Harvard Vision
Student Essays on Our Collective Future
Volume IV
Peter Ulric Tse, Jeremy R. Gray, and Frank Pasquale Editors
Harvard Vision

Student Essays
on Our Collective Future

Volume IV

Peter Ulric Tse, Jeremy R. Gray, and Frank Pasquale

Editors

THE DIPYLON PRESS
CAMBRIDGE, MASSACHUSETTS
Harvard Vision: Student Essays on Our Collective Future

Founding Editor: Isaac Devash
Volume IV
Edited by Peter Ulric Tse, Jeremy R. Gray, and Frank Pasquale
All rights reserved.
No part of this book may be reproduced in any manner whatsoever without written permission, except in the case of brief quotations embodied in articles and reviews.

"Health Care Challenges in the Era of Managed Care"
©1996, A. Biviano

"The Impact of Global Changes on Terrestrial Ecosystems"
©1996, Sebastian Catovsky

"Social and Ethical Dilemmas in the Age of Molecular Medicine"
©1996, Benjamin Ebert

"Poetry and the Modern Self"
©1996, Scott Hess

"Reading with Our Eyes Open: A Literary Critic Weighs in on Smut"
©1996, Marti Hohmann

"Re-Integrating Academic Approaches"
©1996, Chimène I. Keitner

"Nature, Culture, and the Built Environment"
©1996, Deane Rykerson

"Saeculorum Novus Nascitur Ordo (A New Era Begins)"
©1996, Darin Stephanov

"Privacy under Siege"
©1996, Peter Ulric Tse

"Making Biomedical Progress in an Era of Constrained Resources"
©1996, Anne E. West

"China's Quest for a National Identity: A Speculative Essay"
©1996, Guoqi Xu

Copyediting and layout by Cambridge Wordwright, Cambridge, Mass. 02138
Cover based on original design by Susan Manning and Robert Simons
Printed in the United States of America by Towne Printing

The "Veritas" shield is a registered trademark of Harvard University and is used with permission of the Office of Licensing and Trademarks.

First Edition

ISBN 0-9641866-2-4
Privacy under Siege

Peter Ulric Tse

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

The Fourth Amendment to the U.S. Constitution

They could plug in your wire whenever they wanted to. You had to
live—did live, from habit that became instinct—in the assumption
that every sound you made was overheard, and, except in the darkness,
every moment scrutinized.

George Orwell, 1984

We stand at the dawn of several possible information ages. In one of the darker possible futures, the police will stop us for speeding and be able to see within seconds that we have not paid certain taxes, that we have a predisposition for colon cancer, and that we just bought a six-pack of beer. With mandatory “smart” I.D. cards, authorities will be able to tell where we are at all times. With universal hidden surveillance cameras and spy satellites, authorities will
be able to see us almost everywhere outside of our homes and may even be able to scan us there. In another less Orwellian future, authorities will not have unlimited access to information about us. We will have some control over who views this information, because of legal guarantees, and grassroots efforts to keep totalitarian tendencies at bay. Which of these futures becomes reality depends on what we do now to protect ourselves and our rights to privacy.

Many of us are familiar with George Orwell’s dark vision of an all-knowing state apparatus bent on controlling the actions, thoughts, and dreams of its captive citizenry. When the real 1984 rolled around, many were amused at just how wrong Orwell’s prophecy had been. Instead of Big Brother, we had big business and democracy. China and the Soviet Bloc might have succumbed to variants of the Orwellian nightmare, but not the free and open West. A few years later the West’s victory in the Cold War, like its earlier victory over Nazism and fascism, seemed to establish once and for all the superiority of an open system, where the flow of money, information, and ideas was not dictated from above, but was instead permitted to flow according to the invisible hand of market forces, subject only to certain “traffic lights” of regulation that ultimately enhanced flow and the public good.

Ironically, our very openness with regard to the flow of information has led in recent years to Orwellian-scale surveillance. Although the threat of a totalitarian regime seems remote, the invasions of privacy that Orwell predicted are beginning to occur in the West because of the enormous information processing and storage capabilities of computers and related technologies. Fears of a governmental Big Brother have been aggravated by the reality of a horde of little brothers from the private sector who monitor everything from our purchasing preferences to our
able to see us almost everywhere outside of our homes and may even be able to scan us there. In another less Orwellian future, authorities will not have unlimited access to information out us. We will have some control over who views this ornament, because of legal guarantees, and grassroots efforts keep totalitarian tendencies at bay. Which of these futures comes reality depends on what we do now to protect ourselves and our rights to privacy.

Many of us are familiar with George Orwell’s dark vision of all-knowing state apparatus bent on controlling the actions, thoughts, and dreams of its captive citizenry. When the real 84 rolled around, many were amused at just how wrong well’s prophecy had been. Instead of Big Brother, we had big business and democracy. China and the Soviet Bloc might have succumbed to variants of the Orwellian nightmare, but not the open West. A few years later the West’s victory in the Cold War, like its earlier victory over Nazism and fascism, seemed to establish once and for all the superiority of an open system, where the flow of money, information, and ideas was not dictated from above, but was instead permitted to flow according to the invisible hand of market forces, subject only to certain “traffic controls” of regulation that ultimately enhanced flow and the public good.

Ironically, our very openness with regard to the flow of information has led in recent years to Orwellian-scale surveillance. Although the threat of a totalitarian regime seems remote, the visions of privacy that Orwell predicted are beginning to occur in the West because of the enormous information processing and storage capabilities of computers and related technologies. Cases of governmental Big Brother have been aggravated by reality of a horde of little brothers from the private sector who monitor everything from our purchasing preferences to our health records. The motivation is not mind-control as Orwell thought it would be. It is profit.

Monitoring methods have mushroomed with demand, as those in positions of corporate or governmental power wish to keep tabs on potentially unprofitable, profitable, criminal, or troublesome subordinates. For example, corporations are sampling urine for drug content; there is talk of implanting a “smart card” in each automobile to track location and speed; bosses are monitoring e-mail; we are filmed by hidden cameras in banks, supermarkets, and offices every day; and insurance companies are screening people based on their medical history and genetic predispositions for disease. Will there be no limit placed on who can gain access to information about our behaviors and bodies? Will we, the monitored, become increasingly powerless as authorities track and tally information on our whereabouts, doings, and bodies, only to use that information to make decisions that may hurt us?

Since the mid-century, the debate over privacy has primarily focused on a woman’s right to make her own reproductive decisions and control her own body. While various groups continue to fight for the rights of the unborn child, it appears that the rights of the mother have prevailed, at least to the extent that Roe v. Wade in 1973 guaranteed each woman the right to a legal abortion, or that Griswold v. Connecticut in 1965 established the “right to privacy.” The privacy debate has now opened up into several new arenas, as technology has made new forms of control available to authorities and new means of observation available to voyeurs, hackers, employers, and spies. This essay addresses the future of privacy—in particular, the status of information relating to one’s self and the many problems of who has and who should have access to this information.
What Is Privacy?

