UIC John Marshall Journal of Information Technology & Privacy Law

Volume 13
Issue 1 *Journal of Computer & Information Law - Fall 1994*

Article 1

Fall 1994

The Encrypted Self: Fleshing Out the Rights of Electronic Personalities, 13 J. Marshall J. Computer & Info. L. 1 (1994)

Curtis E. A. Karnow

THE ENCRYPTED SELF: FLESHING OUT THE RIGHTS OF ELECTRONIC PERSONALITIES

By CURTIS E.A. KARNOW†

". . . an artificial being, invisible, intangible, and existing only in contemplation of law."[1]

INTRODUCTION

The electronic community is faced with a now classic dilemma: the tug-of-war between the desire for a free flow of information, and need for privacy. The problem can be recast as the pull between freedom of access on the one hand, and, on the other, what might be thought of as the right of self-determination and control over the dissemination of information.[2] Often, the same individuals and organizations are vociferously in favor of both interests.[3] The interests at stake are, respectively, those of the community versus those of the individual. The conflict is the traditional juxtaposition,[4] and raises the traditional issue of rights, responsibilities, and the acceptable bounds of community power.[5] This article suggests that a new legal fiction, electronic personalities, may usefully address these conflicting interests.

---

† Curtis Karnow is a partner at the San Francisco law firm of Landels, Ripley & Diamond, and chairs the firm's Competitive Practices Group. His practice emphasizes intellectual property litigation and computer law. He is a former federal prosecutor and instructor in American Constitutional History at the University of Pennsylvania, and serves as temporary judge with various Bay Area courts. He can be reached through the Internet: karnow@cup.portal.com. This article stems from a speech delivered to the Fourth Annual Computers, Freedom & Privacy '94 Conference on March 1994, Chicago, Illinois.

1. Trustees of Dartmouth College v. Woodward, 17 U.S. 518, 4 Wheat. 518, 636 (1819) (Marshall, C.J. discussing what is now the conventional corporation).

2. *See generally* Joel Reidenberg, *Rules of the Road for Global Electronic Highways: Merging the Trade and Technical Paradigms*, 6 HARV. J.L. & TECH. 287, 289 (1993).

3. *See generally* Steven Levy, *Crypto Rebels*, WIRED, May/June 1993, at 52-54.

4. *See generally* JOHN LOCKE, TWO TREATIES OF GOVERNMENT (London: 1690); JOHN DEWEY, THE PUBLIC AND ITS PROBLEMS (Chicago: 1927). The classic antithesis has been detailed as the tension between (i) society's interests in the fair and efficient functioning, requiring sharing of data, and (ii) the individual's right to privacy. Jeff Smith, *Privacy Policies and Practices: Inside The Organizational Maze*, 36 COMMUNICATIONS OF THE ACM 105 (December 1993).

5. *See generally* LAURENCE H. TRIBE, AMERICAN CONSTITUTIONAL LAW 1302-1421 (2d ed. 1988).

THE CURRENT DEBATE

The controversy on electronic rights, or rights in cyberspace, has been thought of as the extent to which one's activities on-line are, or are not, simple extrapolations of, or variations on, activities in the "real world." For example, email is analogized to the U.S. mails; snooping in databases is analogized to looking through another's file cabinets, and governmental interception of messages is analogized to the routine "wire" or telephone call interception.[6]

Much of this makes good sense, and the analogies generally provide the right result. Breaking into another computer is very much like breaking into someone's office, and both are crimes. There is little mental exertion in taking the notion of property, such as land and chattels, and embracing the more vaporous stuff such as data, ideas and eventually information as such: the law has for a long time protected intellectual property, (the Constitution does it), and trade secrets.

But not all agree that the solution is so simple. Some have argued that the new medium and media require new rights, electronic rights, to reduce ambiguity in the application of Eighteenth century doctrines to the information age;[7] others are clear that it is simply foolish to analogize computer-stored information with documents in a safe, or to compare, for purposes of the first amendment, rights in the public marketplace to those available on an on-line service such as IBM-Sear's Prodigy.

So the debate brings into conflict those (i) who would bring rights wholesale into cyberspace and (ii) who see no room for these rights — divine, natural, or Constitutional — in the new medium. And within the first camp, there is deep dissent on the relationship between the asserted (and opposed) electronic rights of (a) privacy and (b) free access.[8]

The scope of these debates is, always, the extent of rights. These rights, it has always gone without saying, are rights which inhere, if they inhere at all, in the same types of entities we figure have always been protected by constitutions and laws: physical human beings.

---

6. Two federal statutes govern electronic surveillance and interception of domestic wire communications: the Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510-2520 (1988) (Title I) and the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801-1811 (1978) (FISA).

7. Professor Laurence Tribe's address to the first *Computers, Freedom & Privacy* conference suggested this position. *Computers, Law and Privacy Conference*, TIME, April 8, 1991 at 81.

8. *See generally* the various reports of prior sessions of the *Computers, Law and Privacy Conference*, TIME, April 8, 1991, at 81.

