

The Uneasy Case for National ID Cards as a Means to Enhance Privacy

A. Michael Froomkin
University of Miami School of Law
<http://www.law.tm>

TPRC Conference **Draft**, Sept. 1, 2002 - subject to revision

I.	Introduction: Do Not Shoot the Messenger	1
II.	Things Are Worse than You Think	4
	A. Legislative Developments	5
	B. Vastly Increased Data Collection	9
	C. Advances in Computer Storage and Networking Technology Have Made it Vastly Cheaper to Store, Search, and Share Gigabytes of Data.	11
III.	Dangers to Liberty Arising from a National ID System	11
	A. Risks from the Legal Use of Accurate Information	12
	1. Public Sector Uses	12
	2. Private Sector	15
	B. Risks from Reliance on False Information and from Illegal Use of Accurate Information	17
	C. Risk of Over-dependance on Some Feature of the System (Completeness of Database, Ubiquity of Card or Other Token)	20
	1. The Risk of Success	20
	2. The Risk of Dependence	25
	D. Searching for Design Safeguards	27
IV.	The (Very?) Uneasy Case	29
	A. Tying Fair Information Practices to the National ID System	31
	B. Centralizing the Politics of ID Cards	35
V.	Summary	36

ABSTRACT

Once one gets past visceral revulsion, the marginal harms caused by a national ID system are fewer than one might initially believe, although there are genuine dangers to civil liberty and to privacy that we should be wary of.

A fair evaluation of the likely privacy costs of a national ID regime requires a proper understanding of the privacy baseline. A key part of the argument that the marginal cost to privacy of national ID cards may be less than it seems is the claim that things are worse than most people realize.

If the privacy baseline is as poor as I suggest then, somewhat counter-intuitively, there is a (perhaps unlikely) scenario in which national ID cards could be used as an excuse to enhance privacy.

I. Introduction: Do Not Shoot the Messenger

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 systems² 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

¹The 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].

²For 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>; Lynn LoPucki, 80 TEXAS L.J. (2002) (adding to Clarke's definitions).

³For 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>.

have a national debate on ID cards⁴ if we are lucky; if we're unlucky we'll dispense with the debate and go straight to the cards and the databases.

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 mis-uses by government officials.⁵ In its most likely forms, a national ID system could also contribute to the continuing erosion of personal privacy,⁶ 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 are not large enough to outweigh the other costs of a national ID system.⁷ 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. My argument begins with a 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, credit card, or perhaps even

⁴Current 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 Driver's License Modernization Act of 2002, H.R. 4633, sponsored by Reps. Jim Moran (D-VA and Tom Davis (R-VA)) which amends the Federal highway provisions and mandates the standardization of State driver's license systems within five years, so that each state will have "in effect a driver's license and identification card program." The system includes the establishment of standards for biometric data deployed on the card, interoperability with other identification systems, and must be part of an effort to link with other State motor vehicle databases electronically. The bill also mandates the implementation of procedures for accurately documenting the identity and residence of an individual before issuing a license or card.). However, § 815 of the Homeland Security Act of 2002 prohibits a national ID [cite].

⁵See *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.

⁶See 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>

⁷Proponents 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).

a biometric.⁸ A related claim is that the 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 databases⁹ 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.¹⁰ 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.¹¹

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 not necessarily superior to the 'no ID at all' world we have lost. The key is to take half a leaf from the legal treatment of passports and have the government own the national ID numbers; however, 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. In such a regime, the government could condition the use of the index number by both the public and private sectors on adherence to national data protection and privacy rules. To the argument that decent privacy rules at the federal level are

⁸Legislation introduced in May by Rep. Jim Moran and Tom Davis, would mandate biometric data chips in driver's licenses, *see supra* note 4. 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 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).

⁹The 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 opt-out, based in large part on existing medical records. See Simpson Garfinkle, *Database 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).

¹⁰[ACES discussion to come]

¹¹E.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)

unlikely, I respond that the proper comparison is not utopia, but rather the ‘virtual’ ID card world, on in which the locations at which privacy-destroying decisions occur 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.

II. Things Are Worse than You Think

This paper is primarily concerned with *national identification systems* in which a unique identifier (a *national ID*) is associated with every U.S. citizen and permanent resident.¹² 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*.¹³ 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.

