# The Uneasy Case for National ID Cards

A. Michael Froomkin
University of Miami School of Law
http://www.law.tm
froomkin@law.tm

**Draft**, March 2004



Q:\id42.wpd

# Contents

## 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] These proposals have also attracted opposition from those who see national ID cards or national identification numbering systems[2] as threats to privacy and liberty. Whatever one's opinion of the merits, it is undeniable that there is a substantial and powerful community which does advocate national ID cards.[3] Here in the US, it seems that we are fated to 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.[4]

---

[1]The interesting question of how legitimate foreign visitors acquire temporary ID numbers, or function without them, is beyond the scope of this paper. 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 definitions 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); see also Roger A. Clarke, *Human Identification in Information Systems: Management Challenges and Public Policy Issues* (1994), http://www.anu.edu.au/people/Roger.Clarke/DV/HumanID.html#PPI; *see also* Lynn LoPucki, *Human Identification Theory and the Identity Theft Problem*, 80 TEXAS L. REV. 91 (2001) (adding to Clarke's definitions).

[3]Polling 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), http://www.wired.com/news/conflict/0,2100,47073,00.html (quoting question asked by Pew Research Center poll). For example, Larry Ellison: "the question is not whether the government should issue ID cards and maintain databases; they already do. The question is whether the ones we have can be made more effective, especially when it comes to finding criminals." Larry Ellison, *Digital IDs Can Help Prevent Terrorism*, The Wall Street Journal (October 8, 2001), http://www.oracle.com/corporate/index.html?digitalid.html.

See also Nicholas D. Kristof, *May I See Your ID?*, New York Times (March 17, 2004), http://www.nytimes.com/2004/03/17/opinion/17KRIS.html?ex=1394946000&en=938b60e9bdb051f7&ei=5007&partner=USERLAND (advocating mandatory national ID cards).

[4]Section 815 of the Homeland Security Act of 2002 states that "Nothing in this chapter shall be construed to authorize the development of a national identification system or card." 6 U.S.C.A. § 554.

There are however a number of narrow national ID requirements in effect today such as Transportation Worker Identification Card mandated by Maritime Transportation Security Act of 2002, Public Law 107-295, which requires ship owners to restrict access to their vessels to workers who have background checks and transportation security cards issued by the federal government.

(continued...)

The US Supreme Court will soon decide *Hiibel v. Sixth Judicial District Court of Nevada, Humboldt County*,[5] which presents the question, "Do the Fourth and Fifth Amendments to the United States Constitution bar the state from compelling people to identify themselves during a police investigation when someone has been seized upon less than probable cause?" The stakes in the *Hiibel* case are simple: everything and nothing. On the one hand, there is much more at issue than the Romantic desire of one freedom-loving cowboy--and millions of would-be freedom-loving cowboys--to be able to tell policemen where they can put their request for ID during a *Terry* stop. If the Supreme Court affirms the 4-3 majority in the Nevada Supreme Court which upheld Nevada's requirement that a person identify himself when stopped,[6] it could forever change the fundamental psychological relationship between the citizen and the state's front-line symbol of authority, the police officer. A decision for the government would increase the chances that the US would adopt a mandatory national ID card regime in the near future. In time, an identification requirement could even affect the political process, as it might have a chilling effect on some forms of political action.

On the other hand, while a decision for Dudley Hiibel would reduce the chances of an official government-sponsored National ID Card, it will not slow the growth of a de facto national ID regime, a development so well past its infancy that it is maturing into a virtual ID card. A hybrid of both formally public and formally private systems of identification, data-retention and correlation,

---

[4](...continued)

More recent proposals in Congress that would mandate components of a national identification system, e.g. the ID card itself, or the networked database system underlying it, include the United States National Health Insurance Act (or the Expanded and Improved Medicare for All Act) of 2003, H.R. 676. The system would require that each citizen be issued a National Health Insurance Card linked with a unique number. The as-yet-unamed 2003 H.R. 3461 would standardize the State ID application process, and prohibit Federal Agencies from accepting a State ID or driver's license as a valid source of identification, unless the applicant can produce two or more documents that are listed in the bill; all documents must be in English.

[5]59 P.3d 1201 (Nev. 2003), cert granted 124 S.Ct. 430 (2003) (to be argued March 22, 2004).

[6]See Hiibel v. Sixth Judicial District Court of Nevada, Humboldt County, 59 P.3d 1201 (Nev. 2002) (upholding Nev. Rev. Stat. 171.123(3) by a 4-3 vote). The statute at issue reads:

> 1. Any peace officer may detain any person whom the officer encounters under circumstances which reasonably indicate that the person has committed, is committing or is about to commit a crime.
>
> ....
>
> 3. The officer may detain the person pursuant to this section only to ascertain his identity and the suspicious circumstances surrounding his presence abroad. Any person so detained shall identify himself, but may not be compelled to answer any other inquiry of any peace officer.
>
> 4. A person may not be detained longer than is reasonably necessary to effect the purposes of this section, and in no event longer than 60 minutes.

Nev. Rev. Stat. 171.123.

this developing virtual national ID card regime needs no federal legislation to become a reality, if indeed it is not already one. It is time, therefore, to re-examine the benefits and consequences of ID cards.

The ID card question is complicated, however, because it 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 the legal rules that could be crafted to constrain misuses. This paper is primarily concerned with national identification systems in which a unique identifier is associated with every U.S. citizen and permanent resident.[7] 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*.[8] The token may have just the ID number, or it may carry other information. This additional information may be designed to aid in authenticating the person proffering the card as the authentic holder of the related ID number, or the card may contain additional information about the holder. Who gets to see and to modify that additional information if it exists are important policy questions. In principle a national ID system does not require a token to function; other possible means include *biometric* linking. And, whether or not there is a physical token, the master database may contain both authenticating and additional information about the holder, raising questions about transparency and access.

This paper makes a cautious and uneasy argument: Once one gets past a certain visceral revulsion, the marginal harms caused by a national ID system are fewer than one might initially believe given the deteriorating state of personal privacy in the face of invasive technology. 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 how those rules might be crafted to minimize harms and maximize benefits. But it is also time to examine carefully just what the potential costs and benefits might be, and how to craft a legal and political strategy calculated to achieve the greatest overall benefits at the smallest cost to privacy.

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 very 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 as an excuse to enhance privacy. Somewhat counter-intuitively, most persons' privacy as against the government will likely to be greater if the ID cards

---

[7]As noted above, *supra* note 1, the issue of identification of foreign visitors is outside the scope of this paper.

[8]For a sensitive discussion of the perils of badly designed cards, see Roger L. Clarke, *Chip-Based ID: Promise and Peril* (1997), http://www.anu.edu.au/people/Roger.Clarke/DV/IDCards97.html

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 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 it 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. Currently decisions with substantial impacts on personal privacy are made in a very decentralized, almost random, fashion. Governments take decisions at every level. Technologists design products or agree standards with anti-privacy implications that sometimes are only felt years later--when sunk costs make change very difficult. Database collection and correlation happen invisibly to the data subject. Privacy advocates are fighting battles they cannot win, if only because there are so many battles, and so many of them happen out of sight.

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 there are reasons to believe that the likely outcome of that debate would at least be no worse than where the current decentralized decisionmaking trajectory is leading, and even reasons to hope that the outcome might be better than it would otherwise be.

## II. Benefits of National ID: Linking Persons to Facts (and Facts to Persons)

A physical ID card is an identifying token that contains a unique identifier. The unique identifier links the holder to databases. The card may also contain various types of stored data that facilitate the authentication of the legitimate holder of the ID, or facts about her. A virtual ID card is not even that – it is just a index number stored somewhere, or more likely many somewheres, that matches attributes of a person (e.g., biometric identifiers) to one or more collections of data.

The value of both 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 (both as regards forgery of the card and authenticity of the data, wherever it resides), and of course on what information it stores or is linked to. If linked to extensive databases, biometric information, and real-time (or near-real-time) activity monitoring – all of which are possible, even likely, developments in the next decade – an ID card system can form the anchor of a wide-ranging system of surveillance, authorization and, optionally, control.

In the most general terms, any identification document or system links persons to facts, and facts to persons. In some cases the ID authenticates a person – it provides assurance about the

identity of the data subject (often the person proffering the ID[9]) to an interested second party. In other cases the ID is evidence that the data subject has the permission or attribute that she asserts. In a third class of common cases, the ID serves primarily as an index that will link an identity to the outcome of a pattern-matching search, for example in data mining customer data or in predictive profiling for law enforcement.

More specifically, the facts that an ID, whether real or virtual, links to persons fall into four broad categories: (1) permanent personal attributes, (2) data about past activities, (3) data about the person's present, and (4) future-oriented information.[10] ID cards arguably provide benefits in managing and using data in each category. As others have made the case for these benefits in some detail, this part seeks only to organize and summarize the case for ID cards and comprehensive national databases and to note a few of the major practical arguments against centralized databases. Discussion of the civil liberties costs of collecting, aggregating, and indexing personal information is reserved for Part IV below.

A. Permanent Personal Attributes

Permanent personal attributes are things a person is born with and is unable to change. At least until gene engineering improves, that includes biometric identifier such as fingerprints,[11] retinas, and DNA.[12] Biometrics have the potential to play a double role in a national identification

---

[9]As noted below, there will be many circumstances, especially in the case of virtual IDs, in which the data subject not only is not proffering the ID, but is unaware that she is the subject of an inquiry indexed by the ID, or otherwise querying data collected and organized into one or more files about her.

[10]Admittedly, for some facts, there a degree of overlap, or even arbitrariness as to which category best applies. For example, an authorization to purchase cigarettes or alcohol based on age could reasonably be called a present fact about a person – the person is over 21. Indeed, while exact age is an ever-changing personal attribute, the attribute of being "over 21" reasonably could be called a fact about a person's past, or even (henceforth) a permanent personal attribute, at least so long as the person is alive.

[11]On the question of reliability of fingerprint see United States v. Llera Plaza, 179 F. Supp. 492 (E.D. Pa. 2002) and Jessica M. Sombat, *Latent Justice: Daubert's Impact on the Evaluation of Fingerprint Identification Testimony*, 70 FORDHAM L. REV. 2819 (2002) (citing United States v. Llera Plaza, 179 F. Supp. 492 (E.D. Pa. 2002)).

[12]Strictly speaking other commonly used biometric identifiers such as the face are not permanent, as they can be changed by surgery. The face also tends also to change due to the effects of age, and can be damaged beyond recognition in serious accidents.

Similarly, other data usually considered to fall in the permanent is at least theoretically changeable: the identity of one's parents can be changed by adoption; ethnicity, once thought to be

(continued...)

regime. First, a national ID card may either store or link to information about the data subject's body, including potentially sensitive genetic information. Second, the biometric information may serve as the identifying or authenticating information that links the person to the card.

1. Centralizing Biometric Data

DNA is a particularly powerful identifier. It is almost unique[13] and (so far) impossible to change. A number of state and federal databases already collect and keep DNA data on felons and others,[14] and there have been suggestions that the federal government should collect a DNA sample from every person arrested in the United States.[15] Such a plan is far from unthinkable—the Icelandic government is compiling a database containing medical records, genetic information, and genealogical information for all Icelanders other than those who specifically opt out.[16]

Centralizing genetic information offers numerous potential benefits, especially to law enforcement. DNA evidence is frequently recovered from crime scenes. In the best case, a national DNA database would allow police to match crime scene DNA to its database in order to identify

---

[12](...continued)
permanent, is increasingly seen as something of a social construct (and in the case of membership in Native American tribes can be legally altered by adoption).

[13]*See DNA Fingerprinting*, ENCYCLOPEDIA BRITANNICA ONLINE <http://search.eb.com/bol/topic?eu=31233&sctn=1&pm=1> (noting that DNA is usually unique with "the only exception being multiple individuals from a single zygote (e.g., identical twins)").

[14]The FBI Combined Index DNA Indexing System ("CODIS") alone currently contains information on 38,000 people. Approximately 450,000 samples await processing. *See* EPIC, *supra* note 36. *But see* Ng Kang-Chung, SOUTH CHINA MORNING POST, Feb. 12, 1999, *Legislators Fear DNA Test Plans Open to Abuse, available in* 1999 WL 2520961 (describing the Hong Kong legislature's fears of "allowing police to take DNA samples from suspects too easily").

[15]Under this proposal, DNA information would become part of a permanent, and sizable, national database: More than fifteen million people were arrested in the United States in 1997 alone. *See* Electronic Privacy Information Center ("EPIC"), Reno Proposes National DNA Database, EPIC Alert, Mar. 4, 1999 <http:// www.epic.org/alert/EPIC_Alert_6.04.html>.

