Policy Analysis
No. 452 September 17, 2002

Human Bar Code
Monitoring Biometric Technologies in a Free Society

by Clyde Wayne Crews Jr.

Executive Summary

Biometric technologies such as voice prints, retina and iris scanners, face-recognition cameras, digitized fingerprints, and even implantable chips containing personal information can benefit us. Such technologies will find their way into cell phones and mobile computers, car doors, doorknobs, and office keys. They can bolster online commerce, locate a missing child, and transmit medical information to doctors. They promise increased security by preventing identity theft.

But no one wants to be treated like a human bar code by the authorities.

What are the benefits and concerns surrounding the further deployment of biometric identification techniques into our lives? Do they promise new levels of physical security and secure commerce—or do they threaten fundamental values of privacy and liberty? What are the distinctions between governmental, commercial, and private use of biometric technologies?

Biometrics range from completely involuntary to potentially involuntary to completely voluntary—in decreasing order of risk. The most pressing threat to liberty is an all-inclusive database mandated by government—a national identification card with biometric identifiers. Such an ID will increase unwelcome surveillance, will blur the distinction between public and private databases, and will undercut a presumptive right to maintain anonymity. The ID would devolve into a general law enforcement tool having nothing to do with response to terrorism.

A less sweeping biometric database would contain criminals and suspects but not the general population. Individuals would be observed, but presumably only to see if they matched a face already in the database.

Allegedly, the collection of information pertaining to criminals will have already taken place by way of proper legal procedures. Nevertheless, many observers doubt that governments can be trusted to discard incidental data collected on innocents. Because the deliberate identification and tracking of individuals using biometrics can constitute an unreasonable search, stringent Fourth Amendment safeguards are critical.

The challenge of the biometric future is to prevent mandatory national IDs, ensure Fourth Amendment protections with respect to public surveillance, and avoid the blurring of public and private databases. Private industry must generate its own information, for purposes limited by consumer choice and consumer rejection. Privacy, security, liberty, and even authentication technology itself will be all the better for it.

Clyde Wayne Crews Jr. is director of technology studies at the Cato Institute.

Do they promise new levels of physical security in the "homeland" and more secure commerce, or do they threaten fundamental values of privacy and even liberty itself?

Introduction

> You can make the country completely safe. All you have to do is make it a police state.
>
> —James Gilmore[1]

Controversy continues in Washington over whether the technology industry should support Internet privacy legislation to deal with unwanted marketing online.

But that debate has been overshadowed by the rise of public surveillance technology and, in particular, biometric technologies. Biometric technologies use individuals' unique physical characteristics for purposes of tracking or authentication. Biometrics gained prominence in 2001 after fans at Super Bowl XXXV were observed by surveillance cameras and their faces compared to a database of criminals' faces using face recognition technology. That event came to be popularly called the "Snooper Bowl."[2] And after the terrorist attacks in New York and Washington, the idea of government-issued national ID cards containing some form of biometric identifying information has been the subject of fierce debate.

Along with the notorious face recognition cameras in use at the Super Bowl, some airports, and numerous city streets and other public places, biometric technologies also include retina or iris scanners, digitized fingerprints and handprints, voice prints, and even implantable rice-sized, radio frequency chips coded with personal information that can be displayed by a scanner. Even the prospect of "brain prints" to identify bad actors is being seriously discussed.[3] Some see widespread deployment of biometric surveillance as a welcome development in a vulnerable America, while others fear it.

What are the benefits and concerns surrounding the further deployment of biometric identification techniques into various facets of American life? Do they promise new levels of physical security in the "homeland" and more secure commerce, or do they threaten fundamental values of privacy and even liberty itself? What are the distinctions between governmental and commercial deployment of biometric technologies, and what policy concerns arise when private companies profit from selling biometric tools to law enforcement or operating the equipment? How are we to devise principles that can help identify proper and improper uses of what has potential to be both one of the most promising and one of the most perilous technologies today?

On the positive side, some emphasize the social benefits of biometrics, such as the crime-fighting potential of cameras on city streets and the terrorist-fighting potential for surveillance in our cities, airports and other installations. And biometric technologies also have significant potential to benefit us as individuals, to protect rather than undercut privacy and security in our day-to-day lives. Better at authentication than the passwords that dominate today, biometrics can facilitate online commerce by helping us securely manage financial records and online transactions.

The technologies will find their way into car doors, doorknobs, and office keys. They'll authenticate use of our cell phones and personal digital assistants and enable verification procedures to access medical information. Implanted microchips have been used to help track pets for years.[4] Over time and with social acceptance, such information-carrying devices will help a parent find a lost child, or even relay information about that same child to doctors. To the extent our descendants embrace the technology, implantation of scannable biometric chips within our bodies may become more accepted and practiced, as has already been done to a limited extent for Alzheimer's patients.[5] As Paul Saffo of the Institute for the Future put it: "The computer has jumped off our desktops and it is insinuating itself into every corner of our lives. Now it's finding its way into our bodies."[6]

Over a much longer time frame, biometrics are expected to help enable ubiquitous com-

puting, or eventual (so the theory goes) seamless interaction between people and machines, so that computers and other machines are aware of our presence and can interact with us. In the even longer run, technologies like face recognition will be the means by which robots can respond and react to us.[7]

But biometric technologies can clearly threaten our liberties as well. Not many want to be tracked by the authorities, or treated like human bar code just because technology has made that easy. Possible applications of biometric technologies range from an involuntary "everybody included" database—exemplified by the calls today for a government-required national ID card—to privately owned and managed "members only" biometric systems that contain data only on individuals who have garnered clearance for a particular private application. Political liberty is threatened by involuntary, government-mandated databases but not by private applications as long as government and private data are kept separate. Policymakers must recognize the relevant distinctions to make rational policy decisions with respect to the inevitable public and private use of biometric identification systems in the years to come.

Government vs. Private Databases and Their Risks to Liberty

In private hands, biometric technologies enlarge our horizons. They expand the possibilities of a market economy by bolstering security in private transactions ranging from face-to-face authentication to long-distance commerce. Some, however, regard the rise of private use of biometrics as an invasion of privacy. And, indeed, there is a danger of law enforcement gaining inappropriate or even routine access to private databases like bank, financial, medical, and travel records.[8] In a voluntary market economy, however—one not characterized by government intrusions on privately generated personal information—biometrics can increase individual liberty.

Government interference with the evolution of biometrics or, worse, domination of the technology, changes the picture dramatically. Governments can use the technology to restrain us and violate our liberty and privacy, a power the market lacks unless the lines get blurred inappropriately. Governmental mandates that require individuals to submit to inclusion in databases can give the entire biometrics industry a black eye and turn society against the technology, sacrificing the promises that biometrics offers. Information acquired through the commercial process must be kept separate from that extracted through government mandates. (Similarly, private companies should not have access to information that government has forced individuals to relinquish.) As the debate over biometrics proceeds, a clear distinction must be made between *commercial* privacy and *official* privacy; privacy in a civil or social setting is different from *political* privacy. As Ayn Rand remarked: "Civilization is the progress toward a society of privacy. The savage's whole existence is public, ruled by the laws of his tribe. Civilization is the process of setting man free from men."[9]

Technology has the potential to bolster privacy and even anonymity, but to do so, the deployment of technology must remain a private-sector phenomenon, free to benefit from market improvements. The best, most secure IDs will be those whose applications are driven by consumer demand and interactions among individuals and businesses rather than implemented by government fiat. To the extent that private companies encourage the blurring between governmental and market databases, they ensure the industry's regulation and politicization.

Technology writer Rob Fixmer has noted the distinction between government IDs and commercial ones:

> A commercial digital ID might be a great convenience in many ways. A combination license, passport, Social Security number, credit card, debit card and door key—an entire, bulging

Government mandates that require individuals to submit to inclusion in databases can give the entire biometrics industry a black eye.

wallet on a single piece of data-impregnated plastic. But in Western democracies, where George Orwell's 1984 is taught with apocalyptic zeal, the notion of an all-knowing government is terrifying. In a world committed to never forgetting victims of Nazi concentration camps, the grotesque image of numbers tattooed on human beings has forever equated forced identification with sheer evil.