Our intuitive understanding may be that privacy amounts to being left alone or being left in peace. But there is more to privacy than not being bothered. Privacy is not solely the absence of intrusions, just as peace is not solely the absence of violent conflict. Privacy is an active process, an assertion of the self against an invasive world, a demarcating of both a physical and mental "self-space" where we can be ourselves. This self-space can include an actual physical territory, such as our home; and, at a very minimum, self-space usually encompasses the physical space of our body. Self-space, however, also includes mental territories where we are in control of our inner life, free from the burdens of extrapersonal interference. Just as we look out of the window to see who is knocking on our physical space, we might screen our calls to avoid invasions of our mental space. Since privacy is a matter of who can gain access to self-space, and self-space encompasses both physical and mental domains, privacy is a complex matter of who can gain access to the inner territories of our homes, bodies, and the personal expressions of our minds. If strangers can gain access to these inner sancta without our consent, then self-space is lost; it becomes desanctified, violated, no longer our own. Since much of what is most valuable in life takes place in the inner sancta of home, body, and mind, when self-space is violated, the very value of our lives is degraded.

We all behave differently when we are in public and when we are alone. To realize that we are being observed when we have been acting in a nonpublic manner is to feel an intrusion into our physical or mental space. Privacy presumes having a
What Is Privacy?

Our intuitive understanding may be that privacy amounts to being left alone or being left in peace. But there is more to privacy than not being bothered. Privacy is not solely the absence of intrusions, just as peace is not solely the absence of violent conflict. Privacy is an active process, an assertion of self against an invasive world, a demarcating of both a physical and mental "self-space" where we can be ourselves. His self-space can include an actual physical territory, such as our home; and, at a very minimum, self-space usually encompasses the physical space of our body. Self-space, however, also includes mental territories where we are in control of our inner life, free from the burdens of extrapersonal interference. Just as we look out of the window to see who is knocking on our physical space, we might screen our calls to avoid invasions of our mental space. Since privacy is a matter of who can gain access to self-space, and self-space encompasses both physical and mental domains, privacy is a complex matter of who can gain access to the inner territories of our homes, bodies, and the personal expressions of our minds. Strangers can gain access to these inner sancta without our consent, then self-space is lost; it becomes desanctified, violated, no longer our own. Since much of what is most valuable life takes place in the inner sancta of home, body, and mind, when self-space is violated, the very value of our lives is degraded.

We all behave differently when we are in public and when we are alone. To realize that we are being observed when we have been acting in a nonpublic manner is to feel an intrusion of our physical or mental space. Privacy presumes having a physical or mental space where control can be exercised over personal actions and thoughts by no one but ourselves. We all protect our self-space by choosing how, when, where, and to whom we reveal inner aspects of ourselves. Just as we wear clothes to reveal and hide aspects of our physical and mental selves, we "wear" behaviors or personas depending on the situation. Just as we choose to whom we reveal our naked bodies, we choose to whom we reveal the most personal parts of our minds. When the choice is taken away from us, and we are physically or mentally disrobed, we feel violated. If a person disregards, for example, a colleague's workplace persona and tries to make sexual advances, then self-space is violated because the victim's control over how his or her self is to be revealed and treated has been violated. Sexual harassment is a violation of mental self-space as much as forcefully removing clothes would be a violation of physical self-space. The natural reactions may include fear, embarrassment, depression, feelings of powerlessness, anger, and loss of trust.

Once our self-space has been violated, whether mildly by an eavesdropping relative or profoundly by a rapist, we no longer feel secure in our personal space, and lose the ability to feel at ease there. But feeling at ease and at home in one's self is thought by many people to be a necessary foundation for happiness. Thus the pursuit of happiness presumes the absence of gross violations of self-space. It presumes a measure of privacy.

Since privacy is an issue of control over self-space and what is to count as self-space, the issue of privacy is a political issue inseparable from other issues relating to the more familiar uses and abuses of power. It is inseparable from questions of physical and intellectual property rights, ownership, or trespass.
Why Does Privacy Matter?

Our need for privacy is probably not an innate desire in the same sense that the avoidance of pain is. While something akin to having secrets or hiding true feelings and intentions may exist across cultures, privacy — like democracy, capitalism, or inalienable rights — is a specific Western cultural construct derived from these more fundamental human tendencies. Many languages, Japanese and Russian, for example, lack an exact native equivalent for the word “privacy.” Actions that we would consider a violation of privacy in America, might elsewhere be considered a gesture of concern. That privacy is a cultural construct, however, does not mean that it is not worth fighting for — no less so than the cultural construct democracy is worth fighting for. Indeed, we might want to fight for democracy and privacy for similar reasons: more is at stake in the present and future privacy debate than unpleasant feelings of being intruded upon. Raw power is at stake: whether or not we will be able to exercise control over ourselves, information about ourselves, and the decisions that will affect us.

The ultimate private space, of course, is the domain of our own thoughts, wishes, fantasies, and intentions. Though they might wish they could, authorities are unable to read minds directly. Instead, they have had to settle for surveillance of people who thought their acts were private. In order to grant federal, state, and local authorities the freedom to infiltrate and document illegal activities, we must grant them the same powers of surveillance over ourselves. Since there are criminals and terrorists who need to be taken off the streets for our own protection, potential surveillance is a compromise each American must accept. Because most of us are usually law-abiding
Why Does Privacy Matter?

Our need for privacy is probably not an innate desire in the same sense that the avoidance of pain is. While something akin to having secrets or hiding true feelings and intentions may exist across cultures, privacy—like democracy, capitalism, or inalienable rights—is a specific Western cultural construct derived from these more fundamental human tendencies. Many languages, Japanese and Russian, for example, lack an exact native equivalent for the word “privacy.” Actions that we would consider a violation of privacy in America, might elsewhere be considered a gesture of concern. That privacy is a cultural construct, however, does not mean that it is not worth fighting for—no less so than the cultural construct democracy is worth fighting for. Indeed, we might want to fight for democracy and privacy for similar reasons: more is at stake in the present and future privacy debate than unpleasant feelings of being intruded upon. Raw power is at stake: whether or not we will be able to exercise control over ourselves, information about ourselves, and the decisions that will affect us.

The ultimate private space, of course, is the domain of our own thoughts, wishes, fantasies, and intentions. Though they might wish they could, authorities are unable to read minds directly. Instead, they have had to settle for surveillance of people who thought their acts were private. In order to grant federal, state, and local authorities the freedom to infiltrate and document illegal activities, we must grant them the same powers of surveillance over ourselves. Since there are criminals and terrorists who need to be taken off the streets for our own protection, potential surveillance is a compromise each American must accept. Because most of us are usually law-abiding citizens, we think that surveillance of our actions would hardly be worth the FBI’s trouble. We expect surveillance to be used against those suspected of criminal activities and expect the authorities to leave us alone if there are no grounds for suspicion.

For most of us, potential surveillance is a compromise comparable to restrictions placed on other basic freedoms. We tolerate these restrictions because they enhance some common good, such as public safety. For example, we do not really have the right to unmitigated free speech since it is illegal to use certain words on the airwaves. We do not really have the right to an unmitigated pursuit of happiness since if what makes us happy infringes on the rights of others, we are usually kept from pursuing those activities. But at what point do tolerable restrictions on our right to exercise our will as we choose become intolerable violations and abuses of power? Few of us mind that the duration and destination of every one of our phone calls is recorded in some database, but monitoring of our conversations would be considered a violation because the content, as opposed to the length, of conversations gives access to our private thoughts.

A balance must be found, then, between protecting the common good and limiting the powers of a potentially overreaching political, military, corporate, and industrial complex often motivated by lust for power and profit. On the one hand, we must acknowledge that any right to privacy we insist on keeping for ourselves is a right that will be shared by child molesters, terrorists, and mass murderers. On the other, we must remember the many times the U.S. government has acted illegally and immorally.