[16]*See* The Icelandic Man Cometh, Bio IT World, http://www.bio-itworld.com/archive/011303/horizons_iceman.html (Jan 13, 2003) (reporting that one third of population had been sampled to date); SIMPSON GARFINKLE, DABASE NATION 193-95 (2000); Mannvernd, Association for Ethical Science, *The Health-Sector Database Plans in Iceland*, July 7, 1998 http://www.simnet.is/mannvernd/english/articles/27.11.1998_mannvernd_summary.html.

suspects.[17] Because current DNA technology uses predefined samples at specific points in the human genetic sequence, the DNA signatures used in matching are only probabilistically unique rather than absolutely unique. And, of course, the presence of a person's DNA at a crime scene does not prove guilt but only suggests presence at the crime scene.[18] Nevertheless, even a short list of matches would be sufficient reason to enquire whether the person identified had motive and opportunity to commit the offense. The prospect of vastly increased and more rapid identification of rapists is alone a powerful argument for the collection of DNA data.[19]

Whether DNA with possible health and employment implications[20] is added to a person's virtual electronic dossier is at present a separate question from whether DNA markers are collected. Currently, U.S. law enforcement share in a national policy to use only DNA markers selected from so-called 'junk' DNA--the parts of the genome which are not expressed in the body. As these parts of the genome have neither a positive nor a negative survival value, random changes or mutations are more likely to get passed down from generation to generation. Junk DNA is thus best suited for identifying familial relationships.[21] The decision to use junk DNA also results from the law enforcement community's conscious policy to avoid acquiring information with any health implications.[22] This policy of choosing DNA with no health implications insulates law enforcement from areas of health policy fraught with potential political conflict. It also represents a lost opportunity to provide a form of free genetic testing that might have health benefits--e.g. identifying predispositions to treatable diseases--for those whose DNA is sampled.

---

[17]See, e.g. Alan Dershowitz, *Identification Please*, BOSTON GLOBE, Aug. 11, 2002 at 14, available at 2002 WL 4142755; David H. Kaye, Michael Smith & Edward J. Imwinkelried, *Is a DNA Identification Database In Your Future?*, 16 CRIMINAL JUSTICE 4 (2001); Mark Rothstein & Sandra Carnahan, *Legal and Policy Issues in Expanding the Scope of Law Enforcement DNA Data Banks*, 67 BROOK. L. REV. 127 (2001). Ben Quarmby, *The Case For National DNA Identification Cards*, 2003 DUKE L. & TECH. REV. 2 (2003). But see Patricia A. Ham, *An Army Of Suspects: The History And Constitutionality Of The U.S. Military's DNA Repository And Its Access For Law Enforcement Purposes*, 2003-AUG ARMY LAW. 1 (July/August, 2003).

[18]It only "suggests" presence since there are scenarios in which DNA-bearing substances could be planted at the scene or could have drifted there by natural means.

[19]See, e.g. *UK Police Chief Calls for National DNA Database*, NATURE, May 14, 1998. But see Jeffrey S. Grand, *The Blooding Of America: Privacy And The DNA Dragnet*, 23 CARDOZO L. REV. 2277 (2002).

Note, however, that the presence of sperm recovered from a rape complainant is not proof of guilt, but only of intercourse.

[20][cites on controversies regarding genetic testing programs to come]

[21]See GARFINKLE, *supra* note 16, at 48-49.

[22][awaiting permission to cite personal communication]

2. The Body As Password

As technologies for distinguishing body parts such as irises, faces and fingerprints[23] improve, it seems increasingly attractive to use the "body as password."[24] Rather than base access to the individual's data on knowledge of a passphrase or a PIN, or on possession of a hardware token such as a smart card,[25] access can be conditioned on something unique about the person.

To the extent that reliance on biometric identifiers may prevent information from being stolen or improperly disclosed, it is a privacy-enhancing technology. Some banks already use iris scans to determine whether a person is entitled to withdraw money from an ATM.[26] The United States government uses biometric identifiers in the border crossing identification cards issued to aliens who frequently travel to and from the United States on business,[27] as do several states seeking to prevent fraudulent access to welfare and other benefits.[28]

---

[23]For a list of possibilities, see Java Card Special Interest Group, *Introduction to Biometrics* <http://www.sjug.org/jcsig/others/biometrics_intro.htm>.

[24]Biometrics can be used both for identification (who is this?) or authentication (what permissions does this person have?). *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) <http://www.registratiekamer.nl/bis/top_1_5_35_1.html> (discussing the various applications of biometrics).

[25]*See generally* Ontario Info. & Privacy Comm'r, *Consumer Biometric Applications: A Discussion Paper* <http://www.ipc.on.ca/web_site.eng/matters/sum_pap/papers/cons-bio.htm> (discussing biometrics, its benefits and concerns, and its effects on privacy); See Roger Clarke, Information Technology and Dataveillance, 31 Comm. ACM 498 (May 1988) (defining dataveillance as "the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons"), http://www.anu.edu.au/people/Roger.Clarke/DV/CACM88.html.

[26]*See, e.g.*, Guy Gugliotta, *The Eyes Have it: Body Scans at the ATM*, WASH. POST., June 21, 1999, at A1 <http://www.washingtonpost.com/wp-srv/national/daily/june99/scans21.htm>.

[27] *See* 8 U.S.C.A. § 1101(a)(6); Theta Pavis, *U.S. Takes Immigration in Hand*, WIRED, Sept. 15, 1998 <http://www.wired.com/news/news/technology/story/15014.html> (describing INSPASS system, which relies on handprints).

[28]*See* JOHN D. WOODWARD, JR., U.S. DEP'T OF COMMERCE, COMMENTS FOCUSING ON PRIVATE SECTOR USE OF BIOMETRICS AND THE NEED FOR LIMITED GOVERNMENT ACTION § II.B (1998) <http://www.ntia.doc.gov/ntiahome/privacy/mail/disk/woodward.htm> ("Arizona, California, Connecticut, Illinois, Massachusetts, New Jersey, New York and Texas are using finger imaging to prevent entitlement fraud. Florida, North Carolina and Pennsylvania have biometric operational systems pending."); Connecticut Department of Social Services, *Digital Imaging: Connecticut's*

(continued...)

Despite their potential uses as privacy-enhancers, biometrics have disadvantages as a personal identifier and as the 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 a biometric identifier, the more it is likely to be used, and the greater the amount of data likely to be linked to it.[29] Because a biometric is a part of the person, it can never be changed. It is true that current indexes, such as social security numbers, are rarely changed, which is why they are popular indexes, but in extreme cases one can leave the country or join a witness protection program. As far as we know, changing an iris or a fingerprint is much more difficult.[30] Second, some biometrics, particularly those that involve DNA typing, could disclose extraneous information about the data subject, such as race, sex, ethnicity, propensity for certain diseases, and (as the genome typing improves) even more.[31] Others may provide the capability to detect states of mind, truthfulness, fear, or other emotions.[32]

Whether or not it uses biometrics, a national ID card that uses reliable data,[33] and is

---

[28](...continued)
*Biometric Imaging Project* <http://www.dss.state.ct.us/digital.htm> (providing links to extended descriptions of biometrical imaging of AFDC and General Assistance recipients for identification purposes).

[29]*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) <http://www.ipc.on.ca/web_site.eng/matters/sum_pap/PAPERS/biometric.htm>.

[30]However, there is some evidence that fingerprint recognition systems can be fooled by a fake gelatine finger. See BBC News, *Doubt cast on fingerprint security* (May 17, 2002), http://news.bbc.co.uk/1/hi/sci/tech/1991517.stm ("Fake fingers made out of common household ingredients can fool security systems that use fingerprints to identify people").

[31] *See id.* at § 4. In addition, some people, for religious or personal reasons, find submitting to a biometric testing to be unacceptable. Even if the scan does not require a blood sample or other physical invasion, it may encroach on other sensibilities. *See* Ontario Info. & Privacy Comm'r, *supra* note 136, at text following note 168 ("Having to give something of themselves to be identified is viewed as an affront to their dignity and a violation of their person. Certain biometric techniques require touching a communal reader, which may be unacceptable to some, due to cultural norms or religious beliefs.").

[32]*See* Dutch Data Protection Authority (Registratiekamer et al.), *supra* note 137, §§ 2.2-2.3.

[33]This assumption elides important issues which are examined in the NRC REPORT, *supra* note 1.

sufficiently tamper-proof, and secure[34] to reliably identify and authenticate the holder would be valuable in a host of both public and private transactions, from public benefits to banking, from building security to -- so long as the CAPS identification program is in place -- the authorization to board commercial airlines. The average middle-class American now carries an array of plastic and paper identifiers in her wallet. Some of these identifiers, such as credit cards for example, do more than just identify the holder, they also indicate an authorization for future action--in the case of the credit card, a credit line. (The authorization aspect is discussed in Section D below.) Some forms of authorization are independent of identity, for example a movie ticket that says "Admit One," but authorization is increasingly tied to identity. The people who control resources, whether it is admittance to a building or the sale of a security not only want or need to know who you really are in order to allow the interaction or transaction, but they want or need to keep a record of it as well.

B. Past Attributes

Past attributes are facts about a person's life activities. They differ from permanent attributes in that they are not congenital, and ordinarily not biometric either.[35] Examples include medical data, employment and criminal history, and legal or economic facts such as insurance claims, civil litigation, bankruptcies, and transaction history.

1. Health

The costs and benefits of centralizing health records have been extensively canvassed in the debates over the Health Insurance Portability and Accountability Act of 1996 (HIPAA) privacy rules.[36] Patients, especially accident victims and others unable to provide their medical histories when needed, obviously benefit from a system that may make life-saving information accessible to emergency medical personnel. Centralizing medical information can also make new types of longitudinal and other statistical medical research practicable, which may have important benefits for the entire population. On the other hand, if medical data is to be available to emergency responders then it cannot be protected as thoroughly as other data since there exists a large and varied group of persons who may need it. Combine this group with the participants in the medical payments system and medical data may be widely shared indeed.[37] Once collected, and especially once circulated to the participants in the health care delivery system, the data are likely discoverable

---

[34]This is far from easy. See generally BRUCE SCHNEIER, SECRETS AND LIES (2003). *If* the card were secure, tamper-proof, and difficult to counterfeit then it would vastly reduce the risk of identity theft.

[35]Again, it bears mentioning that there are always borderline cases, such as a lost limb, which could reasonably be described as either a (henceforth) "permanent," "past" or "present" condition.

[36]See, e.g., Peter Swire & Lauren Steinfeld, *Security and Privacy After September 11: The Health Care Example*, 86 Minn. L. Rev. 1515 (2002) [cites to come]

[37]See generally Mike Hatch, *The Privatization of Big Brother: Protecting Sensitive Personal Information from Commercial Interests in the 21st Century*, 27 WM. MITCHELL L. REV. 1457(2001).

in litigation.[38]

2. Employment and Criminal History

Many employers conduct background checks on employees. Most state require checks for criminal histories for day care workers and teachers.[39] Centralizing employment and criminal records would facilitate these checks, and improve their quality.

The United States does not have a general social policy of allowing convictions to become 'spent' as do many Commonwealth countries, although there are provisions for expungement of some convictions.[40] Streamlining and centralizing criminal background checks could also lead to an increase in them, which might make it more difficult for people to put their past behind them. Even when convictions are expunged, they may not be removed from every file.[41]

3. Transactions/Payment History

As storage and information retrieval costs drop, it becomes increasingly possible to imagine a world in which all transactions of any economic importance are recorded and stored. It could be possible to construct a near-real-time model of the entire economy. An essentially accurate 'model'

---

[38]See Johanna G. Averill, *HIPAA Privacy Rules*, 51 LA. B.J. 280 (December, 2003/January, 2004).

[39]See U.S. Department of Justice, Office of Juvenile Justice and Delinquency Prevention, *Guidelines for Screening of Persons Working With Children, the Elderly, and Individuals With Disabilities in Need of Support* 9 (1998), at http://www.ncjrs.org/pdffiles/167248.pdf.

[40]See, e.g. UK Rehabilitation of Offenders Act 1974; Australian Commonwealth Spent Convictions Scheme, http://www.privacy.gov.au/act/convictions/.

The Arizona Republic recently discovered that the 74-year old Chairman of the Smith & Wesson Holding Corporation spent more than a decade in prison for using a sawed-off shotgun to commit holdups in the 1950s, forcing his resignation from the Chairmanship. See Greg Schneider, *Gunmaker Supports Ex-Chairman: Director Committed Holdups in 1950s*, Washington Post, E01, February 28, 2004. James Minder had been known as the "Shotgun Bandit". Vanessa O'Connell, *Smith & Wesson chief's past returns*, http://www.baltimoresun.com/business/bal-smithwesson031504,0,3033057.story?coll=bal-business-headlines . It appears that no one at Smith & Wesson had ever thought to ask a man who had by then founded a company that helped special needs children and spent two decades doing philanthropic work about his earlier life. Nor is it obvious that even his serious criminality decades earlier lessened his suitability for the job in light of his subsequent good works.

[41]See, e.g. Daniel D. Blinka & Thomas J. Hammer, Supreme Court Digest, 75-AUG Wis. L. 33, 34 (2002) (noting that Wisconsin law does not require district attorneys and law enforcement agencies to expunge their records documenting the facts underlying an expunged conviction record). See also infra, text at note -.

of the economy would be valuable for economic forecasting and planning.[42] An accurate record of every firm and indeed every resident's income and expenditures would also make perfect tax assessment possible. Instead of relying on decreasingly reliable self-reporting,[43] the government could simply send out accurate annual tax bills in early January.

C. Present Facts

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 she is bringing to the checkout counter, or the speed at which she is driving her car.

Present facts differ from past facts in that they are subject to change. For example current ownership of one's home is present fact, one subject to change if the home is sold, given away, or otherwise alienated. In contrast, last year's purchase of that real property or of a chattel is a fact which cannot be changed.[44] Present facts about a person include citizenship, current employment, martial status, religion, residence, salary, and visas.