A national ID system does not require 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.¹⁴ Government data practices are regulated by the Privacy Act, but these limits do not apply to law enforcement,¹⁵ 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

¹²The interesting question of how legitimate foreign visitors acquire temporary ID numbers, or function without them, is beyond the scope of this paper. Cf. NRC REPORT, *supra* note 1, at -.

¹³For 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>

¹⁴E.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).

¹⁵5 USC § 552A

sometimes true also, as governments sometimes seek to use their databases as a source of revenue¹⁶ – subject to a possible backlash from the public.¹⁷

Writing in 1986, Joseph W. Eaton stated, that "on a *de facto* basis, the United States already has a national ID system."¹⁸ 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 fifteen years ago.

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,

¹⁶Cf. *Lamont v. Commissioner of Motor Vehicles*, 269 F. Supp. 880 (1967) (denying injunction to block sale of DMV registry data).

¹⁷Some 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 ZDNET NEWS, available at <http://zdnet.com.com/2100-11-513639.html?legacy=zdn>.

¹⁸JOSEPH W. EATON, *CARD-CARRYING AMERICANS 2* (1986). See also *id* at 82-84.

one of the most common identity documents in the US.¹⁹ Since 1936 "there have been almost 40 congressionally authorized uses for it as an identification number."²⁰ 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 dependant tax credit.²¹ 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")²² 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.²³ Under IRCA the employer kept the I-9 on file for possible inspection rather than submitting it to a federal agency which meant that there was no serious control in place to monitor the use of false documents. In contrast, the Illegal

¹⁹See generally, United States General Accounting Office, Government and Commercial Use of the Social Security Number is Widespread (Letter Report, February 1999).

²⁰ Sobel at 56 (citing 145 Cong. Rec. E3 (daily ed. Jan. 6, 1999) (statement of Hon. Ron Paul))

²¹Internal 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 , at 56-57.

²²Immigration 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.).

²³Employers 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.

Immigration Reform and Immigrant Responsibility Act of 1996²⁴ ("IIRIRA"), established a five-state "Pilot Program" of computerized SSN verification, and also mandated the development of prototype counterfeit-resistant social security cards.²⁵ IIRIRA also requires that birth certificates and driver's licenses be standardized.

Similarly, the Personal Responsibility and Work Opportunity Reconciliation Act of 1996,²⁶ 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.²⁷ 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 1996²⁸ (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.²⁹

²⁴Pub. L. No. 104-208, 110 Stat. 3009-546 (1996) (codified as amended in scattered sections of 8 U.S.C.)

²⁵The Welfare Reform Act requires on the Social Security Administration ("SSA") to "harden" the social security card.

²⁶Pub. L. No. 104-193, 110 Stat. 2105 (1996) (codified in scattered sections of 42 U.S.C.).

²⁷There are approximately 7 million outstanding child support orders, Sobel 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>)

²⁸Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified at scattered sections of 26, 29, and 42 U.S.C.)

²⁹"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
(continued...)

Air travelers are profiled by a \$2.8 billion monitoring system that uses a secret algorithm to compare their personal data to profiles of likely terrorists.³⁰ 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.³¹ 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.³²

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."³³ Increasingly, data collected by law enforcement agencies includes digitized biometric information, including DNA profiles.³⁴

After tax returns and the census, both of which are subject to special privacy protections,³⁵

²⁹(...continued)

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).

³⁰See Declan McCullagh, You? A Terrorist? Yes!, Wired, Apr. 20, 1999 <<http://www.wired.com/news/news/politics/story/19218.html>>

³¹See Security of Checked Baggage on Flights Within the United States, 64 Fed. Reg. 19220, 19222 (1999) (Apr. 19, 1999) [updated cites coming] John Gilmore: Free to Travel, 28 Privacy Journal 1 (Aug. 2002).

³²Gilmore suit.

³³Eaton, *supra* note 18 at 104.

³⁴See, 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 requirement); *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).

³⁵Although the IRS Code, 26 U.S.C. § 6103 (1988 & Supp. V 1993), provides for the
(continued...)

one of the most widespread governmental data collection device is driver's license applications, as most of the US adult population holds a driver's licences, 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 require an (often digitized) photo.

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.³⁶ And the federal government combs similar data to find possible tax cheats,³⁷ and other suspected lawbreakers.³⁸ 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.³⁹ 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

³⁵(...continued)

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.