I doubt those views changed on September 11. Let the private sector identify us in ways that expand our options as consumers, while protecting our assets. Give law enforcement agencies access to those identities on a strictly controlled basis.[10]

There will inevitably be some blending of public and private purposes. It is certainly the case that tax dollars will be saved by having private industry with specialized expertise develop the technologies that the government uses for its purposes, just as the Defense Department benefits from contracting with private companies to build weapons. To keep government-mandated and market-developed databases separate over the coming years, one principle might be that private companies not be permitted to access data that is collected by government mandate. Otherwise the biometrics industry will be one defined by government regulation rather than market demand.

Private companies might not be permitted to access data that is collected by government mandate.

With that bit of distinction between the appropriateness of government-mandated and private databases, it is apparent that the deployment of biometrics technologies poses a range of threats against which citizens must stand guard.

High Risk: Government-Mandated Database of All Citizens

> We don't automatically have to call it a national ID card, that's a radioactive term.
>
> —Rep. Jane Harman (D-Calif.)[11]

The most pressing threat to privacy and individual liberty is an all-inclusive involuntary database—one mandated by government in which everyone is forced to participate.

This kind of database corresponds to proposed national ID card systems with biometric identifiers. The identifiers would likely take the form of mathematical representations of one's face, iris, fingerprints, and so forth, encoded into a magnetic strip or chip.

Oracle Corporation CEO Larry Ellison, a prominent early promoter of the idea after September 11, offered free software to help establish and maintain integrated governmental ID databases. (Ellison claims it's not such a leap since the government already maintains extensive databases on all of us.)[12] Such proposals were initially rejected by the Bush administration but received wide consideration by some members of Congress; and more recently Homeland Security Advisor Tom Ridge indicated that the administration is investigating linking nationwide driver's license databases.[13] That move comes on the heels of Congress having already asked the Department of Transportation to investigate the idea of linking state driver's license databases.[14] The leading institutional backer of the idea is the American Association of Motor Vehicle Administrators, which recommended streamlining driver's license data across the states and even seeks $100 million from Congress to help foot the bill.[15] (Yet even in the face of government funding the AAMVA denies that the proposal would lead to a national ID.)

Other supporters of national IDs include Sen. Dianne Feinstein (D-Calif.) and Rep. Nancy L. Johnson (R-Conn.). The leading legislative vehicle appears to be a bipartisan bill (H.R. 4633) introduced by Virginia Reps. James Moran (D) and Tom Davis (R). Their bill would establish driver's license and ID standards that incorporate biometrics and require "standards to ensure interoperability and the ability to store multiple applications created by government agencies and private entities."[16] Yet, "this is not a national data file,"

says Moran.[17] Note the blending of public and private purposes.

No Such Thing as a "Voluntary" National ID Card

Most proponents claim that a national ID system could be voluntary. But it doesn't seem possible to sustain a voluntary system given the incentives that would be brought to bear: terrorists would not volunteer to sign up, as Cato Institute constitutional studies scholar Robert A. Levy argued, and the "predictable failure of a voluntary system will lead to compulsory IDs."[18] And even a "voluntary" ID would contain underlying compulsory elements: part of the driver's license push by the AAMVA is to link Immigration and Naturalization Service data as well as Social Security and Bureau of Vital Statistics data.[19] That in itself exposes the critical problem with government-mandated IDs: by incorporating information collected across agencies, the AAMVA's proposed ID starts off as being fundamentally compulsory since it would ride atop already-administered mandatory databases.

The motive behind the recent interest in a national ID is apparent, even understandable: backers claim that such a system might have thwarted the attacks of September 11. Moran and Davis hail from the very state in which some of the terrorists had received phony driver's licenses and likely feel a compelling need to respond. Others note that the attacks might have been thwarted if certain participants, who were stopped for traffic violations prior to September 11, had been forced to produce some kind of a national, biometric ID.[20]

Of course, it is not necessarily the case that more surveillance and tracking of ordinary citizens would improve security. It is not apparent that had the USA PATRIOT Act[21] been in place the attacks would have been averted.[22] Likewise, it is not apparent that a national ID card could have averted them. Rather, still-unresolved intelligence failures seem to have been the real problem. Revelations poured forth since the attacks: advance knowledge about Middle Eastern noncitizens receiving training at U.S. flight schools;[23] extraordinarily lax personnel background checks at airports; intelligence about proposed attacks-by-airliner not being taken seriously by FBI headquarters; and poor awareness of the whereabouts and status of noncitizens, embarrassingly demonstrated when new Visa applications from the Immigration and Naturalization Service arrived for terrorists six months to the day after their deeds. Also criticized had been a lack of adequate communication between domestic law enforcement and foreign intelligence agencies, a fault that lies with Congress since the split of duties between the FBI and CIA is legislatively mandated.[24] These are the sorts of matters that need attention before sacrificing liberties. With respect to terrorism, government massively failed at its core mission—protecting citizens.[25] Yet its response has been to demand that citizens give up ever more of their freedom in the name of security.

Moreover, as Timothy Lynch of the Cato Institute has argued, "The terrorists will very easily be able to get around a national ID card system. They can bribe people who issue the cards, they can bribe people who check the cards, and . . . recruit young men in their early 20s . . . who have not yet come to the attention of our law enforcement and intelligence agencies."[26]

Nonetheless, Rep. Jane Harman (D-Calif.) has claimed that public objections to a national ID card will vanish if there's a second wave of attacks.[27] She's probably right: a poll by the University of Michigan's Institute for Social Research found that 7 in 10 Americans would give up some civil liberties for improved security.[28] However, this is where principled political leadership is called for: If liberty is a Constitutional right, the power of the majority is limited, and majorities—especially temporary majorities—shouldn't be authorized to take away the legitimate right of innocent individuals to be free of invasive government ID systems.

"Show Us Your Papers"

Many critics of national IDs, such as Marc

Even a "voluntary" ID would contain underlying compulsory elements.

Rotenberg of the Electronic Privacy Information Center, have noted that mandatory IDs would lead to many new checkpoints in society that simply don't exist now.[29] Everyone would be included in a database thanks to a government mandate and would eventually be trackable anywhere. That capability would lead even private entities to ask for ID everywhere: at the Cineplex, the concert, the stadium, Disneyland, and so on.

Governmental abuse is most worrisome. Columnist William Safire called the national ID a "discredit" card:

> The universal use and likely abuse of the national ID—a discredit card—will trigger questions like: When did you begin subscribing to these publications and why were you visiting that spicy or seditious Web site? Why are you afraid to show us your papers on demand? Why are you paying cash? What do you have to hide? . . . Beware: It is not just an efficient little card to speed you through lines faster or to buy you sure-fire protection from suicide bombers. A national ID card would be a ticket to the loss of much of your personal freedom. Its size could then be reduced for implantation under the skin in the back of your neck.[30]

Given an all-encompassing database and easily scannable cards or implants, it will no longer be "show us your papers": one's vital statistics will be readily observable by the authorities.

Such implantation is the ultimate expression of the "big brother" scenario that scares so many. And given an all-encompassing database and easily scannable cards or implants, it will no longer be "show us your papers": one's vital statistics will be readily observable by the authorities.

The Progressive Policy Institute downplays such fears, noting that smart cards can make it easier to catch abusers of the card, that they will "make it easier to create a digital paper trail on government employees who access your data."[31] (In that case, however, a better alternative may be to focus surveillance on government employees, particularly since intelligence failures by such employees seem to have missed the signs leading to September 11.)

Given bureaucratic mission creep, official applications of a national ID card would likely expand to cover such things as underage drinking, petty crime, fighting the drug war, tracking deadbeat dads and welfare cheats, registering guns, and so forth. The ID would morph into a general law enforcement tool having nothing to do with the terrorism that presumably prompted its creation. (For example, where face recognition systems are widely deployed in the U.K., low-level criminals rather than terrorists are the main target.[32]) In a 1995 Cato Institute study, the authors described how a national ID system would impinge on privacy, having been invoked as a tool to monitor illegal immigration, manage a national health care program, and execute background checks.[33] Uses can go well beyond any national security justification, but pressures created by an official ID card would likely prove irresistible.