We realize that power and lack of accountability lead to abuses when we survey America’s past and find so many examples where the government has intentionally deceived and
mistreated the people it was created to protect. Even if we overlook slavery and genocide of native peoples as the dark side of a benighted and not so distant past, events of this century offer no reason to take comfort. For example, since 1940, the U.S. government has secretly exposed more than 23,000 American citizens to radiation and released biological agents in hundreds of government-backed experiments (Lee 1994), incarcerated tens of thousands of Americans because of their Japanese ancestry, conducted numerous secret wars abroad, and committed assassinations both abroad and at home. There are always henchmen, such as Oliver North of the Iran-Contra scandal, who will use covert means to accomplish what they believe to be their patriotic duty. There is no reason to believe that those in power will not use the new information-gathering technologies against people not in power. Given the abuses of the past, we might expect that they will again misuse their power; accordingly, we must take preemptive and preventive measures to protect ourselves.

Confronted by the potentially invasive and morally corrupt nature of government organs like the police, FBI, CIA, NSA, and IRS, citizens have generally had two means of recourse. One is to operate within the system and try to have legislation passed that will protect ordinary folk from abuses of power. The Bill of Rights was a first attempt at such legal guarantees. The other way to counteract an overzealous authority is to operate outside the system. Protest has taken many forms in this country, from civil disobedience to terrorism. In the case of protecting privacy, violent means are not likely to thwart surveillance since violence cannot undo the technological developments that allow invasions of privacy. Only legal and technological protections can counteract the essentially technological threat of modern forms
istreated the people it was created to protect. Even if we overlook slavery and genocide of native peoples as the dark deed of a benighted and not so distant past, events of this century offer no reason to take comfort. For example, since 1940, the U.S. government has secretly exposed more than 23,000 American citizens to radiation and released biological agents in hundreds of government-backed experiments (Lee 1994), carcerated tens of thousands of Americans because of their Hispanic ancestry, conducted numerous secret wars abroad, and committed assassinations both abroad and at home. These always henchmen, such as Oliver North of the Iran-Contra scandal, who will use covert means to accomplish what they believe to be their patriotic duty. There is no reason to believe that those in power will not use the new information-gathering technologies against people not in power. Given the abuses of the past, we might expect that they will again misuse their power; accordingly, we must take preemptive and preventive measures to protect ourselves.

Confronted by the potentially invasive and morally corrupting nature of government organs like the police, FBI, CIA, NSA, and IRS, citizens have generally had two means of recourse. One is operate within the system and try to have legislation passed at will protect ordinary folk from abuses of power. The Bill of Rights was a first attempt at such legal guarantees. The other way to counteract an overzealous authority is to operate outside the system. Protest has taken many forms in this country, from civil disobedience to terrorism. In the case of protecting privacy, blunt means are not likely to thwart surveillance since violence must undo the technological developments that allow invasions of privacy. Only legal and technological protections can interact with the essentially technological threat of modern forms of surveillance, as we find today in attempts to create encryption programs to protect sensitive transmissions on the Internet.

Where, then, can we reach a reasonable compromise point between an individual's right to privacy and the authorities' need to maintain public security and trust? Complete privacy would not serve the public good because terrorists could operate with impunity. Complete and indiscriminate surveillance capabilities would not serve the public good either because people would distrust and attempt to subvert the government, as the recent surge in militia and separatist groups makes amply clear. The most promising compromise is to permit warranted surveillance only on grounds of individual suspicion. This is what was intended by the phrase "probable cause" in the fourth amendment, and its stipulation that authorities must attain a warrant prior to conducting a search. Unfortunately, a number of recent cases, culminating in the 1995 Supreme Court ruling Vernonia School District v. Acton (considered below), seems to undermine the requirement of individual suspicion, and pushes society closer to an Orwellian situation of constant and unwarranted surveillance.

In short, privacy issues are involved any time self-space stands to be violated. We have entered an era when extensive information is kept on each one of us in databanks used by credit agencies, medical personnel, insurance companies, and the government, even though we have done nothing criminal. Whether this information pertains to genetic history, sexual orientation, or purchasing records, we ought to be able to decide what aspects of this stored information can be made public or used against us. Because of unprecedented technological developments, however, information is easily stored, gathered, processed, and obtained. Although people in the past had to deal with potentially damning, publicly accessible information
Harvard Vision

about themselves circulating in the form of gossip and reputation, people must now confront anonymous databases that contain just about any information about themselves that a computer might automatically track. The problem is that lacking discernment, computers will pass sensitive self-information on to anyone knowing the access code. Mistakes can occur, as when the credit rating of the entire town of Norwich, Vermont, went bad one day a few years ago, after somebody, somewhere, typed in the wrong code.

More worrisome, self-information can be used against us, as when insurance companies deny coverage. Or it can fall into the wrong hands. In the coming decade a debate will rage over the legal basis for the control of self-information. The debate is not an academic one; it is a struggle for power in which the power of the individual is pitted against the growing power of authorities, whether corporate, religious, or governmental.

The Privacy Battle in Social Context

It must be understood that the debate over privacy is only one aspect of a much larger power struggle and societal transformation that America is presently undergoing. Simply put, technological developments and trends toward internationalization have caused stressful economic dislocations as workers scramble to enter the information age while being forced to compete with cheap foreign labor. At the same time, various cultural movements have redistributed power, as women, gays, non-whites, immigrants, and other traditionally excluded groups have gained access to the airwaves, government offices, universities, and living rooms of America. It has been hard to cope with so many rapid and disorienting changes. The recent increase in white male militias and separatist groups has as
Harvard Vision

about themselves circulating in the form of gossip and reputation, people must now confront anonymous databases that contain just about any information about themselves that a computer might automatically track. The problem is that lacking discernment, computers will pass sensitive self-information on to anyone knowing the access code. Mistakes can occur, as when the credit rating of the entire town of Norwich, Vermont, went bad one day a few years ago, after somebody, somewhere, typed in the wrong code.

More worrisome, self-information can be used against us, as when insurance companies deny coverage. Or it can fall into the wrong hands. In the coming decade a debate will rage over the legal basis for the control of self-information. The debate is not an academic one; it is a struggle for power in which the power of the individual is pitted against the growing power of authorities, whether corporate, religious, or governmental.

The Privacy Battle in Social Context

It must be understood that the debate over privacy is only one aspect of a much larger power struggle and societal transformation that America is presently undergoing. Simply put, technological developments and trends toward internationalization have caused stressful economic dislocations as workers scramble to enter the information age while being forced to compete with cheap foreign labor. At the same time, various cultural movements have redistributed power, as women, gays, non-whites, immigrants, and other traditionally excluded groups have gained access to the airwaves, government offices, universities, and living rooms of America. It has been hard to cope with so many rapid and disorienting changes. The recent increase in white male militias and separatist groups has as much to do with the perceived predatory nature of the federal government as it has to do with the economic and cultural dislocations and redistributions of power that have taken place over recent decades. While the anger in the land may be justified in some instances, violence cannot succeed in undoing the technological developments that underlie much of the economic and cultural dislocations that are ultimately fueling this anger. Technological developments—TV, the abortion pill RU-486, the Internet, birth control pills, and electronic surveillance—are genies out of the bottle. The cultural possibilities that they have opened up are also here to stay. Pat Buchanan, Pat Robertson, Ralph Reed, and other cultural conservatives may try to turn the clock back to some imagined Rockwellian era, but power is already too diffuse and the culture has changed too much to go back to the 1950s. If Roe v. Wade were ever overturned, we would probably find both men and women taking to the streets in protest. Nevertheless, the reason politicians like Buchanan have such appeal is that they are advocating a stop to all this change. There is a real danger that an authoritarian movement will grow as ordinary people seek simplistic solutions to all the stresses associated with America’s rapid cultural and economic changes.

