THE TWO-TIERED ETHICS OF ELECTRONIC DATA PROCESSING

Edmund F. Byrne, Indiana/Purdue University at Indianapolis

Who owns electronic data, and under what conditions may another take them for his or her own use without being considered a thief? The electronic data processing (EDP) industry's answer to these questions is that electronic data belong to no one before they are collected but once collected they are property, so only those who take *collected* data without authorization are stealing. Personal privacy is unquestionably involved in the original taking; but the major EDP users routinely sacrifice such concerns to the preeminence of private property. But, I argue, this selective approach to the claims of private property is built on assumptions more readily associated with conquest than with a community of equals.[1]

In particular, the major EDP users operate under four questionable assumptions: (1) that at no point in the process do electronic data belong to their subjects; (2) that electronic data are not a public good; (3) that the major collectors and their consumers are not free riders; but (4) others are if they use what has been collected without paying. Though inconsistent if laid out on a level playing field, these assumptions are mutually tenable if ownership rights are reduced to the prerogatives of power. But this two-tiered ownership system creates a rule of law in behalf of the strong while leaving the weak in a state of nature—in other words, a two-tiered ethics of EDP.

This two-tiered ethics is arguably efficient; but, I contend, it is not equitable. To support this contention, I will assess the current state of affairs by drawing on two concepts familiar to political economists: public goods and free riders; but I will add a third concept to their repertoire: the Reluctant Samaritan.

l. Taking, in a Bifurcated Polity

It is generally considered wrong to take something that belongs to someone else. If the taker is acting in behalf of a group, however, the status of the group makes a difference. A taker is more likely to be praised if doing so, say, for a respected intelligence agency than if in the service of a pariah organization. If the group is, or is acting for, a major corporation, some may complain; but its actions will be socially tolerated if they are consistent with the principles of market liberalism.[2]

Market liberalism divides society into a public sphere and a private sphere and justifies this division by the complementary ways in which each serves the interests of private property. This assignment of political preeminence to private property tends to exempt owners from responsibility for non-owners; and anything can in principle be owned. But not everything is worth owning: goods are not worth owning if an owner's costs exceed benefits. If the benefits are nonetheless desirable, an alternative to purely private ownership may be constructed.

Public goods (PGs), according to economists, are by nature nonexcludable: if available to payers, they are available to nonpayers as well; hence, according to a traditional argument, their fair distribution requires government intervention, notably by means of taxation and law enforcement. So the economist's concept of a public good has a *negative* connotation: government is involved only by default. This negative connotation is, however, misleading. If equal distribution is considered a necessary condition for a PG, then none exists (even the most commonly cited example, national defense, manifestly benefits some more than others); but if the equal distribution requirement is dropped, then all goods are in some respect PGs because none is perfectly excludable. So some government (private, if not public) would seem to be a necessary condition for *effective* ownership of any goods. This is especially so because of the free rider problem.

To an economist, a free rider is one who receives a benefit without helping to cover its costs. A free rider is not a thief, in any moral sense, because the free rider takes some of a PG which by definition is not exclusively owned; but such taking is an obstacle to equitable distribution. To a market liberal, then, if there were no free riders, there might be no need for government; thus is the free rider a construct with which to justify government intervention to defenders of absolute market hegemony. That being its function, however, its applicability is imprecise. After all, we all enjoy benefits for which we do not pay. The powerful in particular enjoy exceptional benefits without necessarily having contributed anything to make their enjoyment possible. The powerless are portrayed as having few resources to contribute, but they do contribute to others' benefits by enduring both exclusion from, and spill-over costs of those benefits. So a more equitable ethic than is currently in favor would reconsider what counts as a contribution and thus who really rides free. This can be clarified by revising the traditional concept of a Good Samaritan.

A Good Samaritan, traditionally understood, is a voluntary surrogate payer for benefits not otherwise available to a nonpaying other. According to this definition, almost everyone is a Good Samaritan with regard to others, most commonly, one's children, but, through institutionalized arrangements, strangers

as well. It assumes, however, that the existing distribution pattern is fair so a Good Samaritan's giving is gratuitous. This puts have-nots in an unenviable position; so market liberals sometimes encourage haves to perform acts of compassion. Gratuitous compassion cannot be relied on, though, to meliorate substantially a maldistribution of private property. It is therefore tempting to revise the Good Samaritan concept to include reluctant, disempowered contributors to others' well-being—in short, Reluctant Samaritans. Yielding to this temptation, however, would undermine the market liberal concept of a free rider. Three observations will suggest why this is so.