Unfortunately, the proposed House legislation (H.R. 4633) on driver's license modernization puts to rest any notion that the cards would be limited in scope and confined to narrowly prescribed governmental interests. The bill requires that chips be capable of storing not just fingerprints but other data like medical information and credit card numbers.[34] The impulse for private sector businesses to piggyback on such an ID would be irresistible, much like the widespread use of the Social Security number by private entities. If Social Security had never existed (or perhaps if it were to become fully privatized and optional), no government-generated numbers would exist for the private sector to exploit. That fact should be remembered with respect to integrated national databases. Rather than allow the private sector access to new (coercively extracted) data on individuals, policymakers should move in the opposite direction. The private sector would have to come up with its own alternatives anyway if reformers succeeded in privatizing Social Security. (Indeed, perhaps even prospectively restricting private sector use of the Social Security number in favor

of prodding the private sector to develop its own alternatives makes sense, but that's a battle for another day.)

An Unnecessary Loss of Anonymity

As the government's surveillance of citizens is made easier, the effect on political speech and anonymity can become oppressive and stunting. The Electronic Frontier Foundation's Lee Tien argues that "perfect surveillance, even without deliberate abuse, tends to chill political, artistic, and scientific activity."[35] Maintaining citizens' protections against unreasonable monitoring is crucial in a free society for political purposes; Undermining anonymity can discourage legitimate civil disobedience. As Robert Levy noted in a response to a claim by Alan Dershowitz that no citizens' right to be anonymous is "hinted at in the Constitution":

> That turns the Constitution on its head. The Ninth Amendment tells us we have an untold number of rights that are not enumerated in the Constitution. The question is not whether we have a right to anonymity, but whether government has the power to take it away. . . . To be sure, the right to anonymity is not absolute. But before stampeding toward a national ID, we should listen to Justice William O. Douglas, who cautioned a half-century ago: "To be let alone is indeed the beginning of all freedom."[36]

While there is no guaranteed "right" to anonymity in one's public actions, private property rights are the means by which people have the ability to protect their anonymity. Citizens have the right to legitimate, peaceful civil disobedience and communication using their own property and resources. Anonymity and pseudononymity are "cornerstones of free speech," as noted by attorney Jonathan Wallace: "The Supreme Court has consistently held that anonymous and pseudonymous speech is protected by the First Amendment. In [a] recent statement . . . the Court invalidated an Ohio ordinance requiring the authors of campaign leaflets to identify themselves."[37] In 2002, the Court struck down an ordinance requiring Jehovah's Witnesses and other door-to-door canvassers to carry written identification permits.[38] Proliferation of forced identification facilitated by a government mandated ID systems undermines the means of self-maintained privacy, and even of one's option of "starting over" in life. Short of engaging in fraud or harming others, an individual's presenting various faces to the world in different contexts is legitimate.

While people will gladly give up information about themselves in exchange for services in the marketplace, those very markets, albeit not perfect ones, are the mechanisms that sustain the possibility of retracting that information or modifying it in the course of social give and take. Entrepreneurs, such as those engaged in the business of facilitating online commerce, have been struggling for years to enhance privacy assurances for individuals. Washington presumably supports such efforts in principle; legislators have introduced a number of bills to allegedly protect online privacy.[39] Particularly in an era in which the Internet can facilitate anonymous speech, and in which businesses are developing tools whereby individuals can shop anonymously, a national ID would represent a bizarre rejection by the government of its own alleged commitment to privacy.

The legitimate role of a government in a free society is properly limited to those functions necessary to protect rights. Governments must be monitored by citizens rather than the other way around. (That of course is the meaning of the famous phrase, "Eternal vigilance is the price of liberty.") If government is bloated and engaging in functions that are outside its proper role and amassing data on citizens besides, it has plainly overstepped its bounds. But if it does these things while bolstered by a national ID, which inevitably retards political opposition to governmental power, it becomes much more difficult for non-anonymous (and perhaps fear-

As government surveillance of citizens is made easier, the effect on political speech and anonymity can become oppressive and stunting.

The detrimental impact of a national ID on individual liberty will blur public and private databases, faciliate unwelcome surveillance, and undercut a presumptive right to anonymity.

ful) citizens to rein in that very government and restore it to its proper function. (This, by the way, is the risk of the "e-Government" movement, the purpose of which is to facilitate sharing of information across agencies. If government is swollen beyond its constitutional limits, then the sharing of information about citizens is not appropriate. Government should not be "efficient" at roles that it should not be performing in the first place.)

ID cards are the mark of an overgrown, aspiring, government, not a limited one. The case for systematically tracking the populace has yet to be made. A proper, limited government should have no means of assembling a national, integrated database on innocent citizens.

A national ID's detrimental impact on individual liberty is apparent. To recap: it is involuntary, it will blur public and private databases. facilitate increased unwelcome surveillance, and undercut a presumptive right to anonymity. But a national ID poses another, albeit more practical, problem as well: it dampens critical competitive market forces that would otherwise drive improvements in authentication technology.

Many "National" IDs Are Needed—But Not a Government-Mandated One

Aside from the national ID's involuntary character and its incompatibility with personal and political liberty, the potential uses of ID technologies are too divergent to seriously entertain the idea of a single national, government-sanctioned ID. Few individuals want all parties, governmental or not, to have access to all the information that exists about themselves in a central location, as a national ID card would facilitate and encourage. Having numerous IDs, rather than a single one, can be perfectly appropriate in civil society (recall that individuals may present different faces to the world in different contexts). Moreover, the requirements of commercial and social society differ from the limited needs of official civic and political identification. As noted, a national ID would inappropriately blur the two, just as the Social Security number is often used for private identification purposes even though it isn't supposed to be. Like the Social Security card, the national ID would become a de-facto ID not just for governmental purposes but for private ones as well.

Often IDs won't need to be "national," but rather localized for particular applications. We typically want our IDs to contain only that information we choose to release for limited purposes, and a mandatory national ID would diminish that control. An ID that functions as an office key, for example, may not need to be part of a database containing bank records, medical records, Social Security payment history, or one's last will and testament. Then again, in the course of things, consolidating certain categories of information may be perfectly appropriate. The point is we don't know ahead of time, and requiring a premature consolidation or creating a government ID that makes the pooling irresistible is unwarranted. Moreover, while ID proponents hold that there would supposedly be "multilevel access so that only the right people get access to the right information," author Simson Garfinkel notes a "checkered track record" in Europe where hacking widely used "smart cards" for free phone calls or satellite TV "is a cottage industry."[40]

Boosters of a national ID argue that the ID will prevent identity theft and protect public safety. But national ID cards aren't necessary to secure those values; indeed they can undermine those goals. There appears to be a demand for multiple systems of authentication, depending upon circumstances, and commerce does seem to have room for many IDs whose purposes do not necessarily overlap. Combining them all—or prodding such a combination—into any sort of national database would be detrimental to individual rights, privacy and security.

For example, a private, nonmandatory ID, such as Microsoft's Passport verification system, might become widely accepted online and even national or international in scope. In that sense, Passport might very well eventually qualify as a "national" ID. But that doesn't create an argument for turning such technologies into an official national identification sys-

tem through government prodding. Sun Microsystems's Chris Bergh (who is chief technology officer at marketing automation company MarketSoft as well as a patent holder on the technology foundation of Passport) notes with regard to winners in the marketplace: "There won't be just one identity service. There will be hundreds if not thousands of identity services."[41] He continues:

> Identity is bigger than any one company. Likewise, a person is bigger than any one identity. As MIT professor Sherry Turkle said in Life on the Screen: Identity in the Age of the Internet, individuals will have multiple personae on the Internet—one for work, one for online shopping, one for banking and more for their personal interests. All of these "masks" will be founded in one true, master identity, which will live everywhere, and in several transparent services. Every identity will point to the same credit card, if you like, or every identity will point to a different one. Likewise with billing address and shipping destination.[42]

It may be that IDs that are national in scope will emerge. However, the "multiple ID" approach appears to be the verdict of the marketplace so far. The most prominent illustration of this is the fate of Microsoft's "Hailstorm" services. Introduced with much fanfare in March 2001 with the intention of harmonizing individuals' information across the Web and making it accessible via various kinds of hardware devices, the system ran into opposition. The opposition came, however, not just from privacy advocates, which has certainly been the case, but from potential partners who are reluctant to yield control to Microsoft over consumer information that they might wish to govern themselves for either strategic reasons or out of concern over security.[43] Such is the nature of the security and identification business. No one is ready to relinquish all control, and no one knows yet what's going to best satisfy wary consumers.