LEGAL FICTIONS, NEW AND OLD

But physical human beings are not the only entities protected at law, nor the only entities that have rights. And routine doctrines of standing (the analysis of who —or what— may bring a lawsuit or complain about an asserted violation of rights) have traditionally comprehended more than individual, physical, human beings.

Most obviously, corporations, partnerships, and associations have substantive rights, and have the procedural right to bring suit. They also have rights to due process of law, to have those substantive rights enforced. Companies sue, and can be sued; they have lawyers and can invoke first amendment rights to free speech. All of this is quite separate, by definition and intent, from the rights and liabilities of the individual human beings who jointly own the company.

The law abounds in further examples: we find a plethora of specific entities with rights and standing to sue or be sued,[9] and quasi-entities,[10] or procedures which dispense with the need for the specific real humans who have the real interest in the lawsuit.[11]

---

9. For example, partnerships of all sorts, trusts, sole proprietorships, estates in bankruptcy and estates in probate, governmental entities such as municipalities, states, transportation boards and on and on. In a wide variety of contexts, "organizations" [which can encompass virtually any imaginable construct] conduct legal business such as lobbying, exercising first amendment rights, and often suing and being sued; although in the latter capacity, the standing of the organization may be precisely co-terminus with that of its real members. Associated General Contractors v. City of Jacksonville, 113 S. Ct. 2297 (1993) (on behalf of various civil rights organizations, this author prepared the *amicus* brief in that case). Those members, however, need not be humans: they may be corporations or other business entities. *See, i.e.*, Hunt v. Washington State Apple Advertising Commission, 432 U.S. 333, 97 S. Ct. 2434 (1977) (association has standing to assert the claims of its members even if the association has suffered no injury).

10. Note for example, so-called *in rem* proceedings in which specific items such as cars, ships, and money are "litigants." *See, e.g.*, The Gylfe v. The Trujullo, 209 F.2d 386 (2nd Cir. 1954) (ship collision litigation); United States v. $149,442.43 in U.S. Currency, 965 F.2d 868 (10th Cir. 1992); United States v. One (1) 1976 Cessna Model 210L Aircraft, 890 F.2d 77 (8th Cir. 1989). *Compare* the famous, or notorious, dissent of Justice Douglas in Sierra Club v. Morton, 405 U.S. 727, 741, 743 (1972), where Douglas suggested that trees and other inanimate environmental objects [ridges, groves of trees, lakes, "or even air"] should have standing so that environmental suits could be filed directly on their behalf. The suggestion was not warmly received by other judges, with very good reason. Standing, and the legal existence and inhering rights the standing doctrine implicates, are ineffectual without clear (i) methods of identification and (ii) forms of accountability. In short, no rights without responsibility. (Compare my discussion of electronic personalities below.)

11. Class actions use a few individuals to represent the interests of others; other representatives guardians ad litem, e.g. in example for children or incapacitated adults; and state attorneys general who litigate on behalf of citizens of states.

There is room, in the law, for a variety of entities with a variety of competing interests, and humans are not always the first choice.[12]

The corporation was molded to its modern form by extraordinary developments in trade and economics.[13] I suggest the extraordinary developments in technology, and specifically the information, or digital, revolution, gives rise to a new legal entity: the electronic persona.

The new entity is bred between the anvil of free flow of information, and the hammer of security and privacy. As with the development of the corporate form, the central function of the new legal entity is simultaneously to (i) provide access to a new means of communal or economic interaction, and (ii) shield the physical, individual human being from certain types of liability or exposure.

At first, the notion of an electronic persona rises as a convenience, a shorthand; and in that spirit I offer the contraction "eperson" or "eper."[14] Later, the term may become indispensable to ordinary discourse; we are at that point now.[15] Subsequently, the notion may mature [sic] into the legal jargon. When such terms become a necessary convenience in the law, they are near to the blessed status of a legal reification; also known as a legal fiction.[16] Legal fictions are not small potatoes; cases are won and lost on their adoption.[17]

---

12. *See* American Dental Association v. Shalala, 3 F.3d 445 (D.C. Cir. 1993), in which the statutory term "entity" was held to apply not to humans, but only groups and organizations. Under the 1986 Health Care Quality Improvement Act construed in this case, it is an "entity" which has the duty and obligation to make certain reports, and which thusly may incur certain forms of liabilities.

13. *See e.g.*, MORTON J. HORWITZ, THE TRANSFORMATION OF AMERICAN LAW 1780-1860 111 *et seq.* (1977); *see generally*, DAVID WARSH, THE IDEA OF ECONOMIC COMPLEXITY (1984).

14. Better terms may come. And I actually prefer the terms "tuples" by analogy to peoples, and "tupern" by analogy to "person." The notion of tuple-space inspires the analogy. *See generally* DAVID GELERNTER, MIRROR WORLDS (1992). To date, I have seen allusions to avatars, personae, agents, virtual people, virtual team-mates, knowbots, alter egos, personages and so on. These do not all have the same meaning; and none, as far as I know, have the legal connotation that I intend with my term. Nevertheless they have in common the depiction of personae that inhabit only the electronic world, and that in some fashion stand in for, or represent, an originating human. *See also* JOHN BRUNNER, THE SHOCKWAVE RIDER 42 ("olivers" as electronic alter egos) (Ballentine Books, New York: 1975).