Although the hegemony of Caucasian men has weakened somewhat, there are other tendencies counteracting past trends toward a more equitable and meritocratic distribution of power. One is an increasing maldistribution of wealth. Those who fail to find a niche in the information economy are getting left behind. There are fewer and fewer jobs to go around for the poorly educated, as corporations move to the third world to take advantage of cheaper labor costs. And the people who used to hold America’s blue collar and basic white collar jobs—the people who hold families and neighborhoods together—are getting poorer, more numerous, and more frustrated each year. At the
same time, many Americans have given up on their commitment to bring the poor to the table of America's bounty. The increase in school segregation, cuts in education, walled communities, and welfare and affirmative-action bashing all attest to this trend.

Another tendency serving to counteract past redistributions of power is an increasing concentration of power in the hands of authorities, allowing them to act with less and less accountability. If present trends toward disempowerment of the poor and weak in favor of increased empowerment of the rich and strong continues, we can expect a populist backlash that could rock America to its core. Either that, or the American Dream will die at the armed gates of its wealthy suburbs. If a major economic downturn exacerbates present faultlines, we should not expect the disenfranchised to follow a leader who is sensitive to the privacy needs of individuals. If past history is any indication, he will be an authoritarian who offers authoritarian solutions.

Issues of privacy, therefore, cannot be dissociated from broader issues relating to the distribution of power in society. Advocates of privacy rights must support all individual rights since these are all connected. When power is decentralized and democracy thrives, privacy rights flourish. When power is overcentralized, privacy rights fall victim to the unaccountable abusers of power.

Privacy and the Law

While the word "privacy" is not mentioned anywhere in the U.S. Constitution, many people believe that their right to privacy is implicitly protected not only by the right to the pursuit of happiness, but also by the fourth amendment. This amendment seems to have been intended by the framers of the
Harvard Vision

same time, many Americans have given up on their commitment to bring the poor to the table of America’s bounty. The increase in school segregation, cuts in education, walled communities, and welfare and affirmative-action bashing all attest to this trend.

Another tendency serving to counteract past redistributions of power is an increasing concentration of power in the hands of authorities, allowing them to act with less and less accountability. If present trends toward disempowerment of the poor and weak in favor of increased empowerment of the rich and strong continues, we can expect a populist backlash that could rock America to its core. Either that, or the American Dream will die at the armed gates of its wealthy suburbs. If a major economic downturn exacerbates present faultlines, we should not expect the disenfranchised to follow a leader who is sensitive to the privacy needs of individuals. If past history is any indication, he will be an authoritarian who offers authoritarian solutions.

Issues of privacy, therefore, cannot be dissociated from broader issues relating to the distribution of power in society. Advocates of privacy rights must support all individual rights since these are all connected. When power is decentralized and democracy thrives, privacy rights flourish. When power is overcentralized, privacy rights fall victim to the unaccountable abusers of power.

Privacy and the Law

While the word “privacy” is not mentioned anywhere in the U.S. Constitution, many people believe that their right to privacy is implicitly protected not only by the right to the pursuit of happiness, but also by the fourth amendment. This amendment seems to have been intended by the framers of the

Privacy under Siege

Bill of Rights, with their ample firsthand knowledge of tyranny, to protect citizens from excessive encroachment by the government. Justice Blackmun argued in Roe v. Wade that a right to privacy was implied not only by the fourth amendment, but also by the fourteenth amendment’s notion of ordered liberty. Others have argued that privacy is also protected by the ninth and tenth amendments. The reader may judge:

The enumeration in the Constitution of certain rights, shall not be construed to deny or disparage others retained by the people.
— Ninth Amendment

The powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people. —Tenth Amendment.

No state shall ... deprive any person of ... liberty ... without due process of law. — The "liberty clause" of the Fourteenth Amendment

While it is debatable whether these amendments specifically protect privacy, they were clearly designed to keep the federal government from becoming too powerful while allowing the people to rule themselves unhindered by authoritarian interference. The recent movement to devolve power to the states is a response to decades of increasing centralization of federal power, which seemed to threaten the notion of self-governance that such amendments were meant to safeguard.

Although numerous court cases and laws have created a hodgepodge of specific protections against the disclosure of private information, there is no overarching law that forbids the disclosure of information that a person might want to keep private. For example, after a list of the videos rented by Robert Bork was made public during his confirmation hearings in 1987, the disclosure of such lists was made illegal by the Video Privacy
Harvard Vision

Protection Act of 1988. However, there is still no comparable protection against the disclosure of medical records, which contain much more sensitive and potentially damning information than anyone’s taste in videos. This absurd discrepancy was made sadly clear when the late Arthur Ashe was forced to hold a press conference to announce that he was infected with the AIDS virus because this information had been leaked against his will (Moseley-Braun). Since there is no comprehensive law against disclosure, we are all potential victims. For example, some hospitals (including Harvard’s UHS clinic) require patients to sign a form stating that the result of the test will become part of their permanent medical record, where insurance companies can access it and use the results as a basis to refuse them coverage. Other hospitals (such as Mass General) offer free and confidential tests. Clearly, the present hodgepodge of practices and legislation is a mess, and some more general privacy protections are called for.

While there are laws that protect privacy, these are largely inadequate, especially when it comes to preventing the new modes of privacy violation ushered in by the information revolution. The last major attempt at legislating comprehensive privacy protection was the Privacy Protection Act of 1974, which significantly protects citizens from privacy violations by record-keeping government agencies and guarantees access to most government records containing self-information. However, there is little protection against private sector access and abuse of self-information. For example, as “smart cards,” containing extensive digital information about the user, become more widespread, specific protections will be needed that allow users to view and correct their digitally encoded records and photographs. Protections are also needed against misuse of personal information in the private sector, and they must
rotection Act of 1988. However, there is still no comparable rotection against the disclosure of medical records, which ontain much more sensitive and potentially damning information nan anyone's taste in videos. This absurd discrepancy was made sadly clear when the late Arthur Ashe was forced to hold press conference to announce that he was infected with the IDS virus because this information had been leaked against is will (Moseley-Braun). Since there is no comprehensive law against disclosure, we are all potential victims. For example, some hospitals (including Harvard's UHS clinic) require patients sign a form stating that the result of the test will become art of their permanent medical record, where insurance companies can access it and use the results as a basis to refuse em coverage. Other hospitals (such as Mass General) offer se and confidential tests. Clearly, the present hodgepodge of actices and legislation is a mess, and some more general ivacy protections are called for.

While there are laws that protect privacy, these are largely adequate, especially when it comes to preventing the new odes of privacy violation ushered in by the information volution. The last major attempt at legislating comprehensive ivacy protection was the Privacy Protection Act of 1974, which plicantly protects citizens from privacy violations by record-eping government agencies and guarantees access to most Vernon records containing self-information. However, there little protection against private sector access and abuse of If-information. For example, as “smart cards,” containing tensive digital information about the user, become more Despand, specific protections will be needed that allow users view and correct their digitally encoded records and otographs. Protections are also needed against misuse of rsonal information in the private sector, and they must specifically limit the ability of companies to transfer data on people without their consent.

