Privacy and the Encryption Debate

Adam Moore

. . . trusting the government with your privacy is like trusting a Peeping Tom with your window blinds.

—John Perry Barlow, "Introduction to PGP" [1]

Regulated [weak] encryption would provide considerably greater security and privacy than no encryption . . . . We must balance our competing interests in a way that ensures effective law enforcement and intelligence gathering.

—Dorothy Denning, "To Tap or Not to Tap" [2]

Introduction

The tension between privacy and surveillance or public accountability has long been an area of intense philosophical and political debate. Many defend the view that upstanding and good citizens should not fear robust government surveillance because they have nothing to hide—hiding from public scrutiny is the domain criminals or those with suspect moral characters. On the other side of the "nothing to hide" view are defenders of privacy rights that limit invasions into private domains. There has always been a tenuous balance between individual privacy and public accountability. Searches and seizures may be conducted in private domains but only if certain conditions are met. Moreover, the Privacy Act of 1974 "regulates virtually all government handling of personal data." [3]

This balance, however tenuous, is being threatened by the ever increasing flow of data streams across electronic networks. The world of the future is a digitally networked world and information is its currency. The data that flows across computer networks, satellite transmissions, television broadcasts, and cellular phones could be about financial transactions, vot-

Adam Moore has a Ph.D. in philosophy from Ohio State University and teaches at Eastern Michigan University. He is the author of, "Employee Monitoring and Computer Technology" (forthcoming in *Business Ethics Quarterly*), "Intangible Property: Privacy, Power, and Information Control," *American Philosophical Quarterly* 35 (October 1998) and is the editor of *Intellectual Property: Moral, Legal, and International Dilemmas* (Lanham, MD: Rowman & Littlefield, 1997), in which he contributes "Introduction to Intellectual Property" and "Toward A Lockean Theory of Intellectual Property."

Knowledge, Technology, & Policy, Winter 2000, Vol. 12, No. 4, pp. 72–84.

ing trends, or personal medical records. The ones and zeros that make up digital information streams transfer content almost flawlessly—any content. An e-mail message could contain sensitive personal information or plans for criminal activity.

In this article I will consider a number of issues related to governmental and societal control of information. More specifically, I will focus on the question of when privacy rights to control certain kinds of information may be justifiably overridden in the name of public security. For example, the wiretap laws of 1968 give certain government agencies limited authority to conduct wire surveillance. In a digitally networked world, however, encoding programs allow individuals to encrypt information so that no one (in theory) could ever view this information without a pass key. If digital cell phones, e-mail messages, electronic transfers, and the like are encrypted with unbreakable codes, then governments will have a difficult time spying on and catching criminals.

Moreover, if money, sales, and services can all be hidden through the use of encryption software, then governments may have a difficult time collecting taxes. For example, if financial advice is sold and the transfer of funds encrypted, then it would be virtually impossible for any government to discover this transaction and levy a tax. Business conducted over secure lines, whether a computer network or a cellular phone transmission, may become impossible to trace. Financial privacy guaranteed through the use of strong encryption software could have a profound impact on governmental redistributive models.[4]

Nevertheless, I will argue that a government mandated standard of weak encryption is not justified—security arguments are not forceful enough to override individual privacy rights. In fact, security arguments actually cut in the other direction. It is only through the use of strong encryption that we can obtain an appropriate level of security against industrial espionage, unwarranted invasions into private domains, and information warfare or terrorism.

Privacy and Information Control [5]

Privacy may be understood as that condition where others do not have access to you or to information about you. I hasten to note that there are degrees of privacy. There are our own private thoughts that are never disclosed to anyone, as well as information we share with loved ones. Furthermore, there is information that we share with mere acquaintances and the general public. These privacy relations with others can be pictured "in terms of a series of 'zones' or 'regions' . . . leading to a core self."[6] Thus, secrets shared with a loved one can still be considered private, even though they have been disclosed.

A right to privacy can be understood as a right to maintain a certain level of control over the inner spheres of personal information. It is a right to limit public access to the "core self"—personal information that one never discloses—and to information that one discloses only to family and friends.

