseudonymity,* and (4) *traceable pseudonymity*. These categories allow one to disentangle concepts that are otherwise conflated: whether and how an author identifies herself as opposed to whether and how the real identity of the author can be determined by others.[71]

To make the examples that follow clearer, in each case Alice will be the person sending an e-mail message to Bob. Ted, Ursula, and

68. The expense of hiring foreign legal counsel, and possible language difficulties are only some of the problems. Many legal systems require that an act be an offense in both jurisdictions before allowing a prosecution, or in some cases even discovery, to proceed. The recent successful effort by the Church of Scientology to get information from a remailer operator succeeded because the remailer was a "traceable pseudonymous" remailer, *see infra* text at note 80, not a true anonymous remailer.

69. For a description of a prototype anonymizing WWW browser, see Annonymizer FAQ, *available online URL* http://anonymizer.cs.cmu.edu:8080/faq.html.

70. The URL is http://www.c2.org.

71. For an example of the dangers of conflatation, see Long, *supra* note 25. The author states that "[i]nevitably, each user [of a remailer] is subject to the integrity and trustworthiness of the server's administrator." *Id.* at 1184. In fact, as described in the text below, this is true only of *traceable* anonymity and pseudonymity; untraceable anonymity, for example, does not require that the author trust any individual, only that the message be routed through a large enough number of remailers to ensure that there is one trustworthy person somewhere in the chain.

Victor will be remailer operators, and Carol a judge with subpoena power.

1. Electronic Anonymity

Electronic anonymity can be "traceable" or "untraceable." Only the latter offers real security to the speaker.

a. Traceable anonymity

A remailer that gives the recipient no clues as to the sender's identity, but leaves this information in the hands of a single intermediary, is a system of traceable anonymity. In the simplest example, Alice sends an unencrypted e-mail to a remailer operated by Ted, with instructions to forward the e-mail to Bob. Ted's remailer deletes Alice's identifying return address and sends the message on to Bob purporting to be from "nobody@remailer.com."

Alice has no way of knowing whether Ted has logged the message, keeping a record of Alice and Bob's e-mail addresses, or indeed the entire text of the message. If Ted has done this, then Bob can find out who sent him the message by persuading Ted to tell him—or, in some cases, if the message appears to violate a law, by enlisting the aid of Carol, a judge with subpoena power. Of course, if Ted lives in another country, outside Carol's jurisdiction, there may be little that Carol can do to assist Bob in his quest to persuade Ted to reveal Alice's identity. Many countries do have agreements for judicial assistance, but these can be costly, difficult, and in many cases require that the act complained of be illegal in both nations.[72]

Although traceable anonymity offers the lowest security, it suffices for many purposes. Some messages do not require any more security than a new header. There have been occasions when I have posted messages to newsgroups and received a great deal of unwanted e-mail in reply because my e-mail signature identifies me as a law professor. One way to avoid getting requests for free legal advice, or long and vicious notes attempting to re-educate me about gun control, is to delete the signature and route comments through a remailer. That simple expedient suffices because the consequences of my being discovered as the author of my posts on legal topics are not terribly severe.

---

72. *But see* the discussion of the anonymous remailer "anon.penet.fi," *infra* text accompanying note 78.

In general, however, sending a message with sensitive information directly to a remailer for immediate forwarding to the intended recipient requires an inordinate amount of trust that the remailer operator will not read or copy the message or report the sender to the appropriate authorities. I have often thought that a nice novel could be written using a crooked remailer operator as its central character: imagine that Ted opens up for business, runs a fine remailer for a few years, collects many guilty secrets, and then retires on his blackmail profits.

Much greater security, and nearly iron-clad anonymity, can be achieved at the price of somewhat greater complexity through the use of "untraceable anonymity."

b. Untraceable anonymity

By "untraceable anonymity" I mean a communication for which the author is simply not identifiable at all. For example, if Alice drops an unsigned leaflet with no fingerprints on Bob's doorstep in the dead of night when no one is looking, her leaflet is "untraceably anonymous."

Current Internet technology allows this form of anonymity by the routing of messages through a series of anonymous remailers. This technique is called "chained remailing" and is about as anonymous as directed communication gets these days. Nothing is foolproof, however: as explained below, if Alice has the bad luck to use only compromised remailers whose operators are willing to club together to reveal her identity, she is just out of luck. If one member of the chain performs, however, Alice can ensure that no one can connect her to the message Bob receives so long as she uses both encryption and chaining. Even these two techniques together may not be enough to foil a determined eavesdropper who is able to track messages going in and out of multiple remailers over a period of time. To foil this level of surveillance, which has nothing to do with the bad faith of the remailer operators, requires even more exotic techniques including having the remailers alter the size of messages and ensuring that they are not remailed in the order they are received.[73]

At the simplest level, encryption ensures that the first remailer operator cannot read the message and effortlessly connect Alice to Bob

73. *See* Lance Cottrell's home page on Mixmaster: *available online URL* http://obscura.com/~loki/Mixmaster.FAQ.html; Remailer-Essay, *available online URL* http://nately.ucsd.edu/~loki/remailer-essay.html (explaining that some remailers intentionally introduce delays ("latency") to make it more difficult for any eavesdropper to link outgoing traffic with incoming messages).

and/or the contents of the message. But encryption also has a far more important and subtle role to play. Suppose that Alice decides to route her anonymous message via Ted, Ursula, and Victor, each of whom operates a remailer and each of whom has published a public key in a public-key encryption system[74] such as PGP.[75] Alice wants to ensure that no member of the chain knows the full path of the other remailers handling the message; anyone who knew the full path would be able to identify Alice from the message Bob will receive. On the other hand, each member of the chain will necessarily know the identity of the immediately previous remailer from which the message came, and of course the identity of the next remailer to which the message will be sent.

Alice thus wants Ted, the first member of the chain, to remove all the information linking her to the message; she is particularly anxious that Ted not be able to read her message since he is the one party in the chain who will know that Alice sent it. Alice also wants Ted to know only that the message should go to Ursula, and to remain ignorant of the message's route thereafter. Alice wants Ursula, the second member of the chain, to know only that the message came from Ted

---

74. In a public-key system, each user creates a public key, which is published, and a private key, which is secret. Messages encrypted with one key can be decrypted only with the other key, and vice-versa. For a fuller description, see Whitfield Diffie & Martin E. Hellman, *New Directions in Cryptography*, IT-22 IEEE TRANSACTIONS INFO. THEORY 644 (1976), and Ralph C. Merkle, *Secure Communication over Insecure Channels*, COMM. ACM, Apr. 1978, at 294; BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY 29 (1994); Whitfield Diffie, *The First Ten Years of Public-Key Cryptography*, 76 PROC. IEEE 560 (1988) (discussing the history of public key cryptography).

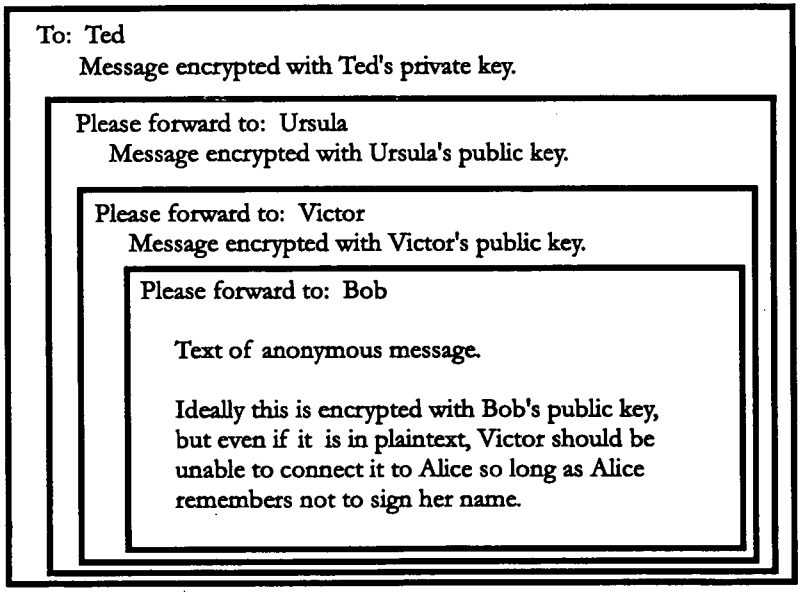
A strong public-key system is one in which possession of both the algorithm and one key provides no useful information about the other key. The system gets its name from the idea that the user will publish one key, but keep the other one secret. The world can use the public key to send messages that only the private key owner can read; the private key can be used to send messages that could only have been sent by the key owner.

Thus, if Alice wants to send a secure e-mail message to Bob, and they both use compatible public-key cryptographic software, Alice and Bob can exchange public keys on an insecure line. If Alice has Bob's public key *and knows that it is really Bob's*, then Alice can use it to ensure that only Bob, and no one pretending to be Bob, can decode the message. A strong public key system makes it possible to establish a secure line of communication with anyone who is capable of implementing the algorithm. (In practice, this is anyone with a compatible decryption program or other device.) Sender and receiver no longer need a secure way to agree on a shared key. If Alice wishes to communicate with Bob, a stranger with whom she has never communicated before, Alice and Bob can exchange the plaintext of their public keys. Then, Alice and Bob can each encrypt their outgoing messages with the other's public key and decrypt their received messages with their own secret, private key. The security of the system evaporates if either party's private key is compromised, that is, transmitted to anyone else.

75. "PGP" stands for "Pretty Good Privacy." *See supra* note 66. It is a type of robust encryption, which when used with a long key is unbreakable in any reasonable period of time by currently known techniques.

and should go to Victor; Victor should know only that it came from Ursula and should go to Bob, although by the time the message reaches Victor, Alice may not care as much whether Victor can read the message since her identity has been well camouflaged.

Alice achieves these objectives by multiply encrypting her message, in layers, using Ted, Ursula and Victor's public keys. As each remailer receives the message, it discards the headers identifying the e-mail's origins and then decrypts the message with its private key, revealing the next address, but no more. If one thinks of each layer of encryption as an envelope, with an unencrypted address on it, one can visualize the process as the successive opening of envelopes, as follows:



Chaining the message through Ted, Ursula, and Victor means that no remailer operator alone can connect Alice to either the text of the message or Bob. Of course, if Ted, Ursula and Victor are in a cabal, or all in Carol's jurisdiction and keep logs that could be the subject of a subpoena, Alice may find that Bob is able to learn her identity. All it takes to preserve Alice's anonymity, however, is a single remailer in the chain that is both honest and either erases her logs or is outside Carol's jurisdiction. In theory, there is no limit to the number of remailers in the chain, and Alice can, if she wishes, loop the message through some

remailers more than once to throw off anyone attempting traffic analysis.[76]

2. *Electronic Pseudonymity*

Suppose Alice is a repeat participant in a broadcast medium such as USENET or a mailing list. She may not wish to sign her name to her messages, but she desires to engage in discussion and debate with other list members and she wishes to do so under a continuous identity. Alice decides to sign her messages as "Andrea." Alice could, however, have chosen to sign her messages as "Frank," on the theory that this might allow her to avoid anti-female discrimination. Indeed, either sex can masquerade as the other; children as adults (and vice-versa). If nothing else, this creates some potential for embarrassment, and concerns some parents.[77]

Like fully anonymous messages, pseudonymous messages come in two varieties: traceable and untraceable. The advantage of traceable pseudonymity is that it gives the sender a consistent name that allows other parties to send replies far more easily than is possible with any untraceable system.

a. Traceable pseudonymity

Traceable pseudonymity is communication with a *nom de plume* attached which can be traced back to the author (by someone), although not necessarily by the recipient. While a traceable pseudonymous system makes it much easier for someone to discover Alice's identity, it usually offers one large compensating advantage: the recipients of Alice's message can usually reply to it by sending e-mail directly to the pseudonymous e-mail address in the "From:" field of the message. The message will then either go to Ted, the remailer operator, who keeps an index of the addresses that link Andrea to Alice, or in the case of commercial service providers who allow subscribers to use pseudonymous IDs, directly to Alice's account.

Anon.penet.fi, probably the best-known "anonymous" remailer, is in fact merely a very user-friendly traceable pseudonymous remailer:

---

76. Not being a political dissident, I confess that I have never used more than a single remailer myself (primarily in order to post to public newsgroups without fear of getting requests for free legal advice), and have never bothered to encrypt any of my e-mail messages; I created my own PGP key, *available online URL* http://www.law.miami.edu/~froomkin/mykey.htm, purely for demonstration purposes.

77. *See supra* note 43 (discussing the importance of identity in contemporary society).

> [Anon.penet.fi] provides a front for sending mail messages and posting news items anonymously. As you send your very first message to the server, it automatically allocates you an id of the form *anNNN*, and sends you a message containing the allocated id. This id is used in all your subsequent anon posts/mails. Any mail messages sent to your-id@anon.penet.fi gets redirected to your original, real address. Any reply is of course anonymized in the same way, so the server provides a double-blind. You will not know the true identity of any user, unless she chooses to reveal her identity explicitly.[78]

The anon.penet.fi system keeps a record of each user's e-mail address. The security of the approximately 8,000 messages that pass through anon.penet.fi daily[79] thus depends critically on the willingness of the operator, Johan Helsingius, a Finnish computer scientist, to refuse to disclose the contents of his index which maps each pseudonymous ID to an e-mail address. In February 1995, the Church of Scientology successfully enlisted the aid of the Finnish police, via Interpol, to demand the identity of a person who had, the Church of Scientology claimed, used anon.penet.fi to post the contents of a file allegedly stolen from a Scientology computer to a USENET group called "alt.religion.scientology." In compliance with Finnish law, Helsingius surrendered the information, believing that the only alternative would have been to have the entire database seized by the police.[80]

The social institution of traceable pseudonymity, which is permitted by a number of commercial Internet providers, is likely to generate some interesting lawsuits. Many commercial ISPs and on-line service providers, such as America OnLine for example, allow users to use any unique name they like as their "user ID," their on-line identifier. When my brother opened an account with an ISP, he used our family name for his account. As a result, when my parents set up an Internet account with the same service provider they were forced to select something different. Their ID is an amalgam of their first names. They could, however, have chosen any combination of letters and numbers

78. The anon.penet.fi help file is *available online URL* http://chaos.taylored.com:1000/0Z/Anonymous-Mail/Remailers/Instructions/Help-file-from-anon.penet.fi.gz.

79. Douglas Lavin, *Finnish Internet Fan Runs Service Allowing Anonymous Transmissions*, WALL ST. J., July 17, 1995, at A7 (reporting 8,000/day figure).

80. *See available online URL* http://www.cybercom.net/~rnewman/scientology/home.html#PENET (describing incident). Differing descriptions of the Scientologists' legal efforts can be found at The Church of Scientology vs. the Net, *available online URL* http://www.cybercom.net/~rnewman/scientology/home.html (critical view); UK Scientology Critics, *available online URL* http://mail.bris.ac.uk/~plmlp/scum.html (even more hostile); Church of Scientology International, *available online URL* http://www.theta.com/goodman/csi.htm (Scientologists' view).

they wanted so long as their ISP had not already assigned that name to someone else. Whether the ISP will release my parents' actual name to anyone who asks is primarily a question of contract law until a subpoena is involved. When people think they have been defamed or otherwise injured by the actions of a user who employs a pseudonym, the party claiming injury is likely to ask courts to require the ISPs to disclose the identity of the subscriber, at least when the ISP is in an accessible jurisdiction.

b. Untraceable pseudonymity

Untraceable pseudonymity works just like untraceable anonymity, except that Alice chooses to sign her message as Andrea, a pseudonym. If Alice is worried that someone else may try to masquerade as Andrea, she can sign her message with a digital signature[81] generated specially for "Andrea," which will uniquely and unforgeably distinguish an authentic signed message from any counterfeit. By participating in discussions under a consistent pseudonym (often abbreviated to "nym" on the Internet) Alice can establish Andrea as a digital persona:

> [N]yms allow for continuity of identity to be maintained over a period of time. A person posting under a nym can develop an image and a reputation just like any other online personality. Most people we interact with online are just a name and an e-mail address, plus whatever impression we have formed of them by what they say. The same thing can be true of nyms. Cryptography can also help maintain the continuity of the nym, by allowing the user to digitally sign messages under the name of the nym. The digital signature cannot be forged, nor can it be linked to the True Name of the user. But it makes sure that nobody can send a message pretending to be another person's nym.[82]

Strictly speaking, a digital persona does not require untraceable anonymity: it is sufficient to have a system that allows one to communicate under a "nym" and to digitally sign one's messages in order to prevent

---

81. Public-key systems allow users to append a digital signature to an unencrypted message. A digital signature uniquely identifies the sender and connects the sender to the message. Because the signature uses the plaintext as an input to the encryption algorithm, if the message is altered in even the slightest way, the signature will not decrypt properly, showing that the message was altered in transit or that the signature was forged by copying it from a different message. A properly implemented digital signature copied from one message has only an infinitesimal chance of successfully authenticating any other message. *See* SCHNEIER, *supra* note 74, at 35.

82. Comments of computer security consultant Hal Finney, *available online URL* http://chaos.taylored.com: 1000/0Z/Anonymous-Mail/Issues/Background-Information.gz.

anyone else from masquerading as the nym.[83] "Publius," the author of the *Federalist Papers*, was known to "his" publisher, and a digital persona can exist even if the persona's ISP knows the persona's real identity. Nevertheless, a nym may have more value, or at least may be experienced as more liberating, if the identity of the person(s) behind the persona is untraceable.[84]

3. *The Human Element: Remailer Operators*

While the technological alternatives described above have their own interest, the most important point for present purposes is that very effective Internet anonymity requires only two things: cryptographic tools, and willing remailer operators. The cryptographic tools are in ready supply.[85] If the user deploys the cryptographic tools properly, the remailer operators need not be known to be trustworthy; since the message is untraceably anonymous if any single operator in a chain is honest, it will ordinarily suffice to route the message through several remailers. The more remailers in the chain, however, the longer it may take the message to get to its destination,[86] and the greater the chance that an operator in the chain will fail to pass the message on down the line.[87]

The supply of remailer operators is the major potential constraint on Internet anonymity.[88] Remailer programs are currently operated by a relatively small number of volunteers located in a few countries; at present they receive no compensation for this service, and in the absence of anonymous electronic cash or the equivalent[89] it is difficult to see how an electronic payment system could be constructed that would

83. So long as the private key in a key pair is not shared with anyone, a digital signature uniquely identifies the author of a document. For a short description of digital signatures, see Froomkin, *supra* note 6, at 895.

84. "The citizen who is truly free in forming her identity should have the opportunity to experiment with roles she does not wish to adopt in public." Seth F. Kreimer, *Sunlight, Secrets, and Scarlet Letters: The Tension Between Privacy and Disclosure in Constitutional Law*, 140 U. PA. L. REV. 1, 69 (1991) (citing Foucault and Goffman). For a suggestion that nyms be granted the legal right to own and borrow money, to transact, and to communicate, see Karnow, *supra* note 41, at 12-13.

85. *See supra* note 66.

86. *See supra* note 73 (discussing concept of "latency").

87. This risk is reduced by the provision of a "remailer pinging service" that regularly checks to see if remailers are forwarding their mail. *See supra* note 65.

88. In addition, remailers do not defend against traditional methods of acquiring information. Encryption may foil a wiretap on the sender's telephone line, but the use of a remailer to send plaintext will not do so, since the message is captured at the source.

89. See *infra* Part III.

not risk undermining the very anonymity the remailers are designed to protect.

The remailer operator's problem is a simple one. No remailer operator can control the content of the messages that flow through the remailer. Furthermore, the last remailer operator in a chain has no reliable way of concealing the identity of the sending machine from the message's ultimate recipient. Suppose, to return to the example above,[90] Alice wants to send an anonymous death threat to Bob via remailers operated by Ted, Ursula, and Victor. If Victor does nothing to mask his e-mail address, Bob will know he was the last to remail the message. Victor can make any attempt to identify him more difficult by forging his e-mail address in the message to Bob, but Victor cannot be certain that this will work. Indeed, he can be almost certain that over time it will fail.[91]

The last remailer in a chain thus risks being identified by an unhappy recipient. An identifiable person is a potential target for regulation. If the remailer operators were made strictly liable for the content of messages that passed through their hands, even though they were unable to learn the content of those encrypted messages, most reasonable people probably would find running a remailer to be an unacceptable risk if they resided in a jurisdiction capable of enforcing such a rule.

Remailer operators already have come under various forms of attack, most recently lawsuits or subpoenas instigated by officials of the Church of Scientology who sought to identify the person they allege

90. *See supra* text following note 75.

91. To understand why this is so requires some background in how an ordinary e-mail message is transmitted from Alice's machine to Bob's via the Internet. Ordinarily the two computers do not communicate directly. Instead Alice's machine sends the message to a machine that it hopes is in Bob's general direction, and the message passes from machine to machine until it finds one that is in regular communication with Bob's. Each machine that handles the message appends "path" information to the e-mail that identifies it as having taken part in the communication. The final recipient receives the entire path data along with the text of the message, but most commercial e-mail packages are designed to avoid displaying this path information to the reader unless she asks for it.

Victor can instruct his computer to lie about its identity, and indeed can forge information suggesting that the message originated elsewhere far away, but he has no way to persuade the machine to which he sends the message to cooperate. As a result, it is possible for a sufficiently motivated Internet detective to identify the first machine to which Victor sent the message, especially if she has several messages to work with. *See* Spam FAQ or "Figuring out Fake E-Mail and Posts," *available online URL* http://digital.net/~gandalf/spamfaq.html. If the machine that communicated with Victor keeps records of its e-mail handling, or if its operator can be persuaded to do start doing so, the Internet detective can identify Victor's machine, and perhaps even Victor, as the source of the remailed message.

used remailers to disseminate copyrighted and secret Church teachings.[92] As a result, operating a remailer is not a risk-free activity today. Indeed, one can imagine a number of creative lawsuits that might reasonably be launched at the operator of a remailer. Examples include a new tort of concealment of identity, a claim of conspiracy with the wrong-doer, and a RICO claim. A remailer operator whose remailer was used to harass someone might face a common law tort claim of harassment. A conspiracy charge would be difficult since it would difficult the prove the element of agreement that is a necessary part of a conspiracy. It is difficult to say that Bob conspires with a stranger, even if he leaves a tool lying in plain sight, knowing that criminals are likely but not certain to come by and use it. If Bob is really ignorant of the identity, content, and purposes of the messages he retransmits, he can plausibly say that there is no agreement between him and the conspirator, and that he should no more be liable for the misuse of his remailer than the rental car company that leases a car to a terrorist. A RICO claim against a remailer could also founder on the lack of agreement.[93] Although it is far from obvious that any of these legal theories would or should succeed, some raise non-frivolous issues and thus would be expensive to defend.

At some point, if the number of remailers becomes small, it becomes technically (if not necessarily politically or legally) feasible for

92. *See supra* note 80.

93. The circuits conflict as to whether a defendant must agree to "personally commit" the predicate acts in a RICO conspiracy but none of the circuits have done away with the need for some sort of agreement between the parties to the conspiracy. The Third, Fourth, Fifth, Sixth, Ninth, and Eleventh Circuits hold that the defendant's agreement to personally commit RICO predicate acts is not required. *See* United States v. Carter, 721 F.2d 1514, 1529 (11th Cir.), *cert. denied sub nom.* Morris v. United States, 469 U.S. 819 (1984); United States v. Adams, 759 F.2d 1099, 1116 (3d Cir.), *cert. denied*, 474 U.S. 971 (1985); United States v. Pryba, 900 F.2d 748, 760 (4th Cir.), *cert. denied*, 498 U.S. 924 (1990); United States v. Elliot, 571 F.2d 880, 902 (5th Cir), *cert. denied, sub nom.* Hawkins v. United States, 439 U.S. 953 (1978); United States v. Joseph, 781 F.2d 549, 554 (6th Cir. 1986), *appeal after remand*, 835 F.2d 1149 (6th Cir. 1987); United States v. Neapolitan, 791 F.2d 489, 494 (7th Cir.), *cert. denied*, 479 U.S. 940 (1986); United States v. Kragness, 830 F.2d 842, 860 (8th Cir. 1987); United States v. Tille, 729 F.2d 615, 619 (9th Cir.), *cert. denied*, 469 U.S. 848 (1984). According to these circuits, the government need only prove that the defendant directly or indirectly conspired to conduct RICO activity. The First, Second, and Tenth Circuits require the government to prove that the defendant agreed to "personally commit" two or more predicate acts in a RICO conspiracy. *See* United States v. Winter, 663 F.2d 1120, 1136 (1st Cir. 1981), *cert. denied*, 460 U.S. 1011 (1983); United States v. Ruggiero, 726 F.2d 913, 921 (2d Cir.), *cert. denied sub nom.* Rabito v. United States, 469 U.S. 831 (1984); United States v. Killip, 819 F.2d 1542, 1548 (10th Cir.), *cert. denied*, 484 U.S. 987 (1987).

the authorities to conduct traffic analysis[94] on all the remailers and make deductions about who sent what to whom. In the absence of a compensation mechanism, or a jurisdiction capable of offering a safe haven for remailers, the cornerstone of Internet anonymity currently relies entirely on the kindness of strangers.

B. Constitutional Constraints on Regulation of Anonymous Electronic Communication

The ease with which anonymous electronic communication lends itself to unaccountable libel, conspiracy, and other harms has led to some calls for regulation;[95] as use of the Internet grows and more users learn about cryptography and remailers, one can reasonably expect calls for regulation to increase. It seems reasonable to ask if such regulations would be constitutional.

The United States Constitution does not guarantee a right to be anonymous in so many words. The First Amendment's guarantees of free speech and freedom of assembly have, however, been understood for many years to provide protections for at least some, and possibly a great deal of, anonymous speech and secret association. As already noted, the *Federalist Papers* were written pseudonymously.[96] In 1958, the Supreme Court upheld the right of members of the NAACP to refuse to disclose their membership lists to a racist and surely vengeful state government,[97] a decision that I imagine almost every lawyer in the US would endorse today—at least on its facts. Simultaneously, however, the United States has nurtured a deep-seated fear of conspirators and conspiracy,[98] with the McCarthyite witch-hunts of the 1950's being only one of the more lurid examples.

Doctrinal discussions of permissible restrictions on the freedom of speech commonly divide the discussion into "political" and "non-political" speech, and the sketch which follows adopts this convention. The

94. Traffic analysis is the study of the sources and recipients of messages, including messages that the eavesdropper cannot understand. *See* Froomkin, *supra* note 6, at 747.

95. *See supra* note 2.

96. Pseudonymity differs from anonymity in a number of ways. Perhaps the most important difference is that pseudonymity allows for the creation and continuity of a "nym"—an alternate identity. *See supra* text accompanying note 82. In the case of the Federalist Papers, "Publius" was in fact three collaborators. On the Internet, "John" may be Jane, or little Johnny.

97. NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449 (1958); for a forceful assertion of a moral right to associational or group privacy, see Edward J. Bloustein, *Group Privacy: The Right to Huddle*, 8 RUT.-CAM. L.J. 219 (1977).

98. I discuss the U.S. hypersensitivity to conspiracy in Froomkin, *supra* note 6, at 850-62.

division into two categories tends, however, to obscure alternate and perhaps more valid ways of describing the extent of the government's power to impose restrictions on speech. In particular, the standard doctrinal approach tends to reify a debatable distinction between purportedly high value and lower value speech. The categories "political" and "non-political" themselves may be overlapping and ultimately unhelpful. For example, outrageous, even obscene, speech can be political.[99] And if the personal is indeed the political all categories collapse into one.

1. Anonymous Political Speech

Political speech receives the highest constitutional protection because it "occupies the core of the protection afforded by the First Amendment;"[100] other types of speech, notably "commercial speech," sometimes receive a reduced level of First Amendment protection. Core political speech need not center on a candidate for office, but can affect any matter of public interest—especially if it is an issue in an election.[101]

The Supreme Court has repeatedly noted the existence of a "profound national commitment to the principle that debate on public issues should be uninhibited, robust, and wide-open,"[102] which would presumably include protections for anonymous speech. Indeed, *McIntyre v. Ohio Elections Commission*, the Supreme Court's most recent opinion on the right to anonymous speech, states that "an author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment" and "the anonymity of an author is not ordinarily a sufficient reason to exclude her work product from the protections of the First Amendment."[103] Despite these ringing words, whether there is a right to be anonymous in the US remains unclear as a general matter, since difficult cases are precisely those in which exceptions are made to fit facts that sit uncomfortably within the rules that apply "ordinarily."[104]

---

99. *See, e.g.*, Hustler Magazine v. Falwell, 486 U.S. 46 (1988).

