Securing Privacy *in the* Internet Age

edited by

PAM CHANDER, LAUREN GELMAN, *and* MARGARET JANE RADIN

14 THE UNEASY CASE FOR NATIONAL ID CARDS

A. Michael Froomkin

A. Michael Froomkin is a professor at the University of Miami School of Law in Coral Gables, Florida, specializing in Internet law and administrative law. He is a founder-editor of ICANNWatch, and serves on the editorial boards of Information, Communication & Society *and* I/S: A Journal of Law and Policy for the Information Society. *He is on the advisory boards of several organizations, including the Electronic Freedom Foundation and BNA Electronic Information Policy & Law Report. Froomkin is a member of the Royal Institute of International Affairs in London. He is also active in several technology-related projects in the greater Miami area.*

I. NATIONAL ID CARDS: THE COMING DEBATE

Proposals abound for the introduction of a national identification system, a computer-based record system in which a unique identifier (a national ID) would be associated with every U.S. citizen and permanent resident.[1] Opponents of national ID cards or national identification numbering systems[2] see them as threats to privacy and liberty. Whatever one's opinion of the merits, it is undeniable that a substantial and powerful community advocates national ID cards.[3] Here in the United States, we will have a national debate on ID cards, if we are lucky; if we're unlucky, we'll dispense with the debate and go straight to the cards and the databases.

The U.S. Supreme Court's decision in *Hiibel* v. *Sixth Judicial District Court of Nevada, Humboldt County*[4] hints, but does not hold, that a requirement that people carrying ID cards show them to police might be constitutional. Although holding that a state may impose a duty on citizens to

identify themselves orally to police officers during a *Terry* stop[5] (at least in the absence of "any articulated real and appreciable fear that his name would be used to incriminate him, or that it 'would furnish a link in the chain of evidence needed to prosecute' him"[6]), the Court noted that "the statute does not require a suspect to give the officer a driver's license or any other document."[7] Furthermore, whether Congress could constitutionally require that all citizens obtain or carry ID remains an open question.

Despite its limited legal reach, *Hiibel* could forever change the fundamental psychological relationship between the citizen and the state's front-line symbol of authority, the police officer. More important, the *Hiibel* decision increases the chance that the United States will adopt a mandatory national ID card regime in the near future. In time, an identification requirement might even affect the political process, as it might have a chilling effect on some forms of political action.

Yet viewed from another perspective, *Hiibel* may not be that significant. No result in *Hiibel* would have slowed the growth of our de facto national ID regime, which is maturing into a virtual ID card. A hybrid of formally public and formally private systems of identification, data-retention, and correlation, this developing virtual national ID card regime needs no federal legislation to become a reality. It is time, therefore, to reexamine the benefits and consequences of ID cards.

The ID card question immediately invokes larger issues: the utility of ID cards and also their dangers depend directly on the extent to which the cards link the data subject to databases and sensors. Similarly, the benefits—and especially the dangers—of ID cards are acutely sensitive to the technical architecture of any ID card system and to the design of legal rules that will constrain misuses. This chapter is primarily concerned with national identification systems in which a unique identifier is associated with every U.S. citizen and permanent resident. That unique identifier may reside in a database and be linked to the individual holder by means of a token such as a national ID card. The token may have just the ID number, or it may carry other information. In principle, a national ID system can function without a token, for example, using biometric linking. And, whether or not there is a physical token, the master database may contain authenticating and additional information about the holder, raising questions about transparency and access.

A national ID card that uses reliable data[8] and is sufficiently tamper-proof and secure[9] to reliably identify and authenticate the holder would be valuable

in public and private transactions. People who control resources—admittance to a building or permission to play online music—want or need to know who you really are in order to allow the interaction or transaction, and they want or need to keep a record of it.

Many people—including me—have an initial negative reaction to government-sponsored national ID systems. Yet the *marginal* harms that could be caused by a well-designed national ID system are fewer than one might initially believe given the ways in which invasive technology are reducing personal privacy. Nevertheless, ID cards present genuine dangers to civil liberty and to privacy that we should be wary of. Whether or not one supports the basic idea, it may be profitable to consider what rules might be crafted to minimize harms and maximize benefits.

A fair evaluation of the likely privacy costs of a national ID regime requires a proper understanding of the privacy baseline. The growth of distributed databases and the ease with which they can be linked means that this baseline is already low. As a result, the marginal cost to privacy of national ID cards is much less than it would be if we were starting from a high-privacy regime. If the privacy baseline is as poor as I suggest, then there is a (perhaps unlikely) scenario in which national ID cards could be used to enhance privacy. Somewhat counterintuitively, most persons' privacy rights against the government could be greater if ID cards are legally required than if they are formally optional because due process and other constitutional rights are difficult to assert when enmeshed in formally "voluntary" systems. Ensuring that the data subject retains a property interest in government-held data about him or her will further enhance personal privacy and other protections against misuse. Similarly, a government-mandated scheme in which the government retained ownership of the ID number would allow the government to condition use of that number on businesses' adoption of privacy principles. The carrot of easy, secure, and reliable identification might suffice to create market-based incentives to get businesses to accept the stick of adherence to substantive privacy conditions.

A mandatory national ID card regime could also form the basis for a political strategy aimed at creating at least a national dialog on privacy issues. Putting a piece of plastic in everyone's pocket would be a stark reminder that privacy is in play. Centralizing the debate at a national level would not necessarily result in the adoption of the best privacy principles, as it would also provide a single target for those lobbying for anti-privacy and data sharing, but it might.

II. BENEFITS OF NATIONAL ID: LINKING PERSONS TO FACTS (AND FACTS TO PERSONS)

The value of real and virtual national ID cards depends on many technical and organizational factors. Chief among these factors are the quality of the data used to establish identity; the security of the system (as regards both forgery of the card and authenticity of the data, wherever they reside); and the information it stores or is linked to. An ID card system, if linked to extensive databases with biometric information and near-real-time activity monitoring, can form the anchor of a wide-ranging system of surveillance, authorization, and, optionally, control.

Although touted as a means of preventing or deterring terrorism, the real benefits of a national ID system probably lie elsewhere. The security benefit from an ID card regime depends first on the quality of the data input into the system, and secondarily on how secure and difficult to forge the cards are. The first problem alone is enormous, as current U.S. identification data are notoriously poor.[10] Similarly, unless there are very substantial improvements in data quality, an ID card regime will provide little additional security against competent foreign terrorists. The greatest near-term benefits of a national ID card regime are likely to be in more routine law enforcement, benefit and tax administration, streamlining of some paperwork such as proof of authorization to work, and the enhanced ability it will give firms that use the ID number as an index to organize their data about their customers.

In the most general terms, any identification document or system links persons to facts, and facts to persons. The facts that an ID, whether real or virtual, links to persons fall into four broad and overlapping categories: permanent personal attributes, data about past activities, data about the person's present, and authorizations, which are a type of future-oriented information. ID cards arguably provide benefits in managing and using data in each category.