³⁶See 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>.

³⁷See, 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).

38

³⁹See 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.⁴⁰ 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.⁴¹

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."⁴² 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 delivery⁴³

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

⁴⁰e.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/>

⁴¹See 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).

⁴²LexisNexis, BatchTrace, <http://www.lexisnexis.com/batch/batchtrace/features.shtml>

⁴³Id.

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 led 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.⁴⁴

C. Advances in Computer Storage and Networking Technology Have Made it Vastly Cheaper to Store, Search, and Share Gigabytes of Data.

As I've described elsewhere,⁴⁵ advances in computer storage and networking technology have made it vastly cheaper to store, search, and share gigabytes of data. 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.⁴⁶

III. 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-dependence on some feature of the system (completeness of database, ubiquity of card or other token).⁴⁷ Most of

⁴⁴See 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).

⁴⁵See Froomkin, *supra* note 6.

⁴⁶See *id.*

⁴⁷The 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

(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 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

⁴⁷(...continued)

lack of subject knowledge of data flows

blacklisting

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>.

at the street corner, a freedom now badly eroded in airports, other places of mass transit, courthouses and other public buildings.⁴⁸ 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,⁴⁹ then either the body will become our ID card or we shall all wear masks.⁵⁰

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 desirable⁵¹, many are not. 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.

A large and rich database invites predictive profiling,⁵² 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.⁵³ 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

⁴⁸See 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).

⁴⁹Current 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).

⁵⁰Both 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>.

⁵¹For example, data matching to combat fraudulent applications for benefits.

⁵²On 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>

⁵³The 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.

conviction information is sent to neighbors of released felons whether those neighbors ask for it or not.⁵⁴ This may only be the tip of the iceberg; a publicly available database might for example contain current addresses and all conviction histories,⁵⁵ creating a class of "social leper."⁵⁶ Whether the loss of "social forgiveness, the principle that over time a citizen's crimes are forgiven," is a good thing or not may be debatable.⁵⁷ But any change of that magnitude should be debated, rather than be a side-effect of technology.

Today, the Privacy Act of 1974⁵⁸ constrains the ability of the federal government 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, and there in the current political climate it is not likely that the courts would find comparable protections in the US Constitution.

The Fourth Amendment protects against unreasonable 'searches' without a warrant. Courts grant search warrants only on a showing of particularized suspicion. A trawl of a database to find potential suspects by definition does not involve a particularized suspicion of anyone, and it is highly unlikely that a request for such a search would meet the standard needed to get a court to issue a warrant. Indeed, a database search more closely resembles a 'general search,' one of the evils that the Fourth Amendment was designed to prevent.⁵⁹ On the other hand, since the subjects 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

⁵⁴'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).

⁵⁵The issue of whether and when convictions should be 'spent', i.e. forgotten, is a controversial one. See T. Markus Funk, *A Mere Youthful Indiscretion? Reexamining the Policy of Expunging Juvenile Delinquency Records*, 29 U. MICH J.L. REF. 885 (1996).

⁵⁶According to Funk, *supra* note 55, 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).

⁵⁷For some though-provoking if rather cold-hearted arguments as to why some common forms of social forgiveness might be harmful, see Funk, *supra* note 55.

⁵⁸Codified at 5 U.S.C. § 552A.

⁵⁹See Michael Adler, Note, *Cyberspace, General Searches, and Digital Contraband: The Fourth Amendment and the Net-Wide Search*, 105 YALE L.J. 1093 (1996).

being the sort of reasonable search that does not require a warrant.⁶⁰ 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.

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 property right in federally held data would provide a special protection, as any statutory attempt to remove this layer of protection would constitute a 'takings' entitling every subject in the database to financial compensation -- and thus providing a strong disincentive to any Congress contemplating changing the database's status.

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. Where currently there is no mechanism by which unproved denunciations to the police, even to the FBI, become part of a file that is communicated widely among government officials, the national ID system -- fueled perhaps by something such as Attorney General John Ashcroft's TIPS proposal -- would create a mechanism by which unverified derogatory information could circulate widely, at least among government agencies.⁶¹ In addition to the obvious possible harms of having law enforcement use these tips as the 'reasonable' basis for traffic stops and searches, there is the more fundamental harm to the body politic of developing an informer and dossier culture.