First, nonpayers have access to many imperfectly excludable benefits for which no one can contribute commensurably. Indeed, most benefits we enjoy require no commensurate contribution (our very existence, for one; a war-free habitat and personal autonomy for others). In particular, we all ride free on the contributions, intentional or not, of preceding generations.

Second, a nonpaying free rider presupposes a payee whose identity is, however, indeterminate. If this payee is construed as being public, the nonpayer might perhaps be a tax evader; if the payee is construed as private, the nonpayer might be a thief. But the former identification is precluded by the public good requirement, and the latter, by the required indeterminacy of obligation. If thieves and tax evaders be alternatively discounted at the extremes, a free rider might mean only one who can, but chooses not to, pay for a benefit that the market cannot effectively provide (say, by voting against a tax). If the nonpayer's *ability* to pay is built into the definition of a free rider, however, then the free rider is by definition richer and more powerful than the Reluctant Samaritan.

Third, no property is immune from a free rider problem: owners are threatened by takers as varied as stagecoach robbers, shoplifters, inside traders, and hostile takeover artists. To keep such losses from exhausting the potential for gain, owners may limit them (say, by enhancing human or technical security) or distribute their impact (say, by insuring providers or increasing charges to consumers). Governments in particular are persuaded to distribute exclusivity costs across their entire population: via taxes, civil and criminal sanctions, and concerted efforts to eliminate noncompliant competitors. Such public loss distribution seldom assures equal access to benefits, but often exacts disproportionate contributions from those denied access.[3] Exclusivist thinkers often stereotype these "least advantaged" as lazy and antisocial; more inclusivist thinkers (e.g., John Rawls) acknowledge that some intra-societal envy may be justified. Historically, the potential for social disruption is one of the principal reasons for safety net policies that have become the welfare state, a system of benefit distribution built politically on rejection of free rider thinking and

collectivization of the Good Samaritan.[4]

As these observations suggest, I think the concept of a Reluctant Samaritan merits further development. Here, however, I propose only to explore how it challenges the bifurcated way in which ownership of EDP is being treated.

2. Ownership and Control of EDP

Computers have no moral principles. Their users do, as much as people in general; but until the recent emergence of an encryption technology that can guarantee government intrusion, few computer experts have been concerned about the vulnerability of data subjects to harmful use of EDP.[5] This might not matter if each user remained isolated with his or her computer. But the ever more communicatory computer makes both the collection of and accessibility to data subject to technological variations on the free rider theme.

Data that enhance either wealth or power are ever easier to collect. So privacy-based objections to their collection give way pragmatically to a property rights debate with regard to their storage and retrieval. For no available means of restricting access is foolproof enough to exclude noncontributing users: technological (especially software) defenses against hackers or virus-planters, though ingenious, are pregnable. So electronic data are a public good in the economist's sense that by their very nature use of them cannot be restricted to payers. This is true, as noted, with regard to any so-called private property; but it is singularly true of data the value of which is a function of its accessibility.

Accessibility is enhanced by, if not dependent on, transmissibility. But this makes transmitted electronic data subject to all the old gold shipper's security problems: it is the stage coach robber revisited, but on a vastly more consequential scale. Protective technology now as then is inadequate. Whether moving gold bullion or electronic funds, neither a human nor a technological armed guard can guarantee the security of in-transit goods. So shippers look to punitive sanctions and enough enforcement to bolster the value of compliance. But if an intruder can hide behind the electronic equivalent of a face-concealing mask, the free rider rides again.

In the absence, then, of reliable technological security, data that are storable or transmittable electronically are declared to be private property, the taking of which is subject to sanctions. But might tends to determine what is right. So the rules imposed on comparatively powerless individuals are seldom applied as rigorously to powerful institutions: purse-snatchers may be imprisoned, but brokerage firms found to have defrauded people of hundreds of millions of

dollars are comparatively lightly fined. Similarly, sanctions are assigned asymmetrically with regard to electronic data.