For example, suppose that I wear a glove because I am ashamed of a scar on my hand. If you were to snatch the glove away you would not only be violating my right to property (the glove is mine to control), you would also violate my right to privacy; a right to restrict access to information about the scar on my hand. Similarly, if you were to focus your x-ray camera on my hand, take a picture of the scar through the glove, and then publish the photograph widely, you would violate a right to privacy.[7] What binds these seemingly disparate cases under the heading "privacy invasions" is that they each concern personal information control. And while there may be other morally objectionable facets to these cases, for example the taxi driver case may also be objectionable on grounds of defamation, there is arguably privacy interests at stake as well.

Having said something about the definition of privacy rights we may ask how such rights are justified. A promising line of argument combines notions of autonomy and respect for persons. A central and guiding principle of western liberal democracies is that individuals, within certain limits, may set and pursue their own life goals and projects. Rights to privacy erect a moral boundary that allows individuals the moral space to order their lives as they see fit.[8] Privacy protects us from the prying eyes and ears of governments, corporations, and neighbors. Within the walls of privacy we may experiment with new ways of living that may not be accepted by the majority. Privacy, autonomy, and sovereignty would seem come bundled together.

A second but related line of argument rests on the claim that privacy rights stand as a bulwark against governmental oppression and totalitarian regimes. If individuals have rights to control personal information and to limit access to themselves, within certain constraints, then the kinds of oppression that we have witnessed in the twentieth century would be near impossible. Put another way, if oppressive regimes are to consolidate and maintain power, then privacy rights (broadly defined) must be eliminated or severely restricted. If correct, privacy rights would be a core value that limits the forces of oppression.[9]

Arguably, any plausible account of human well being or flourishing will have as a component a strong right to privacy. Controlling who has access to ourselves is an essential part of being a happy and free person. This may be why "peeping Toms" and rapists are held up as moral monsters—they cross a boundary that should never be crossed without consent.

Surely each of us has the right to control our own thoughts, hopes, feelings, and plans, as well as a right to restrict access to information about our lives, family, and friends.[10] I would argue that what grounds these sentiments is a right to privacy—a right to maintain a certain level of control over personal information.[11] Lacking complete control of all our personal information, simply because the information is already "out there" and most likely cannot or will not be destroyed, does not detract from the view of personal information ownership. Through our daily activities we each create and leave digital footprints that others may follow and exploit—and that we do these things does not obviously sanction the gathering and subsequent disclosure of such information by others.

Whatever kind of personal information we consider, there is a gathering point that individuals control. For example, in purchasing a new car and filling out the car loan application, no one would deny we each have the right to demand that such information not be sold to other companies. I would argue that this is true for any disclosed personal information, whether it be patient questionnaire information, video rental records, voting information, or employment applications. In agreeing with this view, one first has to agree that individuals have the right to control their own personal information—i.e., binding agreements about controlling information presuppose that one of the parties has the right to control this information.

If I am correct about all of this there is a fairly strong presumption in favor of individual privacy rights. Other things being equal, consent is what justifies a photographer taking pictures of someone in an intimate personal setting, or a news service publishing sensitive medical information about an individual. Most would agree that absent such consent, a serious violation of privacy would have occurred. The question now becomes when, if ever, can this fairly strong presumption in favor of privacy be overridden by public interest security arguments?

Cryptography and Government Access to Information

A prominent view in the encryption verses privacy debate is that good upstanding citizens should have nothing to hide. Why, they ask, should you be worried about government agents poking around your hard drive, reading your e-mail, or looking at your financial records? Only criminals should be worried about such surveillance.

Generally, I am dumbfounded by the naiveté exhibited in these views, as if our government, or other governments, would never use such power immorally or illegally. One of the major battles fought over the U.S. government's weak encryption scheme (Clipper) was a provision that what would have allowed ill-gotten information to hold up in court: "...noncompliance with these procedures [failure to get a warrant or subpoena] shall not provide the basis for any motion to suppress or any other objection . . ."[12] The Fourth Amendment, protecting citizens from "unreasonable searches and seizures," and the decades of supporting case law allowing the suppression of information or evidence that was unjustifiably obtained is quietly swept aside.