15. *See, e.g.*, C. Morningstar & F. Randall Farmer, *The Lessons of Lucasfilm's Habitat*, CYBERSPACE: FIRST STEPS (M. Benedikt, ed. 1992), reprinted in VIRTUAL REALITY 93 - SPECIAL REPORT (AI EXPERT) 23, 25. See the topic of the featured speaker at the *Metropolitan Chapter of the Human Factors & Ergonomics Society's 1993 Annual Symposium (Virtual Reality: Through the Looking Glass*, November 18, 1993): Sudhir R. Ahuja, *Multimedia Communications: Conversations with Real and Virtual People.*

16. This occurs when there is a basis in legal commentary for the orderly, defined use of the term; and an enterprising judge decides to take the plunge. These notes are part of that commentary.

17. There are legal fictions about "notice" to others, such as the content and restrictions of deeds filed in Recorder's offices and elsewhere in City Hall, and items on file with

RESIDENCY: CYBERSPACE

Cyberspace is increasingly the location of information, now digitized information.[18] There is a key, if obvious corollary: we are compelled, in some fashion, to participate on-line if we want the information.

Certainly we may participate because we wish to, as a character in a MUD[19] or browsing for pleasure in the files of an interesting Internet node. But we also participate involuntarily, if often indirectly. And it is this type of interaction especially which gives rise to the eperson. We have these electronic relationships with banks, insurance companies, vendors and credit bureaus, employers, governmental agencies including the courts, the Internal Revenue Service and law enforcement agencies —the list is practically endless[20]— and they all mandate our incorporeal participation. One's interaction with each of these is, in great part, an interaction with information in cyberspace.

And there is a lot of it, this digital information. Where at one time systemantics might have pronounced, "If it isn't official, it hasn't happened,"[21] it is now perfectly credible to suggest that, unless it's in cyberspace, it doesn't exist. This seems a bold reversal: a form of virtual reality edging out the physical thing, but it's plainly true.[22]

---

the U.S. Patent Office, which the law treats as effective as actual knowledge. Suing a corporation when one ought to have sued a stockholder, or vice-vera, can be fatal.

18. Average growth rate for networks (globally) in 1993 was about 7.4 % per month. Larry Press, *The Internet and Interactive Television*, 36 COMMUNICATIONS OF THE ACM 19 (December 1993). The number of hosts and domains advertised in the Internet domain name system have risen during the twelve months from April 1992 to April 1993 as follows: hosts, 67% [from 890,000 to 1,486,000]; domains, 10%.

19. The Internet's FAQ (frequently asked questions) on MUD's says it best:

A MUD (Multiple User Dimension, Multiple User Dungeon, or Multiple User Dialogue) is a computer program which users can log into and explore. Each user takes control of a computerized persona/avatar/incarnation/character. You can walk around, chat with other characters, explore dangerous monster-infested areas, solve puzzles, and even create your very own rooms, descriptions and items. You can also get lost or confused if you jump right in . . . . There are very many kinds of MUD programs out there — probably as many as there are computers that run them. The Tiny- and Teeny- family of MUDs are usually more 'social' in orientation; the players on those MUDs gather, chat, meet friends, make jokes, and discuss things. The LP- family of MUDs are based on roleplaying adventure games. In these, your character runs around killing monsters, finding money, and making experience in the quest to become a wizard . . . .

This and related files are available via the Internet, on the Usenet newsgroup rec.games.mud.announce.

20. ROB KING *et al.*, MASSIVELY PARALLEL COMPUTING AND INFORMATION CAPITALISM, A NEW ERA IN COMPUTATION (MIT: Cambridge: 1993) 216, *et passim*. Information occupations [the information labor sector] blossomed from 17% of the total workforce in 1900 to 55% in 1990. *Id.* at 220-221.

21. JOHN GALL, SYSTEMANTICS 47 (1986).

22. We each have an apocryphal story. A few months ago I was told I hadn't ordered books, nor paid for them, because that was the state of the computerized record. Worse, I

This is far more than simply an agglutination of data, more databanks and on-line resources;[23] and it is more than increased bandwidth,[24] and more interconnectivity.[25] The central, emerging development is the collapse of the virtual and real worlds. Real events are controlled by computers; people operate computers in just the same way regardless of whether real events or "simulations" are the planned outcome.[26] For the interface to both the real and virtual worlds is, increasingly, the machine;[27] and the universal machine itself, the computer.[28]

There is no better example of this collapse of the real and virtual than on the battlefield.

> There is no technological reason why warfare should not eventually becomes completely automated, fought with machines and computerized missiles with no direct human intervention. As the battlefield becomes more automated, the battle itself becomes more like a [video] wargame.[29]

---

paid a parking ticket last fall because the computerized record had the license plate and make of the car I had rented; I hadn't actually parked in the area where the ticket issued, but I knew no one would take my word over the computer register.