Accurate information about present facts, both persistent and transitory, are of obvious interest to both 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 make linking the transaction data to the holder's file easy. Linking CCTV and other camera data to a person would require either more sophisticated facial recognition techniques than currently exist or some other means to identify people at a distance.[45]

---

[42]In due course it might be possible not only to record statistical regularities and correlations but even to identify economic linkages and build a full-scale Leontief model of the economy. Cf. WASSILY W. LEONTIEF, INPUT-OUTPUT ECONOMICS (2nd ed. 1986); INPUT-OUTPUT ANALYSIS: FRONTIERS AND EXTENSIONS (Michael L. Lahr & Erik Dietzenbacher eds. 2001); Wassily W. Leontief, *Input-Output Economics*, SCIENTIFIC AMERICAN, October 1951, at 15; Wassily W. Leontief, *The Structure of the U.S. Economy*, SCIENTIFIC AMERICAN, April 1965, at 25.

[43]Tax cheating is rising. See Jonathan Weisman, *GAO Finds Increase in Tax Evasion*, Washington Post (Dec. 19, 2003), http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A13403-2003Dec18&notFound=true;Crackdown on Tax Cheats Not Working, Panel Says, New York Times (October 20, 2003), http://query.nytimes.com/gst/abstract.html?res=F30D15F73B5A0C738EDDA90994DB404482.

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

[45]One possibility would be to put an RFID emitter on the ID card. In this scenario, the card
(continued...)

Location information is especially valuable to law enforcement: current location information allows police to locate a suspect and stored location information makes possible a wide variety of enforcement techniques.[46] At its most benign, full location information would make it relatively easy to investigate street crime. If the mugging happened at 10:05pm at the intersection of Elm and Main streets, and stored location data allows 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 tracking each of them down will not be difficult. The availability of other biographical information (e.g. age, employment) may also allow the police to prioritize their investigation if the list is long. For example, if the victim describes the mugger as a 20 year old male, there is little reason to interview women and the elderly who happened to be nearby at the relevant time.[47]

Information about assets and transactions is of great interest to both the public and private sectors. Merchants want assurances they will be paid; creditors want assurances that assets exist, and about credit ratings. Firms are interested in capturing marketing data in order to build consumer profiles and to track what sells where to whom. Even in the absence of perfect tax administration,[48] the government can use transaction data to check whether people are spending more money than they admit to earning or having. More accurate identification of participants in the financial system can help identify and prevent money laundering.[49]

---

[45](...continued)
would not only be an ID when presented, but an 'always on' annunciator of identity. Such a device would be, I think, highly unpopular and -- unlike the card itself -- would represent a radical reduction in personal privacy compared to the current or likely status quo. I am not advocating RFID chips on ID cards.

Each RFID chip has a unique signature. If RFID chips become ubiquitous on clothing and other common goods, and if it becomes commonplace to link this information to a purchaser at the time of sale, perhaps as a theft-prevention measure (if, say, your coat is stolen, the RFID tag can be put on a watch list and if it ever triggers a detector the police can be contacted automatically), then the issue becomes moot since everything we own will become a defacto annunciation of our identity at least to those equipped with the right sort of detector.

For an extreme, but amusing, vision of the next step beyond RFID, see David Brin, 2020 VISION: Journalism the Day After Tomorrow, http://www.ojr.org/ojr/workplace/1078288485.php

[46]Location data is also of interest to private marketers; for example, a store may wish to send text messages to advertise to the cell phones of shoppers walking in the vicinity. Aggregate data on shopping patterns may also be of interest to marketers seeking to decide where to locate a store.

[47]The danger, of course, is the creation of the equivalent of a 'usual suspect bit'. See infra text at note -.

[48]See supra text at note 43.

[49]This was one of the justifications proffered by the UK government in support of its national
(continued...)

D. Future (Authorizations)

A security guard recording who enters a building open to all may rely on ID cards as proof that people are who they say they are. More commonly, however, the purpose of an identity confirmation is to determine whether the person is authorized to do something. Thus, for example, a debit card's PIN number provides a limited assurance that the person holding the card is entitled to use 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.

Indeed, authorizations, even more than identification, are likely to be a prime function of a robust national ID card scheme. The card can be used to authenticate registered voters, and to note whether the holder has already voted. It can identify who is eligible for jury duty.[50] Some goods such as alcohol and cigarettes can only be sold to persons over a given age, and some films and magazines are restricted to adults; a card can verify age, or just the state of being "over 21". A card can confirm eligibility for government benefits. Standardizing identification a single national ID card that is difficult to forge would also make it easier to identify benefit fraud..[51]

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

---

[49](...continued)
ID card proposal. See UK Home Office, David Blunkett: *National ID Card Scheme To Be Introduced*, Nov. 11, 2004, http://www.homeoffice.gov.uk/n_story.asp?item_id=675.

[50]A ubiquitous national ID system would provide a better source of jurors than voter rolls or driver's licenses.

[51]See Philip Redfern, *Precise Identification Through a Multi-purpose Personal Number Protects Privacy*, 1 INT'L. J.L. & INFO. TECH. 305, 312 (1994) (arguing that precise personal identifiers used in Sweden, Norway, Finland and Denmark, enable certain efficiencies within the administration of government: one being that the citizen is only required to remember one number; the single identifying number reduces the likelihood of false identifications and duplicate registrations which are commonplace when cross-checking personal data embedded in a system where different numbers are used by multiple agencies); R. Brian Black, *Legislating U.S. Data Privacy in the Context of National Identification Numbers: Models From South Africa and the United Kingdom*, 34 CORNELL INT'L L.J. 397, 444 (2001); Electronic Privacy Information Center, *Poverty and Privacy* (Aug. 20, 2003) (noting that electronic benefits systems and computer matching systems, despite invasion of privacy concerns, serve important state interests; allowing the government the ability to track welfare recipients spending patterns as a means of combating fraud), *available at* http://www.epic.org/privacy/poverty/.

work of all new employees.[52] Critics of this rule argue that the employer sanctions for hiring undocumented aliens creates an incentive for employers to discriminate against legal Hispanic workers and others whom employers might fear are not citizens.[53] A national system of employee identification would put all legal workers on an even footing thus reducing any potential discrimination, reduce any paperwork burden that might be worrying employers, and would also make it easier to ensure that employees received the social security and other benefits to which they are entitled. An efficient and sure method of verifying eligibility to work would make life more difficult for illegal aliens, reducing the benefits of illegal immigration--an outcome which must be treated as a benefit so long as the US retains its immigration laws.

Using a single national identification system to establish the right to do something (e.g., work) creates leverage over most people's economic affairs that can be used to achieve social goals that may not always be directly relevant to the activity itself.[54] One byproduct of the Welfare Reform Act has been the creation of interconnected databases at the local, national and international levels; based on standardized data elements (names, social security and other uniform identification numbers). 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.[55] In theory, any social policy could be enforced

---

[52]*See* 8 U.S.C. § 1324a(a)(1)(B) (1996) (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 .

[53]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).

[54]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).

Presumably there would be an outcry if failure to pay parking tickets were sufficient cause to be denied employment, but there might be less of an outcry if this employment information were used to deduct the cost of unpaid parking tickets (and penalties) at source.

[55]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) (noting the increases in efficiency expected from recent changes made to state law regarding child and spousal support payments as mandated by the Welfare Reform Act of 1996; the source of these newfound efficiencies is a series of databases (operating in unison) which are used to track non-custodial parents who fail to fulfill their court ordered obligations to pay child or spousal support); Valerie Collins, *Identity Cards and Numbers: the Debate Continued*, 10 INTERNATIONAL REVIEW OF LAW, COMPUTERS AND TECHNOLOGY 142 (1996) (noting the argument (continued...)

in a similar manner--producing the danger of creating a class of unemployables.[56]

Already both states and the federal government are using public information to stigmatize offenders. Megan's law was only the beginning.[57] In Miami-Dade county, for example, anyone with access to the Internet can visit the county government's "sexual offender/predator" neighborhood search tool,[58] a part of the "My Neighborhood" initiative. From a handy dropdown menu the concerned citizen can choose to view local maps -- updated on a daily basis -- annotated with dots, each representing a convicted sex offender's residence. Clicking on the list in the left column brings up each offender's photo, a physical description, and an exact address.[59]

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,[60] to enforce licenses that only allow copyrighted (or even public domain) content they provide to be viewed by paying

---

[55](...continued)
that a universal personal identifier would make it much easier to 'relate or merge' information about a single individual contained in different public records, such a system would likely yield large gains in administrative efficiency).

[56]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.

[57] See Megan's Law, N.J. Stat. Ann. § 2C:7-1 to 7-11 (West 2004) (registration of sex offenders); Violent Crime Control and Law Enforcement Act of 1994, Pub. L. No. 103-322, 108 Stat. 2038 (1994) (codified as amended at 42 U.S.C.A. § 14071(federal equivalent of Megan's Law).

[58]http://gisims2.co.miami-dade.fl.us/MyNeighborhood/seop.asp?Cmd=INIT

[59]Id.

[60]See Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981 (1996) <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) <http://www.law.georgetown.edu/faculty/jec/Lochner.pdf>; Julie E. Cohen, *Some Reflections on Copyright Management Systems and Laws Designed to Protect Them*, 12 BERK. TECH. L.J. 161 <http://www.law.berkeley.edu/journals/btlj/articles/12_ 1/Cohen/html/text.html>.

customers. 'Trusted computing'[61] initiatives will prevent computers and other devices from making copies, or even displaying information, without permissions set by the right-holders, trumping the wishes of the operator/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.

Although touted as a means of preventing or deterring terrorism, the real benefits of a national ID system probably lie elsewhere, in crime solving, government benefits (and tax) administration, and in private commercial applications, at least in the foreseeable future. The security benefit from an ID card regime depends as an initial matter on the quality of the data input into the system, and secondarily on the extent to the cards are secure and difficult to forge. The first problem alone is enormous as current US identification data is notoriously poor. Passports, drivers licenses and social security cards can all be obtained with an appropriate birth certificate, or with documents obtained upon presentation of a birth certificate. And birth certificates are notoriously easy to forge or obtain.[62] Similarly, unless there are very substantial improvement in data quality, an ID card regime will provide little additional security against competent foreign terrorists: after all, almost all of the 9/11 hijackers were in the US legally and had no record with the FBI or other security agency. "They could have obtained a legitimate ID card and the authentication checks prior to boarding the plane would have not have revealed anything that would have aroused the suspicions of authorities."[63] Biometric identifiers contribute to the reliable solution of the domestic data quality problem only if they are collected at birth; the correct identification of foreign visitors depends on quantity and quality of data available from foreign sources.

If we started tomorrow, it would still take years, perhaps an entire generation, to achieve reliable biometric identification of everyone born in the USA, not to mention immigrants and visitors. In the interim, the greatest benefits of a national ID card regime are likely to be in 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.[64] These too are valuable benefits.

---

[61]See Chad Woodford, *Trusted Computing Or Big Brother? Putting The Rights Back In Digital Rights Management*, 75 U. COLO. L. REV. 253 (2004).

[62]See NRC Report, *supra* note 1.

[63]Andrew Clement et al., *National Identification Schemes (NIDS) and the Fight against Terrorism: Frequently Asked Questions*, Would a NIDS have prevented the Sept. 11 attacks?, http://www.cpsr.org/program/natlID/natlIDfaq.html#Q3.

[64]For example, profiling of customers could enable 'perfect junk mail' -- sending only advertisements that have a high probability of interesting the recipient. See Froomkin, *supra* note 66 at -.

## III. The Privacy Baseline: Lousy and Getting Worse

Opponents of national ID cards often express the fear that any regime that requires and standardizes ID cards will create new opportunities for abusive law enforcement tactics. Some of these arguments are little more than appeals to fears that seem to find their enduring images from black-and-white movies -- 'Nazis, guns, dogs, trains' -- but the power of these appeals demonstrates that the fear is real and enduring.

A national ID system could have substantial costs including possible effects on liberty, on transactional freedom, and on socio-political psychology, not to mention the increased scope for possible misuses by government officials.[65] In its most likely forms, a national ID system could also contribute to the continuing erosion of personal privacy,[66] but a harmful effect on privacy is not inevitable. At least in theory, it should be possible to design a national identification numbering system that might enhance personal privacy in the US. Alas, the potentially privacy-enhancing features of national ID cards discussed in this paper likely are not large enough to outweigh the other costs of a national ID system.[67] They are also somewhat politically unlikely. If, however, a national ID regime is adopted despite the real liberty dangers, there may be a fall-back political strategy aiming to minimize privacy costs, and perhaps even create some privacy gains.

In order 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 paper 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'. Any merchant or government agency willing to make a small investment will be able to pull up a rich file on an individual keyed to some existing form of identification, perhaps a driver's licence or a credit card, or perhaps even a biometric.[68] A related claim is that the

---

[65]See *infra* text at notes --. Neither the danger from private snooping by low-level employees nor the threat of more organized abuse of the sort associated with J. Edgar Hoover should be ignored.

[66]*See generally* A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461 (2000), available online http://www.law.miami.edu/~froomkin/articles/privacy-deathof.pdf

[67]Proponents of a national ID system shoulder a heavy burden. *See* NRC REPORT, *supra* note 1, at 46 (stating, "the committee believes that proponents of a nationwide identity system should be required to present a very compelling case"); Richard Sobel, *The Degradation of Political Identity Under A National Identification System*, 8 B.U.J. SCI. & TECH L. 37 (2002).