100. McIntyre v. Ohio Elections Comm'n, 115 S. Ct. 1511, 1518 (1995).

101. *See* First Nat. Bank of Boston v. Bellotti, 435 U.S. 765, 776-77 (1978).

102. New York Times Co. v. Sullivan, 376 U.S. 254, 270 (1964).

103. *McIntyre*, 115 S. Ct. at 1516.

104. For a contrary view that "*McIntyre* will prove to be dispositive" in providing First Amendment protections to anonymous political speech, see Richard K. Norton, Note, McIntyre v.

Broad prohibitions of anonymous political speech, such as ordinances prohibiting all anonymous leafletting, are an unconstitutional abridgment of free speech.[105] The Supreme Court has also tended to be highly solicitous of the need of dissidents and others to speak anonymously when they have a credible fear of retaliation for what they say. Thus, the Supreme Court has struck down several statutes requiring public disclosure of the names of members of dissident groups.[106] Nevertheless, the right to privacy in one's political associations and beliefs can be overcome by a compelling state interest. The state interest in forbidding discrimination in places of public accommodation has been held to be sufficiently compelling to meet this test, at least when the objectives and remedies were sufficiently narrowly tailored to achieve the result when examined with strict scrutiny.[107] In contrast, the recent *McIntyre* decision found that the state's "interest in preventing fraudulent and libelous statements and its interest in providing the electorate with relevant information" was insufficiently compelling to justify a ban on anonymous speech that was not narrowly tailored.[108]

Ohio Elections Comm'n: *Defining the Right to Engage in Anonymous Political Speech*, 74 N. CAL. L. REV. 553 (1996).

105. *McIntyre*,115 S. Ct. at 1521-24; Talley v. California, 362 U.S. 60 (1960).

106. *See, e.g.*, Brown v. Socialist Workers' 74 Campaign Comm., 459 U.S. 87, 91 (1982) (holding that the "Constitution protects against the compelled disclosure of political associations"); Hynes v. Mayor of Oradell, 425 U.S. 610, 623-28 (1976) (Brennan, J., concurring in part) (asserting that a disclosure requirement puts an impermissible burden on political expression); Shelton v. Tucker, 364 U.S. 479, 485-87 (1960) (holding invalid a statute that compelled teachers to disclose associational ties because it deprived them of their right of free association); Talley v. California, 362 U.S. 60, 64-65 (1960) (voiding an ordinance that compelled the public identification of group members engaged in the dissemination of ideas); Bates v. City of Little Rock, 361 U.S. 516, 522-24 (1960) (holding, on freedom of assembly grounds, that the NAACP did not have to disclose its membership lists); NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 462 (1958) ("It is hardly a novel perception that compelled disclosure of affiliation with groups engaged in advocacy may constitute . . . restraint on freedom of association . . . ."); Joint Anti-Fascist Refugee Comm. v. McGrath, 341 U.S. 123, 145 (1951) (Black, J., concurring) (expressing the fear that dominant groups might suppress unorthodox minorities if allowed to compel disclosure of associational ties). *But see* Communist Party of the United States v. Subversive Activities Control Bd., 367 U.S. 1, 85 (1961) (declining to decide whether forced disclosure of the identities of Communist Party members was an unconstitutional restraint on free association); New York *ex rel.* Bryant v. Zimmerman, 278 U.S. 63, 77 (1928) (holding that a required filing of group members' names with the state constituted a legitimate exercise of police power).

107. *See* Board of Directors of Rotary Int'l v. Rotary Club of Duarte, 481 U.S. 537, 544 (1987); *see also* New York State Club Ass'n v. City of New York, 487 U.S. 1, 13 (1988) (stating that freedom of expression is a powerful tool used in the exercise of First Amendment rights); Roberts v. United States Jaycees, 468 U.S. 609, 617-19 (1984) (recognizing that an individual's First Amendment rights are not secure unless those rights may be exercised in the group context as well).

108. 115 S. Ct. at 1519.

Not even political speech is immune from regulation. Despite its privileged position, political speech can be regulated given sufficient cause, especially if the regulation is content-neutral, as a regulation on anonymous speech would likely be. An example of sufficient cause is the state interest in ensuring compliance with campaign finance contribution limits. For example, in *Buckley v. Valeo*,[109] the Supreme Court upheld a statute forbidding donations of more than $1,000 to a candidate for federal office, and compelling disclosure to the Federal Election Commission of the names of those making virtually all cash donations.[110] Since the Court in the same decision essentially equated the expenditure of money in campaigns with the ability to amplify political speech,[111] the decision appears to say that given a sufficiently weighty objective, and a statute carefully written to minimize the chilling or otherwise harmful effects on speech, even political speech can be regulated.[112]

Similarly, in *First Nat. Bank of Boston v. Bellotti*,[113] the Supreme Court struck down a state requirement forbidding corporations from making political contributions except for ballot measures directly affecting its business, but it contrasted the unconstitutional state law with others that it suggested would surely be acceptable: "Identification of the source of advertising may be required as a means of disclosure, so that the people will be able to evaluate the arguments to which they are being subjected."[114] Indeed, the Communications Act requires licensed television and radio stations to identify the sponsors of paid political advertisements at the time the ad is broadcast.[115] Indeed, the licensee has a duty to "exercise reasonable diligence" in identifying the true sponsor of political advertisements.[116]

---

109. 424 U.S. 1 (1976).

110. *Id.* at 23-29, 60-84.

111. *Id.* at 19.

112. *Cf.* Los Angeles v. Taxpayers for Vincent, 466 U.S. 789 (1984) (upholding ban on posting any signs, including political ones, on utility poles). Justice Stevens held, however, that the utility poles were not public fora, *id.* suggesting that the court might not extend this idea to public fora and that *Vincent* may come to be seen as simply a decision upholding a particular time, place, and manner restriction.

113. 435 U.S. 765 (1978).

114. *Id.* at 792 n.32. The Supreme Court again noted the communicative importance of the identity of a speaker, albeit in a different context, in City of Ladue v. Gilleo, 114 S. Ct. 2038, 2046 (1994) (noting that a poster in front of a house associates speech with the identity of the speaker).

115. 47 U.S.C. § 317 (1995). *See also* 47 C.F. R. § 73.1212 (1995).

116. 47 U.S.C. § 317(c) (1995). The D.C. Circuit held that the FCC did not abuse its discretion by ruling that a licensee could satisfy this obligation in the face of undocumented accusations that the apparent sponsor was a front group for tobacco lobbyists by accepting an undocumented

The implications for the regulation of anonymity—even in the context of political speech—are obvious, and were not lost on the Supreme Court of California, which in *Griset v. Fair Political Practices Comm'n* recently upheld a state statute forbidding anonymous mass political mailings by political candidates.[117] The facts involved a political dirty trick: Griset had sent a mass mailing attacking his opponent and pseudonymously purporting to be from a neighborhood association. The court concluded that prospective voters could have been deceived into thinking that Griset had "grass roots" support.[118] The California court reasoned that this sort of deception was the evil that the statute was designed to cure, and that the ban was necessary to further the state's interest in "well-informed electorate" at election time and was "narrowly drawn to meet that goal."[119] The Court therefore distinguished *Griset* from federal Supreme Court decisions, such as *Talley, supra*, *Bates v. City of Little Rock*,[120] and *NAACP v. Alabama*,[121] which held that the First Amendment freedom of association limited the state's ability to pierce an organization's anonymity. One could perhaps read *Griset* as concerning the mis-use of pseudonymity rather than anonymity. The argument would be that there is a greater harm to the political process from a *false* statement of support by a nonexistent "citizen's group" than from an anonymous source, since the latter's secrecy puts readers on notice that the author could be anyone. While this approach is attractive, and probably constitutional, neither the opinion nor the statute makes a distinction between a false statement and one that fails to identify the author.

Quite possibly the Supreme Court would uphold a narrowly tailored statute prohibiting anonymity even in the context of political speech if the statute had clear and palatable objectives. This possibility seems all the more real when one considers the contexts in which the Supreme Court has already sustained limitations on the privacy of individuals engaged in the political process, particularly the *Buckley* deci-

---

assertion from the apparent sponsor that he was the real sponsor in the absence of documentary evidence to the contrary. Loveday v. FCC, 707 F.2d 1442 (D.C. Cir. 1983).

117. Griset v. Fair Political Practices Comm'n, 884 P.2d 116, 126 (Cal. 1994) (upholding CAL. GOV'T CODE § 84305 (West 1994)), *cert. denied*, 115 S. Ct. 1794 (1995)).

118. *Id.* at 125.

119. *Id.* at 123.

120. 361 U.S. 516 (1960).

121. 357 U.S. 449 (1958).

sion.[122] Indeed, the D.C. Circuit upheld the constitutionality of the Communications Act requirement that paid political radio and television broadcasts include the name of the sponsor, and the Court denied certiorari.[123]

Once down this slippery slope of regulation it is notoriously difficult to find a logical place to stop.[124] A particularly difficult case might be a statute that sought to ban all anonymity in political campaigns on the theory that if the message is not signed with the actual name of the author, it is impossible to know whether it originated in a political campaign, and thus constitutes actionable lies about an opponent, or potentially violates campaign finance expenditure limits. This would juxtapose the *Talley-McIntyre* line of cases with the *Buckley-Griset* line of cases. Without forcing everyone to sign their messages there may, it could be argued, be no way to monitor what campaigns spend, and thus no way to ensure they do not seek to get an edge by spending beyond the legal limits.

In the glow of *McIntyre*'s rhetoric about the importance of anonymity to the political and literary tradition, it is all too easy to think that anonymity in cyberspace would surely triumph. Yet there is reason to doubt, especially because in *McIntyre* Justice Stevens himself carefully distinguished earlier cases upholding statutes that sought to preserve the integrity of the voting process, e.g., *Burson v. Takushi*.[125] Additionally, statutes designed to attack the enforcement problems caused by anonymous libelous or electronic violations of intellectual property rights might be in a particularly good position to survive judicial review. As a constitutional matter, the issue is far from resolved.[126]

---

122. *See supra* note 109; *see also* Citizens Against Rent Control v. Berkeley, 454 U.S. 290, 298 (1991); *id.* at 299-303 (Blackmun, J., concurring); *id.* at 308-09 (White, J., dissenting). All Justices agreed that identification requirements in political campaigns could be appropriate.

123. Loveday v. FCC, 707 F.2d 1443 (1983) (upholding 47 U.S.C. § 227(d)(2) (1995) against constitutional challenge), *cert. denied*, 464 U.S. 1008 (1983). *Loveday* might be explained as relying on a special feature of radio and television such as shortage of spectrum, *cf. Turner Broadcasting*, 114 S. Ct. 2445 (1994), but the rule has been extended to cable television also. *See* 47 C.F.R. § 68.318(c)(3) (1995). For arguments in favor of such regulation, see generally Peter F. May, Note, *State Regulation of Political Broadcast Advertising: Stemming the Tide of Deceptive Negative Attacks*, 72 B.U. L. REV. 179 (1992).

124. My first year Torts teacher derided slippery slope arguments as "fear of doing the right thing today for fear of being forced to do the right thing tomorrow."

125. Burdick v. Takushi, 504 U.S. 428 (1992) (upholding law forbidding campaign-related speech within 100 feet of the entrance to polling place).

126. *Cf.* WORKING GROUP ON INTELLECTUAL PROPERTY RIGHTS, INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE (1995) [hereinafter WHITE PAPER ON COPYRIGHT] (proposing a new chapter of the Copyright Act that would prohibit "tampering" with "copy-

2. *Anonymous Non-political Speech*

As ringing a defense of the First Amendment as the *Talley* and *McIntyre* decisions may be, they involved political speech. At most, therefore, they merely suggest the outcome for cases involving anonymous speech that is *not* "political speech" and also not one of the areas of general public concern such as religion, art, or literature, that commentators usually include within the rubric of so-called "core" First Amendment speech.[127] It is also important to understand that the anonymity cases decided by the Supreme Court involved very broadly drafted statutes aimed at political speech, and that the Supreme Court has carefully left open the question whether a statute regulating (or prohibiting) anonymous speech would survive review if the statute were narrowly tailored, e.g., to "provid[e] a way to identify those responsible for fraud, false advertising and libel."[128]

Restrictions on anonymity are more likely to be sustained if they focus on types of non-political speech that have tended to receive the lowest protection. Although in *McIntyre* the Court found that the state's "interest in preventing fraudulent and libelous statements and its interest in providing the electorate with relevant information" was insufficiently compelling to justify a ban on anonymous speech, the weighing might produce a different result if there were some way to tailor it to types of speech that ordinarily receive less protection, such as commercial speech.[129]

Despite some scholarly suggestions that the First Amendment should apply with undiluted force,[130] "commercial speech" tends to be

---

right management information"). This proposal could include information relating to attribution as well as, e.g., devices that charge for access to the work.

127. *See, e.g.*, McIntyre v. Ohio Elections Comm'n, 115 S. Ct. 1511, 1518 (1995) (describing political speech as core speech for First Amendment purposes).

128. *See Talley*, 362 U.S. at 64; *see also McIntyre*, 115 S. Ct. at 1517.

129. If the government seeks to regulate commercial speech that is not false or misleading and concerns a lawful activity a reviewing court must determine whether the regulation promotes a substantial governmental interest, directly advances that interest, and is not more extensive than necessary. Central Hudson Gas & Elec. Corp. v. Public Serv. Comm'n, 447 U.S. 557 (1980). For a discussion of the limits to the *Central Hudson* test see generally *Commercial Speech*, 107 HARV. L. REV. 224 (1992); for criticism of the case, see David F. McGowan, Comment, *A Critical Analysis of Commercial Speech*, 78 CAL. L. REV. 359 (1990).

130. *See, e.g.*, Ronald Coase, *The Economics of the First Amendment: The Market for Goods and the Market for Ideas*, 64 AM. ECON. REV. 384 (1974); Burt Neuborne, *The First Amendment and Government Regulation of Capital Markets*, 55 BROOK. L. REV. 5 (1989); Alex Kozinski & Stuart Banner, *Who's Afraid Of Commercial Speech?*, 76 VA. L. REV. 627 (1990).

subject to greater regulation.[131] Restrictions are more likely to be upheld if they appear plausibly tailored to strike at illegal non-political non-speech "conduct"[132] particularly when the speech "incidentally" burdened is non-political. And restrictions are most likely to be upheld when the speech burdened falls into the ill-defined, and predominately salacious, category of speech that is for all practical purposes disfavored.

An example of the latter is the stringent anti-anonymity provisions that appear in the Child Protection and Obscenity Enforcement Act of 1988,[133] as amended by the Child Protection Restoration and Penalties Enhancement Act of 1990[134] (collectively, "the Act"). The workings of the Act are worth examining in some detail because the Act has been upheld by the D.C. Circuit,[135] and risks setting a precedent for future legislative attempts to restrict anonymous non-political speech. The Act attacks anonymity by requiring that producers of certain kinds of speech ascertain and record information about performers' identities (the "ascertainment requirement"), and that producers affix a notice disclosing their own identity and address (the "disclosure requirement").

The Act's ascertainment requirement is far-reaching. All producers of visual depictions of certain types of "actual sexually explicit conduct"[136] have a duty to "ascertain"[137] the legal name and age of every

131. *See* Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer Council, Inc., 425 U.S. 748, 771 n.24 (1976). The Court has also stated that the overbreadth doctrine is inapplicable in various commercial speech contexts. *See* Village of Schaumburg v. Citizens for a Better Env't, 444 U.S. 620, 638-39 (1980).

132. The lines between speech, expressive conduct, mere conduct, and hybrid forms of these things have generated much litigation and commentary. *See, e.g.*, LAURENCE H. TRIBE, AMERICAN CONSTITUTIONAL LAW 789, 930 (2d ed. 1988); United States v. O'Brien, 391 U.S. 367, 376 (1968) (rejecting First Amendment challenge to law prohibiting the destruction of draft cards); Cox v. Louisiana, 379 U.S. 559 (1965) (calling demonstration a form of "speech plus" entitled to less protection than pure speech).

133. Pub. L. No. 100-690, 102 Stat. 4181, 4485-4503 (1988).

134. Pub. L. No. 101-647, 104 Stat. 4789, 4816-17 (1990), *codified at* 18 U.S.C. § 2257(b)(1) (1995).

135. American Library Ass'n v. Reno, 33 F.3d 78 (D.C. Cir. 1994), *reh'g en banc denied*, 47 F.3d 1215 (D.C. Cir. 1995), *cert. denied*, 115 S. Ct. 2610 (1995).

136. "Actual sexually explicit conduct," 18 U.S.C. § 2557(a)(1) (1995), is defined by reference to 18 U.S.C. § 2256, which defines "sexually explicit conduct" as any visual depiction of sexual intercourse, bestiality, masturbation or sadistic or masochistic abuse. *Id.* at § 2256(2)(A)-(D) (1995).

137. The implementing regulations provide that "secondary" producers, (e.g., a magazine editor and publisher) may discharge this duty by accepting copies of a "primary" producer's records. 28 C.F.R. § 75.2(1)(b) (1995). The regulations define primary producers as "any person who actually

performer so depicted by examining the performer's photographic[138] "identification document."[139] The Act defines "producer" broadly to include everyone "from photographers to printers to page layout artists."[140] It includes all those involved in the production process of "any book, magazine, periodical, film, video tape or other similar matter" and all those involved in their creation, duplication, reproduction, or reissuance after November 1, 1990.[141] However, the definition of "producer" excludes "mere distribution or any other activity which does not involve hiring, contracting for managing, or otherwise arranging for the participation of the performers depicted."[142] (Whether, given this limitation, the Act applies to a person who posts "visual depictions" made after November 1, 1990 of "actual sexually explicit conduct" to a World Wide Web site is an interesting question, one that may turn on whether the act of posting a picture or movie on the Web is exempt "distributing" or covered "duplication, reproduction, or reissuance.")

In addition to ascertaining the performer's real name and age, the producer must also ascertain all aliases "ever used" by the performer including "maiden name, alias, nickname, stage, or professional name," and maintain records of all affected performers cross-indexed by their aliases.[143] A producer who knowingly fails to maintain these records, or knowingly includes inaccurate information, can be punished by a fine and up to two years imprisonment; second and subsequent offenses can result in up to five years imprisonment.[144]

Although the Act does not create penalties for performers who mislead an unwitting producer,[145] one practical effect of the ascertainment requirement is to make it difficult, perhaps impossible, for ef-

films, videotapes, or photographs a visual depiction of actual sexually explicit conduct." 28 C.F.R. § 75.1(c)(2) (1995).

138. The requirement of a photo ID appears only in the Attorney General's implementing regulations, 28 C.F.R. § 75.2(a)(1) (1995), issued pursuant to 28 U.S.C. § 2257(g) (1995).

139. 18 U.S.C. § 2257(b)(1) (1995).

140. American Library Assoc. v. Reno, 47 F.3d 1215, 1217 (D.C. Cir. 1995) (Tatel, J., dissenting from denial of suggestion for rehearing in banc).

141. 18 U.S.C. § 2257(h)(3) (1995).

142. *Id.*

143. 18 U.S.C. § 2257(b)(2)-(3) (1995).

144. 18 U.S.C. § 2257(i) (1995). *Cf.* WHITE PAPER ON COPYRIGHT, *supra* note 126, at 235-36 (relating to regulation of "copyright management information").

145. "This requirement is satisfied if the producer asks the performer for the information." H.R. Doc. No. 100-129, 100th Cong., 1st Sess. 65 (1987) (President's message transmitting 1988 act to Congress); 33 F.3d at 92 (relying on this limiting construction). Presumably, however, a performer who showed obviously phony ID that was accepted as genuine by a producer who knew it was false would face some risk of a conspiracy charge.

fected performers to perform anonymously. The District Court accepted that the Act "is overly burdensome because it will invade the privacy of adult models and discourage them from engaging in protected expression. . . . Many of the artists and adult models engaged in sexually explicit visual imagery have an interest in maintaining their anonymity. Exposure of their true names, aliases, and addresses could subject them to stigmatization, harassment and ridicule from others."[146] On appeal, however, the D.C. Circuit dismissed this argument on the grounds that producer's records are disclosed only to the Attorney General or her delegate, and to producers and publishers further along the chain of production. Judge Buckley asserted, without apparent support in the record, that "we may safely assume that the performers are not concerned over the prospect of being stigmatized, harassed, or ridiculed by the producers they help enrich."[147]

Another practical effect of the Act's ascertainment requirement is to make it impossible for (re)producers to use affected images unless the (re)producer is in direct contact with a producer earlier in the chain of production who had direct contact with the performer, because producers later in the chain of production can discharge their record-keeping obligation only by contact with the performer or with a "primary" producer who was in direct contact with the performer.[148] As a result, it is now potentially a criminal violation to use affected images

146. *See* American Library Ass'n v. Barr, 794 F. Supp. 412, 419 (D.D.C. 1992), *rev'd sub nom.* American Library Ass'n v. Reno, 33 F.3d 78 (D.C. Cir. 1994).

147. *American Library Ass'n*, 33 F.3d at 94. Given that there have been suggestions that some actors are forced to perform at gunpoint, it seems fair to wonder if Judge Buckley's assertion is as self-evident as he thought it was. *See, e.g.*, LINDA LOVELACE & MICHAEL MCGRADY, ORDEAL (1980); *see also* Laura Lederer, *Then and Now: An Interview with a Former Pornography Model*, *in* TAKE BACK THE NIGHT: WOMEN ON PORNOGRAPHY 57 (Laura Lederer ed., 1980) (describing rape and other threats from producers); Robin L. West, *The Feminist-Conservative Anti-Pornography Alliance and the 1986 Attorney General's Commission on Pornography Report*, 1987 AM. B. FOUND. RES. J. 681, 686-88 (summarizing testimony to Meese Commission on Pornography challenging assertion that pornography is "consensually produced by voluntary participants in a voluntary market").

Performers acting for hire who fear their employers may be able to work under a pseudonym; nothing in the social security regulations, for example, appears to prohibit this. *Cf.* 60 Fed. Reg. 42,431 (1995) (amending 20 C.F.R. § 422.120 to state that agency will attempt to contact worker before contacting employer in cases where employees name in wage report differs from name in Social Security records, but that IRS will assess penalty only if social security number is absent or invalid). In such cases the requirement that they give their real name may add to their risks. The effect on a hypothetical unpaid performer engaged in social commentary is, perhaps, even greater.

148. 28 C.F.R. § 75.2(b) (1995).

when the model is unknown or anonymous, regardless of the model's age.[149]

The Act's second attack on anonymity is its disclosure requirement. Affected producers must affix to "every copy" of the covered materials a statement identifying the producer's business premises or other location where the producer can be found, and must maintain the ascertained records at that location.[150] It is a felony for the producer to fail to affix this information, and a felony for any person, whether or not they are a producer, to sell, give, or offer to sell or give[151] any visual depictions of the relevant "actual sexually explicit conduct" which does not have an affixed statement describing where the required records may be located.[152]

Under the Act, therefore, neither performers nor primary producers of affected materials can be anonymous. The D.C. Circuit held that the Act is nonetheless consistent with the First Amendment because it imposes content-neutral burdens on speech, and those burdens are designed to achieve a significant legislative goal.[153] Writing for the panel majority, Judge Buckley suggested that the record-keeping re-

149. This result as applied to obviously adult performers is particularly anomalous given that the purpose of the Act is to combat child pornography. *See American Library Ass'n*, 794 F. Supp. at 417-18 (noting anomaly). The D.C. Circuit alluded to this issue in a discussion of the problems the Act creates for "appropriationist artists," that is, "photographers who create distinct works that incorporate photographs taken by others—typically without permission." *American Library Ass'n*, 33 F.3d at 93. Although the court suggested that "application of the Act to [appropriationist artists] would raise a serious First Amendment problem because of the difficulty they may encounter in securing the information" that the Act requires them to keep on file, it concluded that the record was inadequate to present the issue in "clean-cut and concrete form." *Id.* In contrast, the D.C. Circuit gave short shrift to the District Court's suggestion that the Act "will effectively ban foreign produced images of sexually explicit conduct," even when the performers are adults. 794 F. Supp. at 418. "Foreign producers who wish to peddle their products in the United States should be expected to abide by our laws," the court stated, warning that to rule otherwise would create "a loophole" for domestic child pornographers to send their wares abroad for re-export to the United States. 33 F.3d at 93. By defining the problem as one of "foreign producers trying to peddle their products" rather than one of domestic parties seeking to purchase and re-use, re-package or re-distribute products that can plausibly be defined as speech, the court evaded a constitutional problem posed by the Act.

150. 18 U.S.C. § 2257(c) (1995); 28 C.F.R. § 75.5 (1995).

151. 18 U.S.C. § 2257(f)(4) (1995) (making it an offence "knowingly to sell or otherwise transfer, or offer for sale or transfer" any "book, magazine, periodical, film, video, or other matter, produce[d] in whole or in part with materials which have been mailed or shipped in interstate or foreign commerce or which is intended for shipment in interstate or foreign commerce" but lacking the affixed information about the location of the records).

152. A person selling or giving covered materials has a duty to ensure that the statement has been affixed to the materials, but no duty to determine the accuracy of the contents of the statement or the records required to be kept. 18 U.S.C. § 2257(f)(4) (1995).

153. American Library Ass'n v. Reno, 33 F.3d 78, 81, 84-85. The District Court had found the Act unconstitutional, see American Library Ass'n v. Barr, 794 F. Supp. 412, 418 (D.D.C. 1992).

quirement was no more a content-based burden on speech than were the zoning ordinances restricting the location of "adult" theaters that the Supreme Court upheld in *City of Renton v. Playtime Theaters*.[154] In *Renton* the Supreme Court stated that intermediate scrutiny sufficed when a statute burdens speech because of its subject matter rather than its viewpoint. As a result of *Renton*, "an otherwise content-based restriction on speech can be recast as 'content neutral' if the restriction 'aims' at 'secondary effects' of the speech."[155] The distinction between viewpoint and content neutrality is extremely significant, because the Supreme Court has repeatedly held that "viewpoint neutrality" (in which all speakers on a given subject are discriminated against equally) does not equal content-neutrality,[156] and only content-neutrality is entitled to be judged by the more lenient standard of "intermediate scrutiny" rather than the most exacting standard, strict scrutiny.

Judge Buckley used *Renton* in *ALA v. Reno* to suggest that the Child Protection Act was content-neutral because it aimed at one of the secondary effects of visual depictions of actual sexually explicit conduct (i.e., child pornography) rather than the speech itself.[157] Buckley argued that the Act was no less content-neutral than the zoning restrictions on adult theaters upheld in *Renton*. If subjecting theaters to more stringent zoning because they show blue movies was not a case of viewpoint neutrality deserving strict scrutiny but only a case of content-neutrality deserving intermediate scrutiny,[158] why, Buckley essentially asked, should the Act be any different? The panel majority further relied on the Supreme Court's earlier statement that when speech and non-speech elements are combined in a single course of conduct, "a sufficiently important government interest in regulating the nonspeech element can justify incidental limitations on First Amendment freedoms."[159]

---

154. 33 F.3d at 85 (citing City of Renton v. Playtime Theaters, 475 U.S. 41 (1986)).

155. Boos v. Barry, 485 U.S. 312, 334 (1988) (Brennan, J., concurring in part and concurring in judgment).

156. Burson v. Freemen, 112 S. Ct. 1846, 1850 (1992); *Boos*, 485 U.S. at 319; Arkansas Writers' Project, Inc. v. Ragland, 481 U.S. 221, 230 (1987); Heffron v. Int'l Soc. for Krishna Consciousness, 452 U.S. 640, 648 (regulation "may not be based upon either the content or subject matter of speech"); Consolidated Edison Co. v. Public Serv. Comm'n, 447 U.S. 530, 537-38 (1980); Carey v. Brown, 447 U.S. 455, 462 n.6 (1980).

157. 33 F.3d at 85 (citing *Renton* and *Boos*).

158. *Renton*, 475 U.S. at 46-48.

159. United States v. O'Brien, 391 U.S. 367, 376 (1968) (rejecting First Amendment challenge to law prohibiting the destruction of draft cards).