Permanent personal attributes are things a person is born with and is unable to change. A national ID card can store or link to information about the data subject's body. The biometric information can also serve as the identifying or authenticating information that links the person to the card. As technologies for distinguishing body parts improve, it seems increasingly attractive to use the body as password.[11]

Biometric identifiers enhance privacy when they prevent information from being stolen or improperly disclosed. Even so, biometrics have disadvantages as a personal identifier and are an imperfect basis for authenticating a person's

access to data. First, a biometric provides a unique identifier that can serve as a high-quality index for all information available about an individual. The more reliable the biometric identifier, the more it is likely to be used, and the greater the amount of data likely to be linked to it.[12] But because a biometric is a part of the person, that index is hard to change if needed. Second, some biometrics, particularly those that involve DNA typing, could disclose extraneous information about the data subject, such as race, sex, ethnicity, and propensity for certain diseases.[13]

Past attributes are facts about a person's life activities such as medical data, employment and criminal history, and legal or economic facts such as insurance claims, civil litigation, bankruptcies, and transaction history. These types of facts differ from permanent attributes in that they are not congenital, and ordinarily not biometric either.[14] Allowing others access to these facts can be beneficial; for example, emergency medical personnel can access life-saving information. Centralizing employment and criminal records would facilitate common background checks, improving their quality but at the cost of creating a single point of failure that might make someone unemployable.

Present facts are a hybrid category made up of persistent facts and transitory facts. Persistent facts are past facts that remain true today. Transitory facts are things that can be detected in real time such as a person's current location, the goods the person is bringing to the checkout counter, or the speed at which he or she is driving.

Unlike past facts, present facts can be changed. For example, home ownership is a present fact, subject to change if the home is sold. In contrast, last year's purchase of that real property or of a chattel is a fact that cannot be changed.[15] Present facts about a person include citizenship, current employment, marital status, religion, residence, salary, and visas.

Accurate information about persistent and transitory present facts is of obvious interest to the government and to many private parties. The extent to which present facts can be linked in real time (or near real time) to a national ID depends on the efficacy and deployment of sensors and other data-capture devices. In the case of point-of-sale information, the presentation of an ID card may facilitate linking the transaction data to the holder's file. Linking CCTV and other camera data to a person would require more sophisticated facial recognition techniques than currently exist or some other means to identify people at a distance.

Location information is especially valuable to law enforcement: current

location information allows police to locate a suspect, and stored location information makes new enforcement techniques possible. At its most benign, full location information would make it relatively easy to investigate street crime. If the mugging happened at 10:05 p.m. at the intersection of Elm and Main streets, and stored location data allow the police to identify everyone who was within a block of there during a ten-minute period, producing a list of suspects may be as simple as requesting a printout and calling up current location. The availability of other biographical information (such as age or employment) may also allow the police to prioritize their investigation.

Authorizations are a special type of future-oriented information, as they permit but do not require, some type of activity. Identity confirmations are a common means of determining whether a person is authorized to do something. For example, a debit card's PIN number provides a limited assurance that the person holding the card is entitled to it. The card's most important function, however, is to authorize two parts of the transaction: payment and exchange of goods when the merchant queries the bank to ensure that there are sufficient funds in the account to pay for the purchase.

Authorizations, even more than identification, are likely to be a prime function of a robust national ID card scheme. ID cards can authenticate registered voters and prevent double voting. They can identify a jury pool. Alcohol, cigarettes, and other restricted goods and services can only be sold to persons over a given age; a card can verify precise age, or just the binary over or under twenty-one. A card can confirm eligibility for government benefits. Standardizing identification with a single national ID card that is difficult to forge would also make it easier to identify benefit fraud.[16]

Eligibility for employment is an example of an authorization that could usefully be keyed to a national ID card. Federal law currently requires that employers verify the identity and right to work of all new employees.[17] Critics of this rule argue that the employer sanctions for hiring undocumented aliens create an incentive for employers to discriminate against legal Hispanic workers and others whom employers fear are not citizens.[18] A national system of employee identification would put all legal workers on an even footing, thus reducing potential discrimination; would reduce any paperwork burden that might be worrying employers; and would also make it easier to ensure that employees receive the social security and other benefits to which they are entitled. Reliable and easy verification of eligibility to work would make life more difficult for illegal aliens, reducing the attractiveness of illegal immigration—

an outcome that must be treated as a social benefit so long as the U.S. retains its immigration laws.

Not all uses of a national ID card are necessarily desirable. A strong and ubiquitous system of personal identification would ease the deployment of new technologies designed to maximize revenue for intellectual property at the expense of file sharing and fair use. In particular, intellectual rights holders seek, via digital rights management (DRM) technologies,[19] to enforce licenses that allow copyrighted (or even public domain) content they provide to be viewed only by paying customers. "Trusted computing"[20] initiatives will prevent computers and other devices from making copies, or even displaying information, without permissions set by the rights holders, trumping the wishes of the operator or owner of the hardware. If ID cards are unique, secure, and too necessary to daily life to share with others, then the "trusted" computer or other device can refuse to display the information unless the card is present, greatly reducing the current risk that authorizations such as passcodes will be shared between users.

Using a single national identification system to establish the right to do something (such as work) also creates leverage over most people's economic affairs that could be used to achieve social goals that may not always be directly relevant to the activity itself.[21] The "deadbeat dad" statute requires the federal government to maintain a database with the social security numbers, addresses, and wages of every new hire in the nation so that persons owing child support can more easily be located.[22] In theory, any social policy could be enforced in a similar manner, an outcome with potentially Orwellian overtones.[23]

III. DANGERS TO LIBERTY ARISING FROM A NATIONAL ID SYSTEM

Along with their economic and other benefits, ID cards pose many risks to liberty: (1) risks from the legal use of accurate information; (2) risk of reliance on false information; (3) risk of intentional creation of false information; (4) risks from illegal use of accurate information; (5) risk of overdependance on some feature of the system (completeness of database, ubiquity of card or other token).[24] Most of these classes of risk pose somewhat different dangers in the public and private sectors; in this chapter, I will concentrate on the public-sector risks, but the private-sector risks, which include price discrimination, illegal discrimination, and the enhanced enforcement of fair-use-destroying digital rights management systems, are also substantial.

A. Risks from the Legal Use of Accurate Information

It may seem counterintuitive, but a national ID system poses substantial risks to personal freedom even if the information it contains is accurate and the uses made of it are legal. Part of this seeming paradox comes from the fairly weak privacy protections found in U.S. law, and the weaker protections in the U.S. Constitution.

The least quantifiable, but undoubtedly significant, danger of a national ID system is the moral or psychological cost, especially if the system uses national ID cards. Many people find value in being able to move through life without an obligation to identify themselves, just as there is a value in the right not to be stopped or searched without cause. Correlatively, there may be at least as great a value in having a system of law enforcement in which the enforcers understand that people have that freedom. An ID embedded in a token, such as a card, that might have to be displayed on demand, undermines whatever value we place in being free(ish) from the demand to show our papers at the street corner, a freedom already badly eroded in airports, other places of mass transit, courthouses, and other public buildings.[25]

Although the question is not entirely free from doubt, the Constitution almost certainly imposes at best limited controls on the government's ability to do data mining and conduct law-enforcement-related virtual "general searches" on data under its control. Although some uses of a database are unproblematic, even desirable,[26] many are not.[27] And the more varied and detailed the information in the database, the greater the risks of profiling, of false positives, of efficient stigmatization, and of function creep. Currently, the Privacy Act prevents some of these dangers at the federal level, but it is impossible to imagine that the nation would go to the trouble and expense of setting up a national ID system if it were not going to use it. Even without a formal national ID, the increasing amount of data held by the government, or available to it from the private sector, will make data searching seem more and more attractive.