[68]Legislation introduced in May by Rep. Jim Moran and Tom Davis, would mandate biometric data chips in driver's licenses, *see supra* note ?. On biometrics, see e.g. John D. Woodard, *Biometric Scanning, Law & Policy: Identifying the Concerns--Drafting the Biometric Blueprint*, 59 U. PITT. L. REV. 98 (1997). John D. Woodward, Jr., *Biometrics: Identifying Law and Policy* (continued...)

development of the technologies and practices that enable a de facto national identification system are decentralized and a mix of public and private, including everything from DNA databases[69] and facial recognition data to Microsoft Passport and the US government's plan to offer citizens a single number which they could use to authenticate themselves to multiple government agencies.[70] The technical and institutional variety of these data collection and collation systems makes it extremely difficult, perhaps impossible, for any proposed privacy enhancing technology, e.g. P3P, to address more than a fraction of the threats to privacy. Similarly, experience suggests that any legislative solution is likely to be piecemeal at best, and probably quite limited.[71]

If this is an accurate assessment, it is at least theoretically possible to design a national ID system that would enhance privacy rights above those enjoyed in a 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 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 make travel abroad easier.

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 designed in by giving the individual a property right in at least some of the data held in government files. The ownership and dissemination of private

---

[68](...continued)
*Concerns* in BIOMETRICS: PERSONAL IDENTIFICATION IN NETWORKED SOCIETY 386 (Anil Jain Ed. 1999); Richard Hopkins, *An Introduction to Biometrics and Large Scale Civilian Identification*, 13 INT'L REV. L. COMPUTERS & TECH. 337 (1999).

[69]The extent to which a country can go to establish a national DNA database is demonstrated by the Icelandic government's decision to create a databank of all citizens except those who op-out, based in large part on existing medical records. See Simpson Garfinkle, Dabase Nation 193-95 (2000). On DNA databases in the US and elsewhere see, e.g., *DNA Databases: When Fear Goes Too Far*, Note, 37 Am. Crim. L. Rev. 1219 (2000); *An International DNA Database: Balancing Hope, Privacy, and Scientific Error*, Note, 24 B.C.Int'l & Comp.L.Rev. 341 (2001).

[70][ACES discussion to come]

[71]E.g. the Gramm-Leach-Bliley Financial Modernization Act of 1999. The Act requires companies to give consumers privacy notices explaining the institutions' information-sharing practices. In turn, consumers have the right to limit some - but not all - sharing of their information. See http://www.ftc.gov/bcp/conline/pubs/buspubs/glbshort.htm. A number of firms have designed their privacy notices to be incomprehensible or even meaningless. See Eric Poggemiller, *The Consumer Response To Privacy Provisions In Gramm-Leach-Bliley: Much Ado About Nothing?*, 6 N.C. BANKING INST. 617 (2002).

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 which had been so indexed.[72]

The privacy rules restricting the use of indexed information would be set nationally. While this creates a focal point for regulation, it also inevitably creates 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.

A national ID system does not require tangible national ID cards, although the two go together easily. Indeed, 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.[73] Government data practices are regulated by the Privacy Act, but these limits do not apply to law enforcement,[74] 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[75] – subject to a possible backlash from the public.[76]

---

[72]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).

[73]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- 2725 (2002); Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6503 (2002); Privacy Act of 1974, 18 U.S.C. §§ 2510-2522, 2701-2709 (2002); Electronic Communications Privacy Act of 1986, 5 U.S.C. § 552a (2002).

[74]5 USC § 552A

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

[76]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*, Feb. 7, 1999 (continued...)

Writing in 1986, Joseph W. Eaton stated, that "on a *de facto* basis, the United States already has a national ID system."[77] At the time, and to some extent today, this "system" consisted of a hodgepodge of different identifiers including birth certificates, state-issued ID's such as driver's licenses, social security numbers (SSNs), passports, credit cards and credit scores. Today, not only is there a defacto national ID system, but the richness and detail of the data it includes dwarfs anything available almost two decades ago. Furthermore, although far from completely standardized, the identifiers in use are less heterogenous than they were 20 years ago, and due to the vast improvements in data processing technology are increasingly linked to each other.

Four synergistic sets of changes have enormously increased the coverage and scope of our 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 the these developments. The result is a hybrid public-private system in which a very great amount of information about almost every US resident is available for a small fee. It may be that much of this information remains distributed on separate networks, but the technology to tie them together exists, as do plans to bring it together in the very near future. Relative invisibility is a salient feature of this system, one which results from its 'virtual' nature and the patchwork manner in which it has come into being.

A. Legislative Developments

The modern history of federal and state identification numbers is one of both function creep and intentionally broadened scope.

The US introduced a national pension system in 1936, which brought with it the Social Security number (SSN). The SSN is now, along with state drivers licenses, and birth certificates, one of the most common identity documents in the US.[78] Since 1936 "there have been almost 40

---

[76](...continued)
ZDNET NEWS, available at http://zdnet.com.com/2100-11-513639.html?legacy=zdnn.

[77]JOSEPH W. EATON, CARD-CARRYING AMERICANS 2 (1986). See also id at 82-84.

[78]See generally, United States General Accounting Office, Government and Commercial Use of the Social Security Number is Widespread (Letter Report, February 1999).

congressionally authorized uses for it as an identification number."[79] Before 1973, a US citizen tended to acquire a social security number if he or she joined the wage-earning workforce. Today, most US citizens get their SSN at birth, since the IRS requires their parents to list the SSN of every child from whom they wish to claim a dependent tax credit.[80] The social security database does not completely identify all US residents, since some older couples share a single number. Social Security cards and numbers are notoriously easy to forge or steal, and as a result these are not considered a particularly reliable form of identification.

Since the right to work in the United States depends on the worker's legal status, which the worker must prove by proffering a document, a number of legislative initiatives in the last fifteen years have sought to improve the reliability of these documents and of the monitoring of hiring practices. The current regime began with the Immigration Reform and Control Act of 1986 ("IRCA")[81] required employers to make workers prove that they are U.S. citizens, green card holders, or have a work visa. Would-be workers must fill out and sign an I-9 verification form and provide government identification, such as a passport, in order to work.[82] Under IRCA the employer kept the I-9 on file for possible inspection rather than submitting it to a federal agency which mean that there was no serious control in place to monitor the use of false documents. In contrast, the Illegal Immigration Reform and Immigrant Responsibility Act of 1996[83] ("IIRIRA"), established a five-state "Pilot Program" of computerized SSN verification, and also mandated the development

---

[79] Sobel, *supra* note 67, at 56 (citing 145 Cong. Rec. E3 (daily ed. Jan. 6, 1999) (statement of Hon. Ron Paul)).

[80]Internal Revenue Service Restructuring Act of 1998, Pub. L. No. 105-206, § 6021(c), 112 Stat. 685, 824 (1994) (codified as amended at 26 U.S.C. § 32(c)(3)(D)(i) (2000)). See generally GAO Report, Sobel, *supra* note 67, at 56-57.

[81]Immigration Reform and Control Act of 1986, Pub. L. No. 99-603, 100 Stat. 3359 (1985) (codified as amended in scattered sections of 8 U.S.C.).

[82]Employers may be fined up to $10,000 per violation for employing undocumented aliens 8 U.S.C. § 1324a(e)(4) (2000) and six-months in prison if they demonstrate a pattern of hiring unauthorized aliens. See generally Michael Crocenzi, Note, *IRCA-Related Discrimination: Is It Time to Repeal Employer Sanctions?*, 96 DICK. L. REV. 673 (1992). Requirements were stiffened by the IIRIRA, under which employers may no longer verify that its employee is authorized to work by examining a certificate of U.S. citizenship, certificate of naturalization, or unexpired foreign passport as proof of eligibility to work. IIRIRA requires that employers demand a U.S. passport, a green card, or an alien registration card.

[83]Pub. L. No. 104-208, 110 Stat. 3009-546 (1996) (codified as amended in scattered sections of 8 U.S.C.)

of prototype counterfeit-resistant social security cards.[84] IIRIRA also requires that birth certificates and driver's licenses be standardized.

Similarly, the Personal Responsibility and Work Opportunity Reconciliation Act of 1996,[85] established a central federal registry of newly hired employees at the Department of Health and Human Services (HHS). HHS collects the names, addresses, SSN and wages for everyone hired after the effective date in order to help law enforcement officials in locate parents who fail to pay court-ordered child support.[86] Although this database only has information on persons all hired after October 1, 1997, eventually it will include the entire labor force.

Nearly everyone interacts with the health care system. The Health Insurance Portability and Accountability Act of 1996[87] (HIPPA) envisions the creation of a "unique health identifier" and the creation of a national electronic data collection system for personal health care data. The national health identifier is designed to enable tracking of patients, health care providers, health plans, and treatment events, and particularly to ease portability of health care when workers change jobs. Although the Clinton administration proposed some privacy rules that would have made it more difficult to share medical information without the patient's consent, the Bush administration recently announced its intention to eliminate the most significant privacy protections surrounding that database.[88]

Air travelers are profiled by a $2.8 billion monitoring system that uses a secret algorithm to

---

[84]The Welfare Reform Act requires on the Social Security Administration ("SSA") to "harden" the social security card.

[85]Pub. L. No. 104-193, 110 Stat. 2105 (1996) (codified in scattered sections of 42 U.S.C.).

[86]There are approximately 7 million outstanding child support orders, Sobel, *supra* note 67, at 59 n. 133 (citing U.S. Bureau of the Census, Apr. Current Population Survey: Child Support for Custodial Mothers and Fathers, Oct. 2000, available at http:// www.census.gov/hhes/www/ childsupport/cs97.html).

[87]Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified at scattered sections of 26, 29, and 42 U.S.C.)

[88]"The administration decided to abandon the core of the Clinton rules, a requirement that doctors, hospitals and other health care providers obtain written consent from patients before using or disclosing personal medical information for treatment or paying claims. Instead, providers will have to notify patients of their remaining rights and have to make "a good-faith effort to obtain a written acknowledgment of receipt of the notice." Robert Pear, *Bush Rolls Back Rules on Privacy of Medical Data*, New York Times (Aug. 10, 2002) http://www.nytimes.com/2002/08/10/politics/ 10PRIV.html . See http://www.hhs.gov/ocr/hipaa/finalreg.html Department of Health and Human Services, Standards for Privacy of Individually Identifiable Health Information; 67 Fed. Reg. 53181 (August 14, 2002).

compare their personal data to profiles of likely terrorists.[89] The CAPS (computer-assisted passenger screening) system operates off the computer reservation systems utilized by the major United States air carriers as well as some smaller carriers. Before 9/11, at least, CAPS relied on information that passengers provide to air carriers, and was not connected to law enforcement or intelligence databases.[90] This system is currently the subject of a lawsuit by John Gilmore, who claims the government, under CAPPS II, is preparing to combine travel booking and payment information with data from banks, credit-reporting agencies and other sources and integrate it with lists of suspected terrorists and criminals.[91]

Federal, state and local governments also collect data from a total of about 15 million arrestees each year.[27] The FBI alone "maintains fingerprint and other personal information on roughly 30 percent of the population."[92] Increasingly, data collected by law enforcement agencies includes digitized biometric information, including DNA profiles.[93]

After tax returns and the census, both of which are subject to special privacy protections,[94] one of the most widespread governmental data collection devices is driver's license applications. Most of the US adult population holds a driver's licence, at least outside a few major cities with efficient mass transportation networks. In addition to requesting personal data such as address, telephone number and basic vital statistics, some states collect health-related information, and all

---

[89]See Declan McCullagh, You? A Terrorist? Yes!, Wired, Apr. 20, 1999 <http://www.wired.com/news/news/politics/story/19218.html>

[90]See Security of Checked Baggage on Flights Within the United States, 64 Fed. Reg. 19220, 19222 (1999) (Apr. 19, 1999) [updated cites coming]l John Gilmore: Free to Travel, 28 Privacy Journal 1 (Aug. 2002).

[91]See http://www.freeetotravel.org (detailing *Gilmore v. U.S.* challenge to CAPS airline flyer identification program).

[92]Eaton, *supra* note 77 at 104.

[93]See, e.g. Roe v. Boscoe, 193 F.3d 72 (7th Cir. 1999) (upholding Conn. Gen. Stat. §54-102g, requiring all convicted sex offenders to submit blood sample for analysis and inclusion in DNA data bank on "special needs" exception to ordinary warrant requirment); Gaines v. Nevada, 998 P.2d 166 (Nev. 2000) (upholding Nevada statute requiring DNA samples from persons convicted of wide variety of felonies including murder, mayhem, administration of poison, battery, elder abuse or neglect, home invasion, burglary, and sex offenses).