The rules for data gathering leave subjects in a Hobbesian state of nature and exempt collectors from Locke's reminder to leave enough and as good for others. The individual interloper is disparaged as a threat to capitalist values. Meanwhile, the most consequential laborers in the EDP vineyard are businesses and governments, whose agents gather and transfer great masses of electronic data about people's lives with relative impunity.

Businesses seek any electronic information about actual and potential employees, competitors, and customers that may have cash value. They routinely justify their doing so in terms of benefits to the company; and, in spite of protests which on occasion are translated into lawsuits and proposals for regulatory legislation, few restrictions have been effectively imposed.[6] Inversely, they oppose giving outsiders access; but their opposition is increasingly being neutralized by electronic interlopers operating either within or beyond their workforces.[7] The intrusive hacker, once tolerated as an electronic joy rider, is now portrayed as an isolated or at best loosely affiliated individual indistinguishable from a burglar.[8] But companies' claims to confidentiality are also being challenged by shareholders, competitors, and public interest groups that have legal standing and/or technological capability to acquire information the companies would deny them.[9] This intrusive behavior might eventually render some companies' proprietary claims obsolete, as is already happening to brokerage firms because investors can now access investment information from their own computers.[10] But the major users of EDP still insist that they should be able to exclude uninvited others.

In short, the prerogatives of the gatherer are proportionate to the gatherer's power and influence. In contrast to the uninvited EDP user, a user seen to be enhancing a major institution's well-being is defended. As applied to government, this means: if EDP is used to help keep the ins in, this is a commendable use. Affirmative examples include electronic constituency profiling to "narrowcast" an elected official's targeted mailings, or, inversely, electronic networks that facilitate constituent communication with government, even to the point of tele-debating public issues.[11] A negative example is a chain letter sent out over a computer bulletin board to generate opposition to Desert Storm. The U.S. Federal Communications Commission wanted the network provider to play censor, but commercial interests warned that such assignments of liability might nip an attractive new business in the bud.[12] This concern about liability has cooled enthusiasm for an untrammeled bulletin board market in the electronic information services industry. Family-oriented Prodigy promises to keep its

bulletin board clean; but other electronic networks prefer to be identified only with the medium and not with its messages. This opens the door to such electronic diversions as interactive computer sex play, which is now burgeoning in the United States but has already been suppressed by the Minitel system in France.[13] Though attention-getting, such applications are inconsequential compared with more established institutional uses of electronic data, notably "computer matching."

Through computer matching, personal information originally acquired for one purpose is gleaned for another. Sometimes the transformed information is used only by the entity that produces it. In some U.S. cities, for example, prosecutors store a suspect's answers at a bail-bond hearing, then use them in subsequent proceedings.[14] But other matchers are outsiders, such as the so-called information broker who sucks saleable data from government records by keying in on social security numbers. Antiquated and unenforceable privacy laws succumb to electronic supply and demand, regardless of possible harm to others.[15] Ethically improper? Perhaps. But why should the *use* of collected data be considered unethical if collecting them is not? On this point one might consult liberal theorists who debate the ethics of charging a fee for not revealing harmful information to which one is privy.[16] Personal privacy seldom prevails, however, when those claiming a need to know are political or commercial institutions. Military concerns add weight to popular insistence on data security; but even this consideration seems no longer able to contain the *corporate* passion for information. Restoring balance to this asymmetrical dispensation seems desirable; but this is hard to do without favoring haves over have-nots. Six reasons may be cited here.

First, complete security is not technically feasible. Computer manufacturers used to believe that excluding unauthorized intrusions would be prohibitively expensive. But no physical or positive laws can guarantee the security of information if others want it desperately enough; and inventive hackers have demonstrated that not even systems dedicated to the global transfer of trillions of dollars are secure.[17] The balance sought, then, is between what is desirable and what is affordable; but affordability is relative: larger and richer companies can more easily absorb additional costs.