The Privacy Act states that non-law-enforcement agencies generally may not collect information about First Amendment activities,[28] but it imposes few other limits. Data must be limited to "such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President"[29] and the agency must not release information before making a reasonable effort to assure itself "that such records are accurate, complete, timely, and relevant for

agency purposes."[30] Given the natural bureaucratic desire to amass information "just in case," a tendency that can only have been strengthened by the terrorist attacks of 9/11, these do not seem like very broad protections.

Even with the Privacy Act in place, government law enforcement agencies and intelligence agencies are allowed to amass dossiers that they can mine to create profiles. Indeed, it's alleged that "a federal agency involved in espionage actually did a rating of almost every citizen in this country . . . based on all sorts of information."[31] And here the issue becomes almost metaphysical. One could say that the act of "searching" through a database of personal information, much of it furnished voluntarily either in private commercial transactions or in formally voluntary transactions with a government agency (for example, a driver's license application[32]), is nothing like a search. The data have been alienated before the search, they are no longer the subject's, and their new owner, the government, can do with it as it sees fit. Unless there is some constitutional principle to the contrary, whether there is a reasonable expectation of privacy depends on the legal rights one has over the data, and the law defines what our reasonable expectations are. Thus, unless the subject has a property right in the data that the government holds about him or her, or unless some special form of privacy legislation creates a due-process-like right to protect the data, or unless some privacy or due process right preventing such searches exists in the Constitution, the government may "search" data it owns about us for law-enforcement purposes.[33]

At present, virtual profiling is somewhat constrained by the Privacy Act of 1974,[34] which imposes some limits on the ability of the federal government—especially the parts not involved in law enforcement—to run database searches and conduct profiling in the absence of a particularized suspicion of an individual. Statutes change; enduring and reliable protection, if it exists, must lie in the Constitution.

The Fourth Amendment protects against unreasonable "searches" without a warrant. Courts grant search warrants only on a showing of particularized suspicion. A trawl of a database to find potential suspects by definition does not involve a particularized suspicion of anyone, and it is highly unlikely that a request for such a search would meet the standard needed to get a court to issue a warrant. Indeed, a database search more closely resembles a "general search," one of the evils that the Fourth Amendment was designed to prevent.[35]

On the other hand, because the subjects of the virtual search are unaware of any intrusion, some of the values the Fourth Amendment protects—the

sanctity of the person, the home, and of one's property—suffer less intrusion than with a physical search. Indeed, it has been argued that courts might treat many searches over a database as being the sort of reasonable search that does not require a warrant.[36] And, as noted, if the government owns or leases the data, courts for constitutional purposes might not treat a database trawl as a "search" at all, because there is no intrusion onto the property of the subject.

A national ID database (or any national ID card) without Fourth Amendment and property-like due process protections for its data risks many undesirable outcomes. Vesting title over the data in the subject would prevent many of them. Alternatively, legislation could leave title in the government but give an easement-like right over the use of the data. Any later attempt to remove this propertized protection would constitute a "takings," entitling every subject in the database to financial compensation—providing a strong disincentive to any Congress contemplating changing the database's status.

Property rights alone, however, do not suffice, especially if they do not attach to law enforcement's investigatory files. Currently, there is no official mechanism by which unproved denunciations to the local police, or to the FBI, become part of a file that is communicated widely among government officials. A national ID system and its associated databases—fueled perhaps by something such as Attorney General John Ashcroft's Terrorist Information and Prevention System (TIPS) proposal[37]—would create a mechanism by which unverified derogatory information could circulate widely, at least among government agencies. It might be objected that because the denunciation is unproved, and stands a good chance of being false, it belongs in the category of "uses of false information." But it is the fact *of the denunciation* that is recorded and searchable, and (absent police fabrication) it is true that there was such a communication from the public.

In addition to the obvious possible harms of having law enforcement use these tips as the "reasonable" basis for traffic stops and searches, there is the more fundamental harm to the body politic of developing an informer and dossier culture.[38] Because law enforcement, not to mention intelligence, agencies will resist any rules that require giving persons (suspects) access to data collected about them, or even notice that such an investigation has taken place, any privacy rules will be difficult to enforce. Some nations have created privacy commissioners or privacy ombudspersons charged with monitoring government data collection, retention, and sharing. Though worth trying—it can't hurt—it is not altogether clear how successful these officials have been.[39]

A large and rich database invites predictive profiling,[40] in which data mining is used in an attempt to predict who is likely to be dangerous. Inevitably, predictive profiling creates false positives, and stigmatizing.[41] Indeed, even without profiling, a rich database of accurate conviction information that is made available to the public invites a regime of stigmatization. Already some conviction information is sent to neighbors of released felons whether those neighbors ask for it or not.[42] This may only be the tip of the iceberg; a publicly available database might, for example, contain current addresses and all conviction histories, creating a class of "social leper."[43] Whether the loss of "social forgiveness, the principle that over time a citizen's crimes are forgiven," is a good thing or not may be debatable.[44] But any change of that magnitude should be debated, rather than be a side-effect of technology.

B. Risks from Reliance on (or Creation of) False Information

A fundamental problem with any national ID system is its vulnerability to GIGO, the old computer adage of "Garbage In, Garbage Out." We do not today have in the United States a particularly reliable system of formal identification. Major pieces of ID such as passports, social security numbers, driver's licenses, and credit cards frequently trace back to birth certificates. But the highly decentralized network of birth certificate issuers—hospitals—is notorious for its porousness and unreliability.[45]

A new centralized system would not only build on old risks of reliance on false information but introduce new ones: if IDs are linked to a centralized database relied on by government agencies this creates a particularly powerful place for someone to plant false information. Planted evidence is nothing new, and the possibility that a new system could be abused in the same manner as old ones is not necessarily a reason to fear a new system. Nevertheless, unless the system is engineered very carefully, the danger of virtual planted evidence is very serious. Today, planting evidence requires physical presence, and contact with the crime scene or with the evidence removed from it. Tomorrow, changing the contents of a record to incriminate someone may be as easy, or as hard, as accessing a file. No system is perfect, but the extent of a national ID system's vulnerability to this sort of "inside job" illicit modification will depend in large part on the extent to which the system is designed with this danger in mind. A separate, and perhaps greater, risk is that if the government and the public rely on the system, there is one centralized target for anyone trying to get a false ID—and if they succeed, the ID is too likely to be trusted.

Proper design of information systems can reduce risk of intentional inaccuracy, although no system is foolproof. If the information resides in a central location, then the danger of intentional and accidental inaccuracies can be reduced by *transparency*—ensuring that the data subjects have access to records about themselves. The more dispersed the records are, the less meaningful this protection becomes. ID card systems centralize; thus they make meaningful transparency that much easier.

Centralization of data in a single national system means that large numbers of people will be able to access those data for a wide variety of purposes. The more accesses there are, the greater the chance that inaccurate information will damage the data subject. However, the same centralization that creates this danger also may make it easier to correct inaccuracies in a manner calculated to reach people who previously were exposed to the erroneous datum. A big database is a big target. One would expect the incidence of identity theft to increase—but also that once detected, it should be easier to stop the thief from continuing to profit from it, and the victim from continuing to be charged with the thief's bad acts. Unfortunately, however, if the ID system relies on a biometric and the thief found a way to counterfeit it, the subject may have a problem. Even if it is easy to change ID numbers, it is hard to change corneas.