The courts have not tended to side with individuals suing companies over privacy violations. In a recent case, Dwyer v. American Express Company (652 N.E.2d 1351; Ill. App. Ct., 1995), an individual sued over the release of information compiled from the cardholder's purchasing record. The court ruled:

By using [the card], a cardholder is voluntarily and necessarily, giving information to defendants that, if analyzed, will reveal a cardholder's spending habits and shopping preferences. We cannot hold that a defendant has committed an unauthorized intrusion by compiling the information voluntarily given to it and then renting its compilation.
(Glover 1995)

This decision sets a troubling precedent. While company disclosures of compiled personal information may, in this case, lead to little more than junk mail and some annoying telephone solicitations, other compilations and profiles may be much more harmful. As we enter an age of linked electronic driving licenses, food stamps, Social Security cards, and credit cards, the potential for damning compilations and profiles grows. For example, it would not be in our interest if potential employers could gain access to profiles of our past savings behavior or income levels, especially those to which we ourselves lack access. Since companies are in business to make money, we cannot expect them not to seek such information. The only way to impede the rampant disclosure of personal information is to regulate it and make certain types of disclosure illegal.

In recent years, a number of bills have been introduced to protect privacy in a more systematic way. In the 103d Congress, Senator Patrick Leahy (D-Vermont) submitted “The Health Care
Privacy Protection Act" (S. 2129), which would have criminalized the release of medical information. Senator Paul Simon (D-Illinois) supported a fairly comprehensive Privacy Protection Act (S. 1735), which would have, among other things, prevented abuses of electronic monitoring in the workplace. These bills were introduced in 1993-94 but failed to pass. In the present 104th Congress, two new bills are under consideration, "The Medical Records Confidentiality Act" (S. 1360), backed by Senators Robert Bennett (R-Utah) and Leahy, and "The Fair Health Information Practices Act" (H.R. 435) backed by Representative Gary Condit (D-California). The Bennett-Leahy and Condit bills would greatly increase medical record confidentiality and patient access to medical records. It is in our interest as receivers of medical care to have these or similar bills passed, but certain lobbies are fighting confidentiality.

Legislation may not suffice. An amendment to the Constitution may be necessary, and we can expect a growing political movement to attempt to accomplish this in coming years. On March 26, 1991, Harvard Law School Professor Laurence Tribe proposed as part of his keynote address to the First Conference on Computers, Freedom, and Privacy, and for the first time in his career as a renowned constitutional scholar, the following constitutional amendment:

This Constitution’s protections for the freedoms of speech, press, petition, and assembly, and its protections against unreasonable searches and seizures and the deprivation of life, liberty, or property without due process of law shall be construed as fully applicable without regard to the technological method or medium through which information content is generated, stored, altered, transmitted or controlled.
Privacy Protection Act" (S. 2129), which would have criminalized the release of medical information. Senator Paul Simon (D-Illinois) supported a fairly comprehensive Privacy Protection Act (S. 1735), which would have, among other things, prevented abuses of electronic monitoring in the workplace. These bills were introduced in 1993-94 but failed to pass. In the present 104th Congress, two new bills are under consideration, “The Medical Records Confidentiality Act” (S. 1360), backed by Senators Robert Bennett (R-Utah) and Leahy, and “The Fair Health Information Practices Act” (H.R. 435) backed by Representative Gary Condit (D-California). The Bennett-Leahy and Condit bills would greatly increase medical record confidentiality and patient access to medical records. It is in our interest as receivers of medical care to have these or similar bills passed, but certain lobbies are fighting confidentiality.

Legislation may not suffice. An amendment to the Constitution may be necessary, and we can expect a growing political movement to attempt to accomplish this in coming years. On March 26, 1991, Harvard Law School Professor Laurence Tribe proposed as part of his keynote address to the First Conference on Computers, Freedom, and Privacy, and for the first time in his career as a renowned constitutional scholar, the following constitutional amendment:

This Constitution's protections for the freedoms of speech, press, petition, and assembly, and its protections against unreasonable searches and seizures and the deprivation of life, liberty, or property without due process of law shall be construed as fully applicable without regard to the technological method or medium through which information content is generated, stored, altered, transmitted or controlled.

Privacy under Siege

Although the word “privacy” is not used here, privacy would be better protected under Tribe's amendment because technological developments are the primary reason that privacy is under siege. Tribe's amendment would probably make searching someone's database without his or her knowledge or permission tantamount to a search through personal effects without a warrant. With pro-authoritarian judges like Antonin Scalia dominating the Supreme Court, however, even such an amendment might fail to protect privacy, as the following case makes disturbingly clear:

On June 26, 1995, the Supreme Court ruled 6-3 in a precedent-setting case, *Vernonia School District 47J v. Acton et al.*, that a student may be barred from participating in sports for refusing to take drug tests, on the premise that an athlete should have, in Justice Scalia's words, “a reduced expectation of privacy.” The tests involve submitting a urine sample in the presence of a monitor who makes sure no tampering or deception occurs. Scalia justified his position by arguing that athletes used to public locker rooms and urinals should not be shy about submitting a monitored urinalysis. This seems to directly contradict the fourth amendment, yet the highest court in the land has had its say on privacy, and it does not bode well for the health of civil liberties. Why, after all, should being a student athlete be considered “probable cause,” which the fourth amendment requires before a search takes place? Will millions of student athletes now have to submit to intrusive bodily searches whether or not there are grounds for individual suspicion? Who is to decide who is to have “a reduced expectation of privacy,” Justice Scalia? Will employees, teachers, and anyone in a public capacity soon have a reduced expectation of privacy? Will the senators and judges themselves be required to submit urine samples?
Harvard Vision

According to Scalia, an individual’s expectations of privacy must be balanced against an authority’s needs to maintain authority. Warrantless searches of students were first established in *New Jersey v. T.L.O.* (469 U.S. 325, 1985). In that case a student sued because her purse was searched after tobacco smoke was detected in the bathroom. Although the legitimacy of warrantless searches was established here, the ruling was tempered by the requirement of individualized suspicion. That is, it would be legal to search only an individual suspected of breaking rules or laws on specific evidence pointing to that individual. It would be illegal to search all students according to this 1985 decision. Note, however, that the 1995 *Vernonia School District v. Acton* case allows warrantless searches without individualized suspicion, and therefore further undermines individual rights, and the fourth amendment’s intended protections against authoritarianism.

The fourth amendment is under siege elsewhere. On February 8, 1995, the Republican Congress, as part of its “Contract with America,” passed legislation that would greatly extend the ability of federal authorities to search without first obtaining a warrant. In the past, warrantless searches were deemed reasonable if evidence was in plain view or if evidence might be imminently destroyed. The Exclusionary Rule Reform Act (H.R. 666), introduced by Representative Bill McCollum (R-Florida), states:

Evidence which is obtained as a result of a search and seizure shall not be excluded in a proceeding in a court of the United States, if the search or seizure was carried out in circumstances justifying an objectively reasonable belief that it was in conformity with the Fourth Amendment. The fact that evidence was obtained pursuant to and within the scope of a warrant constitutes prima facie evidence of the existence of such circumstances. (McCollum)

In other words, the FBI needs only to believe that it needs to
Harvard Vision

According to Scalia, an individual’s expectations of privacy must be balanced against an authority’s needs to maintain authority. Warrantless searches of students were first established in New Jersey v. T.L.O. (469 U.S. 325, 1985). In that case a student sued because her purse was searched after tobacco smoke was detected in the bathroom. Although the legitimacy of warrantless searches was established here, the ruling was tempered by the requirement of individualized suspicion. That is, it would be legal to search only an individual suspected of breaking rules or laws on specific evidence pointing to that individual. It would be illegal to search all students according to this 1985 decision. Note, however, that the 1995 Vernonia School District v. Acton case allows warrantless searches without individualized suspicion, and therefore further undermines individual rights, and the fourth amendment’s intended protections against authoritarianism.