2. Private Sector

The private sector could legally misuse accurate information to engage in several forms of legal discrimination.⁶² 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

⁶⁰Id. at 1097.

⁶¹It 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.

⁶²See 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 link between fingerprint symmetry and sexual preference. Many jurisdictions do not forbid discrimination on the basis of sexual preference.

is always the danger of the accidental or intentional release of embarrassing facts.⁶³

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 face recognition equipment might 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. As I've argued before,

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

⁶³As 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.

demographic information thought to be correlated with preferences.⁶⁴

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.

A particularly likely consequence of a national ID regime would be to simply 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 DRM-enabled world also undermine the consumer's ability to acquire reading matter anonymously.⁶⁵ 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.

B. Risks from Reliance on False Information and from Illegal Use of Accurate Information

A fundamental problem with any national ID system 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.⁶⁶

A new centralized system would not only build on old risks of reliance on false information but introduce new ones: a centralized database relied on by government agencies is a particularly powerful place for someone to plant false information. There are at least three distinct dangers. The

⁶⁴*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>.

⁶⁵For an argument that the Constitution recognizes such a right see Julie Cohen, *The Right to Read Anonymously*

⁶⁶[N Report]

first is changing the contents of a record to incriminate someone, for example inserting an image of someone into a photo taken by a surveillance camera near the scene of the crime -- the virtual equivalent of planted evidence. 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.⁶⁷ The 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 don't. 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. The third 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, it's too likely to be trusted.

A national ID system also creates new opportunities for the illegal use of accurate information. Here, however, the problem is primarily one of increased opportunity, rather than of new classes of dangers. Similarly, chief new danger relating to reliance on false information arises from the possible ubiquity of the database. The more people there are with access to the central database, and the greater the number of legitimate reasons to use it, the greater the likely propagation and harm from any inaccurate information.

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 was the reality of a J. Edgar Hoover 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 today, any increase in the quantity and scope of the data will only make it a more attractive place to snoop.

One argument often made against a national ID system is that were there ever to be a totalitarian government⁶⁸ the database would make roundups of disfavored classes easier.⁶⁹ Certainly

⁶⁷Keeping 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>.

⁶⁸Cf. SINCLAIR LEWIS, *IT CAN'T HAPPEN HERE* (1935).

⁶⁹See, 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, (continued...)")

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"⁷⁰ -- give this concern a new saliency. Even given the amount of data requested in the decennial census, and the charges that it was misused to help locate Japanese-Americans for their internment during WWII,⁷¹ it still could 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.⁷² Personally I find this argument unpersuasive given the existence of massive private databases such as Batchtrace.⁷³ A government prepared to build interment camps is prepared to buy, or take, the privately held data it believes it needs.

Commentators have also argued that large databases facilitate illegal private discrimination,⁷⁴ 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.⁷⁵ Certainly many private acts of

⁶⁹(...continued)

which are more attuned to the openness and freedoms which are supposed to be the hallmarks of democratic government.").

⁷⁰See Katharine Q. Seelye, *Judge Questions Detention of American in War Case*, NY Times (Aug 14, 2002), <http://www.nytimes.com/2002/08/14/national/14DETA.html>

⁷¹DAVID BURNHAM, *THE RISE OF THE COMPUTER STATE* 20, 23-25 (1983).

⁷²See 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>

⁷³See supra text at note -.

⁷⁴See generally Oscar H. Gandy, Jr., *THE PANOPTIC SORT: A POLITICAL ECONOMY OF PERSONAL INFORMATION* (1993).

⁷⁵Whether this is really a national ID issue or not is complex. Of employers are able to request DNA testing before hiring then arguably whether there is a database or not is moot. 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. 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 (continued...)

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.⁷⁶ Unfortunately, however, if the ID system relies on a biometric and the thief found a way to counterfeit it, the subject may have a problem. Even if it is easy to change ID numbers, it is hard to change corneas.