C. Risk of Illegal Use of Accurate Information

A national ID system also creates new opportunities for the illegal use of accurate information. Here, the problem is primarily one of increased opportunity, rather than of new classes of dangers.

Public-sector dangers from the illegal use of accurate information include the familiar problems of both organized and unauthorized snooping into public records. The prospect of a J. Edgar Hoover with a computer and a national ID database is not an attractive one—but neither is the prospect of J. Edgar Hoover's successors forced to operate without those tools. Similarly, unless audit tools are carefully built into the system and used properly, the existence of a database makes it likely that employees will sometimes misuse it for private purposes; although similar dangers exist currently, any increase in the quantity and scope of the data available will only make the database a more attractive place to snoop.

One argument often made against a national ID system is that were there ever to be a totalitarian government,[46] the database would make roundups of disfavored classes easier.[47] Certainly recent efforts to find and interview

immigrants and student-visa holders from the Middle East in the wake of 9/11—combined with the Bush administration's arguments that the government has the legal right to detain U.S. citizens without trial or counsel for indefinite periods upon a government official's unsupported declaration that the citizen is an "enemy combatant"[48]—give this concern a new saliency. It can be argued that a national ID database would make a difference because data about people, such as their addresses, would be updated continuously, rather than once every ten years with the census. Census data on residence date quickly, given that 16 percent of the U.S. population moves to a new residence every year.[49] Personally, I find this argument unpersuasive given the existence of massive private databases. A government prepared to build internment camps is prepared to buy, or take, the privately held data it believes it needs.

D. Risk of Over-Dependence

One of the greatest risks of a national ID system, with or without cards, is success. One of the most obvious dangers is that dossier inspection might become a routine part of major transactions such as employment and credit.[50] General reliance on a national ID card or on a centralized dossier creates at least three sorts of risks. Unless the system is more secure than is likely with current technology it may, by creating an unjustified sense of security, make users more vulnerable to identity theft. Identity theft or impersonation will be especially problematic if there is a biometric component to the authentication mechanism because we may lack a means to generate a replacement ID once the theft of the original is discovered. Routinized credentialing also destroys the ability of people to move and transact anonymously, undermining an important privacy right with implications for political and civil liberty.[51]

But perhaps the greatest danger if a national ID system really takes off is that people will become dependent on it for ordinary life, creating an attractive chokepoint for all sorts of regulation. If an enhanced national ID card[52] becomes ubiquitous, and is routinely presented for purchases, proof of age, transport, payment of tolls, and perhaps to cut off stop-and-frisk-upon-reasonable-suspicion *Terry* stops,[53] then anything that makes the ID harder to use becomes a powerful sanction. If the card or the data are government property, then many of the constitutional protections one might expect could be missing. If no taking of private property is involved, the only possible grounds for a due-process-based objection to government interference with one's use and enjoyment of the ID is an objection based on a liberty interest. Although

such arguments sometimes swayed the courts in the context of passport denials, it was easy to show that without a passport, foreign travel was next to impossible. It is doubtful whether such a showing would be as easy in cases about a national ID card (or number), especially in its early days when the precedents are being set.

Even if there are difficulties in actively sanctioning people for information in their dossiers, there will be considerably fewer barriers to making a "clean" record a precondition for some permits or benefits. Lest this seem far-fetched, consider that "[f]ifteen states now link driver's licenses with school attendance and performance."[54] A significant feature of a national ID system is that it creates a whole new avenue of leverage that can be applied by government to encourage and discourage behaviors. How one feels about this may depend on the goals it serves, or on one's more general beliefs about the propriety of social engineering.

IV. BETTERING THE PRIVACY BASELINE: THE (VERY?) UNEASY CASE FOR MANDATORY FEDERAL NATIONAL ID CARDS

To understand how a national ID system could be designed to achieve limited privacy gains, it is important first to understand the current privacy landscape. Indeed, the argument in this chapter relies on one key factual assertion: the enormous growth of the ability to link distributed databases means that we already have, or will soon have, a "virtual" national identification system, in effect "virtual ID cards." Today, the virtual system is sufficiently pervasive that it includes background data on almost every legal resident, and a very large quantity of transaction data. In the near future, this virtual system will expand to include substantial quantities of medical information, and positional and movement information.[55]

A. The Virtual National ID System

The collection and use of personal data is the key privacy issue[56]; the ID card is only the surface phenomenon. Indeed, the primary importance of a *physical* national ID card is its symbolic effect and its political consequences. As we have seen, the dangers of a national ID *system* are serious. Unfortunately, most of these dangers are equally real whether or not the national ID system includes a physical *card*. Any national database system, combined with any method of authentication, be it a card or other token, a biometric, or even a

challenge-response, has most of the same dangers with only a small difference in degree. The only substantial exception to this rule may be the psychological effects. If it is the case that introducing an identity document that would have to be produced on demand would really work a psychological change on citizens or law enforcement, then a system that relied only on virtual IDs might escape this danger—although why a system that relied on, say, facial recognition scans would be less pernicious is a little difficult to imagine. Psychology, however, works two ways, and the very visibility of a system that relied on a physical card might also have a salutary effect on the average consumer-citizen's privacy awareness.

Whether or not actual national ID cards are introduced, the United States has, or will very soon have, a privatized, de facto, national ID system capable of providing relatively detailed information about almost every resident. At present neither data collection, collation, nor disclosure in the private sector are subject to anything more than limited, patchwork regulation.[57] Government data practices are regulated by the Privacy Act, but these limits do not apply to law enforcement,[58] and as a practical matter, the government can always purchase access to private databases, meaning that information gathered in the private sector is available to the government. The reverse is sometimes true also, as governments sometimes seek to use their databases as a source of revenue,[59] subject to a possible backlash from the public.[60]

Four synergistic sets of changes are creating a virtual national ID system. First, a number of legislative initiatives have required the creation of (ostensibly) special-purpose databases, each of which covers a substantial fraction of the population. Second, increased use of credit and debit cards, store loyalty cards, Web-based marketing, and other private initiatives have collectively allowed retailers and financial intermediaries to amass great amounts of data on consumers. Third, both private and government actors have taken advantage of decreasing costs in camera and other sensor technology to install an expanding base of monitoring equipment on both public and private property. Fourth, advances in computer storage and networking technology have made it vastly cheaper to store, search, and share the gigabytes of data resulting from these developments. The result is a hybrid public-private system in which a very great amount of information about almost every U.S. resident is available for a small fee. Much of this information is currently distributed on separate networks, but the technology to tie them together exists.[61]

It should be possible to design a national ID system that would enhance privacy rights above those enjoyed in the "virtual" national ID system—although these rights would not necessarily be superior to the "no ID at all" world we have lost. The first part of the strategy is to take half a leaf from the legal treatment of passports and have the government own the national ID numbers themselves. Due process rights regarding an individual's use of his or her own number would need to be substantially better than the very limited rights to a passport, and they would be because the ID number would be used in ways that strike closer to core constitutional rights than the right to have government documentation to facilitate travel abroad. The architectural safeguards needed to blunt the dangers of a national ID card system include security, transparency, individual control over personal information, support for multiple IDs (and perhaps even anonymity), and good error handling. Some of these are difficult to engineer. Others have faced, and likely will continue to face, political opposition that makes any broad legislation mandating good practices in the private sector unlikely. Even good design safeguards, however, do only a little to protect against a political decision to misuse the system. Design can reduce the risk of harmful unlawful uses; it is far less potent against a decision to make bad uses lawful.