The fourth amendment is under siege elsewhere. On February 8, 1995, the Republican Congress, as part of its “Contract with America,” passed legislation that would greatly extend the ability of federal authorities to search without first obtaining a warrant. In the past, warrantless searches were deemed reasonable if evidence was in plain view or if evidence might be imminently destroyed. The Exclusionary Rule Reform Act (H.R. 666), introduced by Representative Bill McCollum (R-Florida), states:

Evidence which is obtained as a result of a search and seizure shall not be excluded in a proceeding in a court of the United States, if the search or seizure was carried out in circumstances justifying an objectively reasonable belief that it was in conformity with the Fourth Amendment. The fact that evidence was obtained pursuant to and within the scope of a warrant constitutes prima facie evidence of the existence of such circumstances. (McCollum)

In other words, the FBI needs only to believe that it needs to

Privacy under Siege

search, and it can do so. This, in effect, gives government authorities the right to search at will, since the only grounds they would need is a hunch.

Technology will further extend warrantless search powers. Already it is possible to scan from satellites with extremely high resolution. According to the “open fields doctrine” embodied in such Supreme Court decisions as Oliver v. United States (466 U.S. 170) and Hester v. United States (265 U.S. 57), surveillance obtained from the air does not require a warrant. If the same doctrine is construed to apply to satellite surveillance, we can expect the blue skies that once represented limitless possibility to turn into the blue iris of our watchful government.

Privacy in the Workplace

Employers are increasing their surveillance of employees—from urinalyses to covert checks of e-mail. Although the government is not always trustworthy, some judges and legislators are potential allies in warding off the invasive data collecting of the little brothers of the private sector. Although we have yet to see a full backlash against employer snooping, such a movement is likely to arise in coming years as people increasingly feel that their personal autonomy has been violated by corporations. Laws against employer wiretapping, drug testing, and e-mail snooping are the surest way to stop such invasive behavior in the workplace. But since wealthy corporations are lobbying for surveillance powers, only a grassroots movement against such practices will stand a chance of limiting such practices.

To date, it appears that employers are for the most part having their way in court, and that workplace surveillance has become the norm. In O’Connor v. Ortega (480 U.S. 709, 717
Harvard Vision

[1987]), the Supreme Court eroded constitutional protection against work-related searches and seizures once afforded government employees by the fourth amendment. While public employees may have a “reasonable” expectation of privacy, the level of privacy is to be determined on a case-by-case basis by the employer, FBI agent, or prosecutor. The employer may search without a warrant and without an employee’s consent so long as the search is work-related. Such court-established precedents amount to laws that favor employers over employees.

If the privacy rights of public employees are eroding, then private sector employees have it even worse since private employers are less likely than the government to worry about operating within constitutional guidelines. Numerous court decisions have made it clear that employers have the right to search company-operated areas and determine what an employee might reasonably regard as private; accordingly, it looks as if the battle for privacy in the workplace will have to shift from legal protection to self-protection. Employees are going to become more careful about e-mail and electronic communication generally.

Privacy and Medical Records

The foundation of the doctor-patient relationship is trust and openness. Patients may stop being honest with doctors if they feel that doctors are divulging health information that they thought was confidential to private sector companies that will then use that information to harm them, whether by excluding them from insurance protection or by raising their rates.

If patients and doctors see themselves as engaged in an antagonistic relationship, then we can expect other aspects of the relationship to deteriorate. For example, malpractice suits
[1987]), the Supreme Court eroded constitutional protection against work-related searches and seizures once afforded government employees by the fourth amendment. While public employees may have a "reasonable" expectation of privacy, the level of privacy is to be determined on a case-by-case basis by the employer, FBI agent, or prosecutor. The employer may search without a warrant and without an employee's consent so long as the search is work-related. Such court-established precedents amount to laws that favor employers over employees.

If the privacy rights of public employees are eroding, then private sector employees have it even worse since private employers are less likely than the government to worry about operating within constitutional guidelines. Numerous court decisions have made it clear that employers have the right to search company-operated areas and determine what an employee might reasonably regard as private; accordingly, it looks as if the battle for privacy in the workplace will have to shift from legal protection to self-protection. Employees are going to become more careful about e-mail and electronic communication generally.

Privacy and Medical Records

The foundation of the doctor-patient relationship is trust and openness. Patients may stop being honest with doctors if they feel that doctors are divulging health information that they thought was confidential to private sector companies that will then use that information to harm them, whether by excluding them from insurance protection or by raising their rates.

If patients and doctors see themselves as engaged in an antagonistic relationship, then we can expect other aspects of the relationship to deteriorate. For example, malpractice suits may increase if doctors are seen as puppets of cost-cutting insurance companies and HMOs rather than as upholders of the Hippocratic Oath who are determined to offer the best care possible. Public health may decline as people hide symptoms and illnesses to protect their coverage for when it is "really" needed. If the confidentiality of the lawyer-client relationship were under siege by insurance companies, lawyers would lobby strongly against disclosure. Doctors have been less vocal, perhaps because they are paid by insurance companies more often than by clients.

By excluding people because of preexisting conditions or even presumed genetic propensities for disease, insurance companies may be setting themselves up for a backlash that will eventually force them to provide something closer to universal coverage than they would like. Of course, insurance companies are only thinking of the bottom line, not any ethical responsibilities they might have to society. Since this is natural in our capitalist system, the only way to make sure insurance companies do not exclude people is to regulate them. The traditional basis of insurance has been the sharing of both risk and cost. If only physically and genetically healthy people who are employed can obtain health insurance, then the system will be both unfair and unsustainable. The number of under- and uninsured will mushroom. Already tens of millions of poor Americans lack insurance. These people will increasingly swamp hospital emergency rooms, driving up medical costs for the rest of us. The process of denying insurance will enhance the maldistribution of wealth in this country, and when the dispossessed eventually find their leader, a lot more may change than how medical care is distributed.

The problem of genetic fingerprinting will be central in determining the course of the debate over insurance policy. DNA
fingerprinting is reaching the point where it can be universally applied. Indeed, in the military, DNA fingerprinting is already mandatory. In May, 1996, television news reported that at least three military personnel had refused to give blood and saliva samples to military authorities for DNA fingerprinting, claiming that controls on access to this information were inadequate. All were subsequently court-martialed. In spite of their brave efforts to increase safeguards on personal information, such fingerprinting will, within a decade or two, probably become part of getting a birth certificate or a greencard.

There will therefore be no avoiding some tough ethical questions. Should a person’s DNA code be publicly accessible? Will insurance companies be allowed to screen applicants based on this information? Will we eventually have, in addition to our credit rating, a physical and genetic health rating?