Medium Risk: Governmental "Bad Guy" Databases

Another kind of biometric database, a partial one containing data on criminals, suspects, and other "wanted" individuals, isn't as sweeping as the kind of database that would underlie a national ID card. Such databases would correspond to those underlying the face-recognition cameras used during Super Bowl XXXV. Used for surveillance in public areas, faces are scanned, and features converted to a mathematical representation, presumably only to see if there is a match with someone already in the database.

One criticism of face recognition technology is its failure rate, as the ability to recognize faces on the basis of archived images appears to diminish as time passes despite claims that the facial map remains largely fixed.[44] Yet the accuracy of the technology is really a side issue: eventually it likely will be quite reliable. As the technology improves, supporters argue, bad actors can be identified at the theater or sporting event without disturbing anyone else.

If we start with the assumption—and granted, it is an assumption; it requires taking law enforcement at its word—that the incidental images of innocent individuals are not recorded or are otherwise immediately discarded, face camera surveillance may not count as surveillance of ordinary citizens in the manner critics fear. In other words, the information collection—that pertaining to criminals—has already taken place, presumably under appropriate legal procedures. Alternatively, cameras can actively look for lawbreakers, such as scofflaws engaged in misdeeds, such as painting graffiti.[45] Or they can monitor public events such as rallies and protests, as well as public places such as subway stations.[46] Properly conducted there is no privacy impact on the general population. But concern over whether governments can be trusted to discard incidental data collected on innocents is valid.

A related worry is that private industry can profit handsomely from the exercise of improp-

It may be that IDs that are national in scope will emerge. However, the "multiple ID" approach appears to be the verdict of the marketplace so far.

er surveillance against citizens, an inappropriate state of affairs in a free society. The extent to which private firms profit from and even lobby for this kind of expenditure is a concern; this is where private profit-making is at risk of crossing over into a law enforcement role. In that regard the debate over face recognition systems mirrors that over red-light cameras. In late 2001 in San Diego, a judge threw out nearly 300 tickets issued to motorists because of the contingency fee of $70 per traffic ticket paid to the private vendor of the equipment, Lockheed Martin IMS.[47] The more tickets issued, the more profit for Lockheed.

But properly restrained, public surveillance technology, when used for a "bad guy" database, is not about surveillance of ordinary citizens since the data collection will have already been done. In fact, cameras might even cut down on unwanted searches. If the cameras are doing their job and we assume a setting where police inspection is legitimate (for example, if cameras are merely substituting for uniformed officers on the beat), there may be less need for the random, invasive searches with which we are more familiar. As John D. Woodward Jr. of RAND noted with respect cameras deployed at Super Bowl XXXV, "Face recognition helped to protect the privacy of individuals, who otherwise might have to endure more individualized police attention."[48] Likewise, UCLA law professor Eugene Volokh noted, "At least in some situations, camera systems can promote both security and liberty."[49]

The risk of face camera surveillance is that authorities will use the cameras to learn about particular subjects, thereby violating Fourth Amendment rights.

What Constitutes an Illegitimate Search?

The risks associated with camera surveillance technology differ from those associated with ID cards. ID cards make us relinquish our anonymity. By substituting a government standard for market-based identity technologies, ID cards interfere with the evolution of the very authentication technology of which they are an example. Face camera surveillance, on the other hand, doesn't have the same immediate impact on anonymity since nothing is known about anyone observed (except the "bad guys"). Instead, the risk is that authorities will use the cameras to begin learning about particular subjects, thereby violating Fourth Amendment rights by initiating unwarranted searches or observation of innocent individuals.

Clearly, face recognition technology, like other kinds of camera surveillance technology, makes it easy to begin tracking someone by creating a record for them, with or without their knowledge. It would be easy to begin recording someone's comings and goings with such technologies as traffic light cameras, tollbooth monitors, or face recognition technologies in public spaces. To assemble a diary of someone's movements, one need only save the daily records from a monitoring device and cross-reference them with similar equipment in other locations. (Likewise, biometric chips or ID cards armed with global positioning capability could be used to track individuals). The average Briton is photographed by 300 surveillance cameras a day.[50] In Washington, D.C., the police force has launched the Joint Operation Command Center, comprising 40 screens monitored by 50 officers.[51] Many citizens are understandably bothered and consider the cameras a privacy invasion. Critics also note that "People behave in self-conscious ways under the cameras, ostentatiously trying to demonstrate their innocence or bristling at the implication of guilt," like a group of teens who gave "the finger" to the camera pivoting to follow them,[52] or protestors who wear masks in defiance of cameras.[53]

These are legitimate concerns, but there is no real expectation of privacy in a constitutional sense in open, public areas. Most important is that no records are kept, and no databases created in the normal course of operations. Moreover, as noted, cameras might decrease more invasive physical searches of individuals and other forms of abuse. As Eugene Volokh notes, the camera is more impartial and creates none of the "demeaning pressure" one feels to be "especially submissive" in a search or pullover by a police officer, and there is no wondering whether one is stopped on the basis of "sex or race or age."[54] Nonetheless, critics of camera surveillance systems do have valid fears; thus such systems need to be overloaded with

checks and balances. One important check on abuse would be if citizens had access to the records generated, or if the records were otherwise audited.[55] Others safeguards will need to be developed as well.

With respect to public surveillance, Fourth Amendment protections must be made more clear, for this is an instance in which law has not caught up to technology. James Harper, a lawyer and consultant who operates Privacilla.org, a web clearinghouse on information about privacy issues, summed up in congressional testimony the conditions required to fulfill Fourth Amendment guarantees: "The Fourth Amendment requires a search to be based on probable cause. That is, government investigators must have a reasonable belief that a crime has been committed and that evidence or fruits of the crime can be found. The first question a court will ask when a citizen claims to have been unconstitutionally searched is whether that person had a reasonable expectation of privacy in the place, papers, or information that government agents have examined or taken."[56]

Although there is no general expectation of privacy in public places, neither is there an expectation that one will be purposefully identified and one's movements mapped daily by the authorities. No one simply going about their business should be added to a governmental enforcement database or made the subject of intense daily observation without probable cause and without a court order. In other words, at some point, tracking of an individual without a court order must surely cross over into the territory of an unreasonable search.

Harper noted that the traditional interpretation of the Fourth Amendment as protecting places—our homes—evolved with the 1967 *Katz v. United States* decision,[57] in which a telephone booth had been bugged. In that case, the warrantless eavesdropping was found to have violated Fourth Amendment rights because:

> The Fourth Amendment protects people, not places. What a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection . . . But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.[58]

That the Fourth Amendment protects people and not places must be a defining constraint with respect to the increasing use of biometric surveillance technology by the government. Unfortunately, what will count as a search in the future—given the ease of very intimate, up-close surveillance—remains to be determined. For example, with respect to the government's use of technology to observe an individual's home (in this case, thermal imaging), the recent *Kyllo*[59] decision seems favorable to privacy rights at first glance. The Court found that "obtaining information regarding the interior of the home that could not otherwise have been obtained without physical intrusion into a protected area constitutes a search—at least where (as here) the technology in question is not in general public use." As Cato Institute director of constitutional studies Roger Pilon noted with respect to that case, "the use of a high-tech device does not render what we all know to be a search to be a non-search."[60]

But as pointed out in a recent article by Mark Milone in *Business Lawyer*, Judge Steven's dissent in *Kyllo* points out that, given the Court's interpretation, Fourth Amendment protection seems to erode as soon as the technology attains "general public use."[61] Under *Kyllo*, it appears that once a technology capable of invading privacy is widely used in society, government will also be free to use it. Therefore the unresolved question now, despite both *Katz* and *Kyllo*, is what applications of biometrics against individuals—*wherever they may be*—will count as a search, given that the technologies are so easy to deploy and use. The pressing issue now is the likely erosion in constitutional privacy protection as biometric (and other potential privacy invading) technologies are used not just to observe a home but to track an individual beyond the home. One way or another, govern-

Although there is no general expectation of privacy in public places, neither is there an expectation that one will be purposefully identified and one's movements mapped daily by the authorities.

ments must acquire clearances equivalent to those that they must secure in the non-digital world. Thus, the key focus of the privacy debate over the coming years will likely be the attempt to determine where the line is crossed with respect to everyday biometric surveillance by the government, once the surveillance involves more than one data point concerning an identified individual.