23. *See* Richard Glidewell, *Winners In Data Delivery*, UPSIDE, Feb. 1994, at 60. (increasing ease of securing massive amounts of data via electronic delivery: residential and business listings, financial and SEC filings, etc.).

24. George Gilder, *Interop* '93 keynote speech (San Francisco, August 1993) has suggested that the prospective wide-spread use of fiber optic cable will eliminate bandwidth as a concern for the transmission of data. *See also*, WIRED, September/October 1993, at 38.

25. *Supra* note 19 (increase in internet nodes).

26. Compare formal flight simulators, the heads-up display of a F-16, and current Air Force head-mounted displays used in real airplanes. *See generally*, Lt. Colonel Martin R. Styz, *An Overview of Current Virtual Reality Research And Development Projects By The United States Department of Defense*, Proceedings, LONDON VIRTUAL REALITY EXPO 94, 152 et seq. (London, England, February 1994); Michael Moshell, et al., *Virtual Environments for Military Training: SIMNET, Ender's Game, and Beyond*, VIRTUAL REALITY WORLD, Summer 1993, at v-1; *Industry And Military Show Capability*, 13 CYBEREDGE JOURNAL 14; M. Gembicki and D. Rousseau, *Naval Applications of Virtual Reality*, VIRTUAL REALITY '93, 67 (AI Expert). *See also* David Bella, *Rethinking The Unthinkable*, 12 IEEE TECHNOLOGY AND SOCIETY MAGAZINE 9 (Fall 1993) (formal problems of modeling); *VR-NASA's Training Vision*, 15 CYBEREDGE JOURNAL 1 (May/June 1993) (NASA and armed services). As an expert in the field has noted, "it is a very short step from the simulated world to the real one." Roger D. Smith, *Current Military Simulation and Integration of Virtual Reality Technologies*, VIRTUAL REALITY WORLD, March/April 1994, at 45-50.

27. An outstanding study of this phenomenon is found in SHOSHANA ZUBOFF'S IN THE AGE OF THE SMART MACHINE (New York 1988). "[A] powerful new technology, such as that represented by the computer, fundamentally reorganizes the infrastructure of our material world." *Id.* at 5.

28. *See* David A. Mindell, review of THOMAS B. SHERIDAN, TELEROBOTICS, AUTOMATION, AND HUMAN SUPERVISORY CONTROL (MIT 1992), *in* 12 IEEE TECHNOLOGY AND SOCIETY MAGAZINE 7 (Fall 1993).

29. FRANK BARNABY, THE AUTOMATED BATTLEFIELD: NEW TECHNOLOGY IN MODERN WARFARE 1 (Oxford University Press 1987), *quoted in*, BENJAMIN WOOLLEY, VIRTUAL

An increasing fraction of our social and economic time is spent on-line; in cyberspace if you will. Contracts, business advances, and financial exchanges are accomplished there; politics and sex— well, sexual relations— are conducted there; entertainment, of course, is shifting to that forum. There is nothing to stop the fusion.[30]

But there are important differences between the virtual on-line universe, and the real world. The virtual world is infinite: not just in theory, like the real world, but in a practice, in a way that every inhabitant knows. Time and space are infinitely extendible, and the shape of the place is subject to the whims of the one and of the masses.

There is something else here, too; and that is the power of the immersive experience. Virtual reality, as a wholly engrossing, full sensory experience is available now albeit at high prices; and within a few years at consumer prices. There, anything that be can be supposed will be.

This virtual reality has no inherent restraints: not time, not space, not physical laws; it is total immersion. That is where we do, and will, conduct the business of the 'real' world; that is the residence of the eper.

THE EXPOSURE TO INCURSIONS

But we resist the incursion of the virtual. That way be dragons, for real. The possibilities for fraud and deception are co-extensive with the scope of the imagination here.[31] Given the strikingly intensive experience of a virtual session,[32] there is a substantial potential for emotional attack on the sensibilities of humans. In more ways than one, we need to limit our exposure, our liability.

When we secure a library card, we do not want to be interrogated on our finances; when we buy a plane ticket over the phone with a credit card, we don't feel the need to provide information on our home, where we live, our job, or our mother's maiden name. We are profoundly offended when the Internal Revenue Service collects our writings in a database to do its work or the Central Intelligence Agency engages in domestic spying. Many were horrified when Lotus thought to collect demographic information easily available on-line, and package it in CD-

---

WORLDS 191 (Blackwell 1992). Woolley's book, especially his chapter on hyper-reality from which his quote is taken, strongly makes this point.

30. BENJAMIN WOOLLEY, VIRTUAL WORLDS 133 (Blackwell 1992): "Perhaps cyberspace . . . . is also the place where events increasingly happen, where our lives and fates are increasingly determined. . . ."

31. *See infra* note 36, and accompanying text.

32. WIRED, September/October 1993, at 116; Interview with Dr. Thomas Furness, VIRTUAL REALITY WORLD, Summer 1993, at q-1, ("I've learned how powerful a medium this is. This immersive environment, this "circumambience" of visual, auditory, and tactile information, gives us the opportunity to—in essence—do away with the medium . . . the medium disappears.")