Second, accessibility requirements limit how effectively data can be protected from outsiders. A common approach to this problem is to gradate the data. According to one proposal, they should be divided into three levels of sensitivity.[18] This proposal involves seventeen fewer categories than another which covers everything from published information to blackmail and extortion.[19] Other proposals focus on the security of the hardware-software complex or intra-

organizational levels of responsibility for data protection.[20]

Third, some governments are more sensitized than others about data protection; and this creates an imbalance between and among the countries involved. In Europe, Italy, Portugal, and Belgium have no data protection laws (but Italian automaker Fiat must treat personnel records transmitted from France to Italy according to French standards). Sweden (the first country to enact data protection legislation) requires notifying the data subject, specifies conditions for release of data, and monitors compliance. Canadian statutes, though covering all citizens and permanent residents, focus on economic considerations.[21]

Fourth, the differences in national data protection laws create both opportunities and problems, especially for companies whose profits depend significantly on the use of computerized data. Data are likely to be processed in the country with superior technology; but if the technologies are comparable while the data protection rules are not, profit-oriented companies take advantage of the discrepancy in either direction. The data of security-oriented clients, such as financial services, are stored in a country with more stringent rules (a "data vault"); that of clients for whom access is a priority, say, for credit reporting or subscription processing, in a country with more lenient rules (a "data haven").[22] This could create cross-national equilibrium; but most transnational corporations are not directly involved in exploiting these imbalances and find they hinder their cross-border operations.[23]

Fifth, efforts to make data protection laws uniformly rigorous throughout the developed world have been only minimally successful, especially because businesses do not in general consider such legislation to be in their interest.[24] Thus the U.S. Privacy Act of 1974 applies only to the federal government and exempts most intelligence gathering agencies. Its stated objectives include openness (public scrutiny of federal agency record keeping practices), individual access and participation; and limitations on collection, use and disclosure. But the actual legislation leaves the gathering of information unregulated and establishes only minimal redress under civil or criminal law and no compliance monitoring mechanism. The definition of protected information in this law is constructed by enumeration, so can be expanded only by far-fetched analogies or by amendment. In addition, it conflicts with the Freedom of Information Act (1966, amended 1974, 1976), which while exempting nine categories of information from disclosure leaves implementation to agency discretion.[25]

Many bills have since been introduced in the U.S. Congress to bring the country's privacy protection laws, especially in the area of computer matching, up to European standards; but none is likely to be enacted in the foreseeable future.[26]

European statutes based on the Council of Europe's convention regarding data protection endorse: obtaining and processing data fairly and lawfully; holding them for specified and legitimate purposes, and not using or disclosing them in any way incompatible with those purposes; seeing that they are adequate, relevant, and not excessive; keeping them name-linked no longer than necessary; making them accessible to and correctable by the data subject; and establishing security measures to protect against unauthorized access or destruction.[27] Signatories of this convention, however, legislate its provisions differently. The French version covers only natural persons; the West German statute covers both natural and legal persons, but protects only the former. The British version proscribes using data without their subject's consent; but British common law acknowledges no right of privacy as such.[28] As interaction with eastern European countries expands, even more pronounced differences are coming to the fore.

To meet these challenges, the OECD in 1991 proposed still more extensive controls; but a consortium of major European businesses known as the European Security Forum opposed the proposal as being focused too much on secrecy and too little on reliability. A recent European Community Privacy Directive would require a company doing business in any EC country to register all databases containing personal information, use the data only with the subject's consent, and transfer data only to countries with comparable data protection standards. As noted, such standards are already in place in a number of EC countries, but they tend to be disregarded, partly because large companies want their own secrecy, but not people's, respected.[29]

Sixth, the likelihood of eliminating the inconsistencies and inadequacies in data protection law is minimal. The technology is being transformed and disseminated more rapidly than a legal system monitored by vested interests can possibly control. The U.S. federal government, for example, had only 1,000 central data banks in 1962 but now has 100,000 microcomputers, 27,000 mainframes, 170,000 mainframe terminals, and a million personal computers. The U.S. Internal Revenue Service continues to improve its Taxpayer Compliance Measurement Program; and cross-agency data sharing through computer matching has advanced apace in spite of constitutional concerns about unreasonable searches and seizures. Meanwhile, private sector users of EDP, especially credit bureaus, insurance companies, and private investigators, exercise a potentially devastating power over people's lives that existing laws cannot control. There are, for example, just five major credit bureaus in the United States; and they routinely repackage and sell consumer credit data (however error-ridden) to any buyer.[30]

Laws alone, then, cannot protect the privacy rights of electronic data

subjects. Once the data are collected, their use is limited for the most part only by technology and ingenuity.[31] So people must find other ways to put limits on what data may be collected in the first place. In pursuit of this objective, they can bring about restrictions on collection and use of data by business or by government.