Having found that the Act was a content-neutral regulation that had only an incidental effect on First Amendment rights, Judge Buckley applied intermediate scrutiny and concluded that the Act was constitutional because it furthered the compelling governmental interest of combating child pornography.[160] The dissent countered that the statute was overbroad and would in any case have at most a negligible effect on child pornography because underage actors would get phoney IDs, and because the Act in its own terms[161] precludes the use of the producers' records directly or indirectly in a child pornography prosecution,[162] a limitation presumably designed to address Fifth Amendment concerns.[163] The Supreme Court denied certiorari.[164]

The D.C. Circuit's ruling in *American Library Ass'n* is significant because it permits an anonymity ban to extend to non-commercial, non-political speech on the grounds that the regulation seeks to combat a social harm and only incidentally burdens speech.[165] In theory, if the

160. *American Library Ass'n*, 33 F.3d at 84-85. *Cf.* New York v. Ferber, 458 U.S. 747 (1982) (noting compelling governmental interest in eradicating evils associated with child pornography).

161. 18 U.S.C. § 2257(d) (1993).

162. *American Library Ass'n*, 33 F.3d at 94-95 (Reynolds, J., dissenting). In his later dissent from the denial of rehearing en banc, Judge Tatel, who was not a member of the original panel, argued that,

> The only class of producers whose behavior this statute is likely to influence—those who ignore the age of their models but would nonetheless refuse to employ individuals they knew were minors—could be equally deterred, with no corresponding regulatory burden on protected speech, by rewriting the child pornography statutes to impose criminal liability upon those who recklessly or negligently violate them. . . . While such an approach might allow a few individuals to escape liability by establishing that they had made a reasonable mistake about the age of the model, "even as compelling a societal interest as the protection of minors must occasionally yield to specific constitutional guarantees." United States v. U.S. District Court, 858 F.2d 534, 543 (9th Cir. 1988).

American Library Ass'n v. Reno, 47 F.3d 1215, 1216-17 (D.C. Cir. 1995) (Tatel, J., dissenting from denial of suggestion for rehearing en banc).

163. *See American Library Ass'n*, 713 F. Supp. at 475. An earlier version of the record-keeping requirements of the Act was held to be unconstitutional in American Library Ass'n v. Thornburg, 713 F. Supp 469 (D.C. Cir. 1989), *vacated as moot sub nom.* American Library Ass'n v. Barr, 956 F.2d 1178, 1186 (D.C. Cir. 1992).

164. 115 S. Ct. 2610 (1995).

165. Bans on anonymous publication are not unprecedented. England banned anonymous pamphlets between 1637 and 1694, when licensing laws required that all books bear the name of the author and printer. W.S. Holdsworth, *Press Control and Copyright in the 16th and 17th Centuries*, 29 YALE L.J. 841, 848-49 (1920).

As detailed in *Anonymous Note*, *supra* note 9, at 1084-93 (giving examples from English, French and U.S. practice), a number of state and federal statutes have sought to restrict anonymous speech or the freedom of anonymous association. The Supreme Court has upheld restrictions on anonymous speech and association on several occasions. In Lewis Publishing Co. v. Morgan, 229 U.S. 288 (1913), the Court upheld a requirement that mailers wishing second class mailing status publish a list of editors and proprietors twice annually, but relied on a "now-outdated view of the

government's interest in combatting the effects of child pornography is sufficient to justify the Act's effects on adult performers and those who produce materials containing their visual images, it might be equally constitutional to require that at least non-political messages on the Internet include information sufficient to allow a libel victim to trace the source of the defamation.[166] Nor is it difficult to imagine how one might make similar arguments to defend the prohibition on anonymous faxes that Congress passed in 1991 in order to protect consumers from junk faxes.[167]

The Supreme Court has yet to go so far. The District Court in *ALA v. Reno* found it easy to distinguish the Act from the facts of *Renton*; Judge Buckley held that *Renton* controlled. If Judge Buckley was right, which is itself debatable,[168] the problem is *Renton*: as many

---

first amendment," *Anonymous Note, supra* note 9, at 1089. In Viereck v. United States, 318 U.S. 236 (1943), the Supreme Court upheld a pre-WW I statute requiring foreign agents to register with the Secretary of States, but several subsequent decisions, culminating in NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449 (1958), suggested that the Supreme Court had turned away from the analysis in *Viereck*, *see Anonymous Note, supra* note 9, at 1093-1102.

In United States v. Harris, 347 U.S. 612, 625 (1954), the Supreme Court upheld the Federal Regulation of Lobbying Act, 2 U.S.C. § 267 (1994), which requires those engaged in lobbying to divulge their identities. More recently, lower courts have sustained similar private identification requirements in other regulatory settings involving the workplace, *see, e.g.*, Big Bear Super Market No. 3 v. I.N.S., 913 F.2d 754 (9th Cir. 1990) (upholding worker identification provisions of Immigration Control Act, 8 U.S.C.A. § 1324 against a void for vagueness challenge).

166. *See* 713 F. Supp. at 477 (giving similar examples as one reason to hold that Act was unconstitutional). *See supra* text accompanying note 115 (describing FCC requirement that broadcast paid political advertisements identify sponsor).

167. The Telephone Consumer Protection Act of 1991 (TCPA), Pub. L. No. 102-243, 105 Stat. 2394, *codified at* 47 U.S.C. § 227(d)(2) (1995), requires the FCC to make rules requiring that fax machines mark the name and telephone number of a business or individual sending the fax on the first page of every transmission. 47 C.F.R. § 68.318 (1995) makes it unlawful

> for any person within the United States to use a computer or other electronic device to send any message via a telephone facsimile unless such message clearly contains, in a margin at the top or bottom of each transmitted page or on the first page of the transmission, the date and time it is sent and an identification of the business, other entity, or individual sending the message and the telephone number of the sending machine or of such business, other entity, or individual. The telephone number provided may not be a 900 number or any other number for which charges exceed local or long distance transmission charges. Telephone facsimile machines manufactured on and after December 20, 1992 must clearly mark such identifying information on each transmitted message. Facsimile modem boards manufactured on and after December 13, 1995 must comply with the requirements of this section.

For arguments supporting such regulation, see Michael M. Parker, *Fax Pas: Stopping the Junk Fax Mail Bandwagon*, 71 ORE. L. REV. 457 (1992).

168. The primary reason why Judge Buckley's analysis is questionable is the one pointed to in the dissents: that as the Act itself barred the government from using the information in the records against anyone, there was little grounds to believe that the statute was capable of accomplishing its purported objective.

commentators have noted, *Renton*'s conclusion that distinctions aimed at controlling the "secondary effects" of speech are content-neutral and thus require only intermediate scrutiny is at best manipulable and at worst ridiculous.[169] Nevertheless, unless eroticized speech is a very special form of "low-value speech"[170] an attempt to control anonymous non-political speech might fall within the *Renton* rule, and thus withstand intermediate scrutiny if the measure were backed by a sufficiently weighty governmental purpose. In this context, Professor Tribe's suggestion that the Supreme Court "is beginning to construct a multilevel edifice with . . . categories of less-than-complete constitutional protection" for expression characterizable as "commercial speech . . . offensive speech . . . defamation and possibly the speech of public employees" seems particularly accurate—and ominous.[171]

Despite suggestions to the contrary, the Internet carries a high volume of non-eroticized, and indeed political, speech.[172] As a practical matter, therefore, it would be exceedingly difficult, and probably impossible, to craft a ban on anonymous speech on the Internet that dis-

169. *See, e.g.*, Boos v. Barry, 485 U.S. 312, 334-36 (1988) (Brennan, J., concurring); TRIBE, *supra* note 132, at § 12-3 n.17 (Renton "ill-advised . . . . Carried to its logical conclusion, the doctrine could gravely erode first amendment protections."); Geoffrey R. Stone, *Content-Neutral Restrictions*, 54 U. CHI. L. REV. 46, 115 (1987) (calling decision a "disturbing, incoherent, and unsettling precedent"). Keith Werhan, *The Liberalization of Freedom of Speech on a Conservative Court*, 80 IOWA L. REV. 51, 68 (1994) ("A content-neutral reading of the Renton ordinance is hard to justify. Literally, the ordinance was content-based."). *The Supreme Court, 1985 Term*, 100 HARV. L. REV. 1, 195 (1986) ("The Renton ordinance was content-based regulation of the first order."). *But see* Cass R. Sunstein, *Pornography and the First Amendment*, 1986 DUKE L.J. 589, 612-17 (1986) (defending use of *Renton* analysis in First Amendment/pornography cases).

170. *See* Sunstein, *supra* note 169, at 602-08 (arguing that pornography is low-value speech and hence entitled to diminished First Amendment protection); *see also* TRIBE, *supra* note 132, at 930 (listing near-obscene speech as one of five special types of speech receiving a lower level of First Amendment protection). For a suggestion that the problem with eroticized speech is that judges and legislators dislike it, see Gianni P. Servodidio, *The Devaluation of Nonobscene Eroticism as a Form of Expression Protected by the First Amendment*, 67 TUL. L. REV. 1231 (1993); *see also* David Cole, *Playing By Pornography's Rules: The Regulation of Sexual Expression*, 143 U. PA. L. REV. 111 (1994).

171. TRIBE, *supra* note 132, at 930.

172. *Compare* Martin Rimm, *Marketing Pornography on the Information Superhighway*, 83 GEO. L.J. 1849 (1995) *with* Donna L. Hoffman & Thomas P. Novak, *A Detailed Analysis of the Conceptual, Logical, and Methodological Flaws in the Article: "Marketing Pornography on the Information Superhighway"* July 2, 1995 (version 1.01), *available online* URL http://www2000.ogsm.vanderbilt.edu/rimm.cgi; Jim Thomas, *Some Thoughts on Carnegie Mellon's Committee of Investigation, available online URL* http://sun.soci.niu.edu/~cudigest/rimm/rimm2 (discussion of ethical lapses in Rimm study); Jim Thomas, *The Ethics of Carnegie Mellon's Cyber-porn Study, available online URL* http://sun.soci.niu.edu/~cudigest/rimm/ethics.cmu; The Cyberporn Report, *available online URL* http://www.cybernothing.org/cno/reports/cyberporn.html (collecting URLs criticizing Rimm study); *see also supra* note 56.

tinguished between political and non-political speech and yet was enforceable. Since remailer operators will ordinarily be unable to decrypt the messages that they are forwarding, the operators themselves will be unable to tell whether the message is core First Amendment speech or unprotected obscenities.[173] A ban on anonymous speech cannot therefore meaningfully distinguish by subject matter, nor can it necessarily even distinguish between visual depictions and mere words.

Any meaningful attempt to ban anonymous Internet speech must therefore either attempt to ban it all, or craft some more limited rule that has the same result.[174] A straightforward banning of all anonymous speech is so far from being narrowly tailored to achieve the public purposes (preventing harmful messages from being forwarded or frustrating legitimate law enforcement attempts to trace threatening messages or the plans of conspiracies) that it does not seem likely to survive even cursory review. On the other hand, *Renton* might provide a model for achieving the same end in a different way. If, for example, remailer operators were made strictly liable for carrying messages that are used to conduct terrorist operations, perhaps on a *Renton* theory that some categories of speech have harmful secondary effects, the result would be to force all remailers in the jurisdiction to close since the operators would have no other way to protect themselves from the liability. This hypothetical strict liability statute would be vulnerable to the accusation that it discriminated against points of view that dare not speak openly, and its constitutionality is far from certain, but it is certainly more likely to be found constitutional than a straight ban on anonymous messages.[175]

Given the international nature of the Internet, however, even a clever attempt to ban anonymous remailers one jurisdiction at a time may be ineffectual. Even if every remailer in the U.S. stops operating, there is nothing to stop U.S. citizens from sending and receiving messages via foreign-based remailers—at least not yet. The continuous and conspicuous use of remailers and the equivalent might even be seen

173. *See supra* text following note 75.

174. For a suggestion that the *Renton* approach might be extended to political speech, see Susan H. Williams, *Content Discrimination and the First Amendment*, 139 U. PA. L. REV. 615, 633 (1991) ("Although this question has not yet definitively been answered, the recent case of Boos v. Barry [485 U.S. 312] indicates that an affirmative response by a majority of the Court may not be far off.").

175. "[T]he widest possible dissemination of information from diverse and antagonistic sources is essential to the welfare of the public." Associated Press v. United States, 326 U.S. 1, 20 (1945) (upholding application of Sherman Act to newsgathering agency), *quoted with approval in* Metro Broadcasting v. FCC, 497 U.S. 547, 567 (1990).

to create a reasonable expectation of privacy for Fourth Amendment purposes, thus reinvigorating a part of the Constitution which otherwise appears to be heading towards desuetude.

C. *Practical Constraints: The International Tide*

The Internet is an increasingly multi-national phenomenon. Other countries that lack a First Amendment may desire solutions to the perceived dangers of anonymous communication that are more or less restrictive than those suggested by U.S. law, which itself remains unclear in important respects. Remarkably, however, the reality of the Internet is that the technology for sending e-mail messages anonymously is already in use both here and abroad: the whole world can now enjoy (or suffer) the fruits of anonymous remailers located anywhere. The Constitutional status of anonymous electronic speech remains important: if the U.S. will not or constitutionally cannot ban anonymous remailers, then they will be available for the entire Internet to use. Even if the U.S. attempts to ban anonymous remailers, and even if the Constitution allows this, U.S. law may not be determinative because, as it now stands, the Internet as a whole is not easily amenable to any nation's control. While it is probably within the physical power of the U.S. government to prosecute Internet remailers based in U.S. territory, the government appears to lack the power to deny U.S. residents the benefit of remailers located abroad, although it can certainly raise the costs of getting caught.[176]

The Internet is an international packet switching network and its messages are carried over telephone lines.[177] Short of cutting off one's own international telephone service or concluding an international agreement with all industrialized countries to discontinue telephone service to foreign countries that harbor remailers there is little that one

176. This is by no means a unique example of the Internet making a legal rule obsolete. *See, e.g.*, Ethan Katsh, *Rights, Camera, Action: Cyberspatial Settings and the First Amendment*, 104 YALE L.J. 1681, 1695 n.43 (1995) (describing irrelevance of prior restraint doctrine in age of mass near-instantaneous communication).

177. A *packet switching network* is method by which data can be broken up into standardized packets which are then routed to their destination via an indeterminate number of intermediaries. *See* Bruce Sterling, *Short History of the Internet* (Feb. 1993), *available online URL* gopher://gopher.isoc.org:70/00/Internet/history/short.history.of.Internet.

Multiple packets originating from a single long data stream may use more than one route to reach a far destination where they will be reassembled. This decentralized, anarchic, method of sending information appealed to the Internet's early sponsor, the Defense Department, which was intrigued by a communications network that could continue to function even if a major catastrophe (such as a nuclear war) destroyed a large fraction of the system. *Id.*

can do to keep out messages from any other country, or indeed to keep citizens from sending messages wherever they like.[178] If the government of Ruritania is intent on preventing communication with Great Britain, Ruritania might attempt to require that Ruritanian ISPs refuse to accept messages from computers whose domain name identified them as British. British domain names frequently end with the characters ".uk" and Ruritanian routers might be required to return all messages from those domains. Even if this is technically feasible, such a strategy is unlikely to succeed. First, there are generic domain names such as ".com," ".org," and ".net" that do not identify the country of origin. Second, unless Ruritania has currency and other controls, there is nothing to stop Ruritanian users establishing an account in the U.S. and telnetting to it to access British data.[179] Third, short of a robust international convention, there is no way that Ruritania can prevent people outside Britain from running remailers that "launder" messages from Britain and present Ruritanian computers with acceptable domain names. In short, any effort to censor the Internet organized at the national level (or below) is likely to fail.[180] As John Gilmore put it, "the Net interprets censorship as damage and routes around it."[181]

U.S. law currently imposes few if any legal restrictions on anonymous remailing.[182] U.S. rules can thus be viewed as a baseline; any country with a more restrictive approach to anonymity can expect to

178. Penthouse Magazine's World Wide Web site announces that the web site is "not available" in Ecuador, Egypt, Fiji Island, Formosa, India, Japan, Kenya, Korea, Malaysia, Malta, Mexico, Nigeria, Okinawa, Pakistan, Philippines, Saudi Arabia, Singapore, South Africa, Spain, St. Lucia, Thailand, Trinidad, Turkey, United Kingdom and Venezuela because these nations "prohibit adult material." Penthouse Magazine, Not Available in These Countries, *available online URL* http://www.penthousemag.com/resource/nothere.html. Nevertheless, I am reliably informed that the materials on this web site are accessible from a domain in the United Kingdom whose address ends in ".uk".

179. Even currency controls may not prevent users from establishing foreign Internet accounts since some accounts, on "freenets," are free to the public.

180. Thus, Eugene Volokh's radical predictions about the demise of private speech regulation in the U.S., *see* Volokh, *supra* note 54, at 1836, actually may be too mild because they do not take account of the international nature of the Internet.

181. *Redefining Community*, INFO. WK., Nov. 29, 1993, at 28 (quoting Gilmore). Of course, nothing prevents individual users or system operators from blocking the direct receipt of messages from unwanted sources. *See* Branscomb, *supra* note 25, at 1676. Users, however, will not find it difficult to circumvent these restrictions. *See, e.g.*, Katsch, *supra* note 176, at 1695 n.43.

The discussion in the text applies to Internet functions such as e-mail or World Wide Web requests. In contrast, so long as the number of remailers remains small, it might be technically feasible to eliminate anonymous postings from the USENET (a distributed bulletin board system). *See* Long, *supra* note 25, at 1186-87 (describing operation of "Automatic Retroactive Minimal Moderation").

182. *See supra* text accompanying note 92.

see it undermined by the U.S. rules unless it is willing and able to cut itself off from the Internet entirely.[183] Similarly, should the United States's rules change to restrict anonymity, as they might some day, these new rules will themselves be undermined by persons in any another country with adequate connectivity and a legal regime more congenial to anonymous communication.[184] The proponents of measures to eliminate Internet anonymity are thus likely to find themselves in the position of the counselors to King Canute.[185] Indeed, to the extent that foreign countries with good Internet connectivity such as the Netherlands and Finland already have more permissive rules, those rules effectively undercut the United States' ability to enforce what rules it has.

The difficulty that governments have in reigning in free speech on the Internet or in living with its consequences is particularly visible in the uneasy relationship that several Asian governments have with the Internet. Only North Korea and Myanmar have chosen to remain completely aloof from it.[186] The Vietnamese government overcame its concerns about free movement of information and allowed a small academic and scientific network, "NetNam," to operate, because the government saw the Internet as the "fastest, cheapest way" to improve communications with the rest of the world.[187] The Vietnamese government then apparently had second thoughts about unregulated communications, and decided to set up its own system, using hardware purchased from a US telecommunications company, Sprint. The new system, which is likely to displace NetNam, will have a greater capacity but the government hopes that it will also be controlled more tightly "for technical and security reasons [and] from the cultural aspect."[188] The government intends to keep out foreign pornography and other harmful information sent by foreign organizations.[189] A government

183. For a suggestion that the People's Republic of China may attempt to achieve information autarchy, see Joseph Kahn & Kathy Chen, *Chinese Firewall*, WALL ST. J., Jan 31, 1996, at 1.

184. The Canadian Copyright Act guarantees the right of an author to write under a pseudonym. *See* Canadian Copyright Act § 14.1.

185. *See supra* text accompanying note 2.

186. Philip Shenon, *2-Edged Sword: Asian Regimes On the Internet*, N.Y. TIMES, May 29, 1995, § 1, at 1.

187. *Id.* (quoting Tran Ba Thai, sysop of NetNam).

188. Jeremy Grant, *Vietnamese Move to Bring the Internet Under Control May Backfire*, FIN. TIMES, Sept. 19, 1995, at 6 (quoting Nghiem Xuan Tinh, deputy director of Vietnam Data Communications Company, a subsidiary of Vietnam Post and Telecommunications).

189. *Id.* This may be a reference to the campaign by anti-Communist emigres based in California who sought to overwhelm the Vietnamese Prime Minister's e-mail mailbox. *See* Shenon, *supra* note 186 (describing attempt).

spokesman admitted, however, that the government was uncertain as to how it would achieve these goals, but he promised that the government intended to "think about it."[190]

Meanwhile, in Singapore, the government has promised penalties for anyone caught transmitting pornographic or seditious matter.[191] It has also ensured that its point of view will be represented in a Usenet discussion group, soc.culture.singapore, frequented by its critics. Government spokespersons routinely post messages giving the government's side of issues.[192] Overall, however, the government has chosen to control Internet access since, despite its best efforts, it cannot figure out how to control content:

> The Singapore government knows that it cannot do much to censor the Internet. But it refuses to give up without a fight.
>
> The main control is to limit access—the rationale being that only the determined would get at the materials and not the casual users.
>
> . . . .
>
> Singapore's case is instructive in that it is trying to both control information and yet benefit from the Information Age. Current thinking suggests that it is difficult, if not impossible, to achieve both aims. Nevertheless, Singapore is trying.[193]

As part of its campaign against Internet pornography, the Singaporean government searched the files of users of Technet, one of Singapore's major Internet providers. A scan of 80,000 files with a ".GIF" extension found five pornographic files, resulting in warnings to their owners.[194] Foreign companies with offices in Singapore worried that the Singaporean government would search their data too in the hopes of

---

190. Grant, *supra* note 188.

191. Shenon, *supra* note 186.

192. *See, e.g.*, Philip Taubman, *Cyberspace in Singapore*, N.Y. TIMES, Nov. 8, 1995, at A24.

193. Peng Hwa Ang & Berlinda Nadarajan, *Censorship and the Internet: A Singapore Perspective, available online URL* http://info.isoc.org/HMP/PAPER/132/txt/paper.txt (The lead author is a professor at the School of Communication Studies, Nanyang Technological University.) [hereinafter *Singapore Perspective*].

The Chinese government is also seeking to limit Internet access by keeping costs of local service artificially high, although Internet usage is growing quickly through both campus and commercial servers. Shenon, *supra* note 186. China's post and telecommunications minister, Wu Juchuan, announced that China will exercise control of the information it allows in. "By linking with the internet, we do not mean the absolute freedom of information." Johanna Son, *Asia-communication: Bumps Lie Ahead In Information Superhighway, Inter Press Service, available on line* LEXIS, library News, file Curnws.

China has also announced plans to build a state-owned Internet network called Chinanet. *China Plans own Internet*, FIN. TIMES, Nov. 7, 1995, at 7; *see also* Kahn & Chen, *supra* note 183.

194. *Singapore Perspective*, *supra* note 193.

finding confidential corporate e-mails, and the government had to promise them that it would not do it again.[195]

Just as nations are unable to control the content of Internet speech, so too will they be unable to prevent anonymous communication. This inability to enforce a ban on anonymous Internet communication is not an unmitigated disaster, Justice Scalia's warnings notwithstanding.[196] Although it will impose real costs in untraceable libel, hate speech, and (perhaps) theft of intellectual property,[197] easily available anonymous communication also spells the end of restrictive national policies regarding information. Any government that allows its citizens to become a part of the global electronic network will be forced to live with a freedom of speech even greater than that contemplated by the authors of the First Amendment. The Singaporean example suggests that the ability of even a very authoritarian government to restrict access to the global information network is limited because businesses believe that the value of unrestricted access to these communications is very high.

Even so, governments are not yet powerless. Governments have it within their power to impose some costs, at least in ease of use, on those who wish to communicate anonymously. If banned in one country, anonymous remailers can be found abroad. A country that wishes to ban mail to or from foreign anonymous remailers will find it hard to detect unless it expends great resources monitoring all national traffic. The expenditure will need to be great because it is difficult to distinguish between ordinary mail and mail to anonymous remailers unless the government either bans encryption or maintains a very up-to-date list of foreign remailers. Even an encryption ban is difficult to enforce since some forms of encrypted text are hard to distinguish from other common file formats.[198] Governments have demonstrated that they are capable of acting in concert to seek to control activities such as money

195. Shenon, *supra* note 186. As this article was going to press, the government of the People's Republic of China announced new limits on the exchange of market information regarding the Chinese economy. News reports suggested that the spread of the Internet was one of the government's major concerns. *See* Kahn & Chen, *supra* note 183.

196. *See supra* text accompanying note 46.

197. Technical counter-measures, akin to salting each telephone book with unique false entries to pinpoint the source of any copies, promise to reduce this danger considerably. In addition, customers may prefer to buy products from vendors they know and trust. *See supra* note 21 (statement by RSA spokesman that posting of RC4 source code to the Internet has not slowed sales of RSA licensed products using RC4).

198. A ban on cryptography can be circumvented, at some cost to ease of use, by employing steganography:

laundering which they perceive as a common threat, although the effectiveness of these measures is debated.[199] International actions in this domain include the Vienna Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances[200] regional agreements,[201] a number of mutual legal assistance treaties between the U.S. and other nations,[202] and the creation of a Financial Action Task Force including most of the world's major economies.[203] As yet, there appears to be no equivalent movement to control anonymous remailers, but it is not inconceivable.

The prime effect of a single government's attempt to ban anonymous messages will be to make anonymous communication far less easy to use if one is concerned about getting caught. Loss of ease of use is a significant factor, because the harder a computer technique is to use, the fewer people will use it. Furthermore, the more difficult a computer technique, the more users will make sloppy mistakes that could lead to their being detected.[204] Criminalization drives use at least partly underground, much like the attempt to control drugs has no doubt reduced,

---

Steganography is the art and science of communicating in a way which hides the existence of the communication. In contrast to cryptography, where the "enemy" is allowed to detect, intercept and modify messages without being able to violate certain security premises guaranteed by a cryptosystem, the goal of steganography is to hide messages inside other "harmless" messages in a way that does not allow any "enemy" to even detect that there is a second secret message present.

Markus Kuhn, *Steganography Mailing List*, *available online URL* http://www.thur.de/ulf/stegano/announce.html.

199. *See, e.g.*, Lisa A. Barbot, Comment, *Money Laundering an International Challenge*, 3 TUL. J. INT'L & COMP. L. 161, 164 (1994) (suggesting money laundering continues to grow despite international efforts).

200. United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, Dec. 19, 1988 (E/Conf./82/15), *reprinted in* 28 I.L.M. 493 (1989).

201. *See, e.g.*, Scott E. Mortman, Note, *Putting Starch In European Efforts To Combat Money Laundering*, 60 FORDHAM L. REV. S429 (1992) (discussing EC directive on money laundering); Phyllis Solomon, Note, *Are Money Launderers All Washed Up in the Western Hemisphere? The OAS Model Regulations*, 17 HASTINGS INT'L & COMP. L. REV. 433 (1994) (discussing money laundering provisions of Inter-American Drug Abuse Control Commission's Model Regulations Concerning Laundering Offenses Connected to Illicit Drug Trafficking and Related Offenses).

202. *See* OFFICE OF TECHNOLOGY ASSESSMENT, INFORMATION TECHNOLOGIES FOR THE CONTROL OF MONEY LAUNDERING 113 (1995) (OTA-ITC-630) [hereinafter MONEY LAUNDERING].

203. *See id.* at 115-17.

204. The leading study of "how cryptographic systems fail in practice" concluded that "many products are so complex and tricky to use that they are rarely used properly. As a result, most security failures are due to implementation and management errors." Ross Anderson, *Why Cryptosystems Fail*, 37 COMM. ACM 32-41 (Nov. 1994), *available online URL* ftp://ftp.cl.cam.ac.uk:/users/ria14/wcf.ps.Z.

but in no way eliminated, the use of marijuana and narcotics in the U.S. and other countries.[205]

Widespread access to anonymous communication, even if the communication carries some risk, means that citizens armed with computers will be able to criticize their government—and their neighbors—with less fear of retribution, and will have increased access to messages from around the world giving alternative points of view. Meanwhile, at this writing there is little or no risk involved in using a chain of anonymous remailers, and only a little technical skill is required. As a result, rules seeking to control the export of information such as the International Traffic in Arms Regulations (ITAR) will become even more difficult to enforce.[206] So long as anonymous remailers exist, rules seeking to limit the importation of "subversive" or "obscene" speech become impossible to enforce consistently while the recipient country remains connected to the Internet. Like it or not, we live now in an age of completely free speech, of one limited and anonymous type, for everyone with access to a computer.[207]

III. NEW CHANNELS OF COMMERCE

A great number and variety of businesses have announced plans for or prototypes of Internet-based commercial activities. As many as fifteen percent of consumer purchases may be electronic by the turn of the century.[208] Internet commerce seems poised to evolve in two com-

---

205. On the fate of the War on Drugs in the U.S., see STEVEN B. DUKE & ALBERT C. GROSS, AMERICA'S LONGEST WAR: RETHINKING OUR TRAGIC CRUSADE AGAINST DRUGS (1993).