The key focus of the privacy debate will likely be the attempt to determine where the line is crossed with respect to everyday biometric surveillance by the government.

The Risk of Nuisance Law Enforcement

Another related risk with public surveillance technology—given that it is invoked now to thwart major incidents such as a terrorist attack, is that use of the technology will be expanded to target victimless crimes, like adult drug use. There is also the problem of nuisance law enforcement. Such mission creep will be irresistible to politicians and local police forces. For example, with respect to the red-light cameras, much in the news recently, localities can be tempted to lower speed limits to artificially create violators and criminals. Similarly, Rep. Richard Armey (R-Tex.) noted that yellow-light intervals at intersections have been shortened, corresponding to a rise in red-light scofflaws.[62]

One bright spot in the digital revolution, given the potential loss of Fourth Amendment protections, is that surveillance technologies are cheap, not just for governments, but for individuals as well. As technologies improve and prices decline, they become more widely available to the general public. This means that individuals can turn the electronic eyes right back on the government, exposing abuses of individual rights. The X-10 mini-cam, whose pop-up ads so annoy us on the Internet, sells for about $80. Cheaper digital cameras cost around $20. From relatively low-tech, "stick-it-to-the-man" offerings like the Speed Trap Exchange[63] on the Internet; to the Electronic Privacy Information Center's Observing Surveillance project, which documents Washington, D.C.'s, camera networks;[64] to the Witness project, which documents human rights abuses worldwide,[65] surveillance can be turned back on oppressive or misguided governments.

Lower Risk: Private Members-Only Databases

Another use of biometrics is voluntary databases for particular applications. In such databases, individuals are identified by such means as retina scans and fingerprints, and matched with their previously created record in the database. Such privately owned and managed databases, often developed for purposes of security, tend to be partial databases of "members." (Secure government installations, of course, might appropriately use such systems as well; that is a different matter from governments' directing the technology at ordinary citizens.) Unlike databases of criminals, to which everyone must demonstrate they do *not* belong, these are databases of members, wherein one must show one *does* belong. As far as security is concerned, the benefits of a members-only database can exceed those of the inclusive and involuntary government-driven databases. The manager of the private database is saying, in effect, "You may enter my privately owned building, airplane, parking garage, neighborhood, house, and so forth, but *only if I know who you are.*"

Members-only databases are common and exist where security clearances are needed for entry to sensitive areas: factories, laboratories, secure campuses, and office parks, for example. This kind of system evolves naturally and voluntarily. Its hard to get much more secure than knowing precisely those with whom one interacts. Computer scientist Dorothy Denning points to how such technologies are more secure than password-type security clearances since they aren't dependent upon secrecy for an assortment of applications—rather, they depend upon "liveness."[66] These technologies can make it hard for malicious individuals to impersonate another person.

Along with advanced applications, biometrics such as iris scanners and fingerprint scanners are commercially available. For example, keyboards enabled by fingerprint-scanners sell for under $200,[67] and biometrically enabled mice, which also read fingerprints, are even cheaper, but so far glitches prevent them from being a suitable replacement for passwords.[68]

They can even assure that only the appropriate, living, breathing, certified pilot commands an aircraft.

Private identity systems managed and protected by answerable firms—systems in which owners reserve the right to refuse to admit anyone not a member—may be preferable in numerous cases. Owners may have no interest in matching faces against a database of terrorists, preferring instead to know who you are, rather than that you're not on a list of criminals (although, of course, digital "most wanted" lists are surely imminent in the biometric age). In the Washington, D.C., area, a private "country club" airline service has emerged, in which members agree to a background check, then are scanned when they arrive for a flight.[69] The company prefers to have a database of *customers* who agree with the goal of security and are willing to undergo prior security checks, and who want everyone else on the flight to have undergone the same. The operators, as well as the passengers who elect to use the airline, want to know exactly who is flying with them.

Even at typical airports (despite the federal takeover of airport security), related biometric options have the potential to eliminate much of the new airport check-in nightmare. Some frequent fliers who use special hand-scan IDs are being swept past other passengers waiting in the long security lines. For example, Delta and American Airlines offer such faster processing for premium passengers.[70] Security and comfort come from knowing who the other person is. Although such systems may be disparaged on egalitarian grounds, the holder will have in fact undergone intense background checks, and they may pay considerably more.

Because the need for authentication is so prevalent in so many lines of business, the marketplace is driving the biometrics industry. Not only is the marketplace capable of respecting the rights of individuals *not* to be part of an official government database, markets can offer significant advantages with respect to security, owing to the considerable amount of research and development taking place. Businesses will have to determine, though, what level of surveillance is consistent with customer preferences, as well as employee contentment and morale, and perceptions of fairness.

There is no question that the workplace is increasingly being transformed by biometrics; e-mail and keystrokes have long been easily monitored. Biometrics like retina scanners and voice monitors are on the scene and raise new questions of appropriateness as whereabouts and performance can be more easily ascertained. Motives for monitoring at work have long included tracking productivity and monitoring work flow (such as calls with clients and tracking company vehicles); preventing theft and corporate spying; guarding against liability for what employees do on the job (such as preventing harassment); responsibility for employee health and safety; preventing illegal or pirated software; and preventing personal use of company property. Security rationales since September 11 bolster the case for surveillance for many employers. Notable also is that workplaces have themselves changed because of information technology. As more work is outsourced to telecommuters, observation, perhaps even with biometrics, can replace traditional supervisory relationships.

Workplace use of surveillance technology, whether biometric-based or not, is legitimate. It isn't government's job to interfere with such private arrangements; on the other hand, the techniques must be seen as fair and justified by workers. Already some prize employees negotiate freedom from surveillance as part of benefit and employment packages.[71] Some workplace uses of surveillance technology will come to be regarded as appropriate, whereas others will not. For example, judges at the U.S. Court of Appeals for the Ninth Circuit protested the system set up to monitor usage of their computers by the Administrative Office of the Courts, a Washington bureaucracy.[72] The judges ordered the information technology staff to disconnect the equipment. Selective surveillance may be seen as a class issue, so issues of

Businesses will have to determine what level of surveillance is consistent with customer preferences, employee contentment and morale, and perceptions of fairness.

Fundamentally, biometrics is about increasing convenience and service rather than invading privacy.

fairness matter. As Eric Rolf Greenberg, a director at the American Management Association put it, "if, in the 1950s, the image was of a huge room with all the desks pointing in the same direction and a supervisor walking upon and down the aisles, what we are seeing now is the electronic and biological evolution of that."[73] People have alternatives to that now, and companies have market incentives to use their collective head and proclaim what kinds of surveillance they'll disavow and what lines will not be crossed. For example, companies might make clear a policy of not monitoring web-surfing, or of not sharing data with other organizations or, if they do, making the policy clear.

Clearly the encroachment of biometrics into society, even when not injected by government fiat, will raise important social issues. But fundamentally, biometrics is about increasing convenience and service rather than invading privacy. Since people have alternatives to dealing with business and employers that snoop too much, companies will be induced not to look for things they don't need to know and to provide assurances of privacy. For example, GPS or other tracking of company vehicles might make sense (as in the case of the German trucking company that sought face-recognition technology to thwart hijackings).[74] On the other hand, monitoring trips to the toilet or coffee pot likely does not. Likewise, it seems insulting and misguided for employers to use sensor and smart-badge equipped "Hygiene Guard"[75] to determine if employees have washed their hands. Similar restraint on the part of companies is in order with respect to observing and sharing information about customers; lessons can be learned from mistakes made by Internet firms as well as from successes by firms who make it a priority to safeguard individuals privacy (and even anonymity).