To take another example, in the 1950s the United States government sponsored a coup d'état in Guatemala to overthrow a democratic government that had initiated land reform policies. Information control was essential to the overthrow. By restricting access to the area and planting certain stories and rumors, government officials were able to convince the American public that we were behind the overthrow of a communist dictator.[13]

It would be quite naive of us to think that Big Brother has not already compiled databases on many of us along with algorithms, sometimes called "spiders," to search for certain patterns that point toward criminal activity.

Keeping records of citizens has been, and continues to be, a way for governments to maintain control over their populations.

> Behind a locked door on the second floor of the Beijing Engineering Design Institute is a small room stacked with files from floor to ceiling. There is a file here on each of the institute's 600 employees, and although they are never allowed to peek inside, they live their lives with their files looming over them.

> As part of China's complex system of social control and surveillance, the authorities keep a dangan, or file, on virtually everyone except peasants. Indeed, most Chinese have two dangan: one at their workplace and another in their local police station. . . . A file is opened on each urban citizen as he or she enters elementary school, and it shadows the person through school to college and employment. Particularly for officials, students, professors, and Communist Party members, the dangan contain political evaluations that affect career prospects and permission to leave the country.[14]

Currently, under the Privacy Act of 1974, U.S. citizens can view their government files, although such requests take years and much of the information is blacked out due to national security provisions. The Privacy Act requires that federal agencies:

1. Permit an individual to determine what records pertaining to him are collected, maintained, used, or disseminated;
2. Permit an individual to prevent records pertaining to him obtained by such agencies for a particular purpose from being used or made available for another purpose without his consent;
3. Permit an individual to gain access to information pertaining to him in federal agency records, to have a copy made of all or any portion thereof, and to correct or amend such records;
4. Collect, maintain, use, or disseminate any record of identifiable personal information in a manner that assures that such action is for a necessary lawful purpose, that the information is current and accurate for its intended use, and that adequate safeguards are provided to prevent misuse of such information;
5. Permit exemptions from the requirements with respect to records provided in the act only in those cases where there is an important public policy need for such exemption as has been determined by specific statutory authority; and,
6. Be subject to civil suit for any damages which occur as a result of willful or intentional action which violates any individual rights under the Act.[15]

In reviewing these provisions, it is alarming to see how little control individuals have over their own personal information. Government agencies are limited in what they can do with personal information and individuals may request that inaccurate information be corrected, but this hardly constitutes control in any robust sense.

Moreover, data sharing by different government agencies may lead to the creation of a national database filled with sensitive personal information about most Americans.[16] Kentucky has a law that allows for the suspension of a student's drivers license if that student cuts class. In Detroit, reporters for various news organizations were tracing the strands of a major web of organized crime by recording license plate numbers on autos parked outside a reputed mobster's home. In Los Angeles, a disturbed young man who was infatuated with an actress spotted her at the wheel of her auto, hired a private investigator to run her plate number through a data base, and learned that her address was in the Fairfax neighborhood of Los Angeles. The obsessed fan shot actress Rebecca Schaeffer to death as she opened her front door.[17] When school reports, driving histories, criminal files, library records, income statements, and the like all become connected, there is the danger of bureaucrats allowing this information to be used in suspect ways.[18]

Wire Tapping and Electronic Searches

In *Olmstead v. United States* (1928)[19] the court ruled that the Fourth Amendment against unreasonable searches and seizures applied to physical things like houses, notebooks, and receipts, but not to electronic communications. Thirty-nine years later the Supreme Court, in *Katz v. United States*,[20] overturned the *Olmstead* decision affirming that privacy interests may be found in personal communications as well as "persons, houses, papers, and effects." More recently, Digital Telephony (1994) was signed into law. This law allows the FBI and other law enforcement agencies to eavesdrop on conversations by simply flipping a (digital) switch at headquarters. Moreover, the cost of ensuring this ability may fall on the phone companies. In the end though, law enforcement walked away with much less then they would have liked.