ROM for mass-market vendors. Digital information moves at lightspeed, and it respects no frontiers. We need a coherent theory of limits to information access.

It is also true that as mundane work and social intercourse move from the physical to the electronic world, there is increasing scope for the ownership of things and environments that previously unambiguously belonged to us all, or to no one. Software solutions, in for example, aircraft control systems create "artificial control laws" which may be proprietary, replacing 'natural' systems such as stick and rudder.[33] Physical things like apples and sticks, and physical environments of oxygen and sand, are free; but virtual apples and electronic pointing devices may be the subject of copyright and patent law, and computer environments often belong to someone like AT&T or Microsoft.[34]

We need to limit our exposure to others' claims of property rights; to their exercise of the raw power of ownership.

This is not so much a question of eliminating the information or interaction available on-line: that simply can't be done without dismantling the computer-mediated infrastructure upon which this country, and the global economic society, rests. Rather, the impetus here is to segregate information, to compartmentalize it. In short, there is a felt need to mask oneself, from time to time, place to place, context to context. And such is precisely the function of a personality: there is no privacy without a shield and mask.

Personalities can choose between public broadcasts and private communications. We recognize the right to this bicameral approach with physical persons; we need the same limits in electronic space. Legal electronic personalities — entities with enforceable rights — provide a model. These epers provide the basis for a rationale for limits to access to data.

PREDICATES TO RIGHTS: ACCOUNTABILITY & IDENTIFICATION

It is not much good to allow rights without responsibilities, without accountability. The notion of entitlement is gibberish unless limited; for a plethora of unbounded entitlement is an oxymoron.

At first blush, the notion of an accountable eper, too, sounds like an oxymoron. These things, surely, flicker on and off, as transient as a grounded charge. New ones can be created on whim; a single human

33. Robert D. Dorsett, *Safety In The Air*, 37 COMMUNICATIONS OF THE ACM 146.

34. I have outlined elsewhere a concomitant slow movement from the priority of public law to the supersession of private arrangements, and private fiat, in the protection of technology rights. Curtis Karnow, *Protecting Technology Rights In The International Arena*, PROCEEDINGS, LONDON VIRTUAL REALITY EXPO '94, 91 *et seq.* (Meckler: London, Feb. 1994).

could set a thousand epers free every day.[35] Surely, there is some need for the persistence of a legal entity.

There is indeed such a need: one must be able to hunt down a legal entity, to pin it down, stop it, and if necessary, extirpate it.

But epers are no more transient legal entities. Recall that corporations and organizations of all sorts come and go; they rise and fall like Italian governments. And corporations beget corporations. Not only that, a single human can form a thousand corporations, join a million charitable organizations and leave estates in 50 states.

Essentially two strongly related mechanisms strive to check abuse: (i) the formalities of formation must be observed, or the courts will ignore the corporate form, and (ii) the legal fiction will be ignored in cases of fraud. So, for example, co-mingling the assets of the company and stockholders, failing to call stockholder meetings or have a board, or failing to provide the company with sufficient capital, may all indicate that the corporation does not really "exist." Or if a slew of partnerships and corporations are used to shift funds away from legitimate creditors, they might all be disregarded by the courts.

In short, while all these legal fictions are in some fashion transient, the legal system has appropriate methods of dealing with transgressions. When problems arise, the law first comes after the legal fiction; when the legal form is abused, the law disregards the fiction and comes after the individuals. Similarly, when people are offensive on the net, they are cajoled by the rest to change their behavior; the offenders can be locked out of certain areas or conversational exchanges. Ultimately, the physical human who releases epers for malicious reasons will himself be ex-

35. An eper is a program. The notion of an "object" as used in object oriented programming comes a little closer to the thing I have in mind, because such objects combine notions of data and instructions. Like all software, these things can be replicated and turned off and on. Currently, there are a host of program-like entities that suggest epers. For example, we have software "agents" and "experts" in spreadsheet programs made by Borland and Microsoft that assist the user. *See generally*, Lawrence M. Fisher, *Using 'Usability' To Sell Spreadsheets To The Masses*, N.Y. TIMES, Feb. 6, 1994. Even closer, note the recent announcement of "intelligent" agents made by General Magic. These, once released into the telecommunications net, would execute tasks on behalf of their humans, interact with other agents to conduct business on behalf of the human originator, and report back. *See generally*, Curtis Karnow, *Alters*, WIRED, November 1993, at 114 (written before General Magic announced its product); BUSINESS WEEK, Jan. 24, 1994 (on General Magic's agents); BUSINESS WEEK, Jan. 17, 1994 (same). *See also*, Jim Louderback, *Time To Get Smart About Controlling Your Agent*, PC WEEK, Oct. 11, 1993, at 92; 37 COMMUNICATIONS OF THE ACM (Special Issue: Intelligent Agents), July 1994. Finally, I note some interesting work being done just where we would expect in this context, that is, at the intersection of AI (artificial intelligence) and virtual reality. Jonathan D. Waldern, et al., *A Note on Software Design of Virtual Team-mates and Virtual Opponents*, PROCEEDINGS, LONDON VIRTUAL REALITY EXPO 94 (Meckler: London, February 1994).

communicated or otherwise attacked.[36]

We can also insist on the "formalities" of releasing epers into the net. Epers may be identifiable, as are humans are through their appearance, by the space they take up, and by fingerprints. Security is essential, and security is a direct function of "sophisticated methods of identification."[37] Today, this identification ritual is generally accomplished though passwords, or other forms of semantic fingerprints. For some computer systems, there are varying degrees of access with concomitant identification required. But these systems are limited, and inflexible. A few, not an infinite number of audiences are supported.