Interestingly, however, the marketplace enters the biometric age with individuals seemingly more accepting of modern surveillance technology than is commonly acknowledged. Individuals already use such tools as "nannyware" and "adulteryware" to find out what their kids and spouses, respectively, are up to online. Tracking of patrons in Las Vegas casinos is a given. Yearly pass-holders at Disney World's Magic Mountain can attain clearance by fingerprint.[76] Visa International is exploring biometrics to combat credit card fraud,[77] and ATMs that recognize faces are imminent.[78] At a Kroger grocery in Texas, a test project allows shoppers to leave purses, wallets and IDs at home and pay with a fingerprint (a step on the way to Electronic Product Code technology to allow the checking out of an entire basket of groceries at once).[79] Implanted chips can make medical information from pacemakers, artificial joints, and pumps more readily available to medical professionals.[80] When used in cell phones and personal digital assistants ("Palm Pilots"), biometric identification chips will better enable digital signatures and mobile commerce.[81]

People, especially the young, will likely very easily adapt to tomorrow's cashless, keyless, walletless society. *Cyborg Citizen* author Chris Hables Gray told the *Los Angeles Times* that "I'd be shocked if within 10 years you couldn't get a chip implanted that would unlock your house, start your car, and give you money."[82] It's not hard to envision the convergence of the young people of today who think nothing of multiple body piercings with the mobile-computer wearing "not-quite-cyborgs" of MIT and Xybernaut Corporation. They and their progeny will undoubtedly have fewer qualms about merging man and machine than many do today. Paul Saffo of the Institute for the Future noted, "As some people wring their hands about the invasion of privacy and civil liberty, a whole other generation is going to go, 'Cool! I've always wanted to embed technology in my body.' It's going to be fashion. One sure sign that teenagers will love it is if it terrifies their parents."[83] It won't terrify all parents, of course: for proof, there is already a family in Florida with implanted biometric chips.[84] (However, given that they require injection via a pinky-sized "needle," implanted chips haven't arrived as a mainstream technology just yet.)

With chips being embedded in devices of all sorts (including bodies), as well as such developments as the growth of wireless online access nodes, biometrics is really just a subcategory of tomorrow's vast range of information technologies. As one writer put it, "Look out a few more years and nano-cameras as small as grains of sand will create a world in which the wind has eyes."[85]

Concerns understandably abound, exemplified once again by Marc Rotenberg of the Electronic Privacy Information Center, who asks, concerning of implantable chips, "Who gets to decide who gets chipped?" and seems to regard even family uses of the technology as akin to "putting a leash on a pet."[86] But families, of course, have the right to make such decisions over guardianship themselves. It's difficult to argue that using the technology for disabled parents or for children is a violation of liberty. And, of course, where technologies go too far or are seen as unjust, public outcries can result in their removal, as happened with anti-shoplifting, face-recognition surveillance cameras in Borders Books in London.[87]

However, one risk does deserve special attention, and it has been noted above with respect to governmental surveillance. The boundary between public and private databases can become unacceptably blurred. Deirdre Mulligan of the Samuelson Law, Technology and Public Policy Clinic at the University of California at Berkeley's law school has warned, "The wall between the government and private sector is increasingly porous."[88] With regard to biometrics, one solution to the blurring of public and private databases is to forbid the use by the private sector of government-mandated biometric database information. In other words, commerce mustn't be allowed to rely on government-mandated information—as has occurred with the Social Security card; rather, the private sector must generate its own information, for purposes limited by the market's twin engine of consumer choice and consumer *rejection*. Of course, governmental access to private data gained through the use of biometrics can be obtained by subpoena. But that is an issue apart from biometrics itself, and one that has always been a concern. In that respect, markets can likely provide us with relative anonymity. The question isn't whether it's possible but whether government will permit anonymity.

Summary: Acceptable and Unacceptable Biometrics

To review the three basic categories of biometric deployment, the most invasive is the national ID variety, which represents an involuntary database in which everyone must be included. Such schemes have serious implications for privacy, anonymity, civil disobedience, and the proper relationship of the individual to the state.

The second category of biometrics is characterized by databases of sought-after individuals and relies upon surveillance technologies like face-recognition. These databases properly contain no innocent individuals and, if properly administered, exclude the possibility of involuntary inclusion. However these systems could easily enable tracking of specific individuals, and therefore they require a yet-to-be-developed battery of safeguards to protect Fourth Amendment rights.[89]

The third category is defined not by governmental uses of biometrics but by private commercial and workplace uses of biometric technologies for security, commerce, and monitoring. While government-driven databases contain information on "wanted" individuals, this category encompasses technologies limiting access to those among a prescreened group of innocent individuals, that allow users to show that they are who they claim and are not impersonating someone. These uses of biometrics have no implications for *political* liberty; rather, they are voluntary in the sense that their deployment is market driven. Inclusion is voluntary as a condition of access to another's property, or for secure access to one's own personal services (such as financial accounts). Such uses of biometrics are best regulated by market

The boundary between public and private databases can become unacceptably blurred.

forces and evolving social norms, and will continue to be fine-tuned by consumer and employee acceptance or resistance. The "private use" subset of biometrics technologies also seems to offer the best chances for the development of genuinely secure systems.

National Biometrics Standards Undermine National Security

If government rather than the private sector dominates the deployment of biometric technologies, security aims—both national and localized or private—can be undermined. Businesses compete; and one area in which they can compete is in the development of technologies that enhance security. Government-mandated ID technology, presumably acquired as the result of this or that contractor's winning bid, would tend to lock in a set of national standards (since malls, stadiums, workplaces, etc. would likely rely on the national ID for access rather than their own or alternative biometric IDs). That would undermine research and innovation in secure biometrics applications, whereas leaving development in the hands of the private marketplace would help spur the advancement of technologies as a matter of competitive necessity. Government-centric biometrics means an environment of lobbyists and appropriations that locks in certain biometric hardware and software vendors rather than a real marketplace. (In a sense, Larry Ellison was on the right track in offering to provide the national ID software *free*, so that there would be "no question of corporations benefiting."[90] His proposal still doesn't get around the lock-in dilemma—he would obviously be happy if Oracle provided the software of choice.) Politicization of authentication technologies would undermine research and innovation in ever more secure biometrics applications. We shouldn't lose sight of the fact that private businesses have control over security too, in myriad ways, and that experimentation can make us safer. We lose that dynamic if most private companies begin piggybacking on government ID cards.

Private businesses have control over security in myriad ways, and their experimentation can make us safer.

In addition to forcing us to give up information that we may not wish to share, the implementation of a national ID card also creates a "honeypot" of data about millions of individuals, an attractive target for data thieves. And if such data gets placed on the Internet, the risk goes up dramatically. The Internet, where much government information resides, was not designed for this kind of security. It is extremely vulnerable to hackers, because no one can be excluded; anyone can get online via thousands of public access points. After September 11, the federal government removed a considerable amount of data from websites that should never have been posted in the first place, such as details about chemicals contained on site at industrial plants.[91]

The risk of a "Digital Pearl Harbor"[92] even led Richard Clarke, the nation's top cybersecurity official, to call for a separate network (not connected to the Internet) for governmental data, unconvinced that a public network from which no one could be excluded could ever be secure.[93] While the government's ability to keep individual information secure is not the fundamental issue with respect to information collection about private citizens, it is essential to note that government cannot offer assurances that our information will be safe from penetration. Even if national ID data were not placed on the Internet but were on private government networks, the safety of the data would be unlikely. The Department of Defense has been hacked into since September 11, including episodes involving satellite spy pictures and missile secrets.[94] Other government sites and databases consistently fail security tests.