> The Electronic Frontier Foundation led a powerful opposition, backed by AT&T, DEC, Lotus, Microsoft, and Sun Microsystems, which were able to effectively remove on-line information providers from the legislation. The final version . . . also required law enforcement agencies to obtain a court order to obtain telephone transactional information—as opposed to a mere subpoena which was previously required.[21]

But now the stage is set for the encryption debate. If phone and other electronic transmissions are protected with strong encryption, then whether or not law enforcement can jack in is irrelevant.

Encryption

Phil Zimmerman, in 1992, developed an encryption program that was, in large part, built on the work of others. Along with what is now known as public-key cryptography, new encryption algorithms had been developed

by a company called RSA.[22] Private/Public key encryption works in the following way: each individual gets a private key that no one else has access to. Everyone also gets a public key that is widely accessible—perhaps posted on a web page. If Fred wants to send a secret e-mail to Ginger, he types it up, encodes it with Ginger's public key, and sends it to her. She then decodes it with her private key. Public keys can encode messages but not decode them. Private keys can decode messages but not encode them. Simple but brilliant![23] The system RSA developed was powerful and the encryption algorithms were eventually patented.[24] Zimmerman, not wanting such important privacy tools to be monopolized by a single company or government, copied RSA's encryption algorithms and produced an encryption program called PGP—which stands for Pretty Good Privacy. In terms of protection, PGP is a remarkable program that affords the user virtually unbreakable encryption power along with an authentication system that leaves a digital signature which cannot be falsified. PGP was then placed on the Internet and downloaded by thousands of individuals in numerous countries.[25]

RSA cried foul and threatened to sue Zimmerman while the National Security Administration (NSA) questioned him and hinted that use of encryption tools might be unlawful under an Arms Regulation law.[26] It seems that cryptographic tools are listed as national security threats along side of tanks, biological weapons, and nuclear warheads. The National Security Administration's position is that the widespread use of encryption software will allow criminals a sanctuary to exchange information necessary for the completion of illegal activities.

The battle lines over the general use of encryption technology have already been drawn. On one side are the cypherpunks and net-anarchists who champion complete privacy secured by unbreakable encryption algorithms, oddly many of these same individuals also champion the claim that "information wants to be free." These individuals argue that governments have no business reading the e-mail messages that flow between individuals on the Internet or nosing around on network servers looking for incriminating discourse. This is not to deny that governments have a legitimate role to play in protecting individuals against criminal activity. In the most general terms, what many net-anarchists are against is government interference with thought; the thoughts of millions of individuals flowing in bit streams around the globe. Allowing governments to govern thoughts and ideas is quite alarming, for crime it is argued, is about action, not thought.

Many different arguments are given in support of this view, ranging from the privacy right arguments already discussed, to John Stuart Mill's argument for the freedom of thought and expression. Mill argues that allowing complete freedom of thought and expression has certain benefits.

> . . . the peculiar evil of silencing the expression of an opinion is that it is robbing the human race, posterity as well as the existing generation—those who dissent from the opinion, still more than those who hold it. If the opinion is right, they

> are deprived of the opportunity of exchanging error for truth; if wrong, they lose, what is almost as great a benefit, the clearer perception and livelier impression of truth produced by its collision with error.[27]

The problem, frequently cited by the opposition, is that other concerns such as national security or pursuing and stopping criminal activity may overbalance the benefits gained by complete freedom of expression and thought. More importantly, those against the proliferation of strong encryption programs do not want to censure thought or expression but merely want to monitor them. If terrorists and criminals are allowed a sanctuary where information can be disseminated without risk of interception, then national security may be compromised. As already noted, the wiretap statutes of 1968 and 1978 allow government agencies to monitor communications so long as a court order is secured. The idea is to expand this kind of monitoring into computer environments.What the NSA and other government agencies propose is the use of Clipper (also known as Slipjack) encryption which would require a key escrow system.[28] The idea is that government agencies could access encrypted data with a court order by obtaining a copy of the encryption key, which would be stored at some secure site. Furthermore, this strategy not only works for computer networks, but it also works for cordless transmissions such as cellular phone operation, pagers, satellite transmissions, and the like. Current technology leaves cellular phone conversations unprotected and easily intercepted by anyone with the appropriate scanning device. Under Digital Telephony, the government's telephone equivalent of Clipper, all telephone transmissions will be encrypted. Like Clipper, however, there will be a back-door key so that the government can listen in.