In theory, the problem has been solved with the use of public key encryption. There are an infinite number of such encryption keys. The method of encryption allows the encryptor — indeed, an infinite number of such encryptors — to choose a select audience, to create a broadcast for a wide audience or to narrowly focus on a specific target. And, critically, public key encryption allows unassailable identification: one eper cannot imitate another.[38]

Transience is as transience does. Stand-alone PCs are turned off and on every day, providing the metaphor for the ephemeral eper; but in short order this may change. Our machines may be on all the time, like refrigerators or the phone, ready to provide information at any time.

---

36. Internet lore tells of Joey Scaggs, a man of a thousand byte-faces. He impersonated others, and let loose fantastic fibs, such as the invented rumor that the Canadian Government was responsible for some nefarious import ban. This caused others to write by the hundreds of thousands to the Canadian government. Eventually, Scaggs was physically located; other rumors suggest that the defenders of the Net then had a thousand pizzas sent to his home, and implemented other direct, physical retaliation against the real Joey Scaggs. There are lots of rumors about Scaggs; he does exist, but he's invented parts of himself. WIRED, Feb. 1994, at 31. *See also*, Jim Moody, *Online Scam: Danger In Cyberspace*, MULTIMEDIA WORLD, Mar. 1994, at 68 (using on-line alias to con victims into sending money: "her MO is based on creating a false reality and persuading the victim to live in it").

37. Reidenberg, *supra* note 2.

38. *See generally* Brian Hayes, *The Electronic Palimpsest*, THE SCIENCES, September/October 1993, at 10. Among the best known public key encryption programs is Phil Zimmermann's Pretty Good Encryption ["PGP"], generally available as freeware. There is a lot written on public key encryption; see for example, Zimmermann's own zipped manuals accompanying PGP (available via internet FTP from MIT: net-dist.mit.edu pub/pgp); Max Schireson, *Decoding The Complexities of Cryptography*, PC WEEK, Jan. 10, 1994, at 84; John Perry Barlow, *A Plain Text on Crypto Policy*, 36 COMMUNICATIONS OF THE ACM, ACM 21 (November 1993); Steven Levy, *Crypto Rebels*, WIRED, May/June 1993, at 54; Chris Galvin, *The Digital Deadbolt*, COMPUSERVE MAGAZINE, November 1993, at 19; Jonathan Erickson, *Cryptography Fires Up The Feds*, DR. DOBB'S JOURNAL, December 1993, at 6. *See also Computer Security: Hearings Before the Subcomm. on Technology and Competitiveness of the Comm. on Science, Space & Technology, U.S. House of Representatives*, 102nd Cong., 1st Sess. 32, 35-37 (1991) (testimony of Stephen T. Walker discussing export controls on cryptography software).

Electronic personalties may not be inherently more ephemeral than "real" ones. Certain strands from philosophy and other writings on the mind, from Hume[39] to Minsky[40] and Dennett,[41] provide a compelling picture of highly transient and constantly mutating human mental states. The issue is not whether epers (or humans or corporations) can be thought of as transient — they can, of course. The issue is whether persistence can be established in some legally relevant fashion. The answer is in the affirmative.

Finally, under the rubric of accountability, I should briefly note that epers may present the same dangers we face every day from other programs: that of contamination by viruses[42] and other digital malice. Because epers are likely to be modified by their encounters, i.e. by the data and instructions upon which they draw to make decisions,[43] their effect on other systems is not wholly predictable. Appropriate security systems should be put in place, as they should be in any event, to protect against intrusions.[44]

FRAMING RIGHTS TO ILLUMINATE THE PUBLIC/PRIVATE BORDER

The notion of epers provides the framework, espalier, for the debate on conduct in cyberspace. Rights are conferred on epers for the same reason they are conferred on humans in the physical world: because there are powerful forces that we wish to restrain; and we cannot re-

39. DAVID HUME, ENQUIRIES 152-53, 159 (L.A. Selbey-Bigge ed. 1902); DAVID HUME, A TREATISE OF HUMAN NATURE 306-310 *et passim* (E.C. Mossner ed. 1969) ("[t]he identity, which we ascribe to the mind of man, is only a fictitious one . . .").

40. *See generally* MARVIN MINSKY, THE SOCIETY OF MIND (1985).

41. *See generally* DANIEL C. DENNETT, CONSCIOUSNESS EXPLAINED (1991).

42. *See generally* MARK LUDWIG, THE LITTLE BLACK BOOK OF COMPUTER VIRUSES (1991).