That is why, to the extent commercial society relies on comprehensive and secure databases, and it unquestionably does, security techniques must benefit from improvement impelled by the market process. Competition in the creation of secure identity systems and secure access is a fundamental necessity, especially as those systems increas-

ingly incorporate biometrics. Although the private sector may not always keep information secure, there is no better option. Consumers value security, and those private entrepreneurs who best supply that value will profit most handsomely. Innovations will occur in biometric and security standards just as they do in every other good and service sector in the economy. A government "nationalization" of the technologies by crowding out the private sector serves no legitimate ends with respect to enhancing authentication technology.

Conclusion

The proliferation of biometric technologies raises new and challenging questions in a society that enshrines privacy and liberty. Biometrics can either enhance or undermine our liberties depending upon their uses. A framework is needed by which we may resolve issues pertaining to proper and legitimate deployment. Citizens' rights are violated to the extent government engages in surveillance not appropriate in a free society, and to the extent that private sector companies gain profits or police powers from aggressive enforcement of laws. Most fundamentally, governments should not force citizens to submit to biometric identification, which rules out national ID cards. Governments also must recognize that Fourth Amendment protections will apply in the biometric age, which rules out using public surveillance systems to deliberately identify and track individuals without the authority of a court order; other safeguards in the arena of public-place surveillance will need to be developed as well. Finally, with respect to private sector applications of biometrics, access to government-mandated databases must be off-limits. Private sector biometrics, which show enormous promise, must face either the approval or wrath of the public in order to be properly "regulated"—and that process is undercut when the lines between public and private databases are blurred.

Notes

1. James Gilmore, former Governor of Virginia and head of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction,quoted in Molly M. Peterson, "National ID System Provokes Civil Liberties, Security Needs," *National Journal's Technology Daily*, March 27, 2002.

2. The term was used in a February 1, 2001, press release from the American Civil Liberties Union; "ACLU Calls for Public Hearings on Tampa's 'Snooper Bowl' Video Surveillance," www.aclu.org/news/2001/n020101a.html.

3. See David Coursey, "Can 'Brain Fingerprints' Protect Us from Terrorists?" *ZD Net*, October 2, 2001, www.zdnet.com/anchordesk/stories/story/0,10738,2815694,00.html. See also the follow-up article by Coursey, "Brain Fingerprinting: What You Thought, What I Meant," *ZD Net*, October 5, 2001, www.zdnet.com/anchordesk/stories/story/0,10738,2816429,00.html.

4. Michelle McCann, "Microchip Keeps Track of Pets," *Government Computer News*, November 1997, www.gcn.com/archives/sl/1997/November/desk.htm.

5. See, for example, David Streitfeld, "First Humans to Receive ID Chips," *Los Angeles Times*, May 9, 2002.

6. Robert O'Harrow Jr. "Next: An ID Chip Planted in Your Body?" *Washington Post*, December 18, 2001, p. E1.

7. See Ivan Amato, "Big Brother Logs On," *Technology Review*, September 2001, www.technologyreview.com/articles/amato0901.asp.

8. A concern noted by Marc Rotenberg of the Electronic Privacy Information Center in Terry Lane, "Database Regulation Key to ID Cards and Biometrics, Panel Says," *Washington Internet Daily*, October 23, 2001, p. 3.

9. Ayn Rand, *The Fountainhead* (1943: New York: Bobbs-Merrill, 1968), pp. 729–30.

10. Rob Fixmer, "Protecting Your Digital Identity," *Interactive Week*, October 1, 2001, www.eweek.com/article/0,3658,s=722&a=15354,00.asp.

11. Quoted in Dee Ann Davis and Nicholas M. Horrock, "Ridge Eyes New Driver's Licenses," *Washington Times*, May 2, 2002, www.washtimes.com/upi-breaking/02052002-072009-4333r.htm.

12. Larry Ellison, "Digital IDs Can Help Prevent

Terrorism," *Wall Street Journal*, October 8, 2001, www.opinionjournal.com/extra/?id=95001336.

13. Davis and Horroc.

14. Frank Pellegrini, "The National ID that Isn't, Yet," *Time*, January 8, 2002, www.time.com/time/nation/article/0,8599,191857,00.html.

15. See for example, "Your Papers Please," *Washington Times*, January 21, 2002.

16. H.R. 4633, p. 7.

17. Davis and Horrock, 2002.

18. Robert A. Levy, "The ID Idea," *National Review Online*, October 24, 2001, www.nationalreview.com/comment/comment-levy102401.shtml.

19. Noted in Donna Leinwand, "National ID In Development," *USA Today*, January 22, 2002, www.usatoday.com/life/cyber/tech/2002/01/22/id-cards.htm.

20. See Mona Charen, ID Card Idiosyncrasy," *Washington Times*, January 28, 2002, p. A14.

21. H. R. 3162, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, October 25, 2001.

22. For example, see "A Nation's Liberty Is Hijacked," *Connecticut Law Tribune* 27, no. 51 December 14, 2001, p. 21.

23. John Solomon, "FBI Warned of Training before 11th," *Washington Post*, May 3, 2002, www.washingtonpost.com/wp-dyn/articles/A25198-2002May3.html.

24. See, for example, Mark Riebling, "The Real Intelligence Failure," *National Review Online*, May 28, 2002, www.nationalreview.com/comment/comment-riebling052802.asp.

25. Edward H. Crane and Roger Pilon, "Libertarianism Lives," *Wall Street Journal*, May 28, 2002.

26. Christine Hall, "Government Trade Association Calls for North American ID Drivers License," *CNSNews.com*, January 15, 2002, www.cnsnews.com/ViewNation.asp?Page=\Nation\archive\200201\NAT20020115b.html.

27. Davis and Horrock, 2002.

28. Richard Morin, "Poll: Half of All Americans Still Feel Unsafe," *Washington Post*, May 3, 2002, p. A7.

29. See, for example, Elise Ackerman and Paul Rogers, "National ID Debate Is Key Issue for Valley," *San Jose Mercury News*, October 25, 2001, p. 8A.

30. William Safire, "Threat of a National ID," *New York Times*, December 24, 2001, p. 15.

31. Shane Ham and Robert D. Atkinson, "Frequently Asked Questions About Smart ID Cards," Progressive Policy Institute, January 18, 2002, www.ppionline.org/ppi_ci.cfm?knlgAreaID=140&subsecID=290&contentID=250075.

32. Lane, October 23, 2001, p. 3.

33. John J. Miller and Stephen Moore, "A National ID System: Big Brother's Solution to Illegal Immigration," Cato Policy Analysis no. 237, September 7, 1995, www.cato.org/pubs/pas/pa237-es.html.

34. Stephen Levy, "Playing the ID Card," *Newsweek*, May 13, 2002, p. 44.

35. Lee Tien, "The VeriChip: Issues and Concerns," *TechTV Silicon Spin*, March 11, 2002, www.techtv.com/siliconspin/features/story/0,23008,3375488,00.html.

36. Levy.

37. *McIntyre v. Ohio Campaign Commission*, 514 U.S. 334, 115 S.Ct. 1511 (1995). Cited in Jonathan D. Wallace, "Nameless In Cyberspace: Anonymity on the Internet," Cato Institute Briefing Paper no. 54, December 8, 1999. pp. 2–3.

38. *Watchtower Bible and Tract Society of New York, Inc. v. Village of Stratton*, 122 S.Ct. 2080 (2002).

39. Leading vehicles in the 107th Congress are S. 2201, the Online Personal Privacy Act introduced by Sen. Ernest Hollings (D-S.C.) and H.R. 4678, the Consumer Privacy Protection Act of 2002 introduced by Rep. Cliff Stearns (R-Florida).

40. Simson Garfinkel, "Identity Card Delusions," *Technology Review*, April 2002, p. 31

41. Chris Bergh, "ID Wars—It Really Doesn't Matter," *ZDNet*, January 3, 2002, http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2835940,00.html.

42. Ibid.

43. See John Markoff, "Microsoft Has Quietly Shelved Its Internet 'Persona' Service," *New York Times*, April 11, 2002, p. C1.