The government would condition the use of the new national index number by both the public and private sectors on adherence to national data protection and privacy rules. Additional protection against government abuses could be achieved by giving the individual a property right in at least some of the data held in government files. The ownership and dissemination of private sector data would remain a matter of contract, but constrained by the third party's duty to adhere to government-defined data protection rules when using the federally owned ID number to index data, or even when using any data that had been so indexed.[62]

The privacy rules restricting the use of indexed information would be set nationally. Although this creates a focal point for regulation, it also inevitably creates a single point of policy failure, and a large target waiting for capture by industries that will want the minimum restrictions on their ability to process and share personal information. This is undoubtedly a risk, but it is one that should be weighed against the virtual ID card world currently being built, one in which the locations at which privacy-destroying decisions occur are scattered and often invisible. Centralizing the debate at least raises the visibility and salience of the issues. It makes it easier for public-interest coalitions to

form, and reduces the cost of organization for already stretched pro-privacy organizations.

Another major goal of the centralized rules should be transparency—ensuring that the data subject knows what is being recorded about him or her, who has permission to access the data and for what purposes, and (at least for non-law-enforcement access) who actually accesses the data. Transparency as to the data content is essential if persons are to be able to contest and correct errors. Transparency as to access is essential if persons are to be able to monitor against abusive profiling, data-based discrimination, and unsanctioned snooping.

A national ID system threatens anonymous and pseudonymous speech and commerce. The threat to anonymous speech affects a valuable constitutional right—one needed most by persons least able to speak out for it, as they are the ones who have a legitimate fear of retaliation.[63] Anonymous reading is threatened by DRM, which becomes much easier to enforce in a world of strong identification. All of these problems but the last can be greatly ameliorated if the system allows anonymity or multiple pseudonyms[64]—artificial, selectable personae that can be presented to the world and are capable of transacting, reading, and writing. In order not to undermine the binding of identity to person that justifies the ID card system, all pseudonyms would have to be distinguished from primary identities. Setting a 'nym bit would give fair notice to the world that the true identity of the user is masked. A cleverly designed system could permit the passing on of appropriate characteristics and authorizations (such as age) to the user's 'nym if he or she so chooses.

The "OECD Guidelines" or, more formally, the 1980 Organization for Economic Co-operation and Development *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*,[65] set out recommendations for nations concerned about data privacy to "take into account in their domestic legislation," subject only to the minimum limits necessary to preserve national security. Many privacy advocates see the OECD Guidelines as central to fair information practices;[66] others see the Guidelines as insufficient.[67] I am uncertain myself about the relative efficacy of legal protections as opposed to technological ones. But at the dawn of the twenty-first century, what we have in the United States is far too little of either,[68] with relatively little prospect of improvement. Of the federal privacy laws, only the federal Privacy Act of 1974[69] could be accused of having a wide application, and it applies only to records collected by the federal government. Federal privacy regulation of the private sector is spotty at best.[70]

New privacy rules will successfully piggyback on a national ID system only if private-sector data users decide that it is in their economic interest to use the new number. Otherwise, presumably, they can keep on building an alternative system that relies on whatever other identifiers they choose. A single reliable identifier should be of considerable interest to most private-sector data users, as the alternatives that exist today are unreliable due to data quality problems and also because the data are difficult to sort reliably, at least without expense. The carrot of lower transactions costs dangled by easy, secure, reliable, and cheap identification might suffice to create market-based incentives to get businesses to accept the stick of adherence to substantive privacy conditions. The private sector already makes routine use of the SSN despite its known security and uniqueness flaws; a new number that promised uniqueness, full coverage, and greater security would, one hopes, be very popular for e-commerce and even ordinary commerce. Given this attractive carrot, there is scope for some stick, for making adherence to a set of fair information practices rules implementing the OECD guidelines a condition precedent to commercial use of the new ID number.

An even better privacy rule would copy one aspect of the European Data Protection Directive and make obligations to follow privacy principles run with the data subject to the rule regardless of privity. In this version, once a firm chose to use the national ID number to organize or index its data, it would be forbidden to sell parts of the data set to other firms unless they, too, adhered to the same privacy principles. Without this extra provision, the weaker rule, which only imposed these obligations on firms if they used the actual ID number, might be subject to evasions.

B. Optimizing Ownership of Data

Ensuring that data subjects retain an ownership right in data held about them by other private actors is frequently suggested as a way of enhancing personal privacy. The theory is that if each data user must buy the right to share information on a per-transaction basis, this will put the subject on notice as to how data about him or her is being used, and also create an opportunity for the subject to veto unwanted uses. If nothing else, the argument goes, it will allow data subjects to share in the profits accruing from uses of their data.[71] But, as Jessica Litman notes, we usually create property rights in things we want to allow to be sold, not in things we want to keep from being traded.[72] In addition, it seems very implausible that Congress would adopt a sort of moral right for personal data that would run with it no matter who acquired it and

under whatever circumstances.[73] And, if instead the new data property regime only requires a special form of words to allow full alienation of the personal interest in data, then it seems certain that this formulation will quickly find its way into every standard form consumer contract.[74]

Changing default rules for the ownership of privately held data is unlikely to do much to increase personal control over data if people are likely to contract around it without much thought. In contrast, a reliance on property law makes much more sense in the context of public law relating to government-controlled information because it invokes the Constitution.[75] If the federal government retains ownership of the ID number, then government can impose conditions on the use of the number. As the number becomes routinely essential, and as the amount of data subject to privacy rules that run with the index number grows, the private sector will find the number too valuable to avoid. Conversely, giving citizens a property right in noninvestigatory data[76] about themselves held by the government ensures that uses of the data will be subject to constitutional constraints including limits on search and alienation. Firms would be unable to contract around the ID number ownership rule because they would be mere licensees. Whether citizens should ever be allowed to surrender their property interest in their government-held data may be a hard question to answer in the abstract, but in practice, few would choose to waive their protection against government data trawling in the absence of improper pressure.[77]

The simplest way of conditioning the use of a new ID number by third parties on adherence to fair information practices would be to have the government retain ownership of the ID number and any associated card, following the passport model,[78] and to issue rules making data protection run with the use of the number or the data. But, as the legal history of the passport teaches us, this strategy is dangerous because it also opens the door to subsequent changes in law or in the regulations that might substantially affect the freedom of anyone who used the number or card.[79]

Indeed, the right—if right it be—to a passport carries conditions. The passport regulations provide for denying a passport for various grounds that might reasonably suggest the person seeks to leave the country to avoid unpleasant legal consequences.[80] But there is also the political test: the passport can be denied if the "Secretary determines that the national's activities abroad are causing or are likely to cause serious damage to the national security or the foreign policy of the United States."[81]

A national ID system that allows the government to suspend the ID card or make it difficult to use would easily become oppressive unless the citizen had clear rights to the card and also a right to a pre-deprivation hearing. If the card is required for work and for most transactions, it becomes the cornerstone of a citizen's economic identity. If the ID card is routinely required by common carriers and toll authorities, it will function as a de facto internal passport, making any governmental interference with it an assault on the right to travel. Something this important cannot be left to the uncertainties of a legal regime that might or might not distinguish it from the regime contemplated by *Haig* v. *Agee.* Vesting ownership of both the ID card and the number in the person whom they identify would ensure that the due process the Court associates with property rights attaches to governmental attempts to regulate the use and enjoyment of the card. Alas, vesting ownership of the number in individuals revives the scenario in which individuals likely will be invited to sign away their data privacy rights in merchants' standard form contracts.[82] Achieving the best of both worlds may not be possible without a new form of information property ownership, akin to joint (but not several) ownership of real property for both the card and number. Otherwise, one must choose between potential evils: the danger that the government might change the rules, or the danger that the private sector will attempt to contract around them. The first is more dangerous; the second is more certain.