206. *See ITAR page, available online URL* ftp://ftp.cygnus.com/pub/export/export.html. Anonymous communication will be less effective in undermining the ITAR to the extent that its true goal is to restrict the emergence of a standard mass-market encryption product. Until anonymous digital cash is wide-spread, no commercial software publisher in the U.S. will risk violating the ITAR since there is no effective means for them to charge for their products and yet maintain the anonymity they would require to avoid any risk of prosecution.

207. Note that one does not need to own a computer; one simply needs access to a machine one can trust not to log one's communications. In the United States, for example, such a computer might be located in a public library.

208. *Where E-Cash Will Take Off*, BUS. WK., June 12, 1995, at 70. Another estimate suggests more than $200 billion in Internet commerce within five years. John Kavanagh, *Purchases on the Internet 'Could Potentially Exceed $200bn by Year 2000,'* FIN. TIMES, Nov. 1, 1995, at 12 FT-IT (quoting wide variety of estimates). Internet purchases in 1994 were estimated at $240 million. *Id. See also* Edward Mozley Roche, *Business Value of Electronic Commerce Over Interoperable Networks*, Paper Presented at Freedom, Forum, July 6-7, 1995 (Rosalyn, Va.), *available online URL* http://www.commerce.net/information/reference/roche.txt (projecting huge increases in Internet commerce).

plementary directions, which one might call ordinary commerce in tangible things and information commerce.

In the case of ordinary commerce in tangible things, many transactions that are currently carried out by telephone, ordinary mail (e.g., catalog sales), and even in person, may shift to the net. The shopping mall of the future may be on line, and offer everything from video product demonstrations and recorded customer testimonials to technical specifications for the product. Interactive sales may allow merchants to question customers as to their needs and budgets and then guide them to particular products;[209] the products could be manufactured to the customer's size, color, and other specifications based on the customer's specifications. It may even be possible to haggle with the merchant's computer about the price.[210]

From the most practical standpoint, the challenge of Internet commerce is of conducting business via a medium that excels at moving information, but provides a very insecure means of communication. It is not always possible to be certain that persons are who they claim to be, nor is it certain that no one is eavesdropping. Digital cash promises to solve the problem of moving value, but it is too early to say which if any type of digital cash is likely to find wide acceptance in the marketplace. In the mean time, consumer transactions are being conducted by credit/debit card.

A. Internet Credit Card Transactions

In the short run, credit and debit cards provide the simplest, if not necessarily the ideal, means of transferring value over the Internet. These Internet credit card[211] transactions can usefully be divided into three categories:

(1) The customer e-mails the merchant her credit card details (or fills out a form on a World Wide Web page), much as a person cur-

209. *See, e.g.*, Walter R. Baranger, *Taking In The Sites; Car Parking Areas Grow Around the Web*, N.Y. TIMES, Sept. 11, 1995, at D8 (describing home pages of auto manufacturers who offer prototype interactive sales information, querying customer on color, cost and other preferences).

210. The implications of Internet-based price discrimination are substantial, but they are beyond the scope of this article. Professor Gandy argues that profiling will enable new forms of invidious discrimination. *See* Oscar H. Gandy, Jr., *Legitimate Business Interest. No End In Sight?*, 1996 U. CHI. LEGAL F. (forthcoming). One might, however, argue that the Internet empowers consumers more than it empowers those who would take advantage of them since it will put information of how firms treat similarly situated consumers at their fingertips.

211. This discussion uses "credit card" loosely to include debit cards. Although the differences between credit and debit cards are significant in other contexts, the Internet aspects of the transactions are not materially different.

rently sends such information through the ordinary mail. Although there is some risk that this information might be copied en route, particularly if the message originates on Ethernet systems that are vulnerable to in-house packet sniffing, to date such theft of credit card details seems rare at most. The customer's liability for fraudulent use in such cases is subject to the same $50 limit as with any other credit card transaction.[212]

(2) The customer encrypts the credit card data before sending it, e.g., with PGP or with Netscape's Secure Sockets Layer (SSL) protocol. Subject to the constraint that a determined attacker armed with enough computers and time can always break some of the shorter codes in use, this reduces the risk that the credit card details will be copied by a third party. (Other risks include the danger that the cryptographic system is flawed, badly implemented, or used on an insecure platform, e.g., one which stores the data in an insecure manner.)

(3) The customer enters into an agreement with a third party such as First Virtual Holdings, in which the credit card data is transmitted to the third party by some other means. In the case of First Virtual, an early entrant to this market, each transaction is also confirmed by e-mail;[213] in other cases, the customer may be issued some identifying data, such as a PIN or a public-private key pair[214] with which to digitally sign messages. In both cases participating merchants clear transactions through the third party before the charge is posted to the customer's credit card.

In all three categories, the customer needs to have a valid debit/credit card, e.g., Visa, or MasterCard, to make the transaction work. The charges are sent to the bank, or appear on the credit card, and are settled between the buyer, the seller (or the third party) and the card issuer as if the customer had used the card to buy something in an ordinary transaction.

Despite the variety of options, however, the transfer of ordinary commerce in tangible things from existing retail channels to distributed network sales is likely to raise relatively few new legal problems, although there is no reason to expect any of the existing problems associ-

212. *See* 15 U.S.C. § 1643(a)(1)(B) (1994); 12 C.F.R. § 205.6 (1995) (limiting consumer liability to $50 for most unauthorized electronic funds transfers).

213. *See* First Virtual, Welcome to First Virtual, *available online* URL http://www.fv.com:80/info/intro.html.

214. *See supra* note 74.

ated with retail sales to disappear.[215] Indeed, ordinary Internet commerce in tangible things may remain well suited to credit card sales, particularly if the customer's potential liability for fraud remains fixed at $50.[216]

In contrast to ordinary commerce in tangible things that simply moves to the Internet, the sale of information is likely to be transformed. This transformation will bring new legal and social problems in its wake, or at the very least amplify old ones.[217] Although today access to most World Wide Web pages is free and open to anyone with a browser, this may change once the pioneers on the information ocean begin creating exclusive economic zones in their virtual real estate and limiting access to users who have either purchased a password for access or have browsers that are pre-configured to pay charges, perhaps up to a pre-defined limit, for access to World Wide Web pages. Web pages are ideally suited to micro-transactions, in which the reader is charged a trifling fee—a penny or less—for each access,[218] so long as the process of payment can be seamlessly integrated into browsing tools. At present, minute charges such as a tenth of a cent cannot economically be processed through existing credit card systems[219] and this seems unlikely to change in the near future. Thus, a digital means to transfer value, preferably one that does not require the participation of a third party such as a credit bureau or credit card issuer, will be required before micro-charges can become part of the new information economy.[220] It is clear that the potential for growth of Internet infor-

215. For a survey of many of these problems, see Mary Elizabeth Matthews, *Credit Cards—Authorized And Unauthorized Use*, 13 ANN. REV. BANKING L. 233 (1994). Claims of fraud that hinge on forgery or on factual determinations of identity may change if commerce begins to rely on digital signatures. Unless a user loses control of the digital signature (or, more commonly, the passphrase used to get access to the encrypted digital signature), a message signed with a digital signature is undeniably the user's and not a forgery.

One additional issue of importance to the merchant is whether the credit card clearer will regard the transaction as one in which the card is "present" or "not present." Merchants typically have to pay a higher commission, and in some countries may bear more risk, in a transaction where they cannot physically examine the card.

216. Regulation E, 12 C.F.R. § 205.6 (1995).

217. *Cf.* John Mason, *Bank's Security Chains Failed*, FIN. TIMES, Sept. 20, 1995, at 12 (describing banks' fears that hackers will use electronic means to rob banks).

218. *See* Arnold Kling, *Banking on the Internet, available online URL* http://www-e1c.gnn.com/gnn/meta/finance/feat/archives.focus/bank.body.html.

219. *See, e.g.*, Report § 1.1, *available online URL* http://www.nri.reston.va.us:3000/XIWT/documents/dig_cash_doc/Part1.html. The average U.S. credit card purchase today is $60. *Id.*

220. Steve Glassman et al., *The Millicent Protocol for Inexpensive Electronic Commerce, available online URL* http://HTTP.CS.Berkely.EDU/~gauthier/millicent/millicent.html, argues that even digital coins are too expensive for micro-transactions, and that a new form of "scrip" needs

mation commerce is enormous, and that the high fixed costs of credit cards transactions makes them particularly unsuited for high-volume low-value transactions.

B. Digital Cash: A Technical Menu

Cryptologists have worked out methods for creating and transmitting tokens of value—the digital equivalent of cash and checks—over a network like the Internet. This "digital cash," also known as "electronic cash," "E$," or "e-cash," will allow buying and selling goods or services over the Internet. Any digital cash system vastly expands the commercial possibilities of the Internet, particularly if the system has low transaction costs. With low transaction costs, pay-per-view/pay-per-byte systems in which pennies or less are charged to view an article or picture on the World Wide Web become a real possibility.

Depending on which protocol is adopted, the transaction may or may not result in a record of the buyer's participation in the transaction being maintained by either the seller or the bank. Digital cash can leave the audit trail of a credit card purchase, or can provide greater anonymity than paper currency. Without some form of anonymity built into digital cash, however, each payment creates the possibility of a record which, when combined with other similar records, becomes a detailed consumer profile. If digital cash replaces credit cards for ordinary commerce in tangible things, the consequences of this profiling may be no more severe than those caused by the use of credit cards today. If, however, the availability and ease of use of Internet commerce causes consumers to shift cash sales to Internet credit card sales or traceable digital cash, the effect will be to increase the amount of information available on the consumer's buying habits.

If consumers use a traceable payments mechanism for the purchase of information as well as goods, the potential for consumer profiles grows larger still. If Internet tools such as the World Wide Web become a major national and international communications medium with an embedded micro-charging mechanism, every newspaper article accessed, every online catalog perused, every political debate sampled, will leave an information residue. These data can be collected to form a highly detailed profile of the consumer-citizen. The existence

---

to be deployed for micro-transactions. Proposals for two schemes that may meet the exacting requirements of efficient micro-transactions can be found in Ronald L. Rivest & Adi Shamir, *Payword & MicroMint: Two simple Micropayment Schemes* (Nov. 8, 1995), *available online URL* http://theory.lcs.mit.edu/~rivest/RivestShamir-mpay.ps.

of such detailed dossiers on spending and intellectual preferences would be unprecedented.[221]

We are at a very early stage in the development of Internet commerce. Most payment products and protocols are somewhere between the drawing board and the street; few are beyond their field tests. No standards have emerged, but many large financial corporations and banks are preparing to provide consumer electronic financial exchange products.[222] Each of these implementations requires that decisions be made about inevitable tradeoffs between security, anonymity, cost, and ease of use.

Let us assume that the digital cash is to be provided by a bank,[223] and used in a real-time transaction between Alice, a customer, and Bob, a merchant.[224] In a real-time transaction Alice buys information (software, news, art, the right to view a Web page) on-line. There may be only seconds between Alice's proffer of payment and her expectation that Bob will deliver the goods; Bob must confirm the validity of Alice's payment immediately, or run the risk that there will be little he can do if Alice has cheated him. An Internet transaction might of course take many other forms, and these too receive occasional mention in what follows. The transaction could, for example, be a catalog sale transaction in which Alice places an order, makes a payment, and Bob waits until payment clears before shipping the goods. In this model, Bob's risk that the payment will be bad is relatively low since he need only fail to ship the goods.

Because the digital cash is represented by a series of bits, and there are few things in this life easier to copy than bits, the bank is going to be very anxious to ensure that any copies of the digital cash created by Alice or by Mallet, a hostile third party,[225] will be unspendable, or at least very easy to detect. The bank wishes to prevent, or at

221. *See generally* Gandy, *supra* note 210.

222. *See* the long list of companies at the E-cash Index, *available online URL* http://ganges.cs.tcd.ie/mepeirce/Project/proposed.html.

223. Whether a corporation that provides electronic cash services is necessarily required to be licensed as a bank is a question beyond the scope of this article. The provision of digital cash creates obvious issues regarding the backing of currency by electronic banks, control of the money supply, and wonderful new forms of bank fraud.

224. For a far more detailed discussion of the possible participants and their requirements, see generally Mihir Bellare et al., *ikp—A Family of Secure Electronic Payment Protocols* (July 12, 1995), *available online URL* http://www.zurich.ibm.ch/Technology/Security/publications/1995/ikp.ps [hereinafter IBM Research].

225. "Mallet" is the name cryptographers give to a malicious active attacker. *See, e.g.*, SCHNEIER, *supra* note 74, at 31.

very least detect, attempted double-spending of digital cash in order to avoid having to pay twice, and ideally it also wants to be able to figure out who the double-spenders are in order to have them prosecuted for fraud. For example, if the bank's communication with Alice is not encrypted, Mallet might eavesdrop on Alice's telephone line and record the digital cash as it is transmitted and then try to spend it before Alice does. And even if the communication with Alice is secure, the bank wishes to make sure that Alice herself cannot spend a coin more than once.

Bob, the merchant, wishes to be able prove that Alice authorized the transaction, in order to ensure that Alice will not attempt to deny it later ("non-repudiation"). Bob also wants an assurance that Alice has the funds to pay for the transaction, and that the bank will transfer them to him.[226] In some circumstances Bob may also wish to avoid revealing the fact of the transaction. Meanwhile, Alice wishes to ensure that unauthorized payments are impossible, that Bob cannot deny having received her payment, that the fact of transaction is private, and that there is some redress available if Bob defaults or delivers shoddy goods. In some cases, Alice wants the transaction to be fully anonymous—not even Bob should know Alice's identity; in such cases, however, Bob will want to ensure that Alice remains unable to disavow the obligation to pay.[227]

If the transaction is entirely electronic, each of the parties will need a mechanism to ensure the other parties will pay what is required. In a world where fraud is possible, or the transaction has any non-instantaneous aspects (e.g., a warranty, the possibility of product liability suits, the possibility that a party might attempt to repudiate the payment) the parties will want some assurance that the other parties are who they claim to be: bank, Bob, and Alice (the owner of the digital currency). Identity authentication, however, is by far the easiest aspect of the electronic transaction, as it can easily be achieved with digital signatures.[228]

---

226. *See* IBM Research, *supra* note 224, at 4. Unlike the case where Alice offers paper money, Alice's proffer of digital cash does not provide the necessary assurances, because Bob needs to confirm that the digital cash has not been spent previously.

227. *See* IBM Research, *supra* note 224, at 4-6.

228. If the parties have no prior contact, then the digital signatures need to be backed by some evidence of authenticity. This can be provided by either a "web of trust" model, in which the party proffering a signature produces attestations of identity or reliability signed by one or more persons known to the other party or, failing any common acquaintances, by some chain of authenticators culminating in a person known to the other party. Alternately, the digital signature can be backed by a "certificate" by some trusted third party, e.g., the Post Office, attesting to identity. *See* OFFICE OF

Digital cash can be stored in any one of a number of places: in the financial institution's computer, in Alice's and Bob's computers, or on smart cards carried by the customer and the merchant.[229] The digital cash may be backed by actual funds, or it may not. Depending on the system used, if Alice and Bob hold the digital cash, the bank may issue it in the form of digital "coins" which must be aggregated to reach the total amount of the purchase, or Alice and Bob may hold it in a digital account on a smart card which is debited and credited as needed. The system may require that all transactions are cleared by the issuer, or it may allow funds to circulate freely between customers and merchants.

What follows attempts to be a representative sample of the types of digital cash currently being developed. Few of the digital payment systems discussed below allow unlimited direct transferability between holders of electronic funds: with the single exception of the Mondex digital purse model, in all of the digital coin models the recipient of an electronic payment must always return to the bank for a new coin before being able to spend it, although it is theoretically possible for users to modify at least one digital coin payment scheme to allow the coins to be transferred among third party without returning to the bank.[230]

1. The Debit Card Model

One simple, albeit costly, electronic payment strategy that meets the bank's security needs, but not necessarily all of Alice and Bob's, is to require that every transaction between them be cleared through the bank at the time of the transaction. The highest-security version of this model is not really digital cash at all, and is modeled on debit cards:

TECHNOLOGY ASSESSMENT, CONGRESS OF THE UNITED STATES, INFORMATION SECURITY AND PRIVACY IN NETWORK ENVIRONMENTS 55-56 (1994) (OTA-TCT-606) [hereinafter OTA INFORMATION SECURITY] (describing Post Office's proposed certification service); MICHAEL BAUM, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, FEDERAL CERTIFICATION AUTHORITY LIABILITY AND POLICY: LAW AND POLICY OF CERTIFICATE-BASED PUBLIC KEY AND DIGITAL SIGNATURES (1994) (surveying legal and policy issues involved in setting up and running a certification authority); A. Michael Froomkin, *The Essential Role of Trusted Third Parties in Electronic Commerce*, 75 OR. L. REV. 49 (1996).

229. For a taxonomy of smart card types, see David Chaum, *Prepaid Smart Card Techniques: A Brief Introduction and Comparison, available online URL* http://ganges.cs.tcd.ie:80/mepeirce/Project/Chaum/cardcom.html.

230. Note, however, that parties wishing to exchange digital coins without clearing them through the bank must have much greater trust in each other than would otherwise be required. *Id.* In contrast, electronic wallet systems, such as Mondex, which do not store "coins" but instead have a meter that records the value held, lend themselves easily to third-party transferability. *See infra* text accompanying note 256.

the bank requires Bob, the merchant, to contact the bank on-line at the time of payment in order to transfer the funds from Alice's account to Bob's account. If Alice has insufficient funds, the bank refuses to allow the transaction. If the client has the funds, they are transferred from the client's account to the merchant's account at time of sale. An alternative form of this model has the "bank" replaced by a clearing service that forwards the payment instructions to the ordinary banks previously selected by members of the scheme.[231]

Alice's and Bob's identity can be verified using unforgeable digital signatures, making the chances of a fraudulent or repudiable transaction remote so long as both parties carefully protect the passphrases (longer, alphanumeric, versions of bankcard PIN numbers) that access their accounts. There is no danger of double-payment or duplication of digital currency because no digital currency ever leaves the banking system.

One disadvantage of this approach is that on-line verification introduces both delay and expense into the transaction akin to that of ordinary credit cards. The transaction costs associated with the debit-card paradigm make it unsuited for low-value/very-high-volume transactions.[232] The basic debit card model would work for buying a car on-line, or even perhaps a t-shirt, but not for charging a tenth of one cent to read a Web page. The debit-card paradigm also does nothing to protect the privacy interests of either Alice or Bob: the bank has a full record of every transaction. This facilitates auditing, and may be of great value to law-enforcement, but it also means that privacy vis a vis the bank is low, and that the bank will find consumer profiling easy.[233]

---

231. This, in essence, is the strategy behind CyberCash's Money Payments Service (TM), *see* Moneypayments, *available online URL* http://www.cybercash.com/technical/moneympayments.html, and also the "Checkfree Wallet," *see* http://www.checkfree.com, *available online URL* http://www.mc2-csr.com/vmall/checkfree/v20/faq.html. Members of the Money Payments program include Wells Fargo Bank, American Express and Mellon Bank. *Id.* A similar strategy, involving the use of a prepaid VISA ATM/debit card (and a five percent commission charge!) is employed by the (unchartered) "First Bank of Internet." *See Announcement, available online URL* http://ganges.cs.tcd.ie/mepeirce/Project/Press/foi.html.

232. *See, e.g.*, Stefan A. Brands, Centrum voor Wiskunde en Informatic (CWI), *Off-line Electronic Cash Based on Secret-Key Certificates* 1-2 (1995) (Report CS-R9506) [hereinafter Brands 1995], *available online URL* http://www.cwi.nl/ftp/brands/CS-R9506.ps.Z.

233. As discussed in more detail below, *see infra*, it may be easier for regulators to control the transaction data in the bank's possession than the information kept by Alice and Bob.

2. *The Basic Digital Coin*

The basic digital coin model is fairly simple: the Bank issues the user a very large, probabilistically unique, random number (the "serial number" of the coin) signed with the Bank's private key. When Alice wants to spend the coin, she sends it to Bob, who turns it in to the bank either on line, or after the fact. The bank checks the serial number against its list of spent coins and, if the coin has not previously been spent, either credits Bob's account or issues him a new coin with a new serial number.[234] So long as the bank is honest, Alice and Bob both have the proof they need that the transaction, and the payment, occurred. The coin model is also computationally simple to implement. Each coin requires a long, unique, random number, but the bank can re-use the same private-public key pair to sign every coin of a given denomination.[235] The basic coin model does not allow coins to circulate freely: every time Alice spends a coin at Bob's shop, Bob must redeem the coin at the issuing bank, either for traditional funds or a new coin, before he can spend the money.[236]

The basic coin model has two problems. First, if the transaction is on-line in real time, but verification is *off-line* (that is, at some time after the completion of the transaction), Bob may be unable to ensure that the coin Alice is offering him has not previously been spent until it is too late.[237] Bob can check the coin's digital signature against the public key associated with a coin of the purported denomination. This test will distinguish a forged coin from a real one. But without on-line verification Bob cannot tell if a coin already has been redeemed elsewhere at the time Alice wants to buy from him. On-line verification ensures that the coin being proffered is valid, but this verification likely

234. A simple example of this procedure in action is the Netcash "coupon." *See What is Virtual Cash?*, *available online URL* http://www.teleport.com/~netcash/nvasch.html, NetCash Quick Start Guide, *available online URL* http://www.teleport.com/~netcash/ncquick.html.

235. *See* David Chaum, *Achieving Electronic Privacy*, SCI. AM., Aug. 1992, at 96, 96-97 (discussing electronic cash), available online URL *http://ganges.cs.tcd.ie/mepeirce/Project/Chaum/sciam.html.*

236. As a general matter, it is possible to convert coin-based off-line electronic payment systems to allow transferability, but this has practical disadvantages that make that development unlikely. *See* Sefan Brands, *An Efficient Off-Line Electronic Cash System Based on the Representation Problem* 7-8, 52 (1993), *available online* ftp://ftp.cwi.nl:/pub/CWIreports/AA/CS-R9323.ps.Z [hereinafter Brands 1993]; David Chaum & Torben Pryds Pedersen, *Transferred Cash Grows In Size*, ADVANCES IN CRYPTOLOGY: EUROCRYPT '92 390 (proving that it is impossible to construct a transferrable digital coin system "without property that money grows when transferred").

237. Note that if the transaction is not consummated on-line, e.g., in a catalog sales model, Bob can assess the validity of Alice's payment at his leisure.

involves delay and expense.[238] Second, since the serial number of the coin is unique and known to the bank, Bob's redemption of the coin links Alice to the transaction, and the bank ends up with a database containing information on all of its customers; as in the credit-card model, the customers have no privacy.[239]

Basic digital coins are likely to have at most a small effect on the money supply. Whether they have any effect at all depends in large part on how banks and customers manage the coins and whether they use on-line or off-line clearing systems. At one extreme, transactions are cleared on-line and the bank allows Alice to avoid purchasing the digital coins until the moment she needs them. As a result, Alice keeps her funds in an interest-bearing account until she needs a coin. When she wants to transact with Bob she contacts the bank, it issues a coin, and she offers it to Bob who redeems it as soon he receives it from Alice. In this scenario, the digital coin's effect on the money supply is negligible.

At the other extreme, transactions are cleared off-line and the bank requires that Alice acquire digital coins in advance of need, much as one buys travellers checks today. Because on-line clearing is not available, or too expensive to be practical, Bob takes some risk of being paid in previously spent coinage when he accepts a coin from Alice. Bob's need to aggregate coins before redeeming them from the bank introduces further delays between before settlement. In this version, digital coins function much like traveller's checks. Since both travellers checks and cash are part of M1, the narrowest measure of money commonly used by macroeconomists, this alone is not significant. If, however, people choose to hold digital coins instead of ordinary cash, more of the money in circulation will flow into the banking system, increasing the money supply through fractional reserve lending.[240] Digital

238. *See supra* text accompanying note 232.

239. Chaum, *supra* note 235.

240. Suppose that before the introduction of digital cash, the money supply can be represented by,

$M=\frac{(1+c)H}{e+c}$, where

H = high-powered money, i.e., the quantity of money held by banks as reserves;
e = the fraction of deposits that banks hold as reserves; and
c = the fraction of deposits held as pocket cash.

If the introduction of digital cash results in a substitution of digital cash for pocket cash, c will decrease. So long as $e < 1$, i.e., so long as banks hold less than all their deposits as reserves, any decrease in c increases the money supply. *See* ROBERT J. GORDON, MACROECONOMICS 451, 452 n.4 (1978).

coins also could have a small effect on the velocity of money if they enable a greater number of transactions per year, or if the existence of world-wide 24-hour cybermalls encourages people to transact more often.[241]

3. *Blinded Coins*

The basic coin model gives the bank confidence at the price of on-line verification and the opportunity for banks to amass customer spending profiles. It is possible, however, to retain the features of the basic coin model that make it either impossible or at least very risky for people to copy their digital cash and spend it twice without giving the bank an opportunity to create a giant database of who spent what where. In this model, payors, but not payees, can remain anonymous.

Using "blinded coins" Alice can acquire digital cash with a unique serial number from a bank without allowing the bank to create a record of the coin's serial number. Despite the bank's ignorance of the serial number, the number's uniqueness helps ensure that Alice cannot spend it twice. The techniques that achieve this, developed and patented by David Chaum and being marketed by a company he founded called DigiCash, are complex. Like a basic digital coin, a blinded coin begins with a large random serial number, but this time the serial number is generated by Alice, the customer who intends to acquire a coin from the bank. Alice multiplies this serial number by another random factor ("the blinding factor"[242]), and sends the product (the "blinded" number) to the bank. As in the basic case, the bank signs the number with its secret key.

Unlike the basic case, however, *a bank issuing a blinded coin does not know the true serial number of the coin* at the time the bank issues it by affixing its digital signature to the "blinded" number. All that the bank knows is that Alice has purchased a coin of a given denomina-

---

A central bank such as the Federal Reserve Board can offset this effect, however, by increasing the reserve requirement (forcing banks to increase e) for banks that issue electronic cash.

241. According to the pre-Keynsian quantity theory of money, $MV=PQ$, where

M = money supply

V = velocity of money, i.e., the average number of times per year that the money stock is used in making payments for final goods and services.

P = price level

Q = real output.

242. For a description of the blinding protocol, see BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY 112-15 (2d ed. 1996).

tion,[243] and the "blinded" number Alice submitted.[244] In the absence of anonymous bank accounts, the bank knows Alice's identity, and knows how many coins of each denomination Alice is buying. Armed with this information, the bank should be able to comply with rules designed to control money laundering and tax evasion to the same extent as an ordinary bank.[245] Alice's privacy depends in part on there being a sufficiently large volume of coins in circulation such that Alice's purchase and use of the coins does not stand out.

There is yet another way to hide and retrieve Alice's identity. In this variation, the bank does not know who spent the money so long as it is spent only once, but this information is accessible to a designated organization outside the bank.[246] The inventors of this type of digital cash suggest that the trusted third party which would hold the means of de-annonymizing the digital cash should be "a consumer rights organization."[247] Nothing in their protocol, however, would prevent a government from requiring that the organization be the police or the courts. In effect, this protocol opens the door to Clipperized digital cash, in which the government could have access to transactional data subject to Fourth Amendment constraints.[248] It is possible, however, to modify the system of traceable anonymous cash so that the user's identity will only be disclosed if several parties ("trustees") agree.[249] This system of multiple trustees resembles the system of multiple escrow agents envisioned for the keys to the Clipper chip.

All forms of blinded coins are generated as follows. When Alice gets the signed blinded number back from the bank, she performs a mathematical operation that removes the "blinding factor." The result is a coin that looks like a basic digital coin, bears the "true" serial number, and has a digital signature from the bank that authenticates

243. *See* Chaum, *supra* note 235; Hal Finney, *Detecting Double-spending (long), available online URL* http://ganges.cs.tcd.ie/mepeirce/Project/Double/dsarticles.html.

244. The odds of two customers choosing the same serial number are remote if the bank requires that customers choose sufficiently large (e.g., 100 digit) random numbers. When it does happen, it should produce an interesting lawsuit.

245. *See DigiCash, Ecash and Crime, available online URL* http://www.digicash.com/ecash/aboutcrime.html.

246. Markus Jakobsson & Moti Yung, *Revokable and Versatile Electronic Money, available online URL* http://www-cse.ucsd.edu/users/markus/revoke.ps.

247. *Id.*

248. *Cf.* Froomkin, *supra* note 6 (discussing Clipper chip).