43. Lest we envision digital monsters running amuck through the ether, recall that even the most common program we use in daily life — a word processor — is modified by use, and not always predictably. Genetic algorithms and associated programming techniques, whereby development software in essence writes its own programs, may promise more radical departures. Andy Singleton, *Genetic Programming With C*, BYTE, Feb. 1994, at 171. *See generally* JOHN HOLLAND, ADAPTION IN NATURAL AND ARTIFICIAL SYSTEMS (1992).

44. A discussion of such systems is beyond the scope of this article. I note, though, that the handling of mutating polymorphic viruses is not a new problem. For example, we have the so-called Tremor virus, which is a full stealth, self concealing polymorphic virus. It infects the command.com and other *.exe (program) files, including the terminate-and-stay component (TSR) of an earlier edition of Central Point's Anti-virus program; i.e. Tremor is specifically designed to kill a program designed to hunt the virus. Tremor was built with readily available mutation engines. Presumably current anti-virus programs can detect it. *PC Week*, December 27, 1993, at 81.

strain those forces with countervailing raw power. We need a consensus that such raw power shall not ipso facto have its way.

Significant power is employed by those who control the medium: the providers of bandwidth, electricity, fiber, hardware such as satellites and nodes, private electronic space providers such as Sears-IBM's Prodigy, CompuServe, General Electric,[45] and Motorola;[46] universities; and governmental agencies such as the Department of Defense, National Science Foundation and the Federal Communications Commission. And we should also be concerned about the repositories of information: banks and credit services, governmental agencies and the rest: they too must be restrained.[47]

Against these forces epers must be allowed some room, so that literal ownership of (i) the means of communication and (ii) agglutinated information does not thereby confer rights with respect to the content of the communication and the dissemination of the information.

This suggests the outline of a few rights for epers.

Most centrally, epers should have the right to decline to produce information aside from key identification materials: i.e., they must be allowed to act as a shield for the originating human's privacy. To do this, epers need to be able to own money and bank accounts, and they need to have access to credit.

Secondly, epers should not be arbitrarily deleted, and others should not refuse to deal with them. If an eper has the money to buy something like an airplane ticket or make a hotel reservation, or if it seeks out otherwise free information, then it should have the right to complete its task. In short, no redlining.

---

45. These three operate private electronic information transfer stations: there we find bulletin boards and electronic mail for the exchange of information, and data and software for distribution.

46. Motorola is planning the Iridium project: a global communications coverage service based on 66 communications satellites. Joe Flower, *Iridium*, WIRED, November 1993, at 72.

47. In the electronic world, power is as an initial matter wielded by what we would now call a combination of public and private forces; later, in the context of cyberspace, we may well dispense with the line between public agencies and private companies. *See generally* Curtis Karnow, *Implementing the First Amendment in Cyberspace*, VIRTUAL REALITY WORLD/MULTIMEDIA REVIEW, Summer 1993. The dissolution of the line between public and private, and the transition from the public to the private exertion of potentially controlling force is significant, for it eviscerates the traditional restraints on the exercise of overwhelming force. Those traditional restraints are constitutional rights, which act as restraints only on public, or governmental, and not private, power. There are, therefore, grave problems with the applicability of constitutional shackles to the [mostly] privately-owned authorities of the electronic universe. As my article cited above in this note suggests, however, the public forum and other doctrines are available to enfranchise the users of privately owned channels of communications; and a number of statutes impose duties on private individuals (not to discriminate, for example) which can be applied to epers should they be granted legal recognition.

Thirdly, epers should have the right to communicate; to move about in electronic space and to post messages.

These three rights are in short: (i) privacy, the right to be left alone; (ii) the right to be free of discrimination, to be able freely to conduct social and economic business; and (iii) free speech.

I suppose the last — free speech, perhaps the central civil right for humans — is therefore the one least needed by epers. When we talk, we generally want to be recognized as the speaker, because we are proud of our thoughts and because others often do not take kindly to anonymous discourse: credibility and the power of the word are still frequently *ad hominem* affairs.

No, epers are most useful when we need to communicate but still need a shield: when we want to maintain intact the ramified divisions of our social and economic lives. For privacy is not truly a matter of an absolute barricade; it is instead inhibiting the spillover of information from one place to another.

Someone you know has your drivers license number, and your license plate number, and knows the car you drive; many people may know of your arrest record, dozens or more may know how much you earn, the problems with your batty Aunt Cathy; and every store you shop at - thousands of employees? - has your credit card numbers. The local library knows which books you like, the video store knows your taste in home entertainment. The local grocery store knows your addiction to Twinkies or bad wine. And in almost every one of these cases, you gave out the information, and under many definitions of the term, the information is all "public."

One's expectations are not violated by knowing that some unknown has the information; rather, one is bothered when information crosses over an invisible restraint; when the librarian also knows about Aunt Cathy and your athlete's foot, when the people at the hospital know not only about the gall bladder but the four speeding tickets and the fact that you buy ten cans of creamed corn a week.

This is quite different from suggesting that certain facts are inherently private, for few really are. This is too bad, because it is far easier legally to simply block the dissemination of a defined type of information than to erect diverse boundaries to certain distributions of certain information, depending all the time on the context.