In the interest of social stability and justice, insurance companies should not be allowed to discriminate based on medical history or genetic propensities. Since they are companies motivated by profit, they cannot be expected to police themselves honestly. Government regulation, as distasteful as it is to those who believe that the invisible hand can solve all social problems, is the only way to stop insurance companies, and the doctors who are ultimately beholden to them, from using medical records to discriminate against people. At present, insurance companies usually share claims through the Medical Information Bureau. (You can get a copy of your medical record by writing to the Medical Information Bureau, P.O. Box 105, Essex Station, Boston, MA 02112, or calling 617-426-3660.) However, insurance companies are likely to fight any such restrictions, and with the failure of Clinton’s attempt at health care reform, the problem of the uninsured is not likely to vanish soon. The way to reduce cost is not to
ing true. In the military, DNA fingerprinting is already mandatory. In May 1996, television news reported that at least three military personnel had refused to give blood and saliva samples to military authorities for DNA fingerprinting, fearing that controls on access to this information were inadequate. All were subsequently court-martialed. In spite of their brave efforts to increase safeguards on personal information, such fingerprinting will, within a decade or two, probably become part of getting a birth certificate or a green card.

There will therefore be no avoiding some tough ethical questions. Should a person's DNA code be publicly accessible? Will insurance companies be allowed to screen applicants based on this information? Will we eventually have, in addition to our credit rating, a physical and genetic health rating?

In the interest of social stability and justice, insurance companies should not be allowed to discriminate based on medical history or genetic propensities. Since they are companies motivated by profit, they cannot be expected to police themselves honestly. Government regulation, as inapplicable as it is to those who believe the invisible hand can solve all social problems, is the only way to stop insurance companies, and the doctors who are ultimately beholden to them, from using medical records to discriminate against people.

At present, insurance companies usually share claims through the Medical Information Bureau. (You can get a copy of your medical record by writing to the Medical Information Bureau, O. Box 105, Essex Station, Boston, MA 02112, or calling 17-426-3660.) However, insurance companies are likely to resist any such restrictions, and with the failure of Clinton's attempt at health care reform, the problem of the uninsured is likely to vanish soon. The way to reduce cost is not to exclude the people who are most likely to get sick, but to limit incentives for excessive spending. HMOs are now experimenting with measures that discourage doctors from prescribing surgery or other procedures unless deemed necessary. While this trend may bring with it its own injustices, costs will have to be brought down somehow, and this is a more equitable solution than exclusion based on medical or genetic history.

Privacy and the Internet

On February 8, 1996, President Clinton signed the Telecommunications Reform Act into law. That day thousands of homepages went black in protest. Title V, subtitle A of this legislation contains the Communications Decency Act, also known as the Internet Smut Law. Even the President has publicly doubted the constitutionality of this law. Its key phrases are "indecency" and "patently offensive." Those who wish to eliminate lewd images from the Internet have failed to do so with this legislation since it is doubtful whether a naked human being can be considered indecent. If representations of nakedness are indecent, then much of the world's art must be so.

The American Civil Liberties Union has joined several other plaintiffs in challenging the censorship provisions of this act as a violation of the first amendment, which reads: "Congress shall make no law abridging the freedom of speech." Senators Leahy and Feingold (D-Wisconsin) have already proposed a bill to repeal the patently offensive provisions of the Communications Decency Act. It is unlikely that censorship provisions will pass the Supreme Court's "least restrictive means" test, according to which regulation of speech must minimize restrictions placed
Harvard Vision

on lawful speech. Other lawsuits are challenging a provision against talk on the Internet about abortion.

This attempt to control the flow of information from above is probably going to fail. Even if putting “indecent” images on the Internet is banned in the U.S., images will be available from Sweden or Brazil. The very attempt belies a misunderstanding of how the Internet works, where everyone is simultaneously a broadcaster and receiver. Moreover, who is to judge what counts as indecent or patently offensive? Will we use the standards of Cambridge or of Topeka? One recent incident shows just how absurd attempts to legislate information content from above can be. America Online banned use of the word “breast” from all its newsgroups but when the breast cancer support group complained, AOL backed down.

In order to avoid a situation where people flout the law, the Internet Smut Law should be replaced by a system of personal content screening. The argument has been that pornography on the Internet is too easily accessed by children. The solution is to put censorship in the hands of parents. There already exist several programs on the market that allow parents to screen Internet pages against whatever content they find offensive. What is really at stake here is an attempt to dictate the contents of cyberticulture, by forcing certain puritanical values on the Internet community. Indeed, the Internet is just a new arena for this old cultural battle that has yet to reach a compromise or showdown. Since this will be a major cultural battle, one which falls along faultlines similar to those existing in the abortion or textbook debates, we can expect this fierce battle to be protracted but ultimately won by those who fight for individual choice over authoritarian control.

Another problem with antipornography laws for the Internet is that many instances involve only the depiction of sexual acts,
Harvard Vision

in lawful speech. Other lawsuits are challenging a provision against talk on the Internet about abortion. This attempt to control the flow of information from abroad probably is going to fail. Even if putting "indecent" images on the Internet is banned in the U.S., images will be available from Sweden or Brazil. The very attempt belies a misunderstanding of how the Internet works, where everyone is simultaneously a roadcastor and receiver. Moreover, who is to judge what counts as indecent or patently offensive? Will we use the standards of Cambridge or of Topeka? One recent incident shows just how absurd attempts to legislate information content from above can be. America Online banned use of the word "breast" from 11 its newsgroups but when the breast cancer support group complained, AOL backed down.

In order to avoid a situation where people flout the law, the Internet Smut Law should be replaced by a system of personal content screening. The argument has been that pornography on the Internet is too easily accessed by children. The solution is to put censorship in the hands of parents. There already exist several programs on the market that allow parents to screen the Internet pages against whatever content they find offensive. What is really at stake here is an attempt to dictate the contents of cyberspace, by forcing certain puritanical values onto the Internet community. Indeed, the Internet is just a new arena for an old cultural battle that has yet to reach a compromise or showdown. Since this will be a major cultural battle, one which will fall along faultlines similar to those existing in the abortion or textbook debates, we can expect this fierce battle to be retracted but ultimately won by those who fight for individual voice over authoritarian control.

Another problem with antipornography laws for the Internet is that many instances involve only the depiction of sexual acts, without real intercourse occurring. But is a depiction of an illegal act itself an illegal act? If so, then most literature and many films would be illegal since illegal acts are so often depicted in the arts. This area will likely become a legal morass, as technology emerges that permits the computer generation of child porn or other illegal activity that is indistinguishable from the real thing. The questions will shift from the illegal activity to the consequences of realistic depictions. If depictions are deemed to lead to acts against, say, children, then those who want to eliminate such depictions will have a case. Empirical research, however, will have to determine whether pornography in general leads to crime. It is conceivable that it might. But it is also conceivable that it might have the opposite effect. Note that similar claims about TV violence—namely that depictions of murder increase the likelihood of actual murders—have been fairly unsuccessful at eliminating such depictions from TV or film.

Privacy under Siege

Pretty Good Privacy

The government would like to be able to listen in on any electronic communication it chooses. The argument is that government agencies have been able to do this with telephones and faxes, and that they should be able to wiretap the new technologies as well. The government argues that without such powers of surveillance, terrorists and drug lords will become immune from infiltration and surveillance. While this is a serious concern, it must be balanced by a countervailing concern about government wiretapping.

Until last year, the government fought for permission to use the "Clipper chip," a hardware encryption system that would be built into all communication technologies, that would
automatically encrypt messages at the sender end and decrypt them at the receiver end. Government surveillance systems would hold a “backdoor key” that would allow them to decrypt any message. This key would supposedly be protected by a special agency and only given to those with a warrant.

For those who do not trust government pledges to honor privacy, obtain warrants, or keep any backdoor key secret, there is an alternative that the government has been fighting, but that it can do little to stop now. It is called PGP (“Pretty Good Privacy”), and is a shareware encryption and message authentication system written by programmer Phil Zimmerman based on encryption algorithms developed by a company called RSA Data Security.