249. *See* Ernie Brickell et al., *Trustee-based Tracing Extension to Anonymous Cash and the Making of Anonymous Change* (Sandia National Labs print, on file with author, copies available by e-mail from psgemme@cs.sandia.gov).

the true—not the blinded—serial number.[250] Alice can now spend the coin in Bob's shop as if it were a basic coin. In the absence of anonymous bank accounts, Bob must still disclose his identity to redeem the coin. (If for some reason Alice later wants to "stop payment" on the coin because Bob defaulted, she can always reveal the true serial number to the bank.[251])

Like a basic coin, however, the blinded coin is just digitized data. Since the blinding process means that the bank cannot trace the coin's serial number to Alice, some means is required to convince her not to run off and duplicate coins. Preventing double-spending is relatively simple for an on-line clearing system; preventing Alice from cheating a system that relies on off-line clearing is more difficult.

a. Preventing Double-Spending of Blinded Coins With On-Line Clearing (DigiCash)

When Alice spends a blinded coin and Bob presents the coin to the bank for settlement, the bank cannot link the coin to Alice because it has no record of the coin's serial number. Without some means of preventing double-spending, the temptation might be more than Alice could resist. On-line clearing removes all temptation. Since the bank keeps a record of every serial number redeemed, it can check the coin proffered by Bob against the master list. If the coin was previously spent it denies payment. As the clearing is on-line, Bob then is able to tell Alice that the bank has refused to honor her coin, much like a merchant will tell a customer that a credit card company has refused to authorize a purchase.

On October 23, 1995, Mark Twain Bank of St. Louis, Missouri became the world's first financial institution to issue blinded digital coins backed by value. The bank uses software licensed from DigiCash.[252] The system relies on on-line clearing of blinded coins, but de-

250. "The blinding operation is a special kind of encryption that can only be removed by the party who placed it there. It commutes with the public key digital signature process, and can thus be removed without disturbing the signature." *DigiCash, An Introduction To Ecash, available online URL* http://www.digicash.com/publish/ecash_intro/ecash_intro.html#flow; *see also* Brands 1993, *supra* note 236, at 4; Chaum, *supra* note 235; David Chaum, *Security without Identification: Card Computers to Make Big Brother Obsolete, available online URL* http://www.digicash.com/publish/bigro.html.

251. Chaum, *supra* note 235; David Chaum et al., *Untraceable Electronic Cash, in* ADVANCES IN CRYPTOLOGY—PROCEEDINGS OF CRYPTO 88 at 319 (1990).

252. *See* Mark Twain Bank, *First Bank to Launch Electronic Cash, available online URL* http://www.marktwain.com/press1.html. Bank customers download software to hold their coins on their PC. *Id.*

tails of the technical specifications of the system were limited at the time this article went to press.[253] Other financial institutions are likely to be providing similar electronic cash services in the near future. For example, DigiCash has licensed its software to the Swedish Post Office, which owns the retail bank that transacts with accounts held by seventy-five percent of Swedish households.[254]

b. Preventing Double-Spending of Blinded Coins With Off-Line Clearing

On-line clearing is potentially expensive in both time and money. Off-line clearing is usually much cheaper in both. Unfortunately, off-line clearing creates an opportunity for an unscrupulous party to spend the same coin many times since the party accepting the coin will not know it has been spent until it is too late.[255]

Bob's risk that the coin offered by Alice will prove to be worthless is greatest when neither Bob nor the bank knows who Alice is, since Alice will reasonably believe that her anonymity protects her from the consequences of her double-spending. Even if Bob knows Alice's identity but the bank does not, Bob bears considerable risk when the costs of making Alice pay would be greater than the value of the debt. This may include a large set of transactions if Internet commerce becomes global. Nevertheless, if Alice is aware that Bob or the bank knows her identity, she can reasonably fear that Bob might report her to the appropriate authorities, perhaps for criminal prosecution, which should reduce the temptation to double-spend.

The essence of a blinded coin is that the bank does not know the coin's serial number, and hence cannot deduce the payor's identity when the coin is presented for redemption by the payee. In both the basic coin model and the standard blinded coin model, the coin carries no information about Alice. It is possible, however, to encode information about Alice's identity in such a way that if the coin is spent only once the information remains encrypted on the coin. If someone tries to spend a coin that has previously been redeemed, the second spending will disclose the information encoded on the coin about its original

253. Digicash and Mark Twain Bank have promised to make a technical description of the system public. Full details should be *available online URL* http://www.digicash.com/ecash/protocol.html by the time this article is published.

254. Mark Twain Bank, *supra* note 252.

255. *See supra* text following note 236. There is no danger that Alice will just make up a data stream and claim it is a coin, since Bob can check the bank's digital signature.

owner.[256] This system works even if Alice spends the coin with two different merchants.

The second spending can only reveal whatever identifying information the bank encoded into the coin at the time it gave the coin to Alice. The issuing bank is responsible for choosing to encode sufficient information, e.g., a unique identification number, to allow it to trace the coin back to the customer. The bank, however, has a problem: the bank cannot read the information about Alice's identity encoded onto a blinded coin unless Alice spends the coin twice. In other words, the blinding prevents the bank from inspecting the coin at the time of issuance to ensure that Alice has in fact supplied the required information. The bank can, however, use probabilistic methods that make it very likely that Alice will encode her identity on the coin at the time the bank issues the coin. For example, the bank might require that Alice generate a hundred blinded numbers and associated encrypted data fields. The bank could then require that Alice reveal the contents of ninety-nine coins of the bank's choice. If all of these coins turn out to have the proper information about Alice, the odds are good that the 100th coin—the only one that will actually be signed by the bank, and the only one for which Alice does not reveal the contents—does too. If Alice tries to cheat by inserting missing or erroneous information into even one of the 100 coins, the odds are good that the bank will detect it. And if the bank detects attempted cheating, the bank will probably refuse to issue digital coins to Alice ever again.

---

256. Chaum and his colleagues have developed a challenge-response protocol in which the bank asks the person redeeming a coin a mathematical "question" that reveals no identifying data if a coin is being spent for the first time. *See* Chaum, *supra* note 235; *see also* Chaum et al., *supra* note 251; Ecash Homepage *available online URL* http://www.digicash.com/ecash/ecash-home.html.

Brands has developed a complicated "cut and choose" protocol that protects Alice's identity if Alice spends the coin once, but creates a very significant probability that multiple spending will reveal her identity if the parties who have been given the same coin can compare notes. This protocol is better suited to off-line clearing systems than the basic DigiCash model, but it still requires that the victims of multiple spending be able to communicate with each other or the bank reasonably frequently. *See* Brands 1993, *supra* note 236, at 4-5. If the coin is spent a second time, however, a second reply to the question elicits an answer that, when combined with the answer given on first spending, reveals sufficient data for the bank to identify the party to whom it originally gave the coin. *See* Chaum, *supra* note 235. Hal Finney's excellent, brief, but somewhat mathematical explanation of Stefan Brands' optimizations to this procedure can be found *available online URL* http://ganges.c.tcd.ie/mepeirce/Project/Mlists/brans4.html.

Information about the payee can also be encoded on a coin when it is spent, although this is not a necessary part of the protocol.

In an off-line clearing scheme, Bob's security against double spending rests on a challenge-response protocol that discloses Alice's identity if she tries to double-spend. Bob thus bears some risk of being stuck with the digital equivalent of a slug in the vending machine because Alice may have spent the coin elsewhere before he gets it to the bank. Unlike the slug in the vending machine, however, the coin can contain information that identifies Alice to the bank. Whether this suffices to find Alice and get civil or criminal remedies depends on whether the information on the coin is accurate and on the jurisdictions involved.

It may be that blinded coins cannot safely be issued in denominations of any significant size in the absence of an efficient on-line clearing system; Alice could spend even a $1 coin many times in a few minutes and then attempt to vanish.[257] However, if the denomination is small enough, Bob can limit his risk if he checks every small-denomination coin Alice offers to make sure that it is not a duplicate of a coin he has personally received in the past, and makes sure to contact the bank for verification whenever he has received as many coins as he cares to risk holding.[258]

c. Preventing Double-Spending of Blinded Coins With Electronic Wallets

In order to feel confident about issuing blinded coins, banks are likely to require considerable assurance that the coins cannot be spent more than once; banks may also want to minimize the chances of third-party money laundering in order to avoid difficulties with national regulatory authorities. From the bank's point of view it may be cold comfort to be able to identify the person who spent a coin a million times if that person cannot be found.

An electronic wallet is a smart card with a microprocessor on it. The wallet interacts with specially designed card readers, somewhat like bank cards are used in Automatic Teller Machines. Embedding the coin, or at least part of the information needed to use the coin, in a smart card with tamper-resistant features provides greatly added security if the tamper-resistant part of the card is programmed to prevent

257. Brands 1993, *supra* note 236, at 4-5.

258. *See, e.g.*, Shamir et al., *supra* note 220 (describing payword and micromint, two new efficient off-line clearing systems).

double spending.[259] Banks, merchants, even personal computers, might have the necessary smart card readers.

One extension of this model requires that the tamper-resistant part of the card have an electronic "observer" whose participation is required to spend a coin. The combination protects Alice's privacy by having all communications from the observer go via Alice's computer which is programmed to ensure that no transaction details are disclosed. If anyone breaks the tamper-resistance and attempts to double-spend, the blinded coins protocol still applies and the identity of the coin's original owner is revealed.[260] Perhaps the best example of this is the Conditional Access for Europe (CAFE) project, being sponsored by the European Union's ESPRIT program. The CAFE protocol promises to offer high security for the customer, a chance of getting unspent money back if the purse is lost, and payer (but not payee) privacy; so far, however, no actual CAFE products exist beyond prototypes.[261]

4. The Traveler's Check Model

Coin-based digital cash systems have problems with exact change. Digital coins are not divisible without sacrificing customer privacy and also making the payment system much less efficient to operate.[262] Indivisible coins ordinarily have to be aggregated to get the amount needed for a purchase, just as dimes and pennies might be combined to make a 23-cent acquisition. If coins are in small denominations, a large number of coins may be required to buy anything even moderately expensive. At some point, processing a large enough number of coins can introduce transmission delays and information processing costs. If the coins are to be carried on a smart card, large numbers of coins require a card with a larger memory, which increases the investment required to participate in the system.

---

259. Brands 1993, *supra* note 236, at 5-7. One way to look at this is that the electronic wallet model places the blinded coin in a digital purse. *Cf.* Brands 1993, *supra* note 236, at 2; *infra* text accompanying note 264 (describing digital purse).

260. Brands 1993, *supra* note 236, at § 2.2.

261. *See* Jean-Paul Boly et al., *The ESPRIT Project CAFE—High Security Digital Payment Systems* (1994), *available online URL* http://www.informatik.uni-hildesheim.de/FB4/Projekte/sirene/publ/BBCM1_94CafeEsorics.ps; *see also CAFE—Conditional Access For Europe, available online URL* http://www.informatik.uni-hildesheim.de/FB4/Projekte/sirene/projects/cafe/index.html; *The CAFE Project, available online URL* http://www.cwi.nl/cwi/projects/cafe.html; *Digicash, DigiCash products—the CAFE project, available online URL* http://www.digicash.com/products/projects/cafe.html.

262. *See* Brands 1995, *supra* note 232, at 8.

Whatever the price of the good being purchased, Bob needs to provide change if Alice does not happen to have the exact coins required. Thus, Bob needs to have a stock of coins on hand to pay Alice (recall that all coins must be returned to the bank each time they are spent), and Alice needs to be able to deposit coins in the bank as well as withdraw them.

In contrast, an electronic traveller's check system allows Alice to spend each check for any amount up to a predetermined maximum. The bank debits Alice for the maximum value when the check is created, and refunds Alice the difference between the maximum and the amount actually expended. If the check system relies on "blinded" checks, akin to blinded coins, it is possible to design the refund system so that when Alice presents the unexpended portion of the check for a refund, nothing in the refund request itself (other than the amount requested) gives the bank any information that would allow it to link the refund request to a particular payment.[263] Unlike traveller's checks, competitive pressures might force banks to pay some interest on the funds set aside to cover the check.

5. *The Electronic Purse (Mondex Money)*

The electronic purse is a smart card or a computer program that holds and keeps track of the owner's electronic funds balance, much as a copy card or a telephone card stores value. If the purse is on a smart card, the card can be used either with ATMs or with specialized card readers attached to computers or telephones. In the pure implementation, no backups exist: if the card is lost, or the computer disk crashes, the consumer's money is as gone as if a dollar bill were burnt—but the bank gets to keep it.[264] An electronic purse can be designed with whatever privacy, or lack of privacy, the manufacturer desires. If the smart card functioning as the electronic purse has sufficient storage, the card can keep track of every transaction that it touches; the purse can be designed so that this information is accessible only to its owner, or it can be designed so that the information is accessible to others, such as the issuing bank or law enforcement. Similarly, the ATMs and

263. Brands 1993, *supra* note 236, at 50-52. The danger of "linking by complementary amounts" is reduced if a customer groups refund requests together. *Id.* at 52.

264. *See* Mondex, *If My Card is Lost or Stolen, Do I Lose the Money on It?*, *available online URL* http://www.mondex.com/mondex/lost.htm. If the smart card has some form of password protection, then a stolen card is of little value to a thief, *id.* unless the thief can somehow guess or extort the passphrase.

card readers that the smart cards need to communicate with each other and with the bank can also be programmed to keep track of every transaction, but do not have to.

One example of the electronic purse concept is the Mondex system currently being field tested in Swindon, England by a joint venture of NatWest and Midland Bank, in cooperation with British Telecom.[265] The Mondex card is unusual in two respects. First, it is designed to hold up to five different currencies on a single card; second, and more important, it allows direct peer-to-peer fund transfers, without the intervention of a bank.

Little is publicly known about the mechanics of the Mondex system. Mondex representatives have stated that the company intends to restrict information about the workings of its cards, including its public key and the algorithm used, in order to make life that much more difficult for anyone who would be tempted to try to hack the system. The company has stated that it uses digital signatures to distinguish an authentic Mondex transaction from a fraudulent one,[266] and that each card will carry two security systems, one of which will be changed every two years in series.[267] Each card also carries a unique 16-digit identifier that links it to the person who purchased it.[268] The Mondex system has, however, been criticized for relying too heavily on the tamper-resistance of the smart card. According to Mondex's competitors, if an attacker were to manage to break the tamper-resistance of the device, he would be able to introduce new money on the card virtually at

---

265. On the English field test, see, e.g., Leslie Helm, *Cashless Society Gets Closer With Plans For Electronic Currency*, L.A. TIMES, Sept. 6, 1995, at D4, and *Revenue to accept Mondex: Tax payments*, FIN. TIMES, July 8, 1995, at 4 (noting that British tax authorities plan to accept payment via Mondex). On a far more modest U.S. trial, see Jeffrey Kutler & Valerie Block, *Mondex Gains U.S. Foothold With Smart Card Test at Wells*, AM. BANKER, Aug. 3, 1995, at Credit/Debit/ATMs 1 (describing issuance of 90 cards to Wells Fargo Bank employees).

Although the Mondex system appears to be the closest to market in the English-speaking world, "Portuguese banks launched a national electronic purse in February, and more than 500,000 cards are expected to be issued this year." Richard Wolffe, *Banks Unzip The First £20m 'Electronic Purse'*, FIN. TIMES, July 3, 1995, at 5.

266. Mondex, *How Secure is Mondex?, available online URL* http://ww.mondex.com/mondex/secure.htm.

267. Tim Jones, Mondex Chairman, *Security and Security Policy in Internet Payment Systems*, Remarks at Worldwide Electronic Conference, Bethesda, MD (Nov. 19, 1995) [hereinafter Jones Remarks].

268. Mondex, *What About Privacy?, available online URL* http://www.mondex.com/cmondex/anon.htm.

will. And if the system of breaking the cards were to be widely published, the issuing bank would be helpless.[269]

Exactly how much privacy the Mondex card provides the user is a subject of considerable dispute. The Chairman of Mondex has stated that the company has not yet decided how much transaction logging the card will do when it graduates from field tests to commercial use. Meanwhile, Simon Davies, a Visiting Professor of Law at Essex University, a well-known privacy advocate and gadfly, has alleged that Mondex card readers keep records of up to the last 500 cards used in the reader, despite Mondex's claim that the cards are as anonymous as cash; Professor Davies has filed a false advertising complaint with the UK Trading Standards Board.[270] Mondex states that the card itself keeps a record of the last ten transactions;[271] there have been allegations that the card is designed to download this information to the central bank every time the card is placed in an ATM.[272]

Digital purses with currency that does not have to be cleared through the issuing bank raise a number of intriguing regulatory problems beyond the scope of this article. Among them are: (1) what regulations might be appropriate to reduce the harmful consequences of the "meltdown scenario" in which someone cracks the security of the electronic smartcards and begins minting her own apparently legitimate digital cash; (2) how to prevent smart cards from becoming a tool of money laundering; (3) how to monitor issuing banks to ensure that they do not issue more card-based currency than customers have actually purchased; (4) transborder regulatory questions including consumer protection, the role of non-bank banks in foreign markets, possible loss of seignorage, and bank exposure to multiple and differing concepts of escheat.[273] More than any other implementation of electronic cash, digital purses such as Mondex threaten to erode the control

269. *See* Stefan Brands, *Centrum voor Wiskunde en Informatica (CWI), Off-line Cash Transfer by Smart Cards* 2 (1994) (CS-R9455), *available online URL* http://www.cwi.nl/ftp/brands/CS-R94tt.ps.Z; Steven Levy, *E-Money*, WIRED, Dec. 1994, at 174, 177 (quoting David Chaum).

270. Gavin Clarke & Madeleine Acey, *Mondex Blows Users Anonymity*, NETWORK WK., London, Oct. 25, 1995 at 1.

271. *Id.*

272. There have been suggestions that the system is programmed to copy this information, and the card's internal error log, every time a card is used to contact the bank. "Rev. Mark Grant," Mondex, 18 July 1995 (posting to cypherpunks@toad.com).

273. *Cf.* European Commission, DGXV, *Study on the legal and regulatory aspects of the issue and use of pre-paid cards (multi-sector electronic purses and wallets), available online URL* http://www.cec.lu/en/comm/dg15/paystud.html (describing planned study).

of central bank authorities over the money supply.[274] Central banks appear to be concerned: "although none of the central banks have pointed the finger at [Mondex] by name, one governor [of the European Monetary Institute] delivering a recent speech on the subject in his native language reportedly dropped into English to declare: 'Purse to purse, No!'"[275]

When Alice pays Mondex to put money on a smart card, the transaction increases the money supply until the credit is redeemed. Unlike other payment schemes such as checking accounts, travellers checks or even digital coins, the Mondex scheme allows, even encourages, participants to refrain from redeeming stored value at the bank. The Mondex card's ability to transfer value from one card to another thus increases the effective money supply.[276] When Alice puts $10 into her checking account, the bank has use of the money (and Alice has a claim on the bank), but Alice does not have the use of the money[277] until she takes it out again. The only time when the bank and Alice both have the use of that $10 is during any float period between when Alice writes a check and the bank honors it.[278] Furthermore, advances in technology have been reducing this float period compared to the past; debit cards eliminate it. In contrast, when Alice purchases $10 worth of credit for her Mondex card, the bank has the use of the $10 (and Alice has a claim on the bank), but Alice also has the use of a

274. The effect will be within the power of central banks to control so long as Mondex money is issued by banks whose reserve requirements can be increased. *See supra* note 240. If, however, Mondex money were to be issued by a poorly monitored non-bank financial institution or one not subject to reserve requirements, the effect on the money supply could become more pronounced.

275. Paul Rodgers, *Banks in Cash Card Warning; Fears of Abuse by Forgers and Money Launderers*, THE INDEPENDENT, July 9, 1995, at B1.

276. Interestingly, if the issuing bank treats the transaction as a purchase of digital cash, rather than a deposit, then there is no need for an abeyance account, or even deposit insurance. Aside from issues of risk management if there is a run on digital cash or a catastrophic failure of the card encryption scheme, it would seem the bank might be able to escape the effects of abandoned property laws that require untouched accounts to escheat to the state after a period of time. A lost Mondex card is thus pure profit to the bank. *See* Richard Field, *Re: E-Cash: Mondex*, e-mail to list e-cash@nptn.org, 18 Aug. 1995.

Nevertheless, whether the transaction in which a customer exchanges pocket cash for digital cash counts as a "deposit" to the bank or a "sale" of a product by the bank is of little macroeconomic relevance if the central bank is able to adjust reserve requirements to require banks to hold reserves for any digital cash they issue.

On the other hand, the Chairman of Mondex has suggested that the loss of seignorage alone will cause governments to nationalize his operations within 20 years. Jones Remarks, *supra* note 267.

277. Unless Alice is a business with a floating charge on her account, in which case she has in effect borrowed against it.

278. This is a short period. *See generally* 12 C.F.R. § 236 (1995).

$10 store of value. If she purchases something from a merchant who does not return the funds to the bank, but instead either holds the funds or makes another purchase, the money supply has effectively increased because the same $10 is circulating as money on the card and as money that the bank can loan out in its customary manner.[279] An unscrupulous bank, or one based in a country that enjoys a very relaxed regulatory regime,[280] might become tempted to "mint" its own unbacked electronic funds, which it might loan to customers, or use to meet its own obligations. If electronic messages stored on smart cards are not considered "money," however, such actions might even comply with banking laws.

C. *Regulation of Digital Cash*

The policy-maker's perspective on digital cash generally and anonymous digital cash in particular is complicated by uncertainty about the capabilities of the technologies, on the market's reaction to them, and on their effect on privacy and law enforcement. The policy-maker's task is further complicated by the multiple and sometimes conflicting objectives that her policy might be designed to serve.

1. *The Privacy Calculus*

The effect of a digital cash system on privacy depends on which system is used and, often, the details of how it is implemented. The systems canvassed above range from privacy-destroying to having a mixed effect on privacy. The major privacy-enhancing feature offered by any of these systems as compared to traditional cash is that transactions under most schemes need not be face-to-face, a potentially significant privacy advantage given the prevalence of in-store video cameras. Ordinary cash itself, after all, is less than completely anonymous since it is usually exchanged in person, bears a unique serial number, carries fingerprints, and can easily be marked for identification.[281]

279. Note that this is a wholly separate and potentially larger effect than the relatively trivial effect that electronic cash which is cleared might have on the velocity of money.

280. Mondex has signed agreements with banks in Hong Kong, Canada and the United States. None of these jurisdictions is notorious for its relaxed banking regulation, but Hong Kong will become part of the Peoples Republic of China in 1997.

281. Indeed, the technology now exists to track the movement of unmarked bills through the banking system simply by recording their serial numbers. E-Mail from John Gilmore to Michael Froomkin (19 Sept. 1995) (on file with author).

Some digital cash models compare favorably to plastic debit and credit cards; others are no better. The debit card model of digital cash creates a complete accounting record of all transactions. Blinded digital coins provide more privacy than ordinary credit cards, since credit cards create a complete transaction record that is accessible to the issuer; blinded digital coins provide payor, but not payee, anonymity.

In the absence of an installed base of smart card readers on personal computers, digital coins in tiny denominations appear most suited to Internet information commerce.[282] Arguably, the basic digital coin "does not deserve to be called cash . . . because it lacks the distinguishing characteristic" of ordinary money—its anonymity.[283] As each transaction is cleared with the bank it leaves a record. In contrast, blinded cash protects the anonymity of the payor, but not the payee. At this writing, only one financial institution offers blinded digital cash backed by ordinary currency.[284] Even blinded coins or checks only anonymize payments, not receipts. In fairness to digital cash, however, it should be noted that paper money is not as anonymous as it may seem. Large transactions in paper currency often trigger reporting requirements designed to detect money laundering.[285]

Truly anonymous digital cash would be possible with an anonymous bank account. If the bank account is anonymous, then withdrawals and deposits cannot be traced to the owner. Digital cash would actually enhance transactional privacy if banks that support digital cash become willing to open anonymous accounts, and to accepts deposits in digital cash. In this scenario, anonymous bank accounts, combined with anonymous purchases and payment, would be even more private than

---

282. *See supra* note 220.

283. Finney, *supra* note 243.

284. *See supra* text accompanying note 252 (discussing Mark Twain Bank).

285. 28 U.S.C. § 6050(i) (1995) requires any person who receives more than $10,000 in cash in the course of a trade or business to file a Form 8300 declaration stating the cash payor's name and other identifying information. This requirement applies to all transactions, even payments to lawyers, and has survived constitutional challenges that it pierces the client's Sixth Amendment right to consult a lawyer anonymously and the client's Fifth Amendment right to consult counsel without self-incrimination. *See, e.g.*, United States v. Goldberger & Dubin, 935 F.2d 501 (2d Cir. 1991). *But see* United States v. Gerner, 5 F.3d 963 (1st Cir. 1995) (denying summary enforcement of summons against law firm on grounds that District Court finding that tax proceeding was pretext for anticipated investigation of client was not clearly erroneous). Federal law requires a U.S. bank involved in a cash transaction exceeding $10,000 to file a report with the Secretary of the Treasury. *See* 31 U.S.C. § 5313(a) (1995), 31 C.F.R. § 103.22(a) (1995). Federal law also makes it illegal to break up a single transaction above the reporting threshold into two or more separate transactions for the purpose of evading the reporting requirement. 31 U.S.C. § 5324(3) (1995). *But see* Ratzlaf v. United States, 114 S. Ct. 655 (1994) (reading strict scienter requirement into statute).

cash, since both the seller and buyer could mask their identity.[286] Even if a bank wanted to offer this service, regulatory authorities would be likely to oppose it.

The electronic purse's effect on privacy is particularly sensitive to how it is implemented. Electronic purses are the only system described above that are designed to allow peer-to-peer funds transfers without requiring the parties to contact a third party. Mondex cards and card readers could be configured to do little transaction logging, which would make them possibly more private than cash, or the hardware could capture and record every transaction. At present, however,

---

286. In earlier drafts I suggested that, regardless of the regulatory environment, even a bank willing to issue anonymous digital cash would be highly unlikely to allow anonymous accounts unless its clearing system was on-line. On-line clearing would allow the bank to prevent double-spending; off-line clearing, I suggested, would leave the bank vulnerable to an infinite amount of respending of the same coin since the anonymous account holder would know that the bank did not know her identity and would know that coins would only be cleared after a transaction was over.

As this article was in proofs, I received e-mail from Stefan Brands, one of the leading developers of digital cash protocols, in which he described an unpublished system he has invented that protects a bank wishing to engage in off-line clearing of anonymous digital cash issued to anonymous bank accounts. Under this protocol, the bank faces no more risk of multiple spending than if it issued "blinded" digital cash to an ordinary account with an identified account holder.

Brands's protocol works as follows:

1. Alice contacts the Bank. She identifies herself to the Bank's satisfaction and provides the Bank with a unique public key that she will use to identify herself in future communications.

2. The Bank issues Alice with a signed blinded credential (for a description of the "blinding" protocol, *see supra* § III.B.3) that I will call a "ticket". The ticket has information about Alice's real identity, but the Bank cannot access that information in a computationally feasible manner unless the ticket is used to open more than one account or a coin backed by that ticket is double-spent.

3. Alice waits while the Bank issues similarly blinded tickets to other people. When there are enough other tickets in circulation, e.g. issued but not used, so as to fog her identity, Alice contacts the Bank anonymously and presents her ticket. The Bank opens an anonymous account, keeping the ticket on file instead of the normal customer information. (Alice could, of course, give the ticket to anyone else, and the Bank would be none the wiser, but since the Bank will be able to seek redress from her if coins issued to the account are double-spent she has a strong incentive not to do this.)

4. Alice purchases coins anonymously using funds in her anonymous account. Each coin issued to her encodes sufficient information about Alice's ticket that if the coin is double-spent it not only reveals the ticket, but also allows the Bank to decrypt the ticket and learn Alice's identity. Nevertheless, no matter how many coins Alice single-spends, the Bank cannot in a computationally feasible manner get this information. Furthermore, there is nothing that the first recipient of a coin, or the bank holding a coin, can do to make it appear a coin was double-spent. *See* E-mail from Stefan Brands to Michael Froomkin, 15 May 1996 (on file with author); E-mail from Stefan Brands to Michael Froomkin, 20 May 1996 (on file with author).

Anonymous digital cash that can be purchased from anonymous accounts and cleared off-line has many interesting possible applications. These coins could, for example, serve as anonymous digital postage stamps. The stamps could be used to compensate remailer operators for remailing anonymous communications. Without some means of compensation, few people are likely to be willing to operate remailers if there is any risk of liability for carrying anonymous messages. *See supra* text accompanying notes 88-94.