[94]Although the IRS Code, 26 U.S.C. § 6103 (1988 & Supp. V 1993), provides for the confidentiality of tax returns, one commentator has described this restriction as "quite permeable." Steven A. Bercu, *Toward Universal Surveillance in an Information Age Economy: Can We Handle Treasury's New Police Technology?*, 34 JURIMETRICS J. 383, 429 (1994); see also Privacy Act, 5 USC § 552a; FOIA, 5 USC § 552; 26 CFR § 601.702.

require an (often digitized) photo. The importance of this data led Congress to protect it in the Drivers Privacy Protection Act (DPPA),[95] which prohibits the release of personal information about an individual obtained by the department in connection with a motor vehicle record. An amendment to the DPPA requires states to get permission from individuals before their personal motor vehicle record may be sold or released to third-party marketers. The Supreme Court upheld the DPPA against a federalism challenge in Reno v. Condon.[96] The *Condon* decision is especially significant because it suggests that the federal data privacy rule attached to a national ID card proposed below could constitutionally be applied to states, as it would regulate them "as the owners of databases."[97]

B. Vastly Increased Data Collection

Most economic transactions other than those paid for in cash create identifiable transaction data. Businesses seek to access the data to 'mine' it for sales leads and other profitable information.[98] And the federal government combs similar data to find possible tax cheats,[99] and other suspected lawbreakers.[100] Market consolidation having tended to reduce the number of firms providing credit information, the size and coverage of the databases under the control of the larger firms has grown. Today, one firm, Acxiom, holds personal and financial information about almost every United States, United Kingdom, and Australian consumer.[101] In many cases, banks and other financial service providers collect information about their clients because the data has commercial value. Indeed, some firms that capture large volumes of transactional information now consider data to be

---

[95]18 U.S.C. § 2721.

[96]528 U.S. 141 (2000).

[97]Condon, supra.

[98]See Ann Cavoukian, Info. and Privacy Comm'r/Ontario Data Mining: Staking a Claim on Your Privacy (1998) <http://www.ipc.on.ca/web_ site.eng/matters/sum_pap/ PAPERS/datamine.htm>.

[99]See, e.g., David Cay Johnston, New Tools for the I.R.S. to Sniff Out Tax Cheats, NY Times, Jan. 3, 2000 <http:// www.nytimes.com/00/01/03/news/financial/irs-tax.html> ("The [data mining] technology ... being developed for the I.R.S.... will be able to feed data from every entry on every tax return, personal or corporate, through filters to identify patterns of taxpayer conduct. Those taxpayers whose returns suggest ... that they are highly likely to owe more taxes could then quickly be sorted out and their tax returns audited."); see also Steven A. Bercu, Toward Universal Surveillance in an Information Age Economy: Can We Handle Treasury's New Police Technology?, 34 Jurimetrics J. 383, 400-01 (1994) (discussing FinCEN and possible privacy problems).

[100]

[101]See Ian Grayson, Packer Sets up Big Brother Data Store, Australian, Nov. 30, 1999 <http://technology.news.com.au/news/4277059.htm>.

one of their chief assets.[102] In other cases, such as compliance with rules requiring the reporting of large cash transactions, firms record data because the government requires them to assist law enforcement efforts.[103]

The breadth of scope and richness of detail in searchable commercial information databases is epitomized by a LexisNexis advertisement for its Batchtrace service. LexisNexis describes the service as a "large-volume, multi-source skip trace and locator service. It scrubs your accounts against our proprietary database, one of the industry's largest and most current collections of locator information."[104] The company boasts of a database that

> includes more than 3.5 billion name/address records compiled from hundreds of independent sources, including:
>
> - Real estate
> - White pages
> - Census
> - Subscriptions
> - Voter
> - National Change of Address (NCOA
> - Proprietary change of address database
> - Electronic directory assistance (via RBOCs)
> - Driver's licenses
> - Motor vehicle registrations
> - Watercraft registrations
> - Professional licenses
> - Credit bureau header files
> - Military directories
> - Aircraft registrations
> - Call center indexes
> - Pizza delivery[105]

When even pizza delivery has become searchable, we are in brave new world of online databases, like it or not.

---

[102]e.g. [banking article] Kim Nash, Casinos hit jackpot with customer data, CNN.com (July 3, 2001), http://www.cnn.com/2001/TECH/industry/07/03/casinos.crm.idg/

[103]See FinCEN, Helping Investigators Use the Money Trail <http://www.treas.gov/fincen/follow2.html>; see also FinCEN, supra note 26, at 5 (stating that analysts may provide information through FinCEN's Artificial Intelligence System on previously undetected possible criminal organizations and activities so that investigations can be initiated).

[104]LexisNexis, BatchTrace, http://www.lexisnexis.com/batch/batchtrace/features.shtml

[105]Id.

Increasingly, non-transactional actions – like walking or driving a car – also cause data to be recorded in searchable databases. Falling costs for cameras and other sensors, combined with cheaper data storage has lead to a rise in public and private surveillance. Increasingly data from surveillance sensors is stored and searchable. Monitoring technologies include cameras, facial recognition software, and various types of vehicle identification systems. Related technologies, some of which have the effect of allowing real-time monitoring and tracking of individuals, include cell-phone location technology, and various types of biometric identifiers.

Like the Batchtrace database, much of the data collection and collation is private. Private information, however, is also likely to become part of the government's database. Commercial profilers routinely sell information to government law enforcement agencies.[106]

C. Cheap Storage, Search, and Sharing of Data

Advances in computer storage and networking technology have made it vastly cheaper to store, search, and share gigabytes of data.[107] Each of these advances is significant. Their synergistic effect is enormous. For present purposes, however, what matters is that these advances in privacy-destroying technology are proceeding apace, regardless of whether the federal government introduces a national ID system, and whether or not we have national ID cards. Every advance in the private sector becomes available to the government for a price. The reverse is not inevitably true, but it tends to be true.[108]

IV. Dangers to Liberty Arising from a National ID System

The risks to liberty arise in five categories: (1) Risks from the legal use of accurate information, (2) Risks from illegal use of accurate information; (3) Risk of reliance on false information; (4) Risk of intentional creation of false information; (5) Risk of over-dependance on some feature of the system (completeness of database, ubiquity of card or other token).[109] Most of

---

[106]See EPIC, Privacy and Public Records, http://www.epic.org/privacy/publicrecords/ (noting that profiling company ChoicePoint provided personal information to at least thirty-five government agencies and Experian, a credit reporting agency, sells personal information to government agencies for law enforcement purposes).

[107]See Froomkin, *supra* note 66.

[108]See id.

[109]The classic survey of the potential dangers of a national ID system remains Roger Clarke's list of the dangers of "Dataveillance".
Dangers of Personal Dataveillance
lack of subject knowledge of data flows
blacklisting

(continued...)

these classes of risk pose somewhat different dangers in the public and private sectors.

A. Risks from the Legal Use of Accurate Information

It may seem counter-intuitive, 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 US law, and the weaker protections in the US Constitution.

1. Public Sector Uses

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. To many people--not just to cowboys-- there is a value in being able to move through life without an obligation to identify oneself, just as there is a value in the right not to be stopped or searched without cause. Correlatively, there maybe 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 now badly eroded in airports,

---

[109](...continued)

Dangers of Mass Dataveillance
- To the Individual
  - witch hunts
  - ex-ante discrimination and guilt prediction
  - selective advertising
  - inversion of the onus of proof
  - covert operations
  - unknown accusations and accusers
  - denial of due process
- To Society
  - prevailing climate of suspicion
  - adversarial relationships
  - focus of law enforcement on easily detectable and provable offences
  - inequitable application of the law
  - stultification of originality
  - increased tendency to opt out of the official level of society
  - weakening of society's moral fibre and cohesion
  - repressive potential for a totalitarian government

Roger Clarke, *Information Technology and Dataveillance*, 31 COMMUN. ACM 498-51 ( Nov. 1987), *available at* http://www.anu.edu.au/people/Roger.Clarke/DV/CACM88.html.

other places of mass transit, courthouses and other public buildings.[110] Even without actual ID cards, or the obligation to carry or reveal them, a national identification system could eventually lead to a similar result at every street corner. If facial recognition software ever becomes effective and reliable,[111] then either the body will become our ID card or we shall all wear masks.[112]

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. While some uses of a database are unproblematic, even desirable,[113] many are not.[114] 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,[115] 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

---

[110]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).

[111]Current trials have revealed some problems with facial recognition software. See, e.g., Jay Stanley and Barry Steinhardt, *Drawing a Blank: The Failure of Facial Recognition Technology in Tampa, Florida*, Jan. 3, 2002, ACLU SPECIAL REPORT *available at* http://www.aclu.org/issues/privacy/drawing_blank.pdf (discussing usage of facial recognition technology in crime fighting in Tampa, and pointing out failures).

[112]Both federal law and the law of several states forbid the wearing of masks in public places. See A. Michael Froomkin, *The Metaphor is the Key: Cryptography, the Clipper Chip and the Constitution*, 143 U. PENN. L. REV. 709, 821-22 (1995)), available online http://www.law.miami.edu/~froomkin/articles/clipper.htm.

[113]For example, data matching to combat fraudulent applications for benefits.

[114]For example, building up list of frequent protestors against government policies.

[115]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).

President"[116] 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."[117] 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.[118]

Even with the Privacy Act in place, both 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."[119] And here the issue becomes almost metaphysical. One could say that the act of searching through a database of personal information, much of it perhaps furnished voluntarily either in private commercial transactions, or in formally voluntary transactions with a government agency (e.g. a driver's license application[120]) 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. Whether there is a reasonable expectation of privacy depends on the legal rights one has over the data; and reasonable expectations, after all, are always set by whatever the law provides. Once lawfully acquired by the government, the data are the government's property, to use as it sees fit unless there is some

---

[116]5 USC § 552a(e)(1).

[117]Id at (e)(6).

[118]This contrasts sharply with a 1991 decision by the Hungarian constitutional court, which found that collecting and processing of personal data without a specific purpose for future use was unconstitutional. See Hungarian Constitutional Court Decision, No. 15-AB of 13 April 1991, *available at* http://www.privacy.org/pi/countries/hungary/hungarian_id_decision_1991.html.

[119]Erik Baard, *Buying Trouble*, VILLAGE VOICE (June 24, 2002), http://www.villagevoice.com/issues/0230/baard.php

[120]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. §§ 2721-2725. The DPPA imposes restrictions on the abilityi of state motor vehicle departments (DMVs) to disclose information collected from drivers and automobile owners without that person's consent. 18 U.S.C. § 2721(a) (prohibiting "any state DMV, or officer, employee, or contractor thereof, from "knowingly disclos[ing] or otherwise mak[ing] available to any person or entity personal information about any individual obtained by the department in connection with a motor vehicle record."). Under the DPPA as amended in 1999, states may no longer imply consent from a driver's failure to opt-out of disclosure, but must obtain affirmative consent from the driver's. Even without consent, however, disclosure is permitted for use "by any government agency" or by "any private person or entity acting on behalf of a Federal, State or local agency in carrying out its functions." 18 U.S.C. § 2721(b)(1) (1994 ed. and Supp. III). Cf. Reno v. Condon, 528 U.S. 141 (2000) (upholding constitutionality of DPPA).

constitutional principle to the contrary. Thus, unless the subject has a property right in the data that the government holds about him, 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 about us for law-enforcement purposes.[121]

Yet, "it was one of the primary aims of the Fourth Amendment to protect citizens from the tyranny of being singled out for search and seizure without particularized suspicion notwithstanding the effectiveness of this method."[122] Whether government data-mining of databases with information on most of the citizenry runs afoul of this principle, or whether the fact that *everyone* is subjected to the same initial level of investigation somehow makes general suspicion more acceptable than particularized suspicion are issues that may not be avoidable for long.

At present virtual profiling is somewhat constrained by the Privacy Act of 1974[123] 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. Being only a creature of statute, this protection can be removed by subsequent legislation. It seems necessary therefore to enquire what constitutional protections may exist to protect personal data held by the government. (Part V below addresses what might be done to enlarge them.)

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 involved 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.[124] On the other hand, since the subjects

---

[121]Another, less persuasive, analogy would treat the data as having been left in the government's plain view. And it is long-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); Dow Chem. Co. v. United States, 476 U.S. 227, 239 (1986) (aerial photograph of chemical facilities does not violate Fourth Amendment); California v. Ciraolo, 476 U.S. 207, 214 (1986) (search of home from airplane does not violate Fourth Amendment); see also United States v. Place, 462 U.S. 696, 707 (1983) (holding that trained drug dogs sniffing at closed luggage is not a search under the Fourth Amendment).

[122] Florida v. Bostick, 501 U.S. 429 (1991) (Marshall, J., dissenting).

[123]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.

[124]See Michael Adler, Note, Cyberspace, General Searches, and Digital Contraband: The (continued...)

of the virtual search are unaware of any intrusion, one of the values the 4th Amendment protects -- the sanctity of the person, the home, and of one's property -- suffers less intrusion than it would 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.[125] It is even arguable that if the government owns or leases the data, courts might not treat a database trawl as a "search" at all for constitutional purposes since there is no intrusion onto the property of the subject.

The absence of a rule that attaches Fourth Amendment and property-like due process protections to data in the national ID database (or any national ID card), opens the door to a wide range of undesirable outcomes. Legislation making clear that the data in the national ID system belonged to the subject would address most of these problems; alternately, legislation could leave title in the government, but say that use of the data would be governed by the same standards that apply to physical property in the home. Giving the individual a genuine property right in federally held data is the preferable solution, however, as it would provide a additional protection against legislative second thoughts. Any later attempt to remove this layer of 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 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[126]--would create a mechanism by which unverified derogatory information could circulate widely, at least among government agencies.[127] In addition to the obvious possible harms of having law enforcement use these tips as the 'reasonable' basis for traffic stops and searches, there

---

[124](...continued)
Fourth Amendment and the Net-Wide Search, 105 Yale L.J. 1093 (1996).

[125]Id. at 1097.

[126]On TIPS see William Matthews, *Ashcroft offers TIPS assurances* (July 26, 2002), http://www.fcw.com/fcw/articles/2002/0722/web-tips-07-26-02.asp.