Whether or not citizens have a property right in their ID number, they ought to own at least part of the data the government holds about them. Personal ownership of government-held data would limit the government's ability to share the data with third parties without the subject's consent. And it would more clearly invoke the warrant requirement before the government "searched" the data as part of a data-mining operation. To be most effective, however, the property right would have to extend not only to data acquired directly from the citizen but also to data the government acquired from commercial databases. At the very least, the government should be subject to the same viral data protection rules as would any other buyer of the data.[83]

V. CONCLUSION

A fair evaluation of the likely privacy costs of a national ID regime requires a proper understanding of the privacy baseline. The current data privacy picture is worse than most people realize, and the odds are it will continue to get worse. In that light, the marginal harms caused by a well-designed national

ID system may be fewer than one might initially believe, although there are genuine dangers to civil liberty and to privacy. In particular, there are possible psychological and moral costs to liberty that are hard to quantify, and serious risks to civil liberties unless some constitutional means can be found to ensure that the government cannot simply revoke or burden the use of the ID without substantial pre-deprivation due process hearings.

There is a (politically unlikely) scenario in which national ID cards could be used as a means to enhance privacy: use of the ID number by third parties could be conditioned on those third parties adhering to fair information practices modeled on the 1980 OECD guidelines. Because using a ubiquitous and reliable numbering system should be very attractive to businesses, they would have an incentive to adopt it, and might accept the bargain that they take the fair information practices obligations with it. Defining the ID number as the property of the government, or as jointly but not severally owned with the citizen, would cut off private-sector attempts to demand that citizens waive their data protection rights.

If an ID card were widely adopted by both government and business, it could become a daily necessity for most residents. If the card becomes a routine requirement for work, transactions, and travel, then it also becomes a target of opportunity for regulation and for law enforcement. Although some of these uses are likely to prove valuable, there is a serious risk of abuse. These dangers can be reduced by giving the data subject a property interest in information the government collects about him or her. If the information is private property, it will enjoy greater, although still bounded, protections under the Fourth and Fifth Amendments, and the government's ability to search it, to construct predictive profiles using it, and especially to sell it to third parties, will all be constrained.

In the thirty years since the relatively far-reaching success of the Privacy Act of 1974, privacy advocates in the United States have enjoyed only sectoral, and sometimes limited, achievements in their attempt to secure federal protection for data privacy, especially as regards data in private hands.[84] The privacy provisions of the Gramm-Leach-Bliley Financial Modernization Act of 1999 are a case in point: they are, in practice, quite weak.[85] Had the HIPPA rules proposed by the Clinton administration taken effect, the story might be different, but the regulations that replace them are also fairly anodyne.

Although there have been successes, the last two decades' explosion of privacy-destroying technologies suggest pretty strongly that standards and

practices unfriendly to data privacy are being set more quickly and in more places than the privacy community can cope with. A perverse advantage of centralized national ID regime would be that it would create a very visible, single target for debate about privacy regulation. Again, this is only a mixed blessing, for although allowing privacy campaigners to focus on one debate, it also allows the interests that tend to oppose restrictions on the use of personal data to unite their lobbying efforts in one massive push for the goldfish bowl society.[86]

Even with such protections in place, an ID card regime is likely to contribute to the continued erosion of personal privacy. Although their adoption is not likely, an ideal set of national ID card rules might actually benefit privacy compared to the rather unappetizing alternative, not least because it would move the debate over privacy rules out of the widely dispersed arenas where it now occurs and where pro-privacy forces tend to be outnumbered, if they are even at the table.

This political calculation may be absurdly optimistic, but the mechanics of ID card implementation nonetheless merit careful thought because there is a real possibility that Congress may enact a national ID card program for reasons of its own, and indeed with REAL ID may have taken the first two steps in that direction. Ironically, the political justification for national ID cards is likely to be their supposed virtues as an anti-terrorism measure, although the cards' true merits probably lie elsewhere in both the short and medium run. Yet if we are to have a national ID card program, it makes sense to work out how it could best be structured to do the least harm to personal privacy—and maybe do some good as well.

NOTES

1. The interesting question of how legitimate foreign visitors acquire temporary ID numbers, or function without them, is beyond the scope of this chapter. *Cf.* Computer Science and Telecommunications Board, National Research Council, *IDs Not That Easy: Questions About Nationwide Identity Systems* (2002) [hereinafter NRC Report].

2. For the seminal formal definition, *see* Roger A. Clarke, *Human Identification in Record Systems* (June 1989); Roger A. Clarke, The Resistible Rise of the National Personal Data System, 5 *Software L. J.* 29, 33-36 (1992).

3. Polling data suggest that, at least in times of crisis, "the public strongly favors a national ID card 'to bolster anti-terrorism defenses.'" *Wired* (Sept. 25, 2001), available at http://www.wired.com/news/conflict/0,2100,47073,00.html (quoting question asked by Pew Research Center poll).

4. 124 S. Ct. 2451 (2004).

5. *Id.* at 2458-59.

6. *Id.* at 2461 (quoting *Hoffman v. United States*, 341 U.S. 479, 486 (1951)).

7. *Id.* at 2457.

8. This assumption elides important issues that are examined in the NRC Report, *supra* note 1.

9. This is far from easy. *See generally* Bruce Schneier, *Secrets and Lies* (2003).

10. *See* NRC Report, *supra* note 1.

11. Biometrics can be used for identification or authentication. *See generally* Dutch Data Protection Authority (Registratiekamer), R. Hes, T.F.M. Hooghiemstra, & J. J. Borking, *At Face Value: On Biometrical Identification and Privacy* 2 (1999), available at http://www.registratiekamer.nl/bis/top_1_5_35_1.html (discussing the various applications of biometrics).

12. *See* Ann Cavoukian, Biometrics and Policing: Comments from a Privacy Perspective 4, in *Polizei und Datenschutz (Neupositionierung im Zeichen der Informationsgesellschaft* (Data Protection Authority ed., 1999) available at http://www.ipc.on.ca/web_site.eng/matters/sum_pap/PAPERS/biometric.htm.

13. *See id.*

14. Again, there are always borderline cases, such as a lost limb, which could reasonably be described as a (henceforth) "permanent," "past" or "present" condition.

15. Similarly, for most people, a criminal record is a fixed fact that cannot be changed. Even here, there are pardons and reversals on appeal, so the categories are somewhat fluid.

16. *See* Philip Redfern, Precise Identification Through a Multi-Purpose Personal Number Protects Privacy, 1 *Intl. J.L. & Info. Tech.* 305, 312 (1994).