Mondex is not well-suited to an Internet payments mechanism because personal computers have no means of accessing Mondex cards without expensive and rare connective hardware. Furthermore, as currently designed, the Mondex system is vulnerable to a "man in the middle" attack when the transacting parties are not face-to-face, making the system more suited to in-store transactions than to Internet transactions.[287] One can imagine ways to use electronic purses to enhance privacy, such as adding value from vending machines paid with ordinary cash; but so long as the card itself is not anonymous, and so long as all cards keep even limited records, the card provides less privacy than traditional cash.

2. *Regulatory Policy Goals and Practical Constraints*

All governments and central banks have an obvious interest in retaining control of the money supply. Central banks should be able to achieve this objective by taking three related steps: (1) Ensuring that issuers of digital cash are subject to the rules that apply to existing, regulated, financial service providers. One simple, if restrictive, means of achieving this would be to limit digital cash issuance to banks. (2) Adjusting reserve requirements to neutralize the effects of changes in the stock of pocket cash.[288] (3) Taking whatever steps are possible to reduce the likelihood of the "meltdown scenario" in which someone cracks the security of a digital cash scheme. All these steps are equally applicable whether or not the digital cash is anonymous.

Whether the U.S. or other governments will choose—or should choose—to regulate anonymous digital cash is more complicated. Citizens are likely to feel, with some reason, that their governments should help create the conditions that make it possible for them to protect their privacy. Data protection laws or changes in property rights over information might contribute to this, but they are uncertain at best. And once information privacy is lost it is difficult to regain as there is almost no way to recall data that are in wide circulation.

On the other hand governments have an interest in preserving their ability to enforce existing laws and regulations, such as tax collection and laws against fraud and illicit transactions. Furthermore, as the

287. Jones Remarks, *supra* note 267. In a man in the middle attack, Mallet inserts himself into the communications channel between Alice and Bob. He relays all of Alice's messages to Bob and vice versa until Alice sends Bob the Mondex money; Mallet sends Bob random and worthless data and walks off with the cash.

288. *See supra* text at notes 240-41.

enforcer of moral values that have been embodied in legislation or, in some cases, as tyrant, governments may desire to control the purchase or movement of information and of funds. Governments are likely to believe, not without reason, that their enforcement abilities would be threatened by the widespread deployment of anonymous digital cash, although traceable digital cash might often make their work easier.

Only fully anonymous digital cash stands much chance of aiding in financial crimes such as money laundering or tax evasion.[289] Banks will continue to have records of the amounts withdrawn by their clients and will know who is depositing digital cash. Law enforcement will, however, have less information than they would have when tracing a wire transfer, since a wire transfer links payor and payee to a single transaction. In contrast, a DigiCash transfer, for example, does not allow the bank or the police to link the two halves of the transaction. Nevertheless, anyone depositing DigiCash to a bank must disclose their identity, just as they do when depositing cash. Indeed, most digital coins make money laundering more difficult than does traditional cash, since digital coins must be returned to the bank after every expenditure. Similarly, in its current form a Mondex card is unlikely to be of much value in money laundering. Even if Mondex cards do not keep transaction records, the value that can be encoded on a card is likely to be limited to $500 or £500.[290] To the extent the government is concerned about these issues, they point towards either outlawing fully anonymous cash, or otherwise complicating its deployment; one means to achieve this is to tilt the regulatory playing field towards forms of digital cash that are not fully anonymous and hope that they achieve market dominance.

---

289. Although the implications of anonymous transactions for taxes, product liability, and copyright, remain to be worked out, it seems to me likely that the effects will be unevenly distributed. I do not believe that the tax system will be deeply affected, since most production and even more consumption involves transactions that are easily monitored for tax compliance. Furthermore, any transaction that encounters the banking system—for example, deposits placed on short-term interest—will be easily traceable for tax purposes so long as the bank is located in a jurisdiction that enlists banks as enforcers of its, or its treaty-partners', tax rules. My income, for example, comes from a salary paid by an institution that has no incentive to make it easy for me to engage in tax avoidance. My house is plainly visible from the street, and as easily taxed as it can be linked to me. Most of what I buy is tangible—things like groceries, diapers and shoes—and can easily be taxed under a VAT system if our current tax system should show signs of collapse. Though some knowledge workers may be able to demand that payment be routed to accounts held at untaxed offshore addresses, thus causing an effect at the margin, these schemes seem likely to remain relatively small in comparison to traditional, more easily taxable, forms of labor and compensation for the foreseeable future.

290. Jones Remarks, *supra* note 267.

Governments have considerably more power to reduce the liquidity, acceptability, and utility of anonymous digital cash than they do to cut off the flow of anonymous speech. Unlike anonymous speech, which does not require any willing parties inside the country other than a single speaker or listener, anonymous cash requires at least two parties, the buyer and seller, and often also involves a trusted third party as well.[291] If anonymous digital cash is banned by a government, many corporations active in that jurisdiction will be reluctant to use it because they are subject to audit and disclosure requirements, and have assets to lose if subjected to civil or criminal penalties. At a minimum, a ban would raise the cost of using anonymous digital cash, perhaps to the point where few people were willing to trade in it. Even a refusal to enforce contracts or debts based on the exchange of anonymous currency would have a significant deterrent effect.

Widespread use of Internet-tradable digital cash might internationalize money. That day seems far away, if it will ever come; to date, even the Mondex card, the most self-consciously international digital cash to be field tested, is linked to national currencies (up to five on one card). In principle there is no reason why, given the international nature of the Internet, its unit of account needs to be pegged to a particular currency.[292] Trading in Internet-provided information, perhaps starting with micro-charges for access to web pages, is ideally suited to a new unit of account, used initially for the internet only. If the issuance of the new monetary unit—perhaps it could be called the "bit"?—could be designed so that the money supply grew at the right speed, one would eventually expect to see transactions in which bits were exchanged for traditional currencies.[293] Amusing as these speculations can be, practice and prudence suggest a different outcome.

Internationalized cash would suffer from a number of serious problems that would have to be resolved before it would be safe to rely on it. First, there is the question of who would issue it. If a single digi-

---

291. *See generally* Froomkin, *supra* note 228.

292. For one slightly over-enthusiastic suggestion that digital cash will not only internationalize money but that private currencies will crowd out national currencies, see Giles Keating, *Electronic Money Is In Race With Emu*, FIN. TIMES, Nov. 2, 1995, at 15.

293. Indeed, there are currently markets in CyberBucks, the currency issued by CyberCash for its test of its software. *See Ecash Market, available online URL* http://www.c2.org/~mark/ecash/ecash.html; *see also Electronic Cash Marketing Mailing List, available online URL* http://www.ai.mit.edu/people/lethin/ecm.html. On November 24, 1995, one shop offered to pay $5 for 100 cyberbucks and offered to pay 100 cyberbucks for $8. *FireCloud Solutions EShop, available online URL* http://www.firecloud.com/eshop/eshop.htm (accessed on Nov. 24, 1995, printout on file with author).

tal currency were to become an international standard, it would require either a central bank or at least an agreed, enforceable, mechanism for controlling the minting of currency. This sort of centralization is unlike the Internet as we know it. More likely, individual issuers around the world would agree on a common protocol for the issuance of "bits," and international banking would be plunged into an electronic repeat of the pre-Civil War financial system. Before the central bank centralization of the mid-19th century, banks commonly issued their own notes, and the discount applied to these notes varied according to the reputation of the bank (which affected the liquidity of the note), and usually the distance the note had travelled from the issuer.[294]

Whether internationalized or simply anonymized, Internet digital cash worries national authorities charged with preventing money laundering.[295] Digital cash is obviously more portable and mobile than ordinary paper currency. So long as funds must clear through a bank, and the payee is not anonymous, the effects of digital cash on money laundering control should be fairly low, since most existing money laundering rules require banks to know who deposits cash.[296] If, however, digital cash that does not have to be cleared through a bank (e.g., a Mondex scheme) becomes widespread, the ability of authorities to control money laundering will depend greatly on the extent to which the scheme allows authorities to trace the funds. The longer the memory on a smart card, and the more information it collects about the smart cards with which it transacts, the more incriminating that card will be if searched or captured by the authorities. Similarly, if smart cards are programmed routinely to dump the contents of their memories to the bank for auditing and verification purposes,[297] then banks will usually have databases that will meet the claimed needs of law enforcement.

If anonymous, untraceable, digital cash without expenditure limits were to be deployed, it would greatly increase the range of interper-

294. *See generally* BRAY HAMMOND, BANKS AND POLITICS IN AMERICA (1957); GLYN DAVIES, A HISTORY OF MONEY 460-61, 465-66, 471-85 (1994). For an extremely interesting discussion of the market mechanics of private notes, see David G. Ordel, *Private Interbank Discipline*, 16 HARV. J. L. & PUB. POL'Y 327 (1993); *see also* Martin S. Eichenbaum & Neil Wallace, *A Shred of Evidence on Public Acceptance of Privately Issued Currency*, FEDERAL RES. BANK OF MINN. QTRLY. REV. [unpag] (Winter 1995) (suggesting that Canadian experience with coupons suggests that private currency may be more acceptable to public then widely believed by economists and lawyers).

295. *See* MONEY LAUNDERING, *supra* note 202.

296. As a result, money launderers use false invoicing, overpricing goods to camouflage the cash flows being laundered. *See* MONEY LAUNDERING, *supra* note 202, at 9-10.

297. *See supra* text accompanying note 272 (allegations that Mondex scheme contains this feature).

sonal transactions that could be conducted anonymously, even if it did not become "a heyday for criminals."[298] One can imagine on-line fraud, in which a digital personality provides attestations from hundreds of satisfied customers, each of whom is nothing more than another digital personality created by the author of the fraud. While it is possible to envision sophisticated reputation systems that would reveal many such manufactured attestations, these do not currently exist, and might be cumbersome to use. Other unsavory possibilities include vastly simplified insider trading in securities transactions, the sale of corporate and personal secrets, blackmail and "perfect crimes."[299] Armed with untraceable digital cash, any transaction that Alice can persuade Bob to undertake for a digital payment can be commanded anonymously, with even Bob ignorant as to Alice's identity. Alice might be more willing to hire a contract killer, for example, if she felt secure that the crime could never be traced back to her; on the other hand, if Bob doesn't know who Alice is, he will demand payment in advance. Killer Bob might not be that interested in advertising his true identity either, which might make Alice unwilling to pay an anonymous stranger in advance.[300]

---

298. Benjamin Wittes, *Government Seeks a Way to Keep Tabs on Computer Cash*, THE RECORDER, Feb. 2, 1995, at 1 (quoting cryptologist Dorothy Denning's suggestion that anonymous cash would be a boon to crime); *see also* Scott Charney, Chief of the Computer Crime Unit, Criminal Division, U.S. Dept. of Justice, *Computer Crime* 9 (Nov. 28, 1994) (unpublished manuscript) (stating "one particular group—criminals—often seek[s] anonymity as well").

299. "Military-grade cryptography plus anonymous re-mailers plus fully anonymous digital cash plus bad guys equals perfect crime," Wittes, *supra* note 298, at 1 (quoting American Banking Association official).

In a perfect crime, Alice commits an act of extortion (e.g., blackmail or kidnapping). Instead of demanding small unmarked bills, Alice demands that Bob force a bank to issue blinded digital cash based on numbers contained in Alice's ransom note, and publish the result. Because the payoff occurs via publication in a broadcast medium such as a newspaper, Alice faces no danger of being captured while attempting to pick up the ransom. If Alice used the right blinding protocol only she can unblind and spend the coins. (Or for extra security, Alice can demand that the blinded coins be encrypted with a public key generated for the occasion.) And because the blinded digital cash is anonymous and untraceable, Alice is able to spend it without fear of marked bills, recorded serial numbers, or other forms of detection. *See* SCHNEIER, *supra* note 25, at 145; Sebastiaan von Solms & David Naccache, *On Blind Signatures and Perfect Crimes*, 11 COMPUTERS & SECURITY 581, 582-83 (1992) (describing the mathematical steps that must be followed in order to effectuate a "perfect crime").

300. Fortunately for Alice, but unfortunately for her target, crypto-anarchist philosopher Tim May has thoughtfully described a protocol for a system involving a mutually trusted (and also anonymous) third party who makes a business of selling escrow services and thus needs to maintain a good reputation, who facilitates such transactions by holding on to the money until the hit is verified. *See* Timothy C. May, *The Cyphernomicon* §§ 2.9, 2.13.9, 8.5, 16.16. (Sept. 10, 1994), *available online URL* ftp://ftp.netcom.com/pub/tc/tcmay/cyphernomicon (May's original version); *available*

In light of these possibilities, even if they are largely theoretical, it would not be surprising if many governments, including the U.S. government, wish to act to discourage or forbid the issuance and use of completely anonymous digital cash, at least forms that allow it to be exchanged in denominations higher than those proposed by Mondex. Although libertarians and advocates of increased privacy are likely to be disappointed, a decision to ban or discourage fully anonymous digital cash is likely to be politically acceptable in the U.S., for example, because it appears to extend the status quo to the digital age. Small cash transactions are largely anonymous today; neither large cash transactions nor most electronic transactions have any anonymity.[301]

A ban on the use of anonymous digital cash for ordinary tangible commerce appears likely to face few constitutional or practical obstacles *as applied to the sale of goods*. Even if the ban made anonymous purchases in tangible goods difficult or impossible, it would probably be constitutional because there is no generalized right to shop anonymously.[302] The constitutional difficulties arise when the same rules are applied to the sale of information, i.e., "speech." As explained below, a ban on anonymous digital cash could greatly obstruct the anonymity of speakers and readers.[303] The practical problems arise from the potential constitutional difficulties: there is no way to create anonymous digital cash that could only be used for commerce in information. Any regulation that aims to control the perceived evils of anonymous cash, e.g., money laundering and illicit trade, perforce impinges on anonymous speech as well.

IV. DATA COLLECTION AND PROFILING: TOWARDS THE ARGUS STATE?

The degree to which digital payment schemes, or the regulations constraining digital privacy schemes, alter user privacy gains significance in light of the revolution in data acquisition, processing and storage. Both public and private organizations are acquiring unprecedented abilities to build, sell, and use consumer profile data. Commerce in con-

---

online URL http://www.apocalypse.org/pub/nelson/bin.cgi/cypernomicon (hypertext version by 3rd party).

301. Governments also have it in their power, at least for the foreseeable future, to limit the use of small-denomination anonymous digital cash, or the use of any blinded digital coins.

302. One can imagine exceptions to the generalization in the text, e.g., there may be a right to buy books anonymously, and there is clearly a right to purchase a membership in an organization or make contributions to it without having the government require that the transaction be disclosed.

303. *See infra* Part IV.C.3.

sumer data is affected by the same technical developments that make digital commerce on the Internet possible—and by the existence of the Internet itself. Every transaction on the World Wide Web, for example, from catalog sales to information acquisition, can be recorded and archived by either party to it. As a result, the Internet could become the mother lode of consumer profile information; parallel developments in the public sphere make it increasingly feasible to monitor what citizens do and where they go. Combine the two, and there is little privacy left.

Databases erode the citizen's control over her personal information in several ways. Computerized records allow a firm to form a consumer profile based on the a customer's transactions with that company.[304] At a slightly more complex level, firms sell customer lists to each other, which may result in junk mail or increased information to the consumer, depending on one's perspective or good fortune. Meanwhile, in the U.S., social security numbers and driver's license numbers (often the same) have become de facto national ID numbers.[305] The most important part of the emerging database phenomenon, however, arises from the combination of the growth in computer processing power with the likelihood that routine personal data collection will soon become nearly ubiquitous. As the cost of data storage plummets, these trends will make it possible to assemble an individual data profile of extraordinary detail by cross-referencing multiple, extensive, databases.[306] These profiles have uses in commerce, in law-enforcement; some applications are benign, some less so.

In the marketplace the concerns arise because markets are imperfect, the consumer's ability to control the extent to which she is profiled are limited, and in an imperfect market profiling threatens to change the balance of power between consumers and sellers. In the public sphere, the concerns relate to chilling effects on the right to read, and the possibility that citizens' movements will be tracked by a combina-

304. This often results in improved service: our local pizza delivery service recently installed caller ID, and linked it to a computerized data base. When I call up, I am greeted by name, and I no longer have to spell the easily misunderstood name of our street.

305. For a short history of the use and abuse of social security numbers, see William H. Minor, *Identity Cards Databases in Health Care: the Need for Federal Privacy Protections*, COLUM. J.L. & SOC. PROBS. 253, 261-68 (1995). Other countries are, or are considering, permitting or requiring citizens to carry electronic national ID cards. *See, e.g.*, George Parker & Paul Taylor, *IT Review Could Lead to Citizens' Transaction Card*, FIN. TIMES, Nov. 9, 1995, p. 11 (describing British government study of multi-purpose "citizens' smart card" proposal).

306. *See* OSCAR H. GANDY, JR., THE PANOPTIC SORT: A POLITICAL ECONOMY OF PERSONAL INFORMATION (1993).

tion of Intelligent Transportation Systems, security cameras, and transactional data.

Despite the very real grounds for concern,[307] the existence of large, interlinked, databases is not inevitably bad for the consumer/citizen. Better, cheaper, information suggests that transactions costs may decrease leading to more efficient markets and increased consumer satisfaction. Some very consumer-friendly technologies, notably intelligent agents, use the consumer's behavior to anticipate her desires and select information that may be of particular interest.[308] And to the extent that public databases and monitoring will lower crime or traffic congestion, citizens benefit from an increased quality of life.

Under current ideas of property in information, consumers are in any case in a poor position to complain about the sale of data concerning them.[309] The alienation of this personal data may have occurred with the citizen's acquiescence. Every transaction has at least two parties; in most cases the fact of the transaction belongs equally to both parties.[310] As the existence of the direct mail industry testifies, both sides to a transaction generally are free to sell the fact of the transaction to any interested third party. Of course, there are exceptions. The parties may by contract provide otherwise, for example by agreeing to a confidentiality clause. And sometimes the law creates a special duty of confidentiality binding one of the parties, e.g., a fiduciary duty or a lawyer's duty to keep a client's confidence.[311] It seems safe to assume, however, that cases where confidentiality is the legal default are relatively rare. It also seems fair to suggest—although it could be debated—that at least in many consumer transactions the marginal value to the consumer of protecting a given datum will be lower then either the cost of negotiating a confidentiality clause (if that option even ex-

307. *See generally* GANDY, *supra* note 306; Gandy, *supra* note 210.

308. For an early prototype of such an intelligent agent, see Anderson Consulting, *Bargain Finder Agent Prototype, available online URL* http://bf.cstar.ac.com/bf/. Interestingly, several of the CD vendors being sampled by the agents adopted a strategy of "locking out" the agents to prevent their prices from being displayed in the prototype. Whether the non-cooperating stores' motive was to avoid excessive load on their Internet servers or to keep competitors from seeing their prices, or something else entirely, is unclear.

309. For an extreme example, see Moore v. Regents of Univ. of Calif., 793 P.2d 479 (Cal. 1990), *cert. denied*, 499 U.S. 936 (1991).

310. *See* Spiros Simitis, *From the Market to the Polis: The EU Directive on the Protection of Personal Data*, 80 IOWA L. REV. 445, 446 (1995) (noting traditional view, now retreating in Europe, that "data . . . were perfectly normal goods and thus had to be treated in exactly the same way as all other products and services").

311. *See* MODEL CODE OF PROFESSIONAL RESPONSIBILITY, Canon 4 (1995); MODEL RULES OF PROFESSIONAL CONDUCT Rule 1.6 (1995).

ists), or the cost of forgoing the transaction, or even the average value of protecting the datum when considered in conjunction with value of protecting all the other data concerning the consumer. Absent some change in the law to make consumers the default owners of the fact of their economic activity, the law gives them little recourse if they lack the market power or the resources to demand confidentiality clauses in the agora. Nor is it obvious that such a change in the law would be seen to comply with the First Amendment and with the U.S. tradition that "the government should not intervene in the marketplace of ideas in the absence of compelling needs,"[312] although I suggest below that someday the need may become compelling.

A. A Primer on Profiling

It is now possible to construct a consumer profile based on widely divergent types of data, to correlate and re-correlate information as never before. A chilling example of this data linkage is the sale by Farrell's Ice Cream Parlor of the names of those claiming free sundaes on their birthdays. The list was purchased by a marketing firm, which in turn sold them to the Selective Service System. Some of the ice-cream eaters soon found draft registration warnings in their mail.[313] More complex matchings use consumer demographics (based on extended zip codes that allow houses to be targeted in small groups) and known buying patterns to target telephone and especially direct mail sales.[314] Similar techniques are used routinely in political campaigns, in which demographic and other data is used to decide which (if any) of the candidate's stands on issues will be sent to the voter.[315]

---

312. Reidenberg, *supra* note 7, at 501.

313. DAVID LYON, THE ELECTRONIC EYE 10 (1994).

314. Gandy, *supra* note 210, at 15-17, 20, 27-28.

315. I know this from personal experience, since I helped implement, albeit not design, such a campaign, using demographics, party registration, presumed national origin based on (Polish-sounding) last name, and party affiliation, in mail and telephone campaign aimed at voters in a 1984 (!) Congressional election. Responses to mail queries as to the household's views, and responses to similar telephone calls and visits by campaign workers, were used to decide which of over a dozen letters (each discussing a different issue) to send to the voter. If the survey found that the voter had no commonality of views with the candidate, but the demographics were favorable, the voter received a bland letter describing the candidate's personal biography and recent good works. The same survey data were used to prime the candidate when he made neighborhood tours. A campaign worker would tell the candidate which of the views expressed by or imputed to the household agreed with his positions, and he would emphasize those views when he spoke to the voters. The data were also used to generate lists of probably supportive voters, who were then contacted on the day of the election to remind them to vote. We offered to provide transportation to the polls if required. We won by less than one percent of the vote.

The ice cream example is trivial compared to what is ahead, given the likely omnipresence of data collection. Data collection will grow in at least five areas: medical history, government records, personal movements, transactions, and reading and viewing habits. Between them these five areas cover most of modern life.

1. Medical History

"The development of population-wide health databases," some of which contain patient identifiable data, "is not a distant concept, but a reality."[316] Between the likely authorized and unauthorized users of any medical records, patient privacy is likely to be low, resulting in the dissemination of information about physical and mental health, genetic history, and treatment choices.[317] This information would be of value for scholarly purposes (e.g., epidemiological studies), regulatory purposes (e.g., assessing quality of care, cost control), and commercial purposes (e.g., malpractice actions and employment and insurance decisions).[318]

The market has begun to broker information in medical histories. Direct marketers offer lists of hypertensives, angina sufferers, diabetics, arthritics, and heavy antacid users.[319] The direct marketers obtain most of this information from the sufferers themselves, by asking them to complete surveys in exchange for free products, or coupons. Commercial health data-base providers collect information from health care providers and insurers then sell the information, without the patient's knowledge, to insurance companies and managed care providers.[320] Equifax, the consumer credit information agency, has purchased several small healthcare firms and formed an alliance with AT&T to computerize millions of paper-based medical records.[321] Private medical in-

316. Lawrence O. Gostin, *Health Information Privacy*, 80 CORNELL L. REV. 451, 464 (1995); *see also* Spiros Simitis, *Reviewing Privacy in an Information Society*, 135 U. PA. L. REV. 707, 710-12 (1987) (discussing "the transparent patient"). Enactment of any comprehensive national healthcare program would accelerate the trend. *See generally id.*; Minor, *supra* note 305.

317. *See* Paul M. Schwartz, *The Protection of Privacy in Health Care Reform*, 48 VAND. L. REV. 295, 300-06 (1995).

318. *See* Gostin, *supra* note 316, at 487-89.

319. Robert Gellman, *Washington Perspectives On Genetics and Privacy*, 3 DICK. J. ENVTL. L. & POL'Y 71, 72 (1994).

320. *See* Gostin, *supra* note 316, at 488; Jonathan P. Graham, Note, *Privacy, Computers, and the Commercial Dissemination of Personal Information*, 65 TEX. L. REV. 1395 (1987).

321. *Outsiders in Health Care. A Cure for All Ills?*, THE ECONOMIST, Nov. 4, 1995, at 67.

formation is also available on the black market;[322] as genetic testing and other methods of predictive health care improve, this information is likely to increase in value.[323]

2. *Government Records*

Drivers licenses in the United States typically show the owner's name, address, height, weight, age, date of birth. Often they also have the owner's social security number, and some medical information; at a minimum a driver's license notes whether the driver requires glasses. Some state licenses also note whether the driver is diabetic or has epilepsy. Most states also require a photograph. Increasingly often, all this data, including the photograph, is digitized and stored electronically on a magnetic strip and in a central record office.[324] The driver's license has been described as a "gold mine of personal information," one that most states routinely sell to anybody who desires it.[325]

In addition to driver's licenses, some states maintain computerized, publicly accessible databases containing criminal or arrest records, and property tax information.[326] Other government databases, not ordinarily public, contain transfer payment information such as welfare, food

---

322. Lois Rogers & David Leppard, *For Sale: Your Secret Medical Records for £ 150*, THE SUNDAY TIMES (London), Nov. 26, 1995, at 1 (describing offer for sale of medical records of "politicians, celebrities and millions of other National Health Service patients").

323. *See, e.g.*, Henry T. Greely, *Health Insurance, Employment Discrimination, and the Genetics Revolution*, *in* THE CODE OF CODES: SCIENTIFIC AND SOCIAL ISSUES IN THE HUMAN GENOME PROJECT 264 (Daniel J. Kevles & Leroy Hood eds., 1992).

324. Gellman, *supra* note 319, at 71.

325. *Id.*; Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553, 612 (1995) [hereinafter *Privacy and Participation*] (stating that "majority of states have traditionally released motor vehicle registration and driver license information"). In 1994, New York State made $8 million from the sale or rental of public records, primarily those furnished by drivers to the Department of Motor Vehicles. *Big Bucks in DMV Data Sales*, PRIVACY J., Sept. 1995, at 5. The data can be used for a variety of marketing with a little creativity,

> Now, take a look at this information all over again and see how valuable it is. Suppose I have a catalog of big and tall clothing, who do I want to send it to? How am I going to find my market? Well, they're not going to send it to me. But I can go through the driver's license information and pick out people of a certain height and weight, and they're the ones I'm going to send my catalog to.
>
> Suppose I am selling glasses or contact lenses. I can get a list of every potential customer in the state simply from the state government. Suppose I'm selling insurance policies aimed at people who just turned sixty-five. Well, if I want a list of people who turned sixty-five on April 15th, 1994, I can get that information from the state.

Gellman, *supra* note 319, at 71.

326. *See Privacy and Participation*, *supra* note 325, at 608. If you own a house, chances are the purchase price, addresses, and other information can be found on LEXIS, library ASSETS.

stamps, social security, and pensions data.[327] National databases include both transfer payment data and other records such as service records and passport applications.

3. *Personal Movements*

Many countries, including the United States, are exploring the possibility of "intelligent transportation systems" (ITS).[328] Under ITS, the position of every vehicle on the road would be monitored to manage traffic flow,[329] prevent speeding and perhaps implement road pricing and even centralized traffic control. A full-blown ITS system might provide law enforcement with continuous real-time surveillance of all vehicles.[330] Less complex systems might create detailed travel records that could be accessed after the fact.[331] Most cellular telephones already report their location every few minutes whenever they are in use or ready to receive calls.[332] Increasingly, both public and private security forces are using microphones and video cameras to record what goes on in city streets, shopping centers, and residential complexes.[333]

4. *Transactions*

Credit card purchases leave a vast trail of transaction records.[334] If digital money makes even small Internet transactions cost-effective, the

---

327. As states move to distributing benefits electronically, *see, e.g.*, *Texas Replaces Food Stamps With Food Cards*, N.Y. TIMES, Nov. 27, 1995, at B5 (describing plan to distribute food stamps via electronic funds transfer at grocery check out), they will inevitably create new databases.

328. *See generally* Symposium: *Privacy and ITS*, 11 SANTA CLARA COMPUTER & HIGH TECH. L.J. 1 (1995).

329. Traffic flow can be managed by adjusting the times of traffic lights, or communicating to drivers the need to consider alternate routes. If the ITS includes a system by which the driver selects the destination but the ITS chooses the route, the system can route around bottlenecks without driver intervention.