[127]It might be objected that since 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 (in the absence of testilying by police, cf. NACDL Prosecutorial Misconduct Committee, *"Testilying" to Get the Job Done*, http://www.criminaljustice.org/PUBLIC/ABUSE/CR000007.htm (quoting from 199r report of New York City Commission to Investigate Allegations of Police Corruption) it is true that there was such a communication from the public.

is the more fundamental harm to the body politic of developing an informer and dossier culture.[128] 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. While worth trying–it can't hurt--it is not altogether clear how successful these officials have been.[129]

A large and rich database invites predictive profiling,[130] 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.[131] 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.[132] This may only be the tip of the iceberg; a publicly available database might for example contain current addresses and all conviction histories,[133] creating a class of "social leper."[134] Whether the loss of "social forgiveness, the principle that over time a citizen's crimes are forgiven,"

---

[128]See TIMOTHY GARTON ASH, THE FILE: A PERSONAL HISTORY (1997).

[129]For a surprisingly pessimistic assessment by a former privacy commissioner, see DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES 406-07 (1989).

[130]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, http://features.slashdot.org/article.pl?sid=01/01/23/2341238

[131]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.

[132]'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).

[133]The issue of whether and when convictions should be 'spent', i.e. forgotten, is a controversial one. *See* T. Markus Funk, *A Mere Youthful Indiscretion? Reexaming the Policy of Expunging Juvenile Delinquency Records*, 29 U. MICH J.L. REF. 885 (1996).

[134]According to Funk, *supra* note 133, at 903 n.85, 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).

is a good thing or not may be debatable.[135] But any change of that magnitude should be debated, rather than be a side-effect of technology.

2. Private Sector

The private sector could legally misuse accurate information to engage in several forms of legal discrimination.[136] A permanent national ID number embedded in a national ID system also would make it easier to propagate and enforce digital rights management technologies. And, there is always the danger of the accidental or intentional release of embarrassing facts.[137]

Not all discrimination is illegal, and what is legal is not always practical. A national ID system might make some legal but difficult discrimination much easier. Merchants equipped with

---

[135]For some though-provoking if rather cold-hearted arguments as to why some common forms of social forgiveness might be harmful, see Funk, supra note 133.

[136]*See generally* OSCAR H. GANDY, JR., THE PANOPTIC SORT: A POLITICAL ECONOMY OF PERSONAL INFORMATION (1993). Strange things can disclose personal information. For example some studies suggest there is a link between fingerprint symmetry and sexual preference. Many jurisdictions do not forbid discrimination on the basis of sexual preference.

[137]As EPIC notes,

> In the process of aggregating profiles, any number of persons may acquire the information of another. In fact, one of the largest commercial profilers, Metromail (now owned by Experian), used prisoners to enter personal information from surveys into computers. This resulted in a stalking case where a prisoner harassed a woman based on information she submitted on a survey. The woman received mail from a convicted rapist and burglar who knew everything about her--including her preferences for bath soap and magazines. In fact, Metromail maintained a voluminous amount of data on the woman. Metromail had twenty-five pages of personal data on her, including her income, and information on when she had used hemorrhoid medicine.
>
> The woman sued (Beverly Dennis, et al. v. Metromail, et al., No. 96-04451, Travis County, Texas.) and as a result of a class-action suit, Metromail may no longer use prisoners to process personal information. During litigation, Metromail claimed that they had not violated the woman's privacy, that they had no duty to inform individuals that prisoners were processing their personal data, and that the data processed was not highly intimate or embarrassing.

http://www.epic.org/privacy/profiling/

But note that while it may be legal to disclose an accurate but embarrassing fact, *threatening* to release an accurate but embarrassing fact is usually called "blackmail" and is a criminal offense. See, e.g., 18 USC § 41.

face recognition equipment might be wish to know when convicted felons - and especially convicted shoplifters - enter their stores. In a world of cameras, face recognition, and constant global position monitoring it might even be possible to subscribe to a service that would warn you whenever a convicted criminal got within fifty feet as you walked down the street.

If ID numbers became a routine part of e-commerce, a national ID system would also enable more perfect price discrimination:

> One can imagine stores tailoring what they present to what they presume to be the customer's desires, based on demographic information that was available about the customer even before the first purchase. Tailoring might extend beyond showcasing different wares: Taken to the logical extreme, it would include some form of price discrimination based on facts known about the customer's preferences, or on demographic information thought to be correlated with preferences.[138]

If merchants allow consumers to shop anonymously or pseudonymously, this will not happen. But if the ID requirement is routine, it becomes much more likely.

As noted above, a particularly likely consequence of a national ID regime would be to simplify the implementation of digital rights management technologies (DRM). Examples of DRM technologies include copy protection and pay-per-play charging devices. Although significant, the commercial aspects of DRM are not a liberty issue. The liberty danger is in the effect that a mating of an ID system with a DRM system would have on First Amendment rights. DRM technologies enforce content licenses that tend to subvert the consumer's right of fair use of purchased books, music, films and other works. Although the right still exists, the DRM technology makes its exercise far more difficult and in some cases impossible. Furthermore, if ID demands become routine, a DMR-enabled world also undermine the consumer's ability to acquire reading matter anonymously.[139] Indeed, in a pay-to-play system, every act of reading could be captured and stored to become part of the consumer's data profile maintained by the licensor of the content.

---

[138] *Speculative Microeconomics for Tomorrow's Economy* (with James Bradford De Long) (book chapter) Internet Publishing and Beyond: The Economics of Digital Information and Intellectual Property 6 (Brian Kahin &Hal Varian, eds., 2000), available online http://www.law.miami.edu/~froomkin/ articles/spec.htm . In 2000 Amazon.com tried out "random-pricing tests" for a couple of weeks. The tests dynamically priced items for sale based on a browsing user's profile. Users did not view the pricing scheme favorably, and Amazon suspended the tests. See, e.g., *Amazon May Spell End for 'Dynamic' Pricing*, USA TODAY TECH REPORT , available at http://www.usatoday.com/life/cyber/tech/cti595.htm.

[139] For an argument that the Constitution recognizes a right to read anonymously see Julie Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981 (1996).

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, drivers 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.[140]

A new centralized system would not only build on old risks of reliance on false information but introduce new ones: if the 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 new systems could be abused in the same manner as old ones is not necessarily a reason to fear it. Nevertheless, unless the system is engineered very carefully, the danger of the virtual equivalent of 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.[141] 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.[142]

A second danger is the addition of false information designed to harass, for example a false statement that someone has an outstanding warrant when in fact they do not. Given that national systems to check for this sort of record exist already, it's hard to see how the existence of a more centralized database greatly increases this danger. A third, and perhaps greater, risk is that if the government and/or the public rely on the system, there is one centralized target for anyone trying to get a false ID--and if they get it, the ID is too likely to be trusted.

Who has the ability to attach information to an actual or virtual file also shapes the extent to which a national database system may make data subjects more vulnerable to the creation of false or irrelevant information. Proper design of information systems can reduce risk of intentional

---

[140]See NRC Study, *supra* note 1, at [chapter 2].

[141]An example would be inserting an image of someone into a photo taken by a surveillance camera near the scene of the crime.

[142]Keeping digitally signed copies of records before and after modification, with the modification carrying a digitally signed copy of the modifiers credential would provide a substantial audit trail -- at the cost of some computational complexity and increased storage requirements. For an introduction to digital signatures see A. Michael Froomkin, *The Essential Role of Trusted Third Parties in Electronic Commerce*, 75 ORE. L. REV. 49 (1996), available online http://www.law.miami.edu/~froomkin/articles/trusted.htm.

inaccuracy, although no system is foolproof. If the information resides in a central location then the danger of both intentional and accidental inaccuracies can be further cured by *transparency* -- ensuring that the data subject has access to records about him. The more dispersed the records are, the less meaningful this protection becomes.

Thus, for example, the United States has legislation regulating key private sector collectors and providers of consumer profiles, notably the Fair Credit Reporting Act;[143] the Privacy Act also creates a right to correct inaccurate data--at least outside the context of law enforcement's investigatory files and of course intelligence data. But even when it exists, the right to correct has limitations. For all that the courts have interpreted it generously,[144] the FCRA, has limitations. First, consumers are only likely to learn about derogatory information in their credit reports if they ask to see them.[145] Second, once a data subject complains to a credit bureau about false information in a file, in practice the burden of proof is on him to prove the error.[146] Centralized storage systems are

---

[143]Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681u (2000).

In Dun & Bradstreet v. Greenmoss Builders, 472 U.S. 749 (1985), the Supreme Court held that consumer credit reports concern no public issue, and thus receive reduced Constitutional protection. Congress recently enacted the fair and accurate transactions act of 2003 (FACTA), ostensibly to make credit monitoring easier. While the act contains a few valuable terms, e.g. requiring a fraud report to one major credit bureau to trigger a duty by it to pass on the report to other major credit bureaus, the act does little more than codify current practices at the national level – and to pre-empt state attempts to legislate stronger privacy rules.

[144]Important decisions include Trans Union v. FTC, No. 00-1141 (D.C. Cir. 2001), cert. denied, 536 U. S. ____ (2002) (holding that tradelines -- credit information that includes name, address, date of birth, telephone number, Social Security number, account type, opening date of account, credit limit, account status, and payment history -- could not be sold for marketing purposes because they constituted a credit report for purposes of FCRA, and rejecting First and Fifth Amendments challenges to FCRA); Trans Union v. FTC, 81 F.3d 228 (D.C. Cir. 1996)("Trans Union I") (holding that the sale of consumer credit reports for marketing purposes violates the FCRA).

[145]However, the Equal Credit Opportunity Act of 1974 requires credit institutions to explain why they deny credit. A denial based on a bad credit report should tend to drive an ordinary consumer to get his credit report post-haste.

[146]The Fair Credit Billing Act of 1974, 15 U.S.C. §§ 1601-67(e), gives individuals the right to correct mistakes in their credit card statements. The Equal Credit Opportunity Act of 1974, 15 U.S.C. §§ 1691-1691(e), prohibits denial of credit on grounds of sex, race, color, religion, national origin, age, or marital status. However, both statutes place the burden of proving errors on the individual; until called to the attention of the controller of data, no duty exists to gather correct information and to update that information. See Michael P. Roch, *Filling the Void of Data Protection in the United States: Following the European Example*, 12 Santa Clara Computer & High

(continued...)

a single point of failure, but should be easier to monitor and audit; decentralized storage may make monitoring and transparency to the data subject more difficult.

Commentators have also argued that large databases facilitate illegal private discrimination,[147] although again here the primary risk seems an increase in quantity rather than the creation of new kinds of discrimination (one exception is the possible use of DNA information to discriminate in employment in order to keep down employers' medical bills).[148] Certainly many private acts of providing false derogatory information are already covered by tort and statute law such as libel or the prohibition on filing of a false police report; the danger here is that there might be an increase in these offenses as it becomes easier to commit them and that enforcement is and remains lax.

Centralization of data in a single national system means that large numbers of people will be able to access it for a wide variety of purposes. The more accesses there are, the greater the chance that inaccurate information will damage its 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.[149] 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.

---

[146](...continued)
Tech. L.J. 71, 90 (1996).

[147]See generally Oscar H. Gandy, Jr., THE PANOPTIC SORT: A POLITICAL ECONOMY OF PERSONAL INFORMATION (1993).

[148]As noted above, see supra text at note -, law enforcement gene typing uses 'junk' DNA that has no health implications. Thus, whether the use of DNA with health implications is really a national ID issue or not is debatable. On the one hand, employers are able to request DNA testing before hiring whether or not the information is in a database. On the other hand, testing is not costless, and in the absence of having results easily available and linked to the applicants national ID number, some employers presumably would not bother. The storage and ease of use may make it more difficult to avoid sharing a negative result once it is linked to a person's ID.

How this plays out depends greatly on the cost of the test and the employer's calculation of the expected cost of medical treatment. At some point when the number of non-testing employers gets too low, their share of the market for employees begins to resemble the classic 'market for lemons' in economic theory -- driving increasing numbers of employers to test anyway. Thus, in some but not all scenarios the national database makes a big difference.

[149]The difficulty of having corrective data catch up with false data is often cited as one of the most painful aspects of identity theft.

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[150] the database would make roundups of disfavored classes easier.[151] 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 they have the legal right to detain US citizens without trial or counsel for indefinite periods upon a government official's unsupported declaration that the citizen is an "enemy combatant"[152]--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 dates quickly, given that sixteen percent of the US population moves to a new residence every year.[153] 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.

---

[150]Cf. SINCLAIR LEWIS, IT CAN'T HAPPEN HERE (1935).

[151]See, e.g.. Roger Clarke, *Information Technology: Weapon of Authoritarianism or Tool of Democracy?*, Jun. 1994, *available at* http://www.anu.edu.au/people/Roger.Clarke/DV/PaperAuthism.html ("Strong tendencies exist to apply information technology to support centralist, authoritarian world views. It is argued that alternative architectures can be readily created, which are more attuned to the openness and freedoms which are supposed to be the hallmarks of democratic government.").

[152]Cf. Padilla v. Rumsfeld, 352 F.3d 695 (2nd Cir. 2003), *cert granted* 72 USLW 3488,2004 WL 95802 (Feb. 20, 2004).