The insidious element in this debate about privacy and the government's ability to pursue and catch criminals is that policy seems to be driving the debate. The NSA and other government officials propose some new key escrow encryption scheme and then try to get it adopted as an industry standard. If all, or most, of our e-mail software, telephone communications, and other transmissions are protected by some "built in" version of Clipper, then one side has won by default.

Cypherpunks and net-anarchists typically respond by claiming that new technology coupled with government monitoring through the use of "back-door" encryption keys will allow invasions of privacy unparalleled in history. John Perry Barlow, a co-founder of the Electronic Frontier Foundation, writes:

> I'm willing to take my chances with the few terrorists and drug lords there are out there rather than trusting government with the kind of almost unlimited surveillance power which Clipper and Digital Telephony would give them. It's a tough choice. But when you look at the evil perpetrated by government over this century in the name of stopping crime, it far exceeds that done by other organized criminals.[29]

Moreover, like the NSA's strategy of winning by default, those who defend strong privacy rights have used this method themselves. Zimmerman's creation of PGP and subsequent dispersal can be viewed as nothing more than an attempt to win by default. No matter what conclusions are reached in the debate about information ownership, privacy, and government access, the cat is already out of the bag, so-to-speak. PGP is available, and barring making its use illegal, it or similar encryption software will be used. Only stupid criminals or those individuals who do not care if the government has access to their personal information will use Clipper when more secure encryption is available.

Putting aside questions about what will actually occur concerning encryption technology, we may ask what *should* be the case. As I have argued, it seems plausible to maintain that individuals have, or should have, control of their own personal information. Consider the following example. Suppose that in a few years a new frequency is discovered and a system developed that allows others to monitor your thoughts. Rather than listening to your words with microphones, recording your movements with remote video cameras, or accessing your hard drive with a back door encryption key, suppose the government could obtain a court order and plug into your very thoughts. Advocates of law enforcement may charge that this is going too far, but there is little difference between this case and the digital profiling that will be possible in a few short years. It seems that digital technology has put us on a very slippery slope and granting governments, the most coercive and oppressive institutions in history, this kind of power is risky to say the least. Consider the following argument given by Ron Rivest, a developer of RSA.

> Given the small number of currently available wiretaps per year (under 1,000) and the ease of using alternative encryption or superencryption it seems plausible to me that law enforcement could expect at most ten "successful" Clipper wiretaps per year. This is a pretty marginal basis for claiming that Clipper will "block crime."[30]

Rivest raises two important points. First, on average there are less than 1,000 legitimately conducted wiretaps per year in the United States. Second, under the current proposal, the use of Clipper is voluntary. This makes the law enforcement argument very suspicious. Are there numerous *illegal* wire taps that strong encryption will block? Is the plan to *outlaw* strong encryption after Clipper, or some other weak encryption standard, becomes the norm? [31]

Consider how easily the "security" argument can be stood on its head. National security for government agencies, companies, and individuals requires strong encryption. The following was taken from a Chinese military newspaper.

> After the Gulf War, when everyone was looking forward to eternal peace, a new military revolution emerged. This revolution is essentially a transformation from the mechanized warfare of the industrial age to the information warfare of the

> information age. Information warfare is a war of decisions and control, a war of knowledge, and a war of intellect. The aim of information warfare will be gradually changed from 'preserving oneself and wiping out the enemy' to 'preserving oneself and controlling the opponent.' Information warfare includes electronic warfare, tactical deception, strategic deterrence, propaganda warfare, psychological warfare, network warfare, and structural sabotage.[32]

With the growing number of attacks on computer networks, it is strong encryption, not weak encryption, that will protect us from information war, industrial espionage, and other unwarranted invasions of private domains. Both the French and Soviets have admitted to "tapping in" and collecting valuable information on U.S. companies—information that was then used to gain a competitive advantage.[33] A report from the CSIS Task Force on Information Warfare & Security notes that "Cyber terrorists could overload phone lines . . . disrupt air traffic control . . . scramble software used by major financial institutions, hospitals, and other emergency services . . . or sabotage the New York Stock Exchange."[34] With all of this at stake we may wonder why the FBI and other law enforcement agencies insist on weak encryption.