330. *See* Margaret M. Russell, *Privacy and IVHS: A Diversity of Viewpoints*, 11 SANTA CLARA COMPUTER & HIGH TECH. L.J. 145, 163 (1995). The Government of Singapore requested bids on a road-pricing system that would communicate with cars and charge their smart cards as they passed various points on the road. Chaum, *supra* note 235, at 101.

331. Russell, *supra* note 330, at 164-65.

332. The famous "low speed chase" of OJ Simpson began when he was located by tracing the movement of his cellular telephone. *Simpson, Under Suicide Watch, is Jailed After a Bizarre Chase*, N.Y. TIMES, June 19, 1994, at 1.

333. *See* Timothy Egan, *Police Surveillance of Streets Turns to Video Cameras and Listening Devices*, N.Y. TIMES, Feb. 7, 1996, at A12.

334. American Express accumulated more than 500 billion bytes of data on how its customers used 35 million charge cards between 1991 and 1994. Laurie Hays, *Using Computers to Divine Who Might Buy a Gas Grill*, WALL ST. J., Aug. 16, 1994, at B1. By 1993, the United States had more than 328 million general purpose (e.g., VISA, MasterCard, American Express, Discover, and Diners

number and range of transactions that leave a collectible and searchable record can be expected to increase unless the payment mechanism is anonymized.

This mass of transactional information can be subjected to sophisticated pattern analysis, dubbed "data mining," by which corporations try to learn more about existing and potential customers.[335] Data mining allows companies to identify client preferences, purchase histories, credit histories, "life stage," and thus the potential value of keeping the client as a happy customer. This information can be used for cross-selling, identifying new customers and targeting existing customers for upgrades or new products.[336]

5. *Reading and Viewing Habits*

The absence of monitors is an important part of the right to read.[337] The degree to which the right to read in private is prized can be seen by the protest generated by the FBI's "Library Awareness Program." In this program FBI agents pressured librarians in certain technical libraries to report on the reading habits of patrons.[338] Tomorrow, rather than the FBI attempting to profile the reading habits of a small

---

Club) credit cards in circulation. The cards were used for $223.92 billion worth of charges in the first six months of 1993. Matthews, *supra* note 215, at 233. Worldwide credit and debit card use continues to increase, although the number of card in use and the willingness of merchants to accept them varies greatly in different countries. *See Paying With Plastic*, THE ECONOMIST, Nov. 4, 1995, at 115.

335. "Data mining is the process of discovering meaningful new correlations, patterns and trends by sifting through large amounts of data stored in repositories, using pattern recognition technologies as well as statistical and mathematical techniques." *Commercial Parallel Processing Conference*, THE COMPUTER CONFERENCE ANALYSIS NEWSLETTER, Oct. 11, 1995 *available online* LEXIS library Nexis, file Curnws (reporting on presentation of Erick Brethenoux, Gartner Group); *see also* Kevin Fogarty, *Data Mining Can Help to Extract Jewels of Data*, NETWORK WORLD, June 6, 1994, at 40 (describing the practice of 'data mining' by which corporations accumulate and manipulate enormous data bases). *Cf.* GTE, *Knowledge Discovery Mine*, *available online URL* http://info.gte.com/gtel/sponsored/kdd/Welcome.html (collecting links to various sources of information on data mining).

336. *Commercial Parallel Processing Conference*, *supra* note 335 (reporting on presentation of Douglas Newell, Tessera Enterprise Systems).

337. On the constitutional protection of the right to read anonymously *see infra* text accompanying note 397.

338. *See* HERBERT N. FOERSTEL, SURVEILLANCE IN THE STACKS: THE FBI'S LIBRARY AWARENESS PROGRAM (1991); Ulrika E. Ault, Note, *The FBI's Library Awareness Program: Is Big Brother Reading Over Your Shoulder?*, 65 N.Y.U. L. REV. 1532, 1532-39 (1990) (describing FBI library monitoring program); AMERICAN LIBRARIES, July/Aug. 1988, p. 562-63. When the program became public in 1987, and encountered heavy criticism, the FBI responded by running "index checks" on 266 critics to see if they were part of a Soviet campaign to discredit the library monitoring program. Gordon Conable, *The FBI And You; Did The FBI Investigate You As Part Of Its*

number of people with suspected foreign connections, businesses will be profiling everyone who uses the World Wide Web.

Even today, it is relatively simple to monitor web page accesses whether or not the person reading a page initiates a commercial transaction. Most Web browsing software is designed to allow routine monitoring. Netscape, for example, tells the owner of every web page the IP address of every visitor to the page[339] and the URL of the page most recently visited by that person. If the user has filled out her e-mail address or name on the "options" page of her program—something Netscape requires before the user can employ Netscape to send an e-mail message—then that information is transmitted too. Web servers routinely log this information. Some companies now send e-mailed advertisements to those who access their pages.[340] It will not be long before they correlate names and locations with telephone numbers and begin follow-up sales calls and letters. The next step, perhaps, would be for someone to begin to either purchase or correlate these logs to build consumer profiles. One can imagine insurance companies wanting to know if applicants have been receiving information on diseases;[341] employers wanting to know about the interests of potential employees; perhaps some governments will want to find the identities of those they consider likely to be subversives.

Traceable payments may expand from the world of tangible goods to the purchase of information. If Internet tools such as the World Wide Web become a major national and international communications medium with an embedded micro-charging mechanism, every newspaper article accessed, every online catalog perused, every political debate sampled, will leave an information residue. These data can be collected to form a highly detailed profile of the consumer-citizen. The existence of such detailed dossiers on spending and intellectual preferences would be unprecedented. Non-anonymous digital coins that clear through a central bank would accelerate this process. Instead of needing a middleman to collect and correlate transactions patterns, the bank would find itself in possession of all the data: amount of purchase, buyer, seller, and (if the transaction is on line) date and time of transaction.

Library Awareness Program? Here's How To Find Out, 3 AM. LIBR. 245 (Mar. 1990), *available online* LEXIS library Nexis, file Arcnws.

339. The importance of this may decrease as services aimed at the home user increasingly move to dynamic IP numbers, in which IP numbers are temporarily assigned to users while logged in and then returned to a pool of available numbers.

340. I have received such advertisements.

341. *See* Greely, *supra* note 323.

Banks, however, present relatively easy targets for privacy regulations, because they are less numerous than the buyers and sellers themselves, and because banks are already a highly regulated industry.

B. Interlinked Databases

"[T]he ability to assemble information selectively, or to correlate existing information, can be functionally equivalent to the ability to create new information."[342] Networks such as the Internet make it unnecessary to attempt to create and store an enormous database in one place. Instead, the information can be maintained by the organization that collects it, and merely accessed on demand by those who so desire.[343]

Private databases are growing quickly. Between them, Equifax, TRW and Trans Union maintain consumer credit data on almost every American who has borrowed money or used a credit card in the last ten years. The trend will intensify. The Internet will bring "telebanking" and home shopping to the personal computer.[344] As "databanks become more prevalent and sophisticated, long-distance, invisible assaults on privacy will occur more frequently."[345] The data stored in "data warehouses" available for data mining will only increase,[346] as will the sophistication of programs designed to mine the data.[347] For example, restaurants commonly use computers to handle patron orders; insur-

342. COLIN BENNETT, REGULATING PRIVACY: DATA PROTECTION AND PUBLIC POLICY IN EUROPE AND THE UNITED STATES 18 (1992); *see also* LYON, *supra* note 313, at 84.

343. *See* DAVID J. CURRY, THE NEW MARKETING RESEARCH SYSTEMS 7-12 (1993).

344. *See* Inquiry on Privacy Issues Relating to Private Sector Use of Telecommunications-Related Personal Information, 59 Fed. Reg. 6842, 6842 (1994) [hereinafter Inquiry on Privacy Issues] ("As the [National Information Infrastructure] develops, Americans will be able to access numerous commercial, scientific, and business data bases . . . [and] engage in retail, banking and other commercial transactions . . . all from the comfort of their homes."); *see also Microsoft and Visa to Provide Secure Transaction Technology for Electronic Commerce*, PR NEWSWIRE, Nov. 8, 1994, *available in* WESTLAW, PRNews-C database (announcing plans to provide secure electronic bankcard transactions across global public networks using RSA encryption).

345. Inquiry on Privacy Issues, *supra* note 344; *cf.* JEFFREY ROTHFEDER, PRIVACY FOR SALE: HOW COMPUTERIZATION HAS MADE EVERYONE'S PRIVATE LIFE AN OPEN SECRET 28 (1992); DAVID BURNHAM, THE RISE OF THE COMPUTER STATE 20, 23-25 (1983).

346. "90% of large companies are building, or planning to build, a data warehouse." *Commercial Parallel Processing Conference*, *supra* note 328 (reporting on presentation of Scott F. Miller, VP High Performance Computing); *cf.* Cheryl D. Krivda, *Data-Mining Dynamite*, BYTE, Oct. 1995, at 97 (describing creation of data warehouses).

347. *See, e.g.*, *Pilot Software Launches Major New Data Mining Initiative*, BUS. WIRE, Nov. 8, 1995, *available online* LEXIS library News file curnws (describing ambitious plan to design techniques to "discover and explore relevant hidden and predicative information housed in massive data warehouses").

ance companies might like to know whether potential customers eat fatty foods, and how much they tend to drink before driving.[348] Often, consumers will benefit from the development of improved screening techniques. For example, many people will prefer "perfect junk mail," in which one receives only advertisements likely to result in a purchase, to the current plethora of catalogs that inundate some homes.

Public databases are increasingly interlinked also. The U.S. government has connected the databases of the Customs Service, the Drug Enforcement Agency (DEA), the IRS, the Federal Reserve, and the State Department. In addition, the Counter Narcotics Center, based at CIA headquarters, brings together the FBI, the DEA, the NSA, the Defense Department, the State Department, and the Coast Guard.[349] The Treasury Department's Financial Crimes Enforcement Network (FinCEN), has compiled a large and sweeping database to further the government's anti-money-laundering activities.[350] Data do not need to be in a single office to be combined into dossiers or to be organized and searched. The Office of Technology Assessment has warned that the "extensive use of computer matching can lead to a virtual national data bank, even if computer records are not centralized in one location"[351]

The distinction between "public" and "private" data in any case may be ephemeral although the public and private sectors may continue to use the data in significantly different ways. As the ice cream example shows, data in private hands can be purchased and used by the government. Similarly, data in public hands often tends to "leak" into private hands,[352] or be sold to raise revenue. Although the sources of the data may begin to merge, the ways in which public and private organizations may use the data raise different concerns.[353]

The existence of large, and linked, databases is potentially alarming in the United States because the U.S. has relatively few data pro-

348. *See* G. Bruce Knecht, *Is Big Brother Watching Your Dinner and Other Worries of Privacy Watchers*, WALL ST. J., Nov. 9, 1995, at B1 (quoting warning by Rep. Jim Moran of Virginia).

349. Robert García, *"Garbage In, Gospel Out": Criminal Discovery, Computer Reliability, and the Constitution*, 38 UCLA L. REV. 1043, 1065 (1991).

350. For an alarming account of FinCEN, see Steven A. Bercu, *Toward Universal Surveillance in an Information Age Economy: Can We Handle Treasury's New Police Technology?*, 34 JURIMETRICS J. 383, 429 (1994).

351. OFFICE OF TECHNOLOGY ASSESSMENT, U.S. CONGRESS, MAKING GOVERNMENT WORK: ELECTRONIC DELIVERY OF FEDERAL SERVICES 144 (OTA-TCT-578 1993).

352. LYON, *supra* note 313, at 12; Simitis, *supra* note 316, at 707.

353. On public disclosure, see the magisterial discussion in Kreimer, *supra* note 84. For an interesting and skeptical account of the issues in private disclosure, see Lillian R. Bevier, *Information About Individuals in the Hands of Government: Some Reflections on Mechanisms for Privacy Protection*, 4 WM. & MARY BILL RTS. J. 455 (1995).

tection statutes along the lines of the European and Canadian models.[354] U.S. data protection laws place some limits on the use of government databases.[355] They also give consumers the right to correct erroneous entries that may be kept in their files by private credit bureaus.[356]

Although the U.S. has enacted fewer data protection laws than many other OECD countries this is not necessarily a permanent condition.[357] There seems to be a widespread belief in the United States that some computerized intrusions on privacy are unconscionable. In 1991, Lotus attempted to market CD-ROM disks that contained the names, address, marital status and estimated income of 80 million householders. Lotus received so many complaints that it felt forced to withdraw the product.[358] The political process has demonstrated that it is capable of reacting swiftly when galvanized by what it perceives to be an outrageous attack on privacy. The Video Privacy Protection Act of 1988[359] was enacted shortly after a newspaper printed the video rental records of Supreme Court nominee Robert Bork,[360] although video watching habits resurfaced as an issue in the confirmation hearings of Clarence Thomas.

Unfortunately, whether data protection laws are effective in providing long-term protection of the privacy of personal information remains uncertain.[361] Data protection laws are likely to work best when the data collectors are few, or operate in industries that are already highly regulated, such as banks. Bigger databases are easier to regulate that many small databases: "the more concentrated the profile data,

354. *See* Paul Schwartz, *Data Processing and Government Administration: The Failure of the American Legal Response to the Computer*, 43 HASTINGS L.J. 1321, 1324 (1992) (stating that from an international perspective, the American legislative response to computer processing of personal data is incomplete); for a careful description and critique of European and Canadian data protection laws, see DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES (1989).

355. *See* Privacy Act of 1974, 5 U.S.C. § 552a (1995).

356. Fair Credit Reporting Act, 15 U.S.C. § 1681 (1995).

357. *See generally* PRISCILLA M. REGAN, LEGISLATING PRIVACY (1995); BENNETT, *supra* note 342.

358. LYON, *supra* note 313, at 15.

359. Pub. L. No. 99-508, 100 Stat. 1860 (codified at 18 U.S.C. § 2701 (1988)).

360. Michael deCourcy Hinds, *Personal But Not Confidential: A New Debate Over Privacy*, N.Y. TIMES, Feb. 27, 1988, at 56.

361. *See* FLAHERTY, *supra* note 354, at 406-07 (concluding extensive comparative study with warning that while it is possible to have effective data protection commissions, it is also possible they will be viewed as "a rather quaint, failed effort").

the greater the privacy that is possible by regulation."[362] As data collection and communication techniques grow, however, it is at least possible, and perhaps likely, that the large centralized database will become as much of a dinosaur as the mainframe, to be replaced by networks of small, interlinked databases continually updated in real time. Data protection regulation would be particularly difficult in such a world. Worse, the international nature of data flows limits the ability of any single nation to enforce its data protections laws.[363] As a result, the European Commission now allows transborder data flows only if the recipient country allows "an adequate level of data protection."[364] Given the mobility of information, even a highly organized international effort to control data flows could be undermined by a "data haven"—the information equivalent to a tax haven—a single nation that offered to warehouse data offshore.[365]

C. *Implications of Profiling for Anonymity Regulation*

In the absence of effective data protection laws, anonymous communication and transactions are the only techniques that are likely to allow one to control the dissemination of personal information and thus even partly realize the idea of home as a secure fortress. Digital anonymity may be a rational response to a world in which the quantity of identifying data on each of us grows daily, and the data become ever easier for government and private parties to access.

When the state is involved in the data collection, it is reasonable to ask if the Constitution imposes constraints on how the data may be used. When the state is not directly involved in the data collection, one can ask if regulation is appropriate and whether the state has the power to regulate the collection, storage, and use of the data. More to

362. Conversation with Peter Swire, Associate Professor of Law, University of Virginia, Jan. 4, 1996.

363. *See* Paul M. Schwartz, *European Data Protection Law and the Restrictions on International Data Flows*, 80 IOWA L. REV. 471, 472 (1995) (noting that even Europe-wide controls on data flows are insufficient to protect privacy in an era of internationalized communications) [hereinafter *European Data Protection Law*]; *Privacy and Participation*, *supra* note 325, at 553 (same).

364. Common Position (EC) No/95 With a View to Adopting Directive 94/ /EC of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995, O.J. (C 93, Apr. 13, 1995), *reprinted in* Appendix, 80 IOWA L. REV. 697 (1995). For a discussion of what constitutes an adequate level, see *European Data Protection Law*, *supra* note 363, at 480-88.

365. For a discussion of European efforts to prevent personal data from leaving Europe without guarantees that it will not be improperly distributed, see *European Data Protection Law*, *supra* note 363.

the point, one must ask whether the state may constitutionally forbid the use of a technique—anonymous digital cash—if the effect of that ban is to remove one of the major techniques available to those who wish to use the Internet as a communicative tool, even when money is required to use the medium, without subjecting themselves to profiling.

1. Privacy-Enhancing Market Solutions Unlikely

It might seem that at least part of the privacy problem could be solved by creating a property right over information about oneself.[366] In this scenario merchants would have to pay for the right to send junk mail.[367] This cost-shifting regime would make particular sense on the Internet today, as many people pay telephone or per-e-mail access charges when they download their e-mail, charges that they have no way to pass on to junk e-mailers. The problem with a property-rights approach is that it could easily be defeated by the realities of modern transactional life. Some U.S. residents might prefer not to give out their social security number. In practice, however, refusing to give out this information will complicate many basic transactions. The telephone company may require an enormous deposit before installing a telephone line—and a much longer delay before installation. Credit card companies will not extend credit. The bank will not lend money to buy a house. For all but the most determined, the attempt to withhold a social security number is likely to be a futile battle, one in which the merchant's economies of scale mean huge costs for the individual who has a taste for privacy that is unsatisfied by the default of zero.[368] A similar process would likely occur in the market for transactional information. Merchants would include a transfer of the right as part of the standard for contract they offered to customers. So long as the courts refuse to rewrite or ignore contracts of adhesion, and as long as in each individual transaction the cost of not providing the information is disproportionate to the loss (which is a function of the cumulation of the transactions, not any single transaction), a property rights approach appears unlikely to have much real influence on database creation.

366. *See, e.g.*, Simitis, *supra* note 316, at 734 (discussing West German Federal Constitutional Court's protection of "informational self-determination").

367. *Cf.* Associated Press, "Junk Mail" Suit Seen as Threat to Direct Marketers, Mar. 11, 1996, *available online* LEXIS, News Library, Curnws file (describing efforts by Ram Aurahami to sue U.S. News & World Report for selling his name to direct marketers without his permission).

368. *See, e.g.*, LYON, *supra* note 313, at 49 (describing lengthy delays introduced into purchase of washing machine by his refusal to supply personal data).

If the property rights approach is impractical, anonymity may be the only technique of resistance to profiling (short of civil disobedience or outright surrender) available to the average citizen.[369]

2. *Beached* Whalen[370]

The growth of profiling technologies means that any attempt to regulate anonymous communication will have implications that extend beyond speech. Even a regulation that exempts pure speech and targets only anonymous transactions could have profound consequences. If profiling is on the increase, and if consumers who have a taste for privacy are unable to secure changes in the standard forms that govern most transactions but make no provision for this preference, then transactional anonymity may become the primary means by which consumers can maintain control over information about themselves. In this view of the world, any attempt to restrict anonymity could affect not just speech rights and the right to read, but other wide-ranging privacy interests as well.

The speech-related privacy interests protected by anonymous communications have a constitutional dimension, even if the precise contours of these rights are unclear.[371] In contrast, the privacy interests threatened by profiling of non-speech commercial transactions currently have little if any constitutional protection. In part this is because many of the profilers are private actors, and the U.S. Constitution does not apply to their actions;[372] however, even when the profiles are maintained, required, or used by the government, there appear to be few applicable constitutional constraints.

The constitutional right to privacy, such as it is, is frequently described as having three components: (1) a right to be left alone; (2) a right to autonomous choice regarding intimate matters; and (3) a right to autonomous choice regarding other personal matters.[373]

Supreme Court decisions relating to privacy issues have tended to be Fourth Amendment cases concerned with a governmental claim in

369. Others have reached similar conclusions in other contexts. For example, "[a]nonymity is the only sure defense" for those exercising upopular constitutional rights that might expose them to violence, Kreimer, *supra* note 84, at 40.

370. Whalen v. Roe, 429 U.S. 589 (1977).

371. *See supra* Part II.

372. The privacy provisions of the state constitution of California have been held to apply to private actors. *See* Hill v. National Collegiate Athletic Ass'n, 865 P.2d 633 (Cal. 1994).

373. *See* TRIBE, *supra* note 132, § 15-1; Ken Gormley, *One Hundred Years of Privacy*, 1992 WIS. L. REV. 1335, 1340.

the context of a criminal investigation of a right to access to a person or to data (papers, telephone calls). "Privacy" in a legal sense is also invoked in special classes of cases that concern the individual's freedom to make important life choices, particularly regarding sexual and reproductive freedom (contraception, abortion). Although both of these lines of cases offer language with suggestive implications for a broader right of privacy, the Supreme Court's major modern discussion of an informational privacy right remains *Whalen v. Roe*.[374]

In *Whalen*, the Court accepted that the right to privacy includes a generalized "right to be let alone,"[375] which includes "the individual interest in avoiding disclosure of personal matters."[376] Despite finding a theoretical right to avoid disclosure of intimate personal matters, however, in *Whalen* the Court allowed New York state to keep a computerized list of prescription records for dangerous drugs and to require physicians to disclose the names of patients to whom they prescribed those drugs.[377] The decision balanced the social interest in informational privacy against the state's "vital interest in controlling the distribution of dangerous drugs."[378] Finding New York's program to be narrowly tailored, and replete with security provisions designed to reduce the danger of unauthorized disclosure, the Supreme Court held that the constitutional balance tilted in favor of the statute.[379] Despite upholding the mandatory compilation and disclosure of prescription data, the Court left the door open to future restrictions in light of technical change, noting that it was "not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized

374. 429 U.S. 589 (1977). For a scholarly analysis of the right to privacy outside the Fourth Amendment context, see Kreimer, *supra* note 84.

375. Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting); *see also* Stanley v. Georgia, 394 U.S. 557, 564 (1969) (finding a constitutional right to 'receive information and ideas, regardless of their social worth').

376. Whalen v. Roe, 429 U.S. 589, 598-99 (1977) (acknowledging the existence of the right, but finding that it could be overcome by a narrowly-tailored program designed to serve the state's "vital interest in controlling the distribution of dangerous [prescription] drugs"); *see* Gary R. Clouse, Note, *The Constitutional Right to Withhold Private Information*, 77 NW. U. L. REV. 536, 547-57 (1982) (collecting and dissecting inconsistent circuit court cases dealing with the right to withhold private information). The right to be left alone, however, is insufficiently compelling to prevent a large number of physical intrusions to bodily integrity when the police seek forensic evidence relating to a criminal investigation. *See* TRIBE, *supra* note 132, at 1331 nn.4-11 (collecting cases).

377. *See Whalen*, 429 U.S. at 593, 603-04.

378. *Id.* at 598.

379. *See id.* at 601-04.

data banks or other massive government files."[380] In so doing, the Court set the stage for claims that the Constitution embodies a right to informational privacy,[381] although the Court has yet to expand on this idea in any significant way.[382]

3. *Anonymous Communication in the Argus State*

It is likely that in the future one will have to pay for access to reading materials on many web pages. It is also possible that the web or its successors will become a major, perhaps *the* major, source of information for many citizens. As noted above, a ban on the use of anonymous digital cash for ordinary tangible commerce faces few constitutional or practical obstacles as applied to the sale of goods.[383] As applied to the sale of reading matter, or information more generally, the ban potentially is problematic. If every visit to a fee-based web page leaves a data trail behind it, the reading habits of some persons are certain to be chilled.[384]

---

380. *Id.* at 605.

381. *See, e.g.*, Francis S. Chlapowski, Note, *The Constitutional Protection of Informational Privacy*, 71 B.U. L. REV. 133, 155 (1991) (concluding that because most theories of personhood assume personal information is a crucial part of a person's identity, there must be a recognized "right to informational privacy based on personhood" and that information is property protected by the Fifth Amendment); Clouse, *supra* note 376, at 541-47 (tracing the development of the right to informational privacy, and noting the Supreme Court's use of a balancing test to determine whether an individual's constitutional rights have been infringed by a government-mandated disclosure of information).

382. In Nixon v. Administrator of Gen. Servs., 433 U.S. 425, 457 (1977), in which the Court rejected Nixon's claim that allowing government archivists to review and classify his presidential papers and effects violated his "fundamental rights . . . of privacy," the Court quoted from *Whalen* and applied *Whalen*'s balancing test. Nixon's privacy interest was found insufficiently strong to outweigh the public interest in preserving his papers. *Id.* at 465. The issue has also been canvassed in several lower court cases. Long, *supra* note 25, at 1192 n.81 (collecting cases).

Perhaps of greater significance are the decisions in Cox Broadcasting Corp. v. Cohn, 420 U.S. 469 (1975), and Florida Star v. B.J.F., 491 U.S. 524 (1989), in which the Court struck down state law privacy claims arising from the accurate publication of arguably private facts that had become matters of public record. The Court did suggest that there "there is a zone of privacy surrounding every individual," 420 U.S. at 487, but it did not say what it was.

The closest thing to an expansion of *Whalen* is the unanimous decision in United States Dept. of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749 (1989). There the Supreme Court held that there was a heightened privacy interest in an FBI compilation of otherwise public information sufficient to overcome a FOIA application. Even if the data contained in a "rap sheet" were all available in public records located in scattered courthouses, the compilation itself, the "computerized summary located in a single clearinghouse" was not. 489 U.S. at 764.

383. *See supra* text at notes 302-03.

384. *See, e.g.*, Fabulous Assoc. v. Pa. Public Util. Comm'n, 896 F.2d at 780, 786 (3d Cir. 1990) (noting testimony before FCC that telephone sex lines suffer enormous loss in calling volume

Depending on precisely what types of digital cash were banned, a prohibition on anonymous digital cash could make it effectively impossible to speak and/or read web pages anonymously whenever any "marked" funds changed hands. Because the loss of anonymity occurs when digital money that identifies its owner changes hands, the anonymity of the author and reader would not be preserved by using either an anonymous web browser or a web page that could not be traced back to its author.

Broadly, two types of prohibitions on anonymous digital cash can be imagined: a ban only on cash that allows both parties to remain anonymous, or a ban that also reaches cash that preserves the anonymity of the payor only. Neither of these hypothetical regulatory schemes affects the anonymity or traceability of Internet speech and readership in which no money changes hands.

First, one can imagine a ban on purely anonymous digital cash, e.g., Mondex-style smart cards with no funds tracing.[385] This narrow prohibition would not affect DigiCash-style blinded digital coins.[386] In this model, the privacy of readers would be unaffected since blinded coins leave the payor anonymous. Furthermore, the author of the web page would give up only a very limited degree of anonymity when she turned the coins in to the bank because nothing about the coin redemption transaction necessarily tells the bank where the cash came from or how the author came to acquire it.[387]

On the other hand, a ban on anonymous digital cash that extended to payer-anonymous schemes could have First Amendment implications for its effect on both authors and readers. A ban on payer-anonymous schemes means that the reader must disclose her identity at least to the issuing bank, and probably to the author as well. It also means that the issuing bank is able to link the author to the reader if not inevitably to the precise reading matter being exchanged.[388] Furthermore, in some schemes the reader may be able to learn the identity of the author.

---

if customers are required to identify themselves); Frederick Schauer, *Fear, Risk and the First Amendment: Unravelling the "Chilling Effect,"* 58 B.U. L. REV. 685, 693 (1978).

385. *See supra* § III.B.5.

386. *See supra* § III.B.3.

387. In an off-line clearing system, an attempt to spend a coin for a second time should disclose the identity of the double-spender. *See supra* § III.B.3. This attempt at fraud waives any claim to privacy.

388. *See supra* § III.B.

This last effect, the loss of anonymity of the author, is the effect most clearly at odds with current First Amendment law.[389] Furthermore, the author also loses if readers are deterred from purchasing the material because they cannot do so anonymously. It is well-established that authors and publishers do not lose their First Amendment rights by charging for their work.[390] The Supreme Court has recognized that a regulatory scheme that denies authors the incentive of compensation "imposes a significant burden on expressive activity"[391] and that "[s]ome of our most valued forms of fully protected speech are uttered for a profit."[392] "[E]ven under marketplace theories, the loss of speakers is not without significance. An idea confined to the margins of public discourse is not likely to have as powerful an impact."[393]

The most serious inhibiting effect might fall on the reader,[394] yet the reader's personal interest (as opposed to the author's interest in having readers) is harder to characterize as within the protection of the First Amendment because it is not obvious that it recognizes a right to read anonymously. Even if there is a First Amendment right to read anonymously, that right will not necessarily outweigh a content-neutral restriction justified by a compelling government interest, especially if there appears to be no alternative regulation that could accomplish the goal. On the other hand, a content-neutral rule that closes down an entire channel of communication may run afoul of the First Amendment.[395]

---

389. Indeed to the extent that the speech was political speech, it would be directly covered by the First Amendment precedents discussed *supra* § II.B.1.