A potentially harm-causing *business* use may be suppressed by consumer protests. This was the case with Lotus Development's set of "lifestyle" CD-ROM databases for "desktop marketing." Generated from credit bureau information to sell to small businesses, especially in the telemarketing industry, the set consisted of data on 120 million U.S. residents and 80 million households and on 7 million businesses. Neither collecting nor using these data is illegal, but a non-binding industry Code of Fair Information Practices discourages using data without the subject's permission for a purpose other than that for which they were collected. What moved Lotus, however, were 30,000 telephone calls and hundreds of computer messages complaining that the proposed use was too intrusive, hence ethically intolerable.[32] This outcome, though encouraging as far as it goes, is troubling because no similar constraints are imposed on *big* businesses.

Governments generally have considerable electronic liberty. But as the recent social consciousness-raising in the former East Germany warns us, unrestrained record-keeping is anathema. In the United States, a proposal to establish a national data bank accessible to all agencies of the federal government has encountered such strong opposition that it has not been carried out—at least not officially. In France, however, the equivalent of a national database has existed since a 1951 decree called for "the collection and centralization of political, social, and economic data about which government needs to be informed." This database, known as the RG (Les Renseignments généraux), was eventually computerized, and now includes not only the kinds of data specified in the 1951 decree but also files on some 370,000 politically important public figures and 70,000 potential terrorists (supplemented by hard copy files on another 600,000 individuals and groups).[33] Such files may be maintained under conditions set forth in a 1978 law that allows the government to store name-linked data without subjects' consent if done for national defense or public security, provided that the authorizing decree passes certain administrative reviews. Appealing to this law, the government announced in 1990 that law enforcement and the RG would add name-linked "sensitive data" about individuals' racial origin, political, philosophical or religious opinions, and union affiliations.[34] Public and political response was almost uniformly negative, so the government canceled the RG authorization.[35]

These glimmerings of consumer and electoral power need to be

intensified until our major institutions are persuaded to protect individual privacy with as much technological efficiency as they apply to protecting their interests in electronic data. This objective is in fact already within the range of possibility, thanks to the emergence of personal identification technologies associated with encryptors, holograms, and biometric devices. Developed primarily to preclude free rider access to ATM machines and other value-yielding equipment, these futuristic devices might be made available just as easily—if not yet inexpensively—to individuals who willingly provide information for one purpose but do not want it disseminated without their authorization. Many businesses, of course, want to control such technologies themselves; but even they must negotiate their prerogatives with governments whose agents still assume that only they should have the ultimate technological trump when it comes to accessing information.[36] Out of this conflict is not likely to come any effective technological protection of personal privacy; rather will agents of our major institutions continue to consider their possession of electronic data to be nine-tenths of the law and increased hegemony, not privacy, the other tenth. Since these institutions now have no countervailing incentive to attune their conquistadorial EDP behavior to respect for persons, organized opposition will have to help lawmakers expand their traditional attitudes about ownership at least enough to include people's interest in controlling their own lives.

This quest for personal control of personal data is, finally, altogether justifiable even under the assumptions of market liberalism. For, subjects of EDP either do not give freely what is taken from them or they give it only for specific purposes, so they are Reluctant Samaritans. If, as data collectors claim, data are property, then the collectors too should pay for whatever they take. Control of privacy, however, begins not with the value added but with the original taking; and on this it is up to the original owner to set a price—or, if he or she so chooses, not sell. This is the way it is with private property. If, alternatively, personal privacy is not something that can be treated as private property, then this practice should be added to the list of exchanges (in, for example, babies, slaves, and nuclear weapons) that are ruled out of the market.[37] In other words, privacy is a public good—both in and beyond the negative sense that economists prefer.

NOTES

1. This wording is meant to reflect Friedrich Rapp's observation that people power presupposes participatory democracy as its instrument.