44. For example, see Stephanie Olsen and Robert Lemos, "ACLU: Face-Recognition Systems Won't Work," *ZDNet News*, Novermber 2, 2001,

www.zdnet. com/filters/printerfriendly/0,6061, 5099140-2,00.html.

45. For example see Janice Rombeck, "San Jose's Message to Graffiti Vandals: You're Being Watched," *San Jose Mercury News*, June 2, 2002, www.bayarea. com/mld/bayarea/3391162.htm?template=content Modules/printstory.jsp.

46. Noted in Spencer S. Hsu, "D.C. Forms Networks of Surveillance," *Washington Post*, February 17, 2002, p. C1, www.washingtonpost. com/ac2/wpdyn/A223412002Feb16?language=p rinter.

47. Len Novarro, "Judge Dismisses 290 Red-Light Camera Tickets," *San Diego Union Tribune*, September 4, 2001.

48. John D. Woodward Jr., "Super Bowl Surveillance: Facing up to Biometrics," RAND Arroyo Center, 2001, www.rand.org/publications /IP/IP209/IP209.pdf.

49. Eugene Volokh, Big Brother Is Watching—Be Grateful! *Wall Street Journal*, March 26, 2002, p. A22.

50. Jeffrey Rosen, "A Cautionary Tale for a New Age of Surveillance, *New York Times Magazine*, October 7, 2001, www.nytimes.com/2001/10/07 magazine/puSURVEILLANCE.html.

51. Noted in William Safire, "'Big Brother' In America," *International Herald Tribune*, February 19, 2002, www.iht.com/articles/48463.html.

52. Rosen, www.nytimes.com/2001/10/07 magazine/puSURVEILLANCE.html.

53. Linda Gibson, "Masked Protesters Fight Face Scans," *St. Petersburg Times*, July 15, 2001, www. sptimes.com/News/071501/TampaBay/Masked_ protesters_fig.shtml.

54. Volokh, 2002.

55. Noted by Jeffrey Rosen in Lane, October 23, 2001, p. 3.

56. Prepared Statement of Jim Harper, Editor of Privacilla.org, at the Hearing on Red-Light Cameras, U.S. House of Representatives Committee on Transportation and Infrastructure Subcommittee on Highways and Transit, July 31, 2001, www.privacilla.org/releases/red-light_camera_ testimony.html.

57. *Katz v. United States*, 389 U.S. 347 (1967), http://laws.findlaw.com/us/389/347.html.

58. Cited in Harper, July 31, 2001.

59. *Kyllo v. United States*, 533 U.S. 27 (2001), http://laws.findlaw.com/us/000/99-8508.html.

60. Associated Press, June 13, 2001.

61. Mark G. Milone, "Biometric Surveillance: Searching for Identity," *Business Lawyer* 57, November 2001, p. 507.

62. Noted in Eric Peters, "Rigging Traffic Lights Hurts Safety," *Detroit News*, August 12, 2001, www.detnews. com/2001/editorial/0108/12/a18-266863.htm.

63. www.speedtrap.org/.

64. http://observingsurveillance.org/.

65. www.witness.org.

66. Dorothy E. Denning, "Why I Love Biometrics: It Is 'Liveness,' Not Secrecy, That Counts," *Information Security*, January 2001, www.infosecuritymag.com /articles/january01/columns_logoff.shtml.

67, Fred McClimans, "Is Biometrics the Answer to Increased Security?" *Network World Fusion*, October 22, 2001, www.nwfusion.com/columnists/2001/1022current.html.

68. Noted in a review written by Carlos A. Soto, "Biometric Security Not Quite Ready to Replace Passwords," *Washington Post*, May 2, 2002, p. E7.

69. Shannon Henry, "For Wealthy, A New Way to Fly on Business," *Washington Post*, April 2, 2002, p. E1, www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A48900-2002 Apr1&notFound=true.

70. Noted in Margaret Carlson, "The Case for a National ID Card," *Time*, January 14, 2002, www.time.com/time/columnist/carlson/article /0,9565,193705,00.html.

71. Noted in Stefanie Olsen, "Big Brother Knocked in 2000," *CNET News.com*, December 28, 2000, http://news.com.com/2100-1017250378. html?legacy=cnet.

72. Neil A. Lewis, "Rebels in Black Robes Recoil at Surveillance of Computers," *New York Times*, August 8, 2001. p. A1.

73. Diane E. Lewis, "Biological Data May Replace ID Cards, *Boston Globe*, June 6, 2001, http:// boston-works.boston.com/globe/articles /062401_privacy.html.

74. Reuters, "Biometrics: Hot Technology, Tough Policy," *ZDNet*, November 14, 2001, http://techupdate.zdnet.com/techupdate/stories/main/0,14 179,2824453,00.html.

75. http://hci.stanford.edu/captology/Examples/hygieneguard.html.

76. Noted in Jeffrey Goldfarb and Daniel Sorid, "Hand-Eye Coordination Drives Biometrics Deals," *Reuters*, May 4, http://story.news.yahoo.com/news?tmpl=story&cid=581&ncid=581&e=10&u=/nm/20020504/tc_nm/column_mergers_dc_8.

77. Ibid.

78. Michael Kanellos, "On the Way—ATMs that Recognize Your Face," *ZDNet Australia*, October 9, 2001, http://zdnet.com.com/2100-1106-530867.html.

79. David Kaplan, "It's Kinda Touch-and-Go: New System Lets Kroger Shoppers Pay with Fingerprint," *Houston Chronicle*, May 15, 2002 p. A.1.

80. Jay Lyman, "The Cyborgs Are Coming, The Cyborgs Are Coming," *News Factor Network*, December 10, 2001, www.newsfactor.com/perl/story/15428.html.

81. Noted in Reuters, "Biometrics: Hot Technology, Tough Policy," *ZDNet*, November 14, 2001, http://tech-update.zdnet.com/techupdate/stories/main/0,14179,2824453,00.html.

82. David Streitfeld, "A Chip ID That's Only Skin-Deep," *Los Angeles Times*, December 19, 2001.

83. Ibid.

84. Julia Scheeres, "They Want Their ID Chips Now," *Wired News*, February 6, 2002, www.wired.com/news/privacy/0,1848,50187,00.html.

85. Adam L. Penenberg, "The Surveillance Society," Wired, December 2001, p. 160.

86. Streitfield, 2002.

87. For example see Rick Perera, "Borders Books Kills Face-Scanning Plan Amid Criticism," *Computerworld*, August 27, 2001, www.computerworld.com/securitytopics/security/story/0,10801,63359,00.html.

88. Robert O'Harrow, "Privacy, Please," *Washington Post*, June 19, 2002, p. H5.

89. Interestingly enough, although the "Snooper Bowl" episode generated outrage, post–September 11 polls indicated a willingness on the part of many to accept even more invasive national ID systems.

90. Ellison, 2002.

91. Angela Logomasini, "When Terrorists Have a 'Right to Know'," Competitive Enterprise Institute, February 11, 2002, www.cei.org/gencon/019,02387.cfm.

92. Ariana Eunjung Cha, "For Clarke, A Career of Expecting the Worst: Newly Appointed Cyberspace Security Czar Aims to Prevent 'Digital Pearl Harbor,'" *Washington Post*, November 4, 2001, p. A10.

93. Associated Press, "Top Cybercop Wants New Net," October 10, 2001.

94. Noted in "Boy of 17 Hacks into Missile Secrets," *Standard Foreign News Desk*, www.thisislondon.com/dynamic/news/story.html?in_review_id=613066&in_review_text_id=582545.

Published by the Cato Institute, Policy Analysis is a regular series evaluating government policies and offering proposals for reform. Nothing in Policy Analysis should be construed as necessarily reflecting the views of the Cato Institute or as an attempt to aid or hinder the passage of any bill before congress. Contact the Cato Institute for reprint permission. Additional copies of Policy Analysis are $6.00 each ($3.00 each for five or more). To order, or for a complete listing of available studies, write the Cato Institute, 1000 Massachusetts Ave., N.W., Washington, D.C. 20001, call toll free 1-800-767-1241 (noon - 9 p.m. eastern time), fax (202) 842-3490, or visit our website at www.cato.org.