The basic idea is that there are two keys: a private key known only to you, and a public key, which you publicize. Anyone can use your public key to write a message that can only be decrypted using your private key. This way people can send you messages, which only you can read, just as you can send them private messages using their public key. If you use your private key to encrypt a message, anyone with your public key can decrypt it, and therefore be certain that it indeed comes from you. Millions of Netscape and Lotus Notes users do not even know that they are sending messages using RSA technology every day. Assuming Zimmerman does not build a backdoor key into PGP, there will be no easy way for the government to wiretap electronic communications. So long as we use PGP, the FBI or National Security Agency would have to break the code of anyone they wished to monitor if that individual used PGP.

Zimmerman gave PGP to several friends in 1991 when it became clear that Congress was contemplating banning it. Once
omatically encrypt messages at the sender end and decrypt them at the receiver end. Government surveillance systems would hold a “backdoor key” that would allow them to decrypt a message. This key would supposedly be protected by a social agency and only given to those with a warrant.

For those who do not trust government pledges to honor privacy, obtain warrants, or keep any backdoor key secret, there is an alternative that the government has been fighting, that it can do little to stop now. It is called PGP (“Pretty Good Privacy”), and is a shareware encryption and message authentication system written by programmer Phil Zimmerman. It is based on encryption algorithms developed by a company called A Data Security.

The basic idea is that there are two keys: a private key known only to you, and a public key, which you publicize. Anyone can use your public key to write a message that can only be decrypted using your private key. This way people can send messages, which only you can read, just as you can send private messages using their public key. If you use your private key to encrypt a message, anyone with your public key can decrypt it, and therefore be certain that it indeed comes from you. Millions of Netscape and Lotus Notes users do not know that they are sending messages using RSA technology every day. Assuming Zimmerman does not build a backdoor key into PGP, there will be no easy way for the government to wiretap electronic communications. So long as PGP, the FBI or National Security Agency would have to ask the code of anyone they wished to monitor if that individual used PGP.

Zimmerman gave PGP to several friends in 1991 when it came clear that Congress was contemplating banning it. Once someone had uploaded it onto the Internet, the cat was out of the bag. Since foreigners had downloaded it, the Justice Department threatened to charge Zimmerman with breaking laws against exporting “munitions” (such as cryptographic programs) that carry a mandatory sentence of six years or more.

A grand jury started gathering evidence in 1993, but the charges were dropped last year. While the government has a legitimate need to thwart criminals, its criminalizing persecution of Zimmerman for several years shows just how much it considers PGP to be a threat to its surveillance powers. Now that PGP is available, all government attempts to build a backdoor into anything can be undermined by running PGP before government authorized encryption. Although the concerns about terrorism are genuine, we can consider the successful dissemination of PGP to be a partial grassroots victory over the erosion of privacy rights in America.

The Social Security Number: An American I.D.?

The SSN, introduced under the Social Security Act of 1935 and originally intended for use only within that program, has turned into a near-universal I.D. number. It is used for identification purposes, for checking credit histories, and linking databases. Certain government forms require your SSN, such as those of the IRS; and any organization that must report to the IRS, such as banks and employers, must also have your SSN. The problem is that many companies that are not required by law to request your SSN, nonetheless do so. The Privacy Act of 1974 (Pub. L. 93-579, Sec. 7) requires that any government agency requesting your SSN has to tell you whether disclosure is mandatory or optional, what authority they have for requesting your number, how your SSN will be used, and what the consequences are if you fail to give out the
number. There is no comparable requirement for companies requesting your SSN. Since multiple databases are keyed by SSN, each time you use this number, you are providing strangers access to information about yourself that you may not be able to correct or challenge, and that may lead to decisions that can harm you. For example, providing your SSN to insurance companies makes it much easier for them to track down your medical records even though they have no legal mandate for (or against) obtaining your SSN. Since SSNs are not always unique, and can be easily concocted or stolen, and because people rarely ask to see the actual card, the SSN is a poor universal I.D. number, even assuming we would want one. Simply being able to recite nine digits is no guarantee of identity.

As individuals we can take some measures to limit circulation of our SSNs (see Hibbert), but we are unlikely to get rid of the SSN since it is also the database key used by the IRS and other government agencies. The system of SSN usage was not planned out, but rather evolved into the present patchwork of uses and abuses. The SSN could conceivably evolve into an American I.D. number and a personal electronic smartcard that you must carry when you leave home. While increasing the surveillance abilities of law-enforcement officials, having a universal I.D. card would make certain forms of privacy a mere remembrance of our once freer past. Only by legislating how such a smartcard can be used will we be able to gain any measure of protection for our privacy. The best way to protect privacy would be to refuse to issue such cards in the first place. Indeed, if the government tries to make all Americans carry a personal smartcard, we can expect significant popular protest.
number. There is no comparable requirement for companies requesting your SSN. Since multiple databases are keyed by SSN, each time you use this number, you are providing strangers access to information about yourself that you may not be able to correct or challenge, and that may lead to decisions that can harm you. For example, providing your SSN to insurance companies makes it much easier for them to track down your medical records even though they have no legal mandate for (or against) obtaining your SSN. Since SSNs are not always unique, and can be easily concocted or stolen, and because people rarely ask to see the actual card, the SSN is a poor universal I.D. number, even assuming we would want one. Simply being able to recite nine digits is no guarantee of identity.

As individuals we can take some measures to limit circulation of our SSNs (see Hibbert), but we are unlikely to get rid of the SSN since it is also the database key used by the IRS and other government agencies. The system of SSN usage was not planned out, but rather evolved into the present patchwork of uses and abuses. The SSN could conceivably evolve into an American I.D. number and a personal electronic smartcard that you must carry when you leave home. While increasing the surveillance abilities of law-enforcement officials, having a universal I.D. card would make certain forms of privacy a mere remembrance of our once freer past. Only by legislating how such a smartcard can be used will we be able to gain any measure of protection for our privacy. The best way to protect privacy would be to refuse to issue such cards in the first place. Indeed, if the government tries to make all Americans carry a personal smartcard, we can expect significant popular protest.

Authoritarianism’s Threat

The essence of privacy is control over mental and physical self-space. As authoritarian threats to privacy increase, we may see an increase in violent anti-government movements, although these will not succeed in undermining the root of surveillance: technology. More successful responses will include legal and self-protective measures. Authoritarianism will be challenged by the Zimmernans of this world and by better legal protection, but increased surveillance is likely to become an unavoidable part of life. Our unrealistically high expectation of complete privacy will be lowered. We will likely become more wary as information we once thought of as private is increasingly used against us. We may come to regard each e-mail letter as an open letter and may find it necessary to ask our doctor if what we say is indeed confidential. In this sense, by advocating surveillance for the public good, government and business will damage it insofar as there will be a further deterioration of public trust of authority.

If privacy is valued and protected, then adults should be allowed to do, say, and think whatever makes them happy, so long as no one else’s rights are violated in the process. Despite the advances we’ve made, America is still a long way from realizing this culture of openness. And with the recent erosion of the legal basis for the right to privacy, the country is becoming less open at the same time that economic and surveillance powers are becoming more concentrated. So long as authoritarianism continues to grow in America, our privacy rights will continue to decline.
References


McCollum, Bill. Quoted at http://www.aclu.org/congress/gut4th.html by the American Civil Liberties Union.