17. *See* 8 U.S.C. § 1324a(a)(1)(B) (prohibiting hiring workers without verifying identity and authorization to work in the United States). Employers must complete an INS Form I-9, Employment Eligibility Verification Form, documenting this verification and stating the type of ID they examined. *See* Verification of Employment Eligibility, 8 C.F.R. § 274a.2.

18. *See, e.g.*, Sarah M. Kendall, Comment, America's Minorities Are Shown the "Back Door" . . . Again: The Discriminatory Impact of the Immigration Reform and Control Act, 18 *Hous. J. Int'l L.* 899 (1996).

19. *See* Julie E. Cohen, A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace, 28 *Conn. L. Rev.* 981 (1996), available at http://www.law.georgetown.edu/faculty/jec/read_anonymously.pdf; Julie E. Cohen, Lochner in Cyberspace: The New Economic Orthodoxy of "Rights Management," 97 *Mich. L. Rev.* 462 (1998), available at http://www.law.georgetown.edu/faculty/jec/Lochner.pdf.

20. *See* Chad Woodford, Trusted Computing or Big Brother? Putting the Rights Back in Digital Rights Management, 75 *U. Colo. L. Rev.* 253 (2004).

21. For a discussion of related concerns, *see* Daniel J. Solove, Access and Aggregation: Public Records, Privacy and the Constitution, 86 *Minn. L. Rev.* 1137 (2002).

22. Personal Responsibility and Work Opportunity Reconciliation Act of 1996, Pub. L. No. 104-193, 110 Stat. 2105 (1996). Samuel V. Schoonmaker, Consequences and Validity of Family Law Provisions in the Welfare Reform Act, 14 *Journal American Academy of Matrimonial Lawyers* 1, 10 (Summer 1997); Valerie Collins, Identity Cards and Numbers: The Debate Continued, 10 *Int'l Rev. L., Computers & Tech.* 142 (1996).

23. Smaller-scale versions of this have happened abroad. For example, during the Cold War,

the West German government kept a secret list of persons who it deemed unfit for government employment due to their political activities. *See* Wikipedia, Radikalenrlass, http://de.wikipedia.org/wiki/Radikalenerlass.

24. The classic survey of the potential dangers of a national ID system remains Roger Clarke's list of the dangers of "Dataveillance." Roger Clarke, Information Technology and Dataveillance, 31 *Commun. ACM* 498-551 (Nov. 1987), available at http://www.anu.edu.au/people/Roger.Clarke/DV/CACM88.html.

25. *See* Michael A. Sprow, The High Price of Safety: May Public Schools Institute a Policy of Frisking Students as They Enter the Building?, 54 *Baylor L. Rev.* 133 (2002).

26. For example, data matching to combat fraudulent applications for benefits.

27. For example, building up lists of frequent protestors against government policies.

28. An agency shall "maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity." 5 U.S.C. § 552a(e)(7).

29. 5 U.S.C. § 552a(e)(1).

30. *Id.* at (e)(6).

31. Erik Baard, Buying Trouble, *Village Voice* (June 24, 2002), available at http://www.villagevoice.com/issues/0230/baard.php.

32. Data provided in a driver's license application is currently protected against release to the private sector-but not to many government agencies-by the Driver's Privacy Protection Act of 1994 (DPPA), 18 U.S.C. §§ 2721-25. *Cf. Reno v. Condon*, 528 U.S. 141 (2000) (upholding constitutionality of DPPA).

33. Another, less persuasive, analogy would treat the data as having been left in the government's plain view. And it is settled that the police may examine anything left in plain view. *See Florida v. Riley*, 488 U.S. 445, 450-51 (1989) (search of home from helicopter does not violate Fourth Amendment).

34. Codified at 5 U.S.C. § 552A(b). The restrictions on law enforcement agencies as regards investigatory records-a potentially broad category-are somewhat less strict.

35. *See* Michael Adler, Note, Cyberspace, General Searches, and Digital Contraband: The Fourth Amendment and the Net-Wide Search, 105 *Yale L.J.* 1093 (1996).

36. *Id.* at 1097.

37. On TIPS, *see* William Matthews, *Ashcroft Offers TIPS Assurances* (July 26, 2002), available at http://www.fcw.com/fcw/articles/2002/0722/web-tips-07-26-02.asp.

38. *See* Timothy Garton Ash, *The File: A Personal History* (1997).

39. For a surprisingly pessimistic assessment by a former privacy commissioner, *see* David H. Flaherty, *Protecting Privacy in Surveillance Societies* 406-07 (1989).

40. On profiling, *see generally* EPIC, Profiling and Privacy Page, http://www.epic.org/privacy/profiling/. Examples of predictive profiles in use today include W.A.V.E. and Mosaic 2000. *See* Jon Katz, *After Columbine: Geek Profiling*, (January 23, 2001), available at http://features.slashdot.org/article.pl?sid=01/01/23/2341238.

41. The case of Richard Jewel is instructive as to the costs to the victim of a false positive. *See generally* http://www.hfac.uh.edu/comm/media_libel/cases-conflicts/tv/jewell.html.

42. Megans Law-type statutes stigmatize sex offenders by notifying neighbors of their presence. *See generally* Dan Markel, Are Shaming Punishments Beautifully Retributive? Retributivism and the Implications for the Alternative Sanctions Debate, 54 *Vand. L. Rev.* 2157 (2001).

43. According to T. Markus Funk, A Mere Youthful Indiscretion? Reexaming the Policy of Expunging Juvenile Delinquency Records, 29 *U. Mich J. L. Ref.* 885, 903 n. 85 (1996), the term originates with Richard S. Harnsberger, Does the Federal Youth Corrections Act Remove the "Leper's Bell" from Rehabilitated Offenders?, 7 *Fla. St. U. L. Rev.* 395 (1979).

44. For some thought-provoking if rather cold-hearted arguments as to why some common forms of social forgiveness might be harmful, see Funk, *supra* note 43.

45. *See* NRC Study, *supra* note 1, at ch. 2.

46. *Cf.* Sinclair Lewis, *It Can't Happen Here* (1935).

47. *See, e.g.*, Roger Clarke, *Information Technology: Weapon of Authoritarianism or Tool of Democracy?* (June 1994), available at http://www.anu.edu.au/people/Roger.Clarke/ DV/Paper-Authism.html.

48. *Cf. Rumsfeld v. Padilla*, 542 U.S. 426 (2004).

49. *See* U.S. Bureau of the Census, *Housing Issues Motivate More Than Half of Movers, Census Bureau Reports* (May 24, 2001) (giving 16 percent figure for year 2000), available at http://www.census.gov/Press-Release/www/2001/cb01-90.html.

50. Employers and insurers are already relying on credit scoring. *See* Insurance Credit Scoring, available at http://www.indianafarmers.com/docs/Credit%20Score%20 Brochure%20 Final%20Version.pdf; Insure.com, How Your Credit History Affects Your Auto and Home Insurance Premiums, available at http://info.insure.com/auto/creditscores.html.

51. *See* A. Michael Froomkin, Flood Control on the Information Ocean: Living With Anonymity, Digital Cash, and Distributed Databases, 15 U. *Pitt. J. L. & Com.* 395 (1996), available at http://www.law.miami.edu/~froomkin/articles/ocean.htm.