There used to be domains of a person's life that were totally inaccessible. A person's home and bedroom, notebook and hard drive, were all sanctuaries against the prying eyes and ears of others. What is alarming is that digital technology is sweeping these domains away. Allowing government restricted access to private telephone conversations may have a cost, in terms of privacy, that we are each willing to tolerate, but few would feel comfortable with allowing the government to freely monitor our motions, speech, and expressions—and fewer still would defend government access to our thoughts.

What grounds these sentiments is the plausible intuition that individuals have rights to control personal information. Would I be doing something morally illicit if I put on my new anti-monitoring suit that afforded me complete protection from every surveillance device except the human eye? It is not as if we have a choice between a ring of gyges problem and a breakdown of privacy.[35] Old fashioned bugging and physical surveillance will continue to work. There will still be government informants who will gladly hand over incriminating evidence in exchange for immunity from prosecution. Moreover, technological advances will allow law enforcement to keep pace with even the most thrifty of criminals.[36] Given this, and my view that individuals have rights to control personal information, I would advocate a standard of strong encryption; let us make government surveillance of private citizens difficult and costly. To put the point another way, I do not think that there is a strong enough "public interest" argument on the side of law enforcement to warrant the level of access permitted by weak encryption standards.

Conclusion

Robert Heinlein, author of *Stranger in a Strange Land* as well as countless other science fiction stories, once claimed that "The sole thing achieved by

any privacy law is to make the bugs smaller."[37] Heinlein may be correct, but that travesties will happen does not sanction them—and maybe we will invent bugs to root out and foil other bugs.

I have argued for individual privacy rights or rights to control sensitive personal information. The explosion of digital technology has made possible severe violations of individual privacy by corporations, news agencies, and the government.[38] If I am correct about all of this, one commonly used "public interest" argument given for limiting privacy rights has been undermined. It is also far from true to claim that the prevalence of strong encryption technology will lead to disaster. While I do not adhere to the view that "rights hold, though the heavens may fall," in this article I have maintained that the security arguments of law enforcement do not come close to meeting the threshold for violating privacy rights. The heavens are far from falling.

Notes

1. John Perry Barlow, "Introduction to PGP," *PGP Guide*.
2. Dorothy Denning, "To Tap or Not to Tap," *Communications of the ACM* (March 1993), reprinted in M. Erman, M. Williams, and M. Shauf, *Computers, Ethics, and Society* (Oxford University Press, 1997), p. 262.
3. E. Hendricks, T. Hayden, J. Novik, *Your Right to Privacy* (Southern Illinois University Press, 1990), p. 3.
4. In *U.S. v. Miller*, 425 U.S. 435 (1976), the court held that individuals do not have a right to privacy in bank records. This, and *California Bankers Ass'n. v. Shultz*, 416 U.S. 21 (1974), led to several other cases undermining what might generally be called "financial privacy." See also *Smith v. Maryland*, 442 U.S. 735 (1979); *Whalen v. Roe*, 429 U.S. 589 (1977); and *California v. Greenwood*, 486 U.S. 35 (1988).
5. A longer version of this section appears in my article "Intangible Property: Privacy, Power, and Information Control" *American Philosophical Quarterly* 35 (Oct. 1998): 365–378. I thank the editors of *APQ* for allowing me to present this material here.
6. Alan Westin, "Privacy in the Modern Democratic State" in D. Johnson and J. Snapper, *Ethical Issues in the Use of Computers* (Wadsworth Pub.: 1985), p. 187.
7. Dean William Prosser, "Privacy," *California Law Review* 48 (1960): 383, 389, quoted in E. Alderman and C. Kennedy, *The Right to Privacy* (New York: Alfred A. Knopf, 1995), pp. 155–156. Legal scholar William Prosser separated privacy cases into four distinct but related torts:

   > *Intrusion*: Intruding (physically or otherwise) upon the solitude of another in a highly offensive manner. For example, a woman sick in the hospital with a rare disease refuses a reporter's request for a photograph and interview. The reporter photographs her anyway, over her objection. *Private facts*: Publicizing highly offensive private information about someone which is not of legitimate concern to the public. For example, photographs of an undistinguished and wholly private hardware merchant carrying on an adulterous affair in a hotel room are published in a magazine. *False light*: Publicizing a highly offensive and false impression of another. For example, a taxi driver's photograph is used to illustrate a newspaper article on cabdrivers who cheat the public when the driver in the photo is not, in fact, a cheat. *Appropriation*: Using another's name or likeness for some advantage without the other's consent. For example, a photograph of a famous actress is used without her consent to advertise a product.

8. Clinton Rossiter puts the point succinctly:

> Privacy is a special kind of independence, which can be understood as an attempt to secure autonomy in at least a few personal and spiritual concerns, if necessary in defiance of all the pressures of the modern society. . . It seeks to erect an unbreachable wall of dignity and reserve against the entire world. The free man is the private man, the man who still keeps some of his thoughts and judgments entirely to himself, who feels no over-riding compulsion to share everything of value with others, not even those he loves and trusts. (*Aspects of Liberty* [Ithica, NY: Cornell University Press, 1958] quoted in Westin, "Privacy in the Modern Democratic State" p. 188).

9. For more about privacy rights see Charles Fried, "Privacy," *Yale Law Journal* 77 (1968): 477; A. Westin and M. Baker, *Databanks in a Free Society*, (New York: Quadrangle Press, 1972); J. Rachels, "Why Privacy is Important," *Philosophy and Public Affairs* 4 (Summer 1975): 323–333; and Paul Weiss, *Privacy* (Southern Illinois University Press, 1983).
10. The view of privacy rights that I am defending is not absolutist—there is still the possibility of reasonable searches and seizures of private domains.
11. Would I be doing something morally illicit if I put on my new anti-monitoring suit that afforded me complete protection from every surveillance devise except the human eye?
12. Clipper Proposal, cited in J. Wallace and M. Mangan, *Sex, Laws, and Cyberspace: Freedom and Censorship on the Frontiers of the Online Revolution* (Henry Holt Publishers, 1997), p. 55.
13. For a somewhat disheartening account of the many illicit government invasions into private domains see Ellen Alderman and Caroline Kennedy, *The Right to Privacy*.
14. Nicholas D. Kristof, "For Chinese, Lives in Files, Perpetually Open and Overhead," *International Herald Tribune*, 19 March 1992, p. 5, quoted by Anne Wells Branscomb in *Who Owns Information?* (Basic Books, 1994), p. 16.
15. U.S. Congress, Office of Technology Assessment, *Federal Government Information Technology: Electronic Record Systems and Individual Privacy*, OTA-CIT-296 (Washington, D.C.: U.S. Government Printing Office, June 1986), quoted in Deborah G. Johnson, *Computers Ethics* (Prentice Hall, 1994), p. 96. For more about current laws and regulations protecting privacy rights see Evan Hendricks, Trudy Hayden, and Jack Novik, *Your Right to Privacy* (Southern Illinois University Press, 1990), and Fred H. Cate, *Privacy in the Information Age* (Brookings Institute Press, 1997).
16. U.S. Congress, Office of Technology Assessment.
17. These three examples come from Carl Hausman's "Information Age Ethics: Privacy Ground Rules for Navigating in Cyberspace," *Journal of Mass Media Ethics* (1994): 135–144.
18. See generally, John Shattuck, "Computer Matching is a Serious Threat to Individual Rights," *Communications of the ACM* 6 (1984): pp. 537–545, and Richard P. Kusserow, "The Government Needs Computer Matching to Root Out Waste and Fraud," *Communications of the ACM* 6 (1984): 546–552.
19. *Olmstead v. United States* 227 U.S. 438 (1928).
20. *Katz v. United States* 389 U.S. 347 (1967). See also *Berger v. New York* 388 U.S. 41 (1967).
21. J. Wallace and M. Mangan, *Sex, Laws, and Cyberspace*, p. 54.
22. Named after the founders and MIT scientists, Rivest, Shamir, and Aldeman.
23. The creators are Whitfield Diffie and Martin Hellman. James Ellis and Clifford Cocks, members of England's secret service community, discovered the basics of this approach prior to Diffie and Hellman but kept it secret. For more about the history of public key cryptography see Steven Levy's "The Open Secret," *Wired Magazine* (April 1999): 108.
24. "To give an idea of the strength of RSA, consider a challenge the team printed in the August 1977 issue of *Scientific American*. It was an encrypted sentence coded in the form of a 129-digit number. The team offers $100, but the world's cryptographers sat stumped for 17 years. In the Spring of 1994 an international team of 600 cryptogra-