We have to face the fact that all this information (and more) is out there, and cannot ever be called back home. It never was back home, of course; medical records and license plates and credit card information have always been widely disseminated. (The forces driving free access and transmission of information are very strong; not just social and political influences, but similar to a force of nature, like gravity or hydrau-

lics.) Information tends to dispersion. Finally, it cannot be controlled. This should be treated as a law of nature.[48]

Here we find the central contribution of the eper. Let us recognize that not being able to move about and act freely in the electronic world is disenfranchisement of the most emphatic sort. As I suggested, the business of the real world is conducted in cyberspace. If one cannot enter there, one cannot act.[49] Epers can provide the anonymity that this compelled exposure would destroy. Multiple epers can conduct business and— this is the point— keep information segregated. Epers are related only through the human progenitor, and that link can be encrypted. In a universe of utterly accessible mutating data, epers help ensure both access and privacy.

For these roles, epers must have at a minimum (i) the right of privacy, the right to be left alone; and (ii) the right to be free of economic discrimination.

CONCLUSION: EPERS, PERSONS & PRIVACY

The recognition of epers, and their admission as bona fide legal fictions, will affect and be affected by our mutating notions of self. These are consequences worth noting, especially as it is all too easy to mistake epers for humans- and to be afraid of that confabulation; or to urge it in some mistaken, bizarre push for the next generation of intelligent beings.

It is always error to mistake the self for its personalities, or the shadow for the object. True, the acts of personalties and their accoutrements — clothes, speech, body gestures, art on the walls — all derive from the self, but they all also protect and shield the self, that internal person who is made up of secrets and thoughts and unshared opinion.

Epers do not replace real people; they protect people, and confusing the two is like confusing a person with his car, clothes, art, and house.

But we are powerfully tempted to the confusion. The line between public and private is a tenuous one, and it constantly changes.[50] Certainly every personality, each public display and every legal fiction says

48. It is primarily for this reason that I have no confidence in laws designed to restrict the spread of data or software. There is nothing more futile than the British or Canadian Governments trying to bar news of high profile lawsuits; or the U.S. Government trying to stop the distribution of strong encryption software, or of erstwhile governments in the Soviet Block trying to block the news. Never mind the Internet and high technology (few in Poland or the Soviet Union had computers); many listened to the shortwave radio.

49. "Sandy Locke, so far as the data-net was concerned, had been deleted from the human race." JOHN BRUNNER, THE SHOCKWAVE RIDER 140 (1975).

50. "So long as it is our habit to confuse art with life, what appears on-stage will appear off; and what appears off-stage will be staged." PHILIP RIEFF, FELLOW TEACHERS 103 (1972).

something about the originating progenitor. Perhaps there is no line, fine or otherwise, between humans and their manifestations. At some point, a person *is* one's armor; wear it long enough, and the flesh and metal stick and blend. So it can be no small thing to take on an incarnation; use it long enough and it may shape the incarnate.

All of this matters very much, because there is no good sense to the idea of privacy until we have separated out the self for protection and from its public appearances. But the problem appears intractable: now as in Dewey's time, "both words, individual and social, are hopelessly ambiguous, and the ambiguity will never cease as long as we think of ourselves in terms an antithesis."[51]

I do not know how it used to be. Perhaps in the Sixteenth Century, or in Chaucer's England, there were precise and understood lines that could pinpoint the private, and save it always from exploitation by the public. I don't think so; and it is not true now. Our notions of privacy are, or should be, wrapped in the delicate finery of manners, in the sometime ephemeral practice of propriety. These depend on an acute sense of context, of what is appropriate, and when. Not, exactly, that there are secrets, but that there are secrets before this person, or in this place. In this framework, it is inappropriate for my doctor to discuss certain matters with my grocer, and inappropriate for the Department of Motor Vehicles to send my record to my local library, improper for my co-workers to know every magazine I subscribe to. For reasons outlined above, laws cannot appease my sense of outrage when these corruptions take place, and laws will not stop their outbreak.[52]

Instead, I must have the right to segregate the information about myself at the very outset and to do business under my chosen aliases; to use my epers. In so doing, I will define what I think of as "private" characteristics, just as I delineate what I am willing to parade in public, incognito.

The growth of the information industries and the cyberspace which they have made have produced a new type of personality. This is the demographic person, whose attributes are statistical, financial, evidenced by records of consumer choice. This is man as junk mail target. Surely this is not what we seriously mean when we speak of the self and its private arena; this is not what needs to be saved from being commingled with the public world. Indeed, this cannot be saved from the public domain.

But, offended by uncontrolled disclosures, we do think that we, our selves, are at risk when these data are spread around. We do lose ourselves in an electronic sea, this sensuous, potent and overwhelming bar-

51. Dewey, *supra* at 186.

52. *See supra* note 49 (law of nature).

rage of input and image; and we lose a strong sense of the inviolate, central self as we conflate self with data about our selves. Let us instead confer these attributes of mass market identity on our public personae, on our epers and other conspicuous incarnations, and so reclaim our distinct, and truly private, selves.