390. *See* Simon & Schuster, Inc. v. Members of N.Y. State Crime Victims Bd., 502 U.S. 105 (1991); Arkansas Writers' Project, Inc. v. Ragland, 481 U.S. 221, 227-31 (1987); Minneapolis Star & Tribune Co. v. Minnesota Comm'r of Revenue, 460 U.S. 575 (1983).

391. United States v. National Employees Treasury Union, 115 S. Ct. 1003, 1014 (1995); *see also* Simon & Schuster, Inc. v. Members of N.Y. State Crime Victims Bd., 502 U.S. 105, 115 (1991) (stating that the imposition of financial burdens may have a direct effect on incentives to speak); Minneapolis Star & Tribune Co. v. Minnesota Comm'r of Revenue, 460 U.S. 575, 585 (1983) (observing that the threat of burdensome taxes "can operate as effectively as a censor to check critical comment").

392. *Fox*, 492 U.S. at 482; *see also* New York Times Co. v. Sullivan, 376 U.S. 254 (1964); Buckley v. Valeo, 424 U.S. 1 (1976) (per curiam).

393. Kreimer, *supra* note 84, at 49.

394. For example, people who were identified as recipients of unpopular information could be subject to various forms of social control, e.g., private blacklisting. *See* Kreimer, *supra* note 84, at 42-50.

395. The place of least-restrictive-means analysis as opposed to mere narrow tailoring in the analysis of content-neutral regulations of speech is a topic far beyond the scope of this article. Ordinarily used in evaluating the constitutionality of time-place-manner restrictions, least-restrictive-means analysis has achieved at least a toehold in content-neutral analysis also. *See* City of Ladue v.

The First Amendment protects the rights of readers up to a point. We have seen that in the U.S. the right to speak anonymously derives from the First Amendment's protection of speech and association.[396] The Supreme Court also has repeatedly stated that the First Amendment protects the right to read (sometimes called the right to receive information),[397] most recently striking down a ban on honoraria to mid- and low-level government employees in part because of the "significant burden on the public's right to read and hear what the employees would otherwise have written and said."[398] That said, the contours of the right to read remain far less well defined than the extent of the right to speak.

The First Amendment right to read is bound up with a variety of understandings of the place of the First Amendment in a system of ordered liberty. It can be said to derive from the right to speak; it can also be viewed as an independent right without which speech would be meaningless. The right to receive information can be seen as an integral part of the individual's right to self-definition and self-actualiza-

---

Gilleo, 114 S. Ct. 2038, 2044 n.11, 2045-47 (1994) (assuming that challenged regulation is content-neutral and then conducting alternative-channels-of-communication analysis); *see also* Geoffrey Stone, *Content-Neutral Restrictions*, 54 U. CHI. L. REV. 46, 57-58 (1987); *cf.* Madsen v. Women's Health Ctr., 114 S. Ct. 2516 (1994) (using time-place-manner analysis to determine whether injunction should be issued that imposed content-neutral burden on speech); City of Los Angeles v. Taxpayers For Vincent, 459 U.S. 1199 (1983) (not requiring least restrictive means); Ward v. Rock Against Racism, 491 U.S. 781 (1989) (same).

396. *See supra* § II.B.I.

397. *See* United States v. National Employees Treasury Union, 115 S. Ct. 1003, 1014-15 (1995) (declaring statute violates First Amendment in part because it "imposes a significant burden on the public's right to read"); Board of Educ. v. Pico, 457 U.S. 853, 867 (1981) ("[T]he right to receive ideas is a necessary predicate to the recipient's meaningful exercise of his own rights of speech, press and political freedom."); Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer Council, Inc., 425 U.S. 748, 756-57 (1976); Procunier v. Martinez, 416 U.S. 396, 408 (1974) (holding that First Amendment right of recipient of prisoner's letter is violated by prison censorship policy, although disclaiming reliance on a "right to read"); Red Lion Broadcasting v. FCC, 395 U.S., 367, 390 (1969) (noting "right of the public to receive suitable access to social, political, esthetic, moral, and other ideas and experiences"); Stanley v. Georgia, 394 U.S. 557, 564 (1969) ("[i]t is now well established that the Constitution protects the right to receive information and ideas"); Griswold v. Connecticut, 381 U.S. 479, 482 (1965) (holding that "the right to receive, the right to read" are protected by the First Amendment); Martin v. City of Struthers, 319 U.S. 141, 143 (1943) (First Amendment 'necessarily protects the right to receive' information"); *see also* Ginsberg v. New York, 390 U.S. 629, 649 (1968) (Stewart, J., concurring) ("[t]he Constitution protects more than just a man's freedom to say or write or publish what he wants. It secures as well the liberty of each man to decide for himself what he will read and to what he will listen."); Lamont v. Postmaster Gen., 381 U.S. 301, 307-08 (1965) (Brennan, J., concurring).

398. United States v. National Employees Treasury Union, 115 S. Ct. 1003, 1014-15 (1995).

tion.[399] Free choice among types of information can be an important part of individual autonomy. Practiced in groups, the exchange and access of information becomes entwined with the right of association, be it a book club, a church reading group, or a political action campaign. Alternately, the right to receive information could be understood as an essential part of the republican vision in which an informed citizenry takes part in a continuing national political and moral debate; if citizens do not have access to information the debate is impoverished to the point of pointlessness.[400] In any of these senses, the right to read undisturbed is indeed a right that "is fundamental to our free society."[401]

In light of the First Amendment's protection of anonymous speech, and of the importance of the right to read, one could argue that the First Amendment protects a right to read anonymously.[402] There is, however, no directly relevant decision of the Supreme Court to support this assertion. The closest thing is *Lamont v. Postmaster General*,[403] in which the Court struck down a statute requiring post offices to refuse

399. "The First Amendment serves not only the needs of the polity but also those of the human spirit—a spirit that demands self-expression. Such expression is an integral part of the development of ideas and a sense of identity. To suppress expression is to reject the basic human desire for recognition and affront the individual's worth and dignity." Procunier v. Martinez, 416 U.S. 396, 427 (1974) (Marshall, J., concurring).

400. In CBS v. Democratic National Committee, 412 U.S. 94 (1973), the Supreme Court upheld an FCC refusal to require broadcasters to sell time to anti-war organizations on the grounds that there was no constitutional right to access to broadcast media. Rejecting the vision of listener rights to receive specific information, the Court instead held that broadcasters had a right to determine what ideas are broadcast.

In *Red Lion*, the Court had previously ruled that listeners had a right to balanced information. In *CBS v. DNC*, however, Chief Justice Burger suggested that listeners could not be relied upon to speak articulately for themselves; broadcasters, although nominally proxies for the public interest, were thus essentially free to act on their own judgment of what best served the public's interest.

CBS v. DNC is often read to stand for the proposition that neither *Red Lion* nor the Constitution require "fairness" in broadcasting, or even as a rejection of the republican vision of a constitutionally protected national conversation. It is important to note, however, that Chief Justice Burger's opinion rests in part on the prudential grounds that were listeners rather than broadcasters to be entrusted with editorial discretion, there would be a danger of chaos. To the extent that this decision relies on a judgment that the public is not competent to speak for itself, it deserves to be rejected; to the extent that this judgment relies on the intermediation of broadcasters, the direct speaker-to-reader communication of the Internet is distinguishable.

401. Stanley v. Georgia, 394 U.S. 557, 564 (1969) (holding that First Amendment protects possession of obscene materials in the home).

402. The storm of protest that greeted the FBI's Library Awareness program suggests that public expectations and intuitions are offended by government monitoring of private reading matter. *See supra* note 338. The Library Awareness program was, however, more directly intrusive than a government policy that merely makes it more difficult for readers to hide their identities.

403. 381 U.S. 301 (1965).

to deliver foreign-mailed communist propaganda unless the addressee specifically requested the material.[404] The Court accepted that this requirement would very likely deter addressees from requesting mail that might be categorized as communist propaganda,[405] and held that the statute therefore was "at war with the 'uninhibited, robust and wide-open' debate and discussion that are contemplated by the First Amendment."[406] Justice Brennan's concurrence underlined the idea that the right to speak means little unless the right of the reader is protected also.[407]

Courts of Appeal have recognized the right to read in terms that suggest anonymous reading may be protected by the First Amendment. "When the effect of banning a form of speech is to prevent receipt of the message by the intended audience, it cannot seriously be argued that the ban is innocuous because it applies only to the mode of speech."[408] Indeed, the Third Circuit held that "[a]n identification requirement exerts an inhibitory effect" which "raises First Amendment issues comparable to those raised by direct state imposed burdens or restrictions."[409] Thus, after concluding that strict scrutiny was the appropriate standard, the Third Circuit struck down a state statute imposing an identification requirement for the use of phone sex services because there was a less restrictive alternative.[410]

The counter-argument to all this would be that the right to read and receive information is a derivative right, as is the right to speak anonymously. The "right" to read anonymously could be described as doubly derivative from the First Amendment; if so, perhaps it need not be derived at all. One also might argue that negative and positive rights should not be confused. Even if there may be a right to be free of government-created registration rules, such as *Lamont*, it does not fol-

404. *Id.* at 302.

405. *See id.* at 307.

406. *Id.* (quoting New York Times Co. v. Sullivan, 376 U.S. 254, 270 (1964)).

407. *Id.* at 308 (Brennan, J., concurring) ("the dissemination of ideas can accomplish nothing if otherwise willing addressees are not free to receive and consider them").

408. Yniguez v. Arizonans for Official English, 69 F.3d 920, 936 (9th Cir. 1995) (enjoining "English only" amendment to state constitution), *cert. granted*, 116 S. Ct. 1316 (1996).

409. Fabulous Assoc. v. Pa. Public Util. Comm'n, 896 F.2d 780, 785 (3d Cir. 1990) (citing *Talley*, 362 U.S. at 64-65).

410. *Fabulous*, 896 F.2d at 787-88. The Third Circuit distinguished F.C.C. v. Pacifica Found., 438 U.S. 726 (1978) (upholding FCC order granting complaint against radio station for broadcasting "patently offensive" language), on the grounds that the telephone was far less pervasive than broadcast media and required the active choice of the listener to receive it. *Fabulous*, 896 F.2d at 783. It is debatable whether that distinction applies to the Internet.

low that the government is foreclosed from taking actions that happen to make it more difficult for people to read anonymously.[411]

There are indeed differences between the facts of *Lamont*, in which the government affirmatively imposed a viewpoint-based burden on the right to read, and a hypothetical ban on anonymous digital cash. Assuming nevertheless, if only for the sake of the argument, that there is a First Amendment right to read anonymously, any law that had the effect of burdening that right would be subject to strict scrutiny if it was content-based, but to considerably lesser scrutiny if the effect on speech was only an incidental effect of a regulatory scheme aimed at non-speech conduct.[412]

A ban on anonymous digital cash would affect all transactions equally, not just speech for pay. As such, the ban would be a content-neutral burden on the right to speak anonymously and/or read fee-based digital materials anonymously. The ban would therefore be subject only to intermediate scrutiny on the theory that speech was incidentally burdened by a more general, legitimate, regulatory scheme.[413]

---

411. As Trotter Hardy pointed out in a discussion of this issue on the cyberia-l discussion list, recognition of a right to read anonymously might pose difficulties for the regulation of reading material that must be denied to particular classes of readers, e.g., material that cannot be furnished to minors. There is, however, a partial technical solution to this problem if a trusted third party can be found to issue anonymous age credentials. The third party would examine the person's proof of majority, then issue a certificate to that effect, signed with the certifying authority's public key. *See* Froomkin, *supra* note 228. The certificate need contain only the public key of the person whose age is being attested, not the person's name, making the credentials both unforgeable and anonymous. Alas, the system is not foolproof. If Alice, age 17, can persuade Bob, age 21, to give her the private key associated with the public key in Bob's certificate, Alice can impersonate Bob and no one on the Internet will be the wiser. It is possible to imagine versions of a digital signature infrastructure in which possession of another person's digital signature created such a risk for the original owner that signature sharing became rare, but this is not inevitable.

412. *See* Boos v. Barry, 485 U.S. 312 (1988); United States v. O'Brien, 391 U.S. 367 (1968); Clark v. Community for Creative Non-violence, 468 U.S. 288 (1984); *see also* United States v. Eichman, 110 S. Ct. 2404 (1990); Texas v. Johnson, 491 U.S. 397 (1989).

413. *See* Turner Broadcasting Sys., Inc. v. FCC, 114 S. Ct. 2445, 2459-62 (1994) (applying intermediate scrutiny after deciding that must-carry provision that distinguished between speakers solely by the technical means used to carry speech is not a content-based restriction); Clark v. Community for Creative Non-Violence, 468 U.S. 288, 293 (1984) (allowing reasonable time, place, and manner restrictions on speech, provided such restrictions are not content-based); City Council of L.A. v. Taxpayers for Vincent, 466 U.S. 789, 804 (1984) (describing an antisign ordinance as content-neutral); Heffron v. Int'l Soc'y for Krishna Consciousness, Inc., 452 U.S. 640, 648-49 (1981) (holding a time, place, and manner regulation on all solicitations at a state fair to be content-neutral); *O'Brien*, 391 U.S. at 367; *see also* David S. Day, *The Incidental Regulation of Free Speech*, 42 U. MIAMI L. REV. 491 (1988) (discussing the development of the less-exacting incidental regulation doctrine for examining free speech concerns); Stone, *supra* note 395, at 46 (exploring the nature of content-neutral review); Ned Greenberg, Note, Mendelsohn v. Meese: *A First Amendment Challenge to the Anti-Terrorism Act of 1987*, 39 AM. U. L. REV. 355, 369 (1990) (distinguishing between

The general rule would be examined to see whether it burdened "substantially more speech than is necessary to further the government's legitimate interests."[414] The legitimate interests put forward in favor of the ban are likely to be compelling, including the need to control money laundering, and to trace illicit transactions, particularly illegal narcotics but perhaps other crimes also.[415] Against such weighty interests, the only claims that would have any reasonable hope of prevailing in traditional intermediate scrutiny balancing would be that the same objectives could be realized with a lesser burden on speech, or that the cost to free speech was too enormous to be tolerated.

There are at least two schemes less restrictive than an outright ban on all forms of anonymous digital cash that might meet the felt needs of law enforcement. The first scheme is simply to ban only fully anonymous digital cash, and to allow payer-anonymous digital cash to circu-

---

regulations that incidentally restrict speech, which are subject to a lower level of scrutiny, and those that directly curtail speech, which are subject to a higher level of scrutiny).

414. *Turner Broadcasting*, 114 S. Ct. at 2469 (quoting Ward v. Rock Against Racism, 491 U.S. 781, 799 (1989)); *see also* Ward v. Rock Against Racism, 491 U.S. 781, 799 (1989); Schad v. Mount Ephraim, 452 U.S. 61 (1981); Schneider v. State, 308 U.S. 147 (1939). Note that not "substantially more" is a less exacting standard than "there be no conceivable alternative." *See* Fox v. SUNY, 492 U.S. 469, 478; Geoffrey R. Stone, *Autonomy and Distrust*, 64 U. COLO. L. REV. 1171 (1993) (discussing standards of review).

This intermediate scrutiny explains why public libraries can keep records of who checks out their books even if the First Amendment does protect a right to read anonymously. The library's record-keeping is a content-neutral rule that burdens no more speech than is necessary to further the government's legitimate interests in getting the books back from bibliophillic and larcenous patrons. Whether libraries can keep the information about the reading habits of their patrons once the books have been returned is a different question. It is difficult to see what interest the government has in this information; book usage statistics, for example, do not require that the identity of the patron be maintained. It may be that the First Amendment, like the American Library Association's cannons of ethics, requires that the library at least refuse to release this information, and perhaps requires that it be routinely erased.

One court rejected these arguments, albeit in a decidedly cursory fashion. *See* Brown v. Johnson, 328 N.W.2d 510 (Iowa 1983) (rejecting challenge to police subpoena for library circulation records based on chilling effect on First Amendment rights of library patrons); *see also* Carolyn M. Hinz, Note, Brown v. Johnson: *The Unexamined Issue of Privacy in Public Library Circulation Records in Iowa*, 69 IOWA L. REV. 535 (1984) (criticizing *Brown* decision for ignoring relevant U.S. Supreme Court precedents, failing to apply strict scrutiny, importance of privacy rights at stake, and failing to consider objective and subjective reasonableness of public expectations of privacy). For a suggestion that library circulation records are valuable social history that should be preserved, see SHIRLEY A. WIEGAND, LIBRARY RECORDS: A RETENTION AND CONFIDENTIALITY GUIDE 1-5 (1994). Indeed, state laws prohibiting the destruction of public records frequently apply to library circulation records. *Id.* at 11. Wiegand also reports a number of cases in which libraries have surrendered circulation information pursuant to court orders, *id.* at 139-44, and one case where the library itself voluntarily published potentially embarrassing patron circulation information in course of a campaign to shame patrons into returning overdue books. *Id.* at 141.

415. *See supra* note 299 (discussing "perfect crimes").

late. While knowledge of the recipients of large amounts of cash is of value to identifying possible money launderers, this is not a perfect solution from the point of view of maintaining the status quo. Under current rules the recipient of a large amount of cash must report the transaction and identify the payer.[416] With payer-anonymous digital cash this is no longer possible. Thus, although a world of merely payer-anonymous digital cash may be acceptable to many privacy advocates, it is unlikely to satisfy law enforcement especially if they were able to persuade legislators of the need for the broader ban. In any event, since this scheme does not fully realize the objectives of a ban on all forms of anonymous digital cash, it is not evidence that the general ban failed to be narrowly tailored for First Amendment intermediate scrutiny purposes.[417]

The second scheme relies on a technical solution. Rather than encode the identity of the owner into the cash in a form that the recipient and/or the digital cash issuer can read, the owner's identity could be encoded in a fashion that only the government, or other trusted third parties, could read.[418] The government's right to access the information in this 'Clipperized cash' could be hedged with procedural safeguards, or it could be triggered automatically whenever a Clipperized digital cash transaction exceeded current reporting limits. This scheme would meet any of the needs of law enforcement that could reasonably be asserted for an outright ban on anonymous cash—and it would protect the privacy of users against profiling by private parties—but it would do so at a cost that privacy advocates are likely to find very hard to accept. Whether this scheme would protect against government profiling of the reading and spending patterns of citizens would depend on the safeguards regulating the government's access to the identifying data.

Because intermediate scrutiny often seems to involve a balancing test,[419] whether a ban on anonymous digital cash " 'unduly constrict[s] the opportunities for free expression'" is likely to be a critical issue.[420]

---

416. *See supra* note 288.

417. A fortiori it is also not evidence that the broad ban failed to find the least restrictive means, if that is the test.

418. *See supra* text accompanying note 300.

419. *See* City of Ladue v. Gilleo, 114 S. Ct. 2038, 2046 (1994) (applying the balancing test); *Clark*, 468 U.S. at 293 (same); Consolidated Edison Co. v. Public Serv. Comm'n, 447 U.S. 530, 535 (1980) (same); TRIBE, *supra* note 132, § 12-23, at 979 (stating that the Supreme Court's balancing test examines "the degree to which any given inhibition . . . falls unevenly upon various groups").

420. *City of Ladue*, 114 S. Ct. at 2045 n.13 (1994) (quoting Stone, *supra* note 395, at 58; *see also* Wayte v. United States, 470 U.S. 598, 611 (1985) (noting that part of the test is whether an

These decisions are frankly contextual: "Each method of communicating ideas is 'a law unto itself' and that law must reflect the 'differing natures, values, abuses and dangers' of each method."[421]

In dissent Justice Holmes described the mails as "almost as much a part of free speech as the right to use our tongues"[422] Anonymous reading may yet come to be viewed as almost as much a part of free speech as the right to use our eyes. As Justice Thomas noted in his concurrence in *McIntyre v. Ohio Electrons Comm'n*, "It is only an innovation of modern times that has permitted the regulation of anonymous speech."[423] Reading has not been a traditional subject of regulation; metering or monitoring reader's habits simply clangs,[424] and if fee-based Internet speech comes to displace television or newspapers as a prime information medium, we may yet find the possibility of this monitoring, even if only by private parties, to be sufficiently intolerable to justify placing restraints on the government's power to deny readers the tools to remain anonymous.

All this is of course speculation. In the short term, and maybe longer, the Internet remains a medium in which speech is free in every sense of the word. The robustness of the speech may be the best evidence that the Internet as a medium will survive well even if anony-

---

"incidental restriction on alleged First Amendment freedoms is no greater than is essential to the furtherance of that interest" (quoting United States v. O'Brien, 391 U.S. 367, 377 (1968))).

421. Metromedia v. City of San Diego, 453 U.S. 490, 501 (1981) (quoting Kovacs v. Cooper, 336 U.S. 77, 97 (1949) (Jackson, J., concurring)); *see also* Tinker v. Des Moines Indep. Community Sch. Dist., 393 U.S. 503, 506 (1969) (First Amendment guarantees must be "applied in light of the special characteristics of the . . . environment"); Healy v. James, 408 U.S. 169, 180 (1972) (same); Southeastern Promotions, Ltd. v. Conrad, 420 U.S. 546, 557 (1975) ("Each medium of expression, of course, must be assessed for First Amendment purposes by standards suited to it, for each may present its own problems.").

422. Milwaukee Social Democratic Publishing Co. v. Burleson, 255 U.S. 407, 437 (1921) (Holmes, J., dissenting); *cf.* Blount v. Rizzi, 400 U.S. 410, 416 (1971) (quoting Holmes's description with approval).

423. 115 S. Ct. 1511, 1529 (1995) (Thomas, J., concurring).

424. In this context, it is also interesting to return to Justice Scalia's dissent in *McIntyre*:

> Principles of liberty fundamental enough to have been embodied within constitutional guarantees are not readily erased from the Nation's consciousness. A governmental practice that has become general throughout the United States, and particularly one that has the validation of long, accepted usage, bears a strong presumption of constitutionality.
>
> . . . .
>
> Where the meaning of a constitutional text (such as "the freedom of speech") is unclear, the widespread and long-accepted practices of the American people are the best indication of what fundamental beliefs it was intended to enshrine.

Id. at 1532-34.

mous speech can only be free. Indeed, from the point of view of some regulatory authorities, it may survive all too well.

V. SUMMARY AND CONCLUSION

Lily Tomlin used to do a routine as an elementary school teacher in which she threatened children that they had better do as she said, or she would make an entry on their "permanent record that will follow you for the rest of your life." If it seemed far-fetched back then—and it didn't always—it seems all too plausible now.

The public worries about threats to its privacy.[425] Yet, most popular conceptions of databases and the effects they are likely to have on social and economic life are simplistic, often focused on the danger of inaccurate records, while the more important implications of database compilation and aggregation remain poorly understood.

The coming growth in transactional and communicative records pose a little-understood danger to personal privacy, in the sense of controlling information about oneself. As records proliferate, fresh starts are harder to come by,[426] and privacy, even personal identity, are be-

425. A 1995 Harris poll found that 80% of those surveyed agreed that "consumers have lost all control over how personal information about them is circulated and used by companies." Knecht, *supra* note 348, at B1, B7.

426. The lack of accountability in anonymous communication enables a certain type of fresh start that may otherwise be hard to come by. *See* Graham, *supra* note 300, at 1395, 1411 (noting that allowing persons to conceal information about their past allows them to avoid unfavorable assumptions otherwise made by others). Indeed, people can reinvent their online persona over and over again.

When and whether people should be allowed fresh starts—or multiple fresh starts—is an interesting legal and philosophical question. For those who came to these shores of their own free will (unlike those who were already here or came in chains), the decision to come to America was itself a choice to start anew. Similarly, during the frontier period, the decision to head out West was for many a new beginning. Short of joining the witness protection program, fresh starts of that type are today more rare, and appear to be institutionalized only in an economic context, via discharge of debt in bankruptcy, see THOMAS H. JACKSON, THE LOGIC AND LIMITS OF BANKRUPTCY LAW 225-52 (1986) (surveying economic and ethical arguments for discharge). *But see* F.H. Buckley, *The American Fresh Start*, 4 S. CAL. INTERDISCIPLINARY L.J. 67 (1994) (arguing that American fresh start rule is too generous to defaulting debtor and does not well serve efficiency goals).

Several moral philosophers, including Kant, Bentham, and Hegel, opposed official pardons. Kant, for example, suggested that pardons have no place in a democratic society, since for the community to fail to punish would be a breach of moral duty. *See* KATHLEEN DEAN MOORE, PARDONS: JUSTICE, MERCY, AND THE PUBLIC INTEREST 28-49 (1989). Nevertheless, despite criticisms that they undermine the deterrent effect of the law, pardons and more general amnesties have been persistent features of the U.S. legal landscape. *See, e.g.*, Leo Martinex, *Federal Tax Amnesty: Crime and Punishment Revisited*, 10 VA. TAX. REV. 535 (1991) (arguing against tax amnesty as ineffective and likely to reduce tax compliance). Conversely, forgiveness and charity are considered virtues by several major religions.

coming less personal, more commodified. There is a drift towards increased surveillance of various forms whether de facto or de jure. Anonymity is the great potential corrective to all these trends, and is relatively easy to achieve in electronic communication over the Internet through a combination of encryption and chained computers running remailer programs. Transactional anonymity is much more difficult to arrange in an electronic payments medium. Protocols for digital coins exist that protect the identity of the payor, but not the payee. Greater transactional anonymity is possible with digital wallets that store value, and allow it to be transferred from user to user, without having to clear the funds through a third party. The degree of anonymity provided depends critically on how the wallets are implemented. It is simple to create wallets that keep full records over every transaction, and send them to the bank, or others, whenever they get a chance.

Globalized communications have already transformed the politics of several countries. Electronic mail is credited with contributing to the failure of the 1991 coup attempt in Moscow.[427] Fax communication and the presence of CNN limited the Chinese government's ability to suppress the Tiananmen Square protests of 1989.[428] The U.S. government's awareness of the presence of TV cameras has greatly shaped the public relations tactics of every foreign military operation since Vietnam.[429]

In at least the medium term, the existence of anonymous remailers and jurisdictions willing to host them means that communicative anonymity is an inevitable consequence of allowing citizens access to the Internet. The same is not true of digital cash. Although nothing is yet standardized, many of the digital coins being tested provide no transactional anonymity to the user; others provide anonymity to payers but not payees. In contrast, smart-card based digital stores of value can be engineered to afford almost any amount of privacy that the system designers choose.

The degree of anonymity afforded to communications and transactions is a critical question because of the continuing growth of personal data profiles. Consumers may have to resort to strong forms of anonymity if they wish to restrict the spread of information about their

427. LYON, *supra* note 313, at 87.

428. *See* Steven V. Roberts et al., *New Diplomacy by Fax Americana*, U.S. NEWS & WORLD REP., June 19, 1989, at 32.

429. *See, e.g.*, Matthew J. Jacobs, *Assessing the Constitutionality of Press Restrictions in the Persian Gulf War*, 44 STAN. L. REV. 675 (1992).

tastes and activities. This is especially true in countries such as the U.S. that have limited data protection laws, but it applies with diminished force even to nations with more regulation because no system of regulation can control all of the ways in which personal data can be stored, disseminated, searched, and used.

Whether or not there is a constitutional right to read anonymously, a ban on anonymous digital cash risks imposing unwelcome and perhaps poorly understood consequences on consumers. If the World Wide Web or its successors become fee-based systems in which readers are charged for access, a ban on digital cash will turn reading habits as well as transactions into tradeable data. This could have a chilling effect on readers and, depending in part on the details of the ban, on authors also.

The Internet is often seen as an anarchic medium. In some ways, as the discussion of anonymous communication demonstrates, it is. The international nature of the Internet makes some kinds of regulation futile. But not all. As the discussion of digital cash shows, ideas of anonymity and the anarchic communicative regime that it allows can be difficult to transfer to the world of commerce. The consequence of traceable transactions, not to mention traceable communication, is that the Internet or related networks may become the foundation of the opposite of anarchy: life in a transparent data ocean, a life in which data recording everyone's movements, tastes, purchases, medical history, reading habits, and contacts with officialdom are commodified and available to some, and perhaps even to all. Perhaps the information ocean is not, after all, the right metaphor. Perhaps we are headed for the information fishbowl.