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

The Privacy Act of 1974 is the key element of the federal government's response to the dangers of public disclosure of government dossiers. There is no question that before the Privacy Act became law, government policy at times authorized harmful disclosures of personal information. During the Vietnam war, for example, the Army stamped discharge papers with 530 different "SPN" code numbers. The codes did not appear on discharge papers issued to servicemen but were available to employers who asked the Pentagon for more detailed records. Unknown to the veterans, including some with honorable discharges, employers who knew the codes could acquire derogatory information about them. Classifications included "drug abuse," "disloyal or subversive security program," "homosexual tendency," "unsuitability--apathy, defective attitudes and inability to expend effort constructively," and "unsuitability--enuresis [bed wetting]."[154] (One issue about President Bush's service record is that no document with his SPN code has been released by the White House.)

SPN codes released to employers but not veterans would be illegal today. In principle,[155] the federal government may not disclose personal data without consent of the data subject.[156] Agencies must allow individual access to copies of their records, and must promptly correct false information or explain why they refuse to do so. Under the Privacy Act, the federal government also must exercise due care in the compilation of personal data and to seek to secure databases from hackers and internal snoops. However, while the Privacy Act applies to databases "maintained by an agency," it does not apply to privately owned and maintained databases, arguably not even if the government is the sole client for the information.[157]

---

[154]See Dana A. Schmidt, Pentagon Using Drug-Abuse Code, N.Y. Times, Mar. 1, 1972, at 11. Receipt of antiwar literature sufficed to be classified as disloyal or subversive. See Peter Kihss, Use of Personal- Characterization Coding on Military Discharges Is Assailed, N.Y. Times, Sept. 30, 1973, at 46. In response to public pressure, the Pentagon abandoned the program and reissued discharge papers without the codes. See Pentagon Abolishes Code on Discharges of Military Misfits, N.Y. Times, Mar. 23, 1974, at 64; Uncoded Discharge Papers Are Offered to Veterans, N.Y. Times, April 28, 1974, at 33.

[155]There are substantial exceptions to this principle, see 5 U.S.C. § 552a(b), including one allowing disclosure "to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought." See also Todd Robert Coles, Comment, *Does The Privacy Act Of 1974 Protect Your Right To Privacy? An Examination Of The Routine Use Exemption*, 40 AM. U. L. REV. 957 (1991).

[156]Id.

[157]Indeed, the creators of the ACES project argued to me that the Privacy Act would not apply even if the contractor created the database at the government's request, and the government was the sole client for that database. This argument receives some support from the definitions in

(continued...)

D. Risk of Over-Dependance

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.[158] General reliance on national ID card or on a centralized dossier creates at least three sorts of risks. First, 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.

Second, routinized credentialing destroys the ability of people to move and transact anonymously. This may seem like an advantage to some, but in fact the ability to be anonymous and pseudonymous is an important privacy right with implications for political and civil liberty.[159]

But perhaps the greatest danger if a national ID system really takes off is that people will become dependent on it for ordinary life:

> A nationwide identity system ... might drive many other forms of identification out of use by subsuming their functionality. Several factors in particular could encourage widespread third-party reliance on the nationwide identity system to the exclusion of current systems. First, if the cost of the system is borne by the

---

[157](...continued)
§ 552a of the privacy act. A "recipient agency" is defined as "any agency, *or contractor thereof*, receiving records contained in a system of records from a source agency for use in a matching program;" (italics added) . But a "source agency" is only "any agency which discloses records contained in a system of records to be used in a matching program, or any State or local government, or agency thereof, which discloses records to be used in a matching program," which leaves out the words "or contractor thereof". And a "record" is defined in a way that arguably leaves out data held by contracts, being "any item, collection, or grouping of information about an individual that is *maintained by an agency*, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph."

[158]Employers and insurers are already relying on credit scoring. See Insurance Credit Scoring, http://www.indianafarmers.com/docs/Credit%20Score%20 Brochure%20Final%20Version.pdf; Insure.com, *How your credit history affects your auto and home insurance premiums*, http://info.insure.com/auto/creditscores.html.

[159]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 online http://www.law.miami.edu/~froomkin/articles/ocean.htm.

> government and its associated agencies .... Second, unless private parties are prevented... from relying on the nationwide identity system, the liability associated with such reliance would be shielded by the government's sovereign immunity. third, even if the private parties were forbidden to rely on the data, it is very likely that private commercial organizations would begin to correlate data about citizens based on their card and/or identity within the system."[160]

This creates an attractive chokepoint for all sorts of regulation.

Suppose, for example, that an enhanced national ID card[161] 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.[162] The threat of removal of this card, or of putting a 'hold' , query, or other black mark into the centralized dossier referenced by the ID number, could become a powerful sanction. If one treats the card or the data as government property, then many of the constitutional protections one might expect could be missing. For example, 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. While 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 were being set.

Certainly there would be grounds for an equal protection claim if the government or its agents acted in, say, a racially discriminatory manner. But in the absence of a discriminatory pattern and practice, equal protection may not have much to say about a consistently applied policy of creating a limited form of social death. Suppose for example that the government action consists of making true and accurate statements in its database (X was stopped and frisked; Y was observed repeatedly in a high-crime area; Z is on our terrorist watch list because he frequently buys pizza with a credit card).[163] Repeated interactions of this sort may become part of a profile, leading some people to be come 'usual suspects'. Worse, if the information is shared with private sector, airlines for example, the government may be able to plead that it should not be responsible for the consequences especially if the information is accurate.

Even if there may be difficulties in actively sanctioning people for information in their

---

[160]NRC REPORT, *supra* note 1, at 30-31.

[161]The problem is equally real with a national ID system that lacks a card, but is easier to visualize with a tangible example.

[162]So named after Terry v. Ohio, 392 U.S. 1 (1968).

[163]Allegedly, frequently buying a pizza with a credit card is one of the factors that 'predicts' likely terrorists. *See* Baard, *supra* note 119 (quoting Larry Ponemon, CEO of consulting firm Privacy Council).

dossiers, there are likely to 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."[164] 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.

These dangers can be summarized in a chart (see next page):

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

| Type of Danger.. | From Government Actors | From Private Actors |
|---|---|---|
| Risks from legal use of accurate info | Virtual 'general searches' on data / data mining<br><br>TIPS (e.g. risk of anonymous denunciations)<br><br>Profiling (danger of false positives, stigmatizing)<br><br>Efficient stigmatization (mega-Megan's laws)<br><br>Function creep<br><br>Moral/psychological costs to free society. | Profiling, legal types social/political discrimination<br><br>More perfect price discrimination<br><br>Aids enforcement of Digital Rights Management (DRM)<br><br>Threat to anonymity<br><br>Accidental or intentional release of embarrassing facts. |
| Risks from illegal use of accurate info<br><br>Risk of reliance on false information (whether created intentionally or not) | "J. Edgar Hoover problem" (abuses by malign officials, in high positions and low)<br><br>Unsanctioned snooping, by government employees<br><br>Totalitarian roundups made easier<br><br>ID's only as good as data used to generate them | Profiling, illegal types social/political discrimination<br><br>Blackmail [already illegal] |
| Risk of over-dependance on some feature of the system (completeness of database, ubiquity of card or other token) | Transparency issues<br><br>Greater harm from identity theft; system likely "fails badly"<br><br>Threat of removal (or addition of notation) becomes powerful sanction<br><br>Desire to collect maximum information 'just in case'<br><br>Function creep<br><br>Threat to anonymity | Transparency issues<br><br>Greater harm from identity theft; system likely "fails badly"<br><br>Over-reliance on non-causation, high-correlation factors in making employment, insurance decisions. |

## V. Controlling the Dangers and Enhancing Privacy: The (Very?) Uneasy Case for Mandatory Federal National ID Cards

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[165] 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 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 there is a physical card, the most important issue is the collection and use of personal data.[166] The primary importance of a physical national ID card is its symbolic effect and any political consequences.[167] Other than the possible psychological effect, ID cards matter not

---

[165]There are a host of less-substantial differences. Of these, the largest may be the different security implications of a system that stores data -- either biometric or otherwise -- on a card as compared to one that stores data centrally, whether or not a card is used for authentication.

[166]See, e.g., Simson Garfinkel, *Will a Mandatory ID Keep Us Safe?*, Apr. 2002, PRIVACY J. (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); Heather Green, *Databases and Security vs. Privacy,* Oct. 8, 2001, Business Week *available at* http://www.businessweek.com/technology/content/oct2001/tc2001108_3550.htm (arguing national ISs is red-herring debate, real issue is the interfacing of existing databases on back end); Robert O'Harrow, Jr., *States Devising Plan for High-Tech National Identification Card*, Nov. 3, 2001, Washington Post *available at* http://www.mvcf.com/news/cache/00501/ (discussing the effort by the American Association of Motor Vehicle Administrators to link their databases into one system); Paul Rogers & Elise Ackerman, *Oracle Boss Urges National ID Cards, Offers Free Software*, Sep. 22, 2001, Mercury News *available at* http://www.gyre.org/news/cache/1206 (discussing Larry Ellison's offer to provide database for national id system to government for free).

[167]There are even, so one hears, entire countries which have national ID cards, some of which, if rumor can be believed, are not yet completely totalitarian. Germany, France, Belgium, Greece, Luxembourg, Portugal, Spain, India, China, Pakistan, South Africa, Thailand, Singapore, Poland, Brazil, Chile, Korea, Malaysia, Italy, Greece, Argentina, Honduras, Guatemala, Kenya have or have had a form of a national identification system in place. See Privacy Org., Identity Card (continued...)

because they are ID cards, but because their introduction becomes an excuse, or a shorthand, for greater scope or greater centralization of national databases–or for a political movement to control them. As described above in Part II, the U.S. already has an widespread, existing, distributed, virtual ID system. (Note that this should *not* be read to mean that current proposals for national ID cards are therefore innocuous, since these proposals would not only require cards, but expand and enhance the underlying databases.) 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.[168]

The existence of this ever-expanding virtual ID system serves as a baseline against which proposals for a national ID *card* system should be measured. One obvious difference between the current virtual system and a hypothetical mandatory ID card regime is that today it remains possible, albeit with enormous effort, to opt-out of the virtual ID system. As a practical matter, though, this difference is more theoretical than real, since to do so requires that one avoid hospitals and the banking and financial system, pay cash, and pay large deposits to utility companies and others who ordinarily expect to run credit checks, and thus demand various forms of identification before entering into long-term contracts. If it doesn't quite require living in a cabin in the woods, a la Thoreau (or the Unabomber), it takes something pretty close.

A. Design Safeguards

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 mis-use the system. Design can reduce the risk of harmful unlawful uses; it is far less potent against a decision to make bad uses lawful.

Good security, including access controls and strong auditing and tracking of access, is needed to protect the data against both internal and external threats. Physical and software controls make hacking less likely, although they tend to have less value against internal threats. Building in auditing and tracking, ideally with off-site real-time logging, means that insiders tempted to misuse the data in some way will at least run the risk of detection -- and the more that the logs are available to outside inspection, the greater the chance of detection. Good security also lessens,

---

[167](...continued)
FAQ (Aug. 24 1996), http://www.privacy.org/pi/activities/idcard/idcard_faq.html; Annie Anton, *National Identification Cards* (Dec. 17, 1996), available at http://www.cc.gatech.edu/computing/SW_Eng/people/Phd/id.html.

[168]See Froomkin, *supra* note 66.

although it by no means eliminates, the chance of intentional forgery of data. Any system that relies on a token, such as a physical card for access, creates another level of security as the user can notice if the card is missing, and it may be harder to hack in without the token. On the other hand, it also introduces new vulnerabilities, since the token itself may be compromised or forged.[169] Making the card the repository for some or all of the information rather than centralizing the information in a database accessed by the card reduces the danger of systemic compromise of the entire database all at once, but increases the importance of securing the card. If biometrics are used, it may be particularly important to avoid storing the information centrally.[170]

Transparency allows the data subject to know 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 more centralized national information system, or even a decentralized one that relies on a common identifier, allows incorrect information to propagate more widely, which is harmful. But it also allows corrections to catch up more quickly. More fundamentally, the idea of a centralized national ID system is in tension with the ideal of individual control over personal information. If the system is mandatory, it will demand basic data regarding existence, such birth place and probably citizenship, and enough information to authenticate the data subject. Even if the system requires certain data, it does not follow that it must require all the data it is capable of holding. Beyond some set minimum, it should be possible to opt out of the system.

Whatever the specifics of the system, good error handling is essential. There needs to be away to correct erroneous data, and there needs to be a way to handle data compromises. Present experience with distributed data systems already illustrates the difficulty of coping with identity theft: victims report that even after they are able to correct erroneous entries in their credit reports, or even criminal records, they are still victimized because corrections do not catch up to all the copies of the original report.[171]

A national ID system threatens anonymous and pseudonymous speech and commerce. The threat to anonymous speech impacts a valuable constitutional right-- one needed most by persons

---

[169]See generally Roger Clarke, *Chip-Based ID: Promise and Peril* (1997), http://www.anu.edu.au/people/Roger.Clarke/DV/IDCards97.html.

[170]Id.

[171]See, e.g., PrivacyRights.org, *It Takes Time and Vigilance to Regain Your Good Name*, http://www.privacyrights.org/victim21.htm ; Written Testimony of Michelle Brown before the U.S. Senate Committee On The Judiciary, Subcommittee On Technology, Terrorism And Government Information, "Identity Theft: How To Protect And Restore Your Good Name" (July 12, 2000), http://www.privacyrights.org/victim8.htm

least able to speak out for it, since they are the ones who have a legitimate fear of retaliation.[172] 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 for anonymity or at least for multiple pseudonyms,[173] 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 would permit the user to pass on appropriate characteristics and authorizations (e.g. age) to her 'nym if she chose to. And, of course, setting the 'nym bit would ensure that it could not be used for things where knowledge of a person's real identity is required.