2. By market liberalism I mean that version of liberalism most readily associated with neo-classical economics, sometimes called utilitarian, in which the concept of a market order is central. See Charles K. Rowley, "The Political Economy of the Public Sector," in *Perspectives on Political Economy*, ed. R. J. Barry Jones (New York: St. Martin's, 1983), esp. pp. 23-24; Andrew Gamble, "Critical Political Economy," *ibid*., pp. 65-68.

3. For details, including conflicts between developed and developing countries over information access, see John Chesterman and Andy Lippman, *The Electronic Pirates: DIY Crime of the Century* (London: Routledge Comedia, 1988).

4. A *public* Good Samaritan program collectively adopted may, of course, exceed its payers' willingness to pay, e.g., due to high operating costs and/or high demand for benefits, causing disillusionment with the welfare state. This reaction, now widespread in many countries, raises serious questions about the welfare state—in particular, whether it is a collective GS (1) by default, (2) by public acknowledgement of special needs, or (3) by virtue of people's collective attention to everyone's basic needs. Underlying these questions, in turn, are unexamined assumptions about the scope of private property claims.

5. See John Markoff, "Wrestling Over the Key to the Codes," *New York Times*, 9 May 1993, p. F9; Rory J. O'Connor, "Balancing Privacy, Opportunity," *San Jose Mercury News*, 31 March 1991, p. 1E+.

6. See Glenn Rifkin, "Do Employees Have a Right to Electronic Privacy? *New York Times*, 8 December 1991, p. F-8; John Markoff, "Remember Big Brother? Now He's a Company Man," *ibid*., 31 March 1991, p. E-7; Paul Katzeff, "Surveillance Legislation Pending," *National Law Journal*, 15 April 1991, p. 1+; Jeffrey Rothfeder, "Looking for a Job? You May be Out Before You Go In," *Business Week*, 24 September 1990, pp. 128, 130; Gary T. Marx and Sanford Sherizen, "Monitoring on the Job," *Technology Review*, November/December 1986, pp. 63-72.

7. See "Throwing the Book at Industrial Spies," *Business Week*, 4 October 1982, pp. 82+; "The Spreading Danger of Computer Crime," *ibid*., 20 April 1981, pp. 86-92.

8. See Craig Bromberg, "In Defense of Hackers," *New York Times Magazine*, 21 April 1991, pp. 45-49; Bart Ziegler, "Limits on Computer Hackers Sought," *Indianapolis Star*, 16 March 1991, p. B-4.

9. See Eric N. Berg, "How Much Should Companies Tell?" *New York Times*, 17 July 1990, p. C1+; "Clearer Rules on Confidentiality," *Business Week*, 11 June 1979, pp. 35-36.

10. Sarah Bartlett, "A California Pension Fund Cuts the New York Umbilical Cord," *New York Times*, 26 August 1990, p. F12; "The Future of Wall Street: Special Report," *Business Week*, 5 November 1990, pp. 119-32. See also "Finance: The Next Hundred Years," *Economist*, 9 May 1992, pp. 97-98.

11. Louis Jacobson, "Let Your Fingers Do the Voting, Maybe," *Wall Street Journal*, 12 August 1992, p. B1+; "The PEN is Mighty," *Economist*, 1 February. 1992, p. 96; Hedrick Smith, *The Power Game* (New York: Random House, 1988), pp. 146-50.

12. Peter Coy and Michele Galen, "Let's Not Let Phone Pollution Hang Up Free Speech," *Business Week*, 19 August 1991, p. 32; John Markoff, "Progress Gets Ham Radio Operators in Trouble," *New York Times*, 14 February 1991, p. A12.

13. Barnaby J. Feder, "Toward Defining Free Speech in the Computer Age," *New York Times*, 3 Nov. 1991, p. E5; John Markoff, "The Latest Technology Fuels the Oldest of Drives," *ibid*., 22 March 1992, p. E5.

14. See Bill Craig, "Big Brother is Watching Indianapolis," *NUVO: The Newsweekly of Indianapolis*, 7-14 November 1990, pp. 8-9, 11. See also Kate McKenna, "IRS List Tracks Dangerous' Taxpayers," *Chicago Tribune*, 14 April 1991, sect. 1, p. 19.