52. The problem is equally real with a national ID system without a card, but is easier to visualize with a tangible example.

53. So named after *Terry v. Ohio*, 392 U.S. 1 (1968).

54. Robert C. Johnston, 15 States Link School Status, Student Driving, *Education Week*, (Nov. 6, 1996), available at http://www.edweek.org/ew/ewstory.cfm?slug=10drive.h16.

55. *See* A. Michael Froomkin, The Death of Privacy?, 52 *Stan. L. Rev.* 1461 (2000), available at http://www.law.miami.edu/~froomkin/articles/privacy-deathof.pdf.

56. *See, e.g.*, Simson Garfinkel, Will a Mandatory ID Keep Us Safe?, *Privacy J.*, (Apr. 2002) (discussing the recent attempts by the states and DOT to create a standard driver's license and link the databases, making a de facto national id).

57. *E.g.*, Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g (2002); Video Privacy Protection Act of 1988, 18 U.S.C. § 2701 (2002); Driver's Privacy Protection Act of 1994, 18 U.S.C. §§ 2721-25 (2002); Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-03 (2002); Privacy Act of 1974, 18 U.S.C. §§ 2510-22, 2701-09 (2002); Electronic Communications Privacy Act of 1986, 5 U.S.C. § 552a (2002).

58. 5 U.S.C. § 552A.

59. *Cf. Lamont v. Commissioner of Motor Vehicles*, 269 F. Supp. 880 (1967) (denying injunction to block sale of DMV registry data).

60. Some state legislatures tried to sell driver's license data to private companies, but the public rebelled. Florida, for example, planned to charge one cent per image. Citizens complained, and the Florida legislation died. *See* Robert Lemos, The Dark Side of the Digital Home, ZDNet News (Feb. 7, 1999), available at http://zdnet.com.com/2100-11-513639.html?legacy=zdnn.

61. A fuller account of these developments can be found in Froomkin, *supra* note 55.

62. The obligation to comply with data protection rules would thus run with the data, just as do the obligations under the European Data Protection Directive. On the Directive *see generally*, Joel Reidenberg & Paul Schwartz, *Data Privacy Law* (1996).

63. It may also make whistleblowing more difficult and dangerous.

64. Roger Clarke suggests additional protections are needed if the system relies on ID cards. *See* Roger L. Clarke, *Chip-Based ID: Promise and Peril* (1997), available at http://www.anu.edu.au/people/Roger.Clarke/DV/IDCards97.html.

65. OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Sept. 23, 1980), available at http://www.oecd.org/document/0,2340,en_2649_34255_1815186_1_1_1_1,00.html [herinafter OECD Guidelines].

66. *See, e.g.*, Marc Rotenberg, Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get), 2001 *Stan. Tech. L. Rev.* 1, 45 (2001) ("It is generally understood that the challenge of privacy protection in the information age is the application and enforcement of Fair Information Practices and the OECD Guidelines."). *See also* Paul M. Schwartz, Privacy & Democracy in Cyberspace, 52 *Vanderbilt L. Rev.* 1609 (1999).

67. *See, e.g.*, Gary T. Marx, *Ethics for the New Surveillance in Visions of Privacy* 39 (Colin J. Bennett & Rebecca Grant, eds. 1999).

68. *See* Froomkin, *supra* note 55.

69. Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (codified as amended at 5 U.S.C.A. § 552a.

70. *Cf.* Fred H. Cate, The EU Data Protection Directive, Information Privacy, and the Public Interest, 80 *Iowa L. Rev.* 431, 438 (1995).

71. *See* Jessica Litman, Information Privacy/Information Property, 52 *Stan. L. Rev.* 1283 (2000) (summarizing and critiquing these arguments).

72. *Id.*

73. There are things we do not allow to be sold in any circumstances, such as babies and limbs and (in most states) sex, but information is unlikely to be added to that select group.

74. Consumers suffer from rational privacy myopia, valuing each bit of data at marginal value, whereas the buyer-aggregator understands that a profile is worth more than the sum of the parts. The buyer is thus willing to pay average value of the bit (modulo transactions costs), which will usually be higher than marginal value for all but the most sensitive data. Hence the observed behavior that Americans will sell their privacy for a frequent flyer mile. *See* Froomkin, *supra* note 55, at 1501.

75. The U.S. government sometimes suggests that current privacy rules such as the Privacy Act may not apply to data held by its contractors subject to government directives. *See, e.g.*, U.S. Department of Homeland Security, *Report to the Public on Events Surrounding JetBlue Data Transfer* (2004), available at http://www.dhs.gov/interweb/assetlibrary/PrivacyOffice_jetBlueFINAL.pdf. I believe this argument misreads the Privacy Act. But whether or not it

does, the loophole should not be available for data indexed via a national ID card or it would erase any meaningful privacy protections.

76. Obviously, creating such a right for data collected in the context of law enforcement investigations would be even more protective of personal privacy, but most would probably find the cost unacceptable.

77. There will undoubtedly be a few exceptions to this principle, *e.g.*, government employees in sensitive positions such as the CIA.

78. *See Lynn v. Rusk*, 389 F. 2d 940, 948 (D.C. Cir. 1967) (stating "the passport, [is] an official document that has consistently been regarded as the property of the Government.").

Currently, the Passport Act, 22 U.S.C.A. § 211a, defines the government's authority to grant and issue passports. Executive Order No. 11295, 31 F.R. 10603 (Aug. 5, 1966).

79. The modern passport cases begin with *Kent v. Dulles*, 357 U.S. 116 (1958) (overturning the secretary of state's decision to deny passports because Congress had not given him that power). The decision avoided the core constitutional issues of a right to a passport as an aid to the right to travel, but the narrowing construction suggested the Court was concerned about it. In a 1965 decision, *Aptheker v. Secretary of State*, 378 U.S. 500 (1964), the Court held that a statute making it a criminal offense for a member of the Communist Party to apply for, renew, or use a passport was unconstitutional on its face. Nevertheless, in 1981 the Court held that even in the absence of explicit statutory authorization, the government could revoke the passport of a U.S. citizen if there was a substantial likelihood of "serious damage" to national security or foreign policy as a result of a passport holder's activities in foreign countries. According to Chief Justice Burger, the Constitution's due process guarantees called for no more than statement of reasons and opportunity for prompt hearing *following* the revocation of the passport. *See Haig v. Agee*, 453 U.S. 280 (1981).

80. *See* 22 C.F.R. § 51.70.

81. *Id.*

82. Although there is no fundamental legal reason why this transaction could not be prohibited, such action seems far less secure politically than a regime in which the government owned the number and set the rules, thus making it impossible for individuals to waive a restriction they do not control.

83. As the OECD Guidelines contemplate exceptions for law enforcement, this is less protection than it might be.

84. First Amendment limits on preventing persons from sharing what they know are one constraining factor. *See* Eugene Volokh, Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop Others from Speaking About You, 52 *Stan. L. Rev.* 1049 (2000).

85. *See* Eric Poggemiller, Note, The Consumer Response to Privacy Provisions in Gramm-Leach-Bliley: Much Ado About Nothing?, 6 *NC Banking Inst.* 617 (Apr. 2002).

86. For a particularly evocative vision of what that might be like, *see* David Brin, *The Transparent Society* (1998).