B. Tying Fair Information Practices to the National ID System

The conventional wisdom among privacy mavens around the world about what should be done to combat privacy-threatening databases of all stripes was succinctly stated by EPIC Executive Director Marc Rotenburg: "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."[174] The "OECD Guidelines" or, more formally, the 1980 Organization for Economic Co-operation and Development Recommendations Concerning and Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data,[175] 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:

---

[172]It may also make whistle blowing more difficult and dangerous.

[173]Roger Clarke suggests additional protections are needed if the system relies on ID cards:

- an important corollary of the 'multiple ids' principle is the maintenance of separation between applications within multi-function chips, in order to assure the integrity of each application, and protect against unauthorised sharing of data and ids; and
- another important application of the 'multiple ids' principle is the implementation of role-ids as well as person-ids, to reflect the facts that individuals perform multiple roles at the same time, and that multiple individuals perform the same organisational function."

Clarke, *supra* note 169.

[174]Marc Rotenberg, *Fair Information Practices And The Architecture Of Privacy (What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 1, 45 (2001); see also Paul M. Schwartz, *Privacy & Democracy in Cyberspace*, 52 VANDERBILT L. REV. 1609 (1999) .

[175]OECD, Recommendation Of The Council Concerning Guidelines Governing The Protection Of Privacy And Transborder Flows Of Personal Data (23rd September, 1980), http://www.oecd.org/oecd/pages/home/displaygeneral/0,3380,EN-document-43-nodirectorate-no-no-10255-29,00.html [herinafter OECD Guidelines]

- A "collection limitation principle" that there "should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject."[176]
- A "data quality principle" that "personal data should be relevant to the purposes for which they are to be used" and, when relevant, "accurate, complete and kept up-to-date".[177]
- Notice and use requirements: data subjects should be told why data is being collected, who will hold it and how, data subjects must be able to access and correct data about them; collected data should not be used for purposes incompatible with the reasons given for collection except where permitted by explicit consent or by law.[178]
- Individuals should have a means of enforcing rules protecting their data privacy.[179]

Whole-hearted application of these principles to the public sector[180] and especially the private sector would indeed address many of the privacy dangers created by the growth of identification systems, whether virtual or card-based.

Although quite sweeping, the OECD Guidelines have been criticized as insufficient,[181] and I confess to some uncertainty myself about the relative efficacy of legal protections as opposed to technological ones. But that is a debate of limited relevance given that at present what we have in the US is far too little of either.[182] While there are a number of federal privacy laws, only the federal Privacy Act of 1974[183] could be accused of having a wide application, and it applies only to records collected by the federal government, not those collected by the private sector. As regards the private sector, federal privacy regulation is spotty at best, covering only particular sectors of the marketplace.[184] For example, the Federal Wiretap Act[185] imposes limits on wiretaps. The Electronic

---

[176]OECD Guidelines ¶ 7.

[177]Id. at ¶ 8.

[178]Id. at ¶¶9-12.

[179]Id. at ¶ 19.

[180]Many of these principles are already found in the Privacy Act.

[181]See, e.g. Gary T. Marx, *Ethics for the New Surveillance* in VISIONS OF PRIVACY 39 (Colin J. Bennett & Rebecca Grant, ed.s 1999).

[182]See Froomkin, *supra* note 66.

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

[184]Cf. Fred H. Cate, *The EU Data Protection Directive, Information Privacy, and the Public*
(continued...)

Communications Privacy Act imposes relatively strict limits on law enforcement access to e-mail in transit, but only feeble limits on law enforcement access to stored communications.[186] Other, almost random, legislative initiatives include the subscriber provisions of the Cable Act of 1984, and the Video Privacy Protection Act.

Legislation enacting the OECD Guidelines might be an important part of the answer to the privacy threats caused by national ID systems. Unfortunately, it seems highly unlikely that Congress is going to enact a broad, meaningful, non-sectoral, privacy statute-- even though the US endorsed the 1980 OECD Guidelines twenty years ago, and indeed a US government agency issued one of the first reports on the need for more attention to the privacy implications of computerized records.[187]

In the absence of any reason to believe that technological solutions will be adopted in the marketplace,[188] the alternatives to a centralized legislative solution seem pretty bleak. Recent experience has shown that technological changes that harm privacy happen quickly, and that industry and defacto standards often are set without much thought to the privacy consequences. There is nothing inevitable about this -- technology can enhance privacy as well as harm it -- but experience suggests that privacy-destroying technologies, particularly linking of databases, seems to spread more quickly than does, say, privacy-enhanced digital cash.[189]

In this depressing context, the right sort of National ID Card policy could actually seem privacy-enhancing--if the price of adoption were private sector compliance with the OECD Guidelines, plus some due process guarantees that would constrain the government's mis-use of the card and associated data.

Absent fairly unlikely legislation forbidding the use of alternatives, 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 alternate system that relies on whatever other identifiers they choose. A single reliable identifier

---

[184](...continued)
*Interest*, 80 IOWA L. REV. 431, 438 (1995).

[185]18 U.S.C.A. § 2518 (2000)

[186]ECPA. See Steve Jackson Games.

[187]See, U.S. Department Of Health, Education And Welfare Records, *Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems* XX-XXIII, at 50 (1973)

[188]A good discussion of the (un)likelihood of this is Rotenberg, *supra* note 174.

[189]On privacy enhanced digital cash, see generally Froomkin, *supra* note 159.

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 is 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.[190]

C. 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 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.[191] There are, however, many good reasons to be skeptical of this argument. 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.[192] 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.[193] 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 itself into every standard form consumer contract.[194]

---

[190]An even stronger 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, that would be forbidden to sell parts of the data set to other firms unless they too adhered to the same privacy principles. Whiteout 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.

[191]*See* Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283 (2000) (summarizing and critiquing these arguments).

[192]Id.

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

[194]Those who argue that this is an efficient solution, one reflected in the slightly lower price
(continued...)

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 two types of government-controlled information: the ID number and non-investigatory data about citizens held by the government.[195] 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 increasingly used, and as the 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 non-investigatory data[196] about themselves held by the government ensures that uses of the data will subject to constitutional constraints including limits on search and alienation. Firms would be unable to contract around the ID number ownership rule since they would be mere licensees. Whether citizens ever should be allowed to surrender their property interest in their government-held data may be a hard question to answer in the abstract, but it is hard to see in practice why an ordinary person would have an incentive to waive her protection against government data trawling in the absence of improper pressure.[197]

1. Federal Ownership of the ID Number

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

---

[194](...continued)
of the good or service which forms the underlying part of the transaction, are referred to my argument that consumers suffer from rational privacy myopia, valuing each bit of data at marginal value, while the buyer/aggregation 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 66, at 1501.

[195]The US government sometimes suggests that current privacy rules such as the Privacy Act may not apply to data held by its contractors subject to government directs. See, e.g. U.S. Department of Homeland Security, Report to the Public on Events Surrounding jetBlue Data Transfer, http://www.dhs.gov/interweb/assetlibrary/PrivacyOffice_jetBlueFINAL.pdf (2004). I believe this argument misreads the Privacy Act. But wether 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.

[196]Obviously, creating such a right for data collected in the context of law enforcement investigations would be even more protective of personal privacy, but at an unacceptable cost.

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

and any associated card, following the passport model,[198] 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.[199]

In the 1956 case of *Kent v. Dulles*,[200] the Supreme Court used statutory construction to narrow the government's power to refuse to issue passports. 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. And, in a 1965 decision, *Aptheker v. Secretary of State*, 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.[201]

Despite these decisions suggesting limits on passport regulation, in 1981 the Court held that even in the absence of explicit statutory authorization, the government could yank the passport of a US citizen if there was a substantial likelihood of "serious damage" to national security or foreign policy as result of passport holder's activities in foreign countries. According to Chief Justice Burger in *Haig v. Agee*, 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.[202]

Indeed, the right -- if right it be -- to a passport carries conditions. The passport regulations provide for denying a passport if the applicant for various reasonable grounds that might reasonably

---

[198]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)

[199]Another danger is that the provision of a national number might become an excuse to further federalize 'garden-variety' commercial frauds. The case of Browder v. U S, 312 U.S. 335 (1941) is instructive in this context. Imagine a version of 18 U.S.C. § 1542 (penalizing willful and knowing false statement in passport application) making it an offense to mis-use the a federal ID card.

[200]357 U.S. 116 (1958) (overturning decision of Secretary of State to deny certain passports on grounds that Congress had not given him the power to do so).

[201] 378 U.S. 500 (1964) (holding unconstitutional § 6 of the Subversive Activities Control Act, 50 U.S.C. § 785).

[202]Haig v. Agee, 453 U.S. 280 (1981) (holding that government may revoke a passport, pursuant to 22 CFR § 51.70(b)(4), on the ground that the holder's activities in foreign countries are causing or are likely to cause serious damage to the national security or foreign policy of the United States even though Passport Act of 1926 did not authorize such revocations).

suggest the person seeks to leave the country to avoid unpleasant legal consequences.[203] 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."[204]

A national ID system that allows the government to suspend the card, or burden it in ways that make it difficult to use, might easily become oppressive unless the citizen had clear rights to it, and also 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 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 their 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.[205] 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.

2. Individual Ownership of Personal Data Held by Government

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

---

[203]For example, if the applicant

- is the subject of an outstanding Federal warrant of arrest for a felony, or an extradition request, or a subpoena involving an investigation of a felony grounds include
- is subject to a criminal court order, condition of probation, or condition of parole, any of which forbids departure from the United States
- is subject to a court order committing him or her to a mental institution, or been declared incompetent;
- has not repaid a certain loans received from the United States
- has been notified by a State agency to be in arrears of more than $5,000 child support.

22 CFR § 51.70

[204]Id.

[205]Although there is no fundamental legal reason why this transaction could not be prohibited, it 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.

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.[206]

D. Centralizing the Politics of ID Cards

As noted above, in the thirty years since the relatively far-reaching success of the Privacy Act of 1974, privacy advocates in the US 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.[207] The privacy provisions of the Gramm-Leach-Bliley Financial Modernization Act of 1999 are a case in point: they are, in practice, quite weak.[208] 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 while allowing privacy campaigners to focus on one debate, but 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.[209]

Nonetheless, there are reasons to hope that a centralized system, especially one that relies on physical cards, would greatly increase support for privacy legislation. The political fact is that *visible* ID systems are much more unpopular than the *virtual* ID systems we currently use. Recent

---

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

[207]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).

[208]See Poggemiller*, supra* note 71.

[209]For a particularly evocative vision of what that might be like, see DAVID BRIN, THE TRANSPARENT SOCIETY (1998).

experience in Japan, not a nation known for protest, supports this.[210] The UK recently engaged in a consultation exercise on so-called "Entitlement Cards"[211] that also caused protests, and the effort is at least delayed.[212] A smartcard in voters' pockets could serve as the constant reminder that privacy is in play.

## VI. Summary

A fair evaluation of the likely privacy costs of a national ID regime requires a proper understanding of the privacy baseline. I have argued that data privacy picture is worse than most people realize, and that the odds are it will continue to get worse. In that light, the marginal harms caused by a national ID system may be fewer than one might initially believe, although there are genuine dangers to civil liberty and to privacy that we should be wary of. 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.

If the privacy baseline is as poor as I suggest then, somewhat counter-intuitively, 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. Since 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.

---

[210] Japan recently introduced a national ID system, to some protest. See JAMES BROOKE, *Japan in an Uproar as 'Big Brother' Computer File Kicks In*, New York Times, Aug. 6, 2002, http://www.nytimes.com/2002/08/06/international/asia/06JAPA.html; Yuri Kageyama, AP, *Japanese Drop Out of New ID System* (Aug 11 2002) (describing Japanese protests to new 11-digit ID numbering system).

[211] *See* UK Home Office, Entitlement Cards and Identity Fraud (July, 2002), http://www.homeoffice.gov.uk/cpd/entitlement_cards.pdf . On the history of ID cards in the UK see Valerie Collins, *Identity Cards and Numbers: the Debate Continued*, 10 INT'L REV. L. COMPUTERS & TECH. 137 (1996).

[212] Centralization may have another benefit: "In the privacy field, it will likely mean a government office with the expertise and authority to advocate on privacy matters...Privacy agencies also provide an effective resource for consumers with privacy concerns and are often times able to respond to privacy complaints without extensive and costly litigation. Such agencies also provide a source of expertise and advice for emerging privacy issues. This has been the experience not only of privacy agencies in Europe but also of those in Canada." Rotenberg, *supra* note 174, at 94-95.

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, travel, then it also becomes a target of opportunity for regulation and for law enforcement. While 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 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.

Even with these protections in place, an ID card regime is likely to contribute to the continued erosion of personal privacy. But as that erosion is proceeding without tangible ID cards, the right question is whether the introduction of tangible cards would improve personal privacy compared to the virtual ID card regime we seem to be headed for anyway. I have argued above that, 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 even if they are at the table. Privacy advocates might not win a single national debate, but better to wager on a single roll of the dice than lose for sure in a series of small games over time.

Even if this political calculation is unduly optimistic, the ID card issue merits careful thought because there is a real possibility that Congress may enact an national ID card program for reasons of its own. 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. 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.