15. "All Things Considered," PBS, 5 January 1991; Peter H. Lewis, "Why the Privacy Issue Will Never Go Away," *New York Times*, 7 April 1991, p. F-4; Kathy Whyde Jesse, "Who's Looking at You," *Indianapolis Star*, 19 November 1990, p. A-12; Robert S. Boyd, "Somebody May be Watching," Knight-Ridder, *ibid*., 24 June 1990, p. F-4.

16. For a recent installment, see Michael Cook, "Liberalism and the Paradox of Blackmail," *Philosophy & Public Affairs*, 21 (Winter 1992): 43-66.

17. R. C. Goldstein, *The Cost of Privacy* (Brighton, MA: Honeywell Information Systems, 1975); John Markoff, "Is the Worm' Turning on U.S. Hackers?" *International Herald-Tribune*, 25 January 1990, p. 3; Steven Mufson, "Exposure to Virus' is Widespread Among U.S.

Funds Transfer Systems," *ibid*., 22 February 1990, pp. 9, 13.

18. The highest level of protection would be assigned only to inherently sensitive intimate (e.g., medical or sexual) data; a medium level of protection, to judgmental data the misuse of which could harm the data subject; and the lowest protection, to biographical data that are sensitive mainly because they may provide access to data that is on a higher level of sensitivity. See Jon Bing, "Classification of Personal Information, with Respect to the Sensitivity Aspect," in *Proceedings of the First International Oslo Symposium on Data Banks and Societies* (Oslo: Scandinavian University Books, 1972); Raymond Wacks, *Personal Information: Privacy and the Law* (Oxford: Clarendon, 1989), pp. 227-29.

19. The Wade System of Gradation of Information, from *Chemical Engineering*, 23 May 1966, as reported by Peter Hamilton, "Privacy and Business Espionage: A Philosophical View," in *Privacy*, ed. John B. Young (New York: Wiley, 1978), p. 292.

20. Sizer and Newman, *The Data Protection Act (Aldershot: Gower, 1984)*, pp. 159, fig. 4, and 169-71. See also "A Classification System?" in *Public Government for Private People*: *Report of Canadian Commission on Freedom of Information and Individual Privacy*, vol. 2 (Toronto: J. C. Thatcher, 1980), pp. 403-08.

21. Canadian Human Rights Act, July, 1977. See Harry S. Katzan, Jr., *Multinational Computer Systems: An Introduction to Transnational Data Flow and Data Regulation* (New York: Van Nostrand, 1980), pp. 77-80. See also the Protection of Privacy Act 1973-74 (Canada), c. 50; the Privacy Acts of Saskatchewan (c. 80), British Columbia (c. 39), and Manitoba (c. 74).

22. Katzen, *Multinational Computer Systems*, pp. vii, 6-8, 81-82.

23. "Privacy Laws Hamper the Cross-Border Flow of Data," *Financial Times*, 19 January 1990, p. 15. See also Patrick E. Cole, "New Challenges to the U.S. Multinational Corporation in the European Economic Community: Data Protection Laws," *New York University Journal of International Law and Politics* 17 (Summer 1985):893-947.

24. See Duncan Campbell and Steve O'Connor, *On the Record: Surveillance, Computers and Privacy: The Inside Story* (London: Michael Joseph, 1986).

25. Privacy Act of 1974 (U.S.), Public Law 93, 579, s. 2(b). For a more expansive account of privacy protection under U.S. federal law see Kent Greenawalt, *Legal Protections of Privacy*; *Final Report to the Office of Telecommunications Policy* (Washington, DC: U.S. Government Printing Office, 1975), pp. 56-63; David F. Linowes, *Privacy in America* (Urbana: University of Illinois Press, 1989), pp. 75-79, 87, and, regarding state laws, pp. 37-39, 79-80, 100, 111-12, 123-24; Richard F. Hixson, *Privacy in a Public Society* (New York: Oxford University Press, 1987), chapter 9.