phers and computer scientists from 24 countries took 8 months and 1,600 workstations to factor the number and crack the code: 'The magic words are squeamish ossifrage.'" J. Wallace and M. Mangan, *Sex, Laws, and Cyberspace,* p. 46.

25. DES, another encryption standard developed by IBM and adopted by the NSA, is tightly controlled and is used to protect sensitive government information. It has also been recently cracked in under 24 hours—in crypto terms, making it obsolete. See James Glave "Code-Breaking Record Shattered," *Wired Magazine* On-line News Flash (Feb. 1999).
26. See Title 22, Section 2778 of the Federal Criminal Code. "Current law lets the executive branch declare a 'national emergency' and restrict encryption exports, which the President has done." Declan McCullagh, "A Baby Step for Encryption," *Wired Magazine* On-Line News (Feb. 1999).
27. John Stuart Mill, *On Liberty,* Chapter II, Of the Liberty of Thought and Discussion.
28. The original Clipper system, which was based on a hardware chip, failed for lack of market support, design flaws, and sustained criticism. In 1995 the government came up with what some have called Clipper II. This was a software solution and conceded that key escrow agencies need not be associated with the government. Once again there was no market support and in 1996, in a draft of a white paper, a third proposal was made—Clipper III. This latest government sponsored encryption scheme is merely Clipper II repackaged. All versions of Clipper allow government agencies access to encrypted information through the use of a second encryption key.
29. John Perry Barlow, "Barlow v. Denning Transcript," (March 10, 1994, on-line debate between John Perry Barlow and Dr. Dorothy Denning, over the Clipper Chip scheme).
30. Ron Rivest, "A Reply to Dorothy Denning," in *Newsday* editorial (February 25, 1995).
31. Recently the United States and 33 other countries signed the Wassenaar Arrangement agreeing to limit strong encryption exports.
32. *Jiefangjun Bao* (The name of a Chinese Army Newspaper) cited in *Wired Magazine,* John Carlin, "A Farewell to Arms" (May 1997).
33. J. Wallace and M. Mangan, *Sex, Laws, and Cyberspace,* 51.
34. Cited in Christopher Jones, "Averting an Electronic Waterloo," *Wired Magazine* On-line News Flash (Feb. 1999).
35. Plato, *Republic,* 359d-360b, trans. G. M. Grube (Hackett Pub. 1974), pp. 31–32.
36. One example that comes to mind is the new technology that can capture an image from a computer screen at a distance. With the appropriate warrant, law enforcement officials can sit nearby and capture information before it is encrypted.
37. Quoted in David Brin's, "The Transparent Society," *Wired Magazine* (December 1996).
38. For an in-depth treatment of information control and privacy related to the workplace and freedom of the press see my two articles "Intangible Property: Privacy, Power, and Information Control," *American Philosophical Quarterly* 35 (Oct. 1998) and "Employee Monitoring and Computer Technology: Evaluative Surveillance v. Privacy," forthcoming in *Business Ethics Quarterly.*