26. See, in particular, hearings records (published by the U.S. Government Printing Office) of the Privacy Protection Act of 1980; the Federal Telecommunications Privacy Act of 1984; the Electronic Communications Privacy Act of 1986; the Computer Matching and Privacy Act of 1987; the Computer Matching and Privacy Protection Act of 1988; the Computer Matching and Privacy Protection Amendments of 1990; An Act to Amend the Computer Matching and Privacy Protection Act of 1988 to Delay the Effective Date of the Act for Existing Agency Matching Programs (1989).

27. Council of Europe Convention for Protection of Individuals with regard to Automatic Processing of Personal Data, arts. 5-8.

28. The Data Protection Act 1984 (UK), Cmnd. 8539, HMSO, 1982; Wacks, *Personal Information*, pp. 82-100, 269-91, 295-301. See also Richard Sizer and Philip Newman, *The Data Protection Act: A Practical Guide*; Rodney Austin, "The Data Protection Act 1984: The Public Law Implications," *Public Law* (1984) 618-34. With regard to a data subject's control of identity-linked data, see Patricia Hewitt, *Privacy: The Information Gatherers* (Amersham: National Council for Civil Liberties, 1980).

29. Tim Castle, "Computer Security Scheme Rejected," *European*, 4-6 October 1991, p. 18; "Computers and Privacy: The Eye of the Beholder," *Economist*, 4 May 1991, pp. 21-23; John

Markoff, "Europe's Plans on Privacy Upset Business," *New York Times*, 11 April 1991, p. A1+.

30. Linowes, *Privacy in America*, esp. pp. 11, 81, 87-89, 92-96; Jeffrey Rothfeder, "Is Nothing Private? Credit Bureaus, Consumer Information, and Privacy," *Business Week*, 4 September 1989, p. 74+. See also John T. Soma and Richard A. Wehmhoefer, "A Legal and Technical Assessment of the Effect of Computers on Privacy," *Denver Law Journal* 60 (1983): 449-83.

31. See Chesterman and Lipman, *Electronic Pirates*, p. 136.

32. "Privacy Concern Raised Over Lotus Marketplace," *CPSR Newsletter* 8:4 (Fall 1990):24-25; Rory J. O'Connor, "Privacy Gets Boost Since Lotus Won't Sell Data Disc," *Indianapolis Star*, 9 February 1991, p. A-11.

33. Jean-Charles Reix, "Les oreilles du pouvoir," *Le Monde*, 3-4 March 1990, p. 6; "Les 440,000 references des RG," *ibid*., 4-5 March 1990, p. 8; Agathe Logeart, "Informatique, fantasmes et libertés," *ibid*., pp. 1, 8. The latter asserts that the files go back to 1941—sinister if true, but perhaps a typographical error.

34. Thierry Portes, "Le fichage fait des vagues…," *ibid*., 3-4 March 1990, p. 6; Jean-Charles Reix, "Les oreilles du pouvoir," *ibid*; Kayser, *La Protection de la Vie Privée*, pp. 290-99. See also W. Kilian, "Person-related data in the non public sphere," in *L'appropriation de l'information: Données nominatives dans le secteur privé* (Paris: Librairies techniques, 1986), pp. 99-109 (business use of name-linked data in West Germany is in conflict with 1977 data protection law).

35. "Tolle general contre le fichier des RG," *Figaro*, 3-4 March 1990, p. 1; "Quand Rocard fait machine arriere…", *ibid*., 5 March 1990, p. 7. This raised questions about the government's motives because it had said antiterrorism was the principal justification for the project: Louise Cadoux, "Les arguments de la CNIL," *ibid*., 4-5 March 1990, p. 8.

36. See Chesterman and Lipman, *Electronic Pirate*, pp. 92-93, 111-15; John Markoff, "U.S. as Big Brother of Computer Age," *New York Times*, 6 May 1993, p. C1; Markoff, "New Communication System Stirs Talk of Privacy vs. Eavesdropping," *ibid*., 16 April 1993, p. A1+; "A Public Battle Over Secret Codes," ibid., 7 May 1992, pp. C1-C2; Keith Bradsher, "U.S. Warns on Advances in Encoding," *ibid*., 30 April 1992, p. C1+. See also n. 5, above.

37. Compare Jeffrey Rothfeder, *Privacy for Sale* (New York: Simon & Schuster, 1992).