C. Risk of Over-dependance on Some Feature of the System (Completeness of Database, Ubiquity of Card or Other Token)

1. The Risk of Success

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. General reliance on national ID card or on a centralized dossier creates at least three sorts of risks. First, by creating a certain sense of security it may make the users more vulnerable to identity theft -- and (especially if there is a biometric component to the authentication mechanism) may make it much more difficult to generate a replacement ID once the theft of the original is discovered. Unless designed implausibly carefully, a national ID system is the sort of system that "fails badly."⁷⁷ "Okay, somebody steals your thumbprint, ...Because we've centralized all the functions, the thief can tap your credit, open your medical records, start your car, any number of things. Now what do you do? With a credit card, the bank can issue you a new card with a new number. But this is your thumb—you can't get a new one."⁷⁸

⁷⁵(...continued)

theory -- driving increasing numbers of employers to test anyway. Thus, in some but not all scenarios the national database makes a big difference.

⁷⁶The difficulty of having corrective data catch up with false data is often cited as one of the most painful aspects of identity theft.

⁷⁷See Charles C. Mann, *Homeland Insecurity*, ATLANTIC MONTHLY (Sept. 2002) (explaining that systems "fail badly" unless designed so that "when something goes wrong with security, the system should recover well.").

⁷⁸Id. (quoting security expert Bruce Schneier).

A second class of danger is that routinized credentialing destroys the ability of people to move and transact anonymously. This may seem like an advantage to some, but as I've argued elsewhere, the ability to be anonymous and pseudonymous is an important privacy right with implications for political and civil liberty.⁷⁹

Depending on who has the ability to attach information to an actual or virtual file, a national database system may make data subjects more vulnerable to the creation of false or irrelevant information. This is hardly an unfamiliar problem in either the private or public sectors. If the information resides in a central location then it can partly be cured by *transparency* -- ensuring that the data subject has access to records about him; the more dispersed the records are, though, the less meaningful this protection. Thus, the United States has legislation regulating key private sector collectors and providers of consumer profiles, notably the Fair Credit Reporting Act.⁸⁰ For all that the courts have interpreted it generously,⁸¹ the FCRA, however, has its limitations. First, consumers are only likely to learn about derogatory information in their credit reports if they ask to see them.⁸² 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.⁸³

⁷⁹See 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>.

⁸⁰Fair 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.

⁸¹Important 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).

⁸²However, 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.

⁸³Fair 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
(continued...)

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]."⁸⁴

SPN codes would be illegal today. In principle,⁸⁵ the federal government may not disclose personal data without consent of the data subject.⁸⁶ 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

⁸³(...continued)

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 Tech. L.J. 71, 90 (1996).

⁸⁴See 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.

⁸⁵There 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).

⁸⁶Id.

maintained databases, arguably not even if the government is the sole client for the information.⁸⁷

Although the Privacy Act does say that non-law-enforcement agencies generally may not collect information about First Amendment activities,⁸⁸ it imposes few other limits. Data must be limited to "such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President"⁸⁹ 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."⁹⁰ 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 and 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.⁹¹

Even with the Privacy Act in place, both government law enforcement agencies are allowed to amass dossiers that they can mine to create profiles. Indeed, it's alleged that "a federal agency

⁸⁷Indeed, 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 § 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."

⁸⁸An 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).

⁸⁹5 USC § 552a(e)(1).

⁹⁰Id at (e)(6).

⁹¹See 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.

involved in espionage actually did a rating of almost every citizen in this country...based on all sorts of information."⁹² 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 application⁹³) is nothing like a search. The data have been alienated before the search, they are no longer the subject's, and their new owner 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; reasonable expectations, after all, are always set by whatever the law provides. Once captured by a third party, the data are in a state akin to that of personal property left in plain sight. And it is long-settled that the police may examine anything left in plain view.⁹⁴ 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, government might "search" data about us for law-enforcement purposes.

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." 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

⁹²Erik Baard, *Buying Trouble*, VILLAGE VOICE (June 24, 2002), <http://www.villagevoice.com/issues/0230/baard.php>

⁹³Data 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 ability 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).

⁹⁴See *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).

particularized suspicion are issues that can no longer be avoided.

2. The Risk of Dependence

One of the greatest dangers 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 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."⁹⁵

Suppose, for example, that an enhanced national ID card⁹⁶ 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.⁹⁷ The threat of removal of this card, or of putting a 'hold', query, or other black mark in to 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 might be missing. For example, if no taking of private property is involved, the only possible grounds for a due process based objection is one based on a liberty interest. While such arguments sometimes but not always swayed the courts in the context of passport denials, it was easy to show that without a passport foreign travel was next to impossible. Its doubtful whether such a showing would be as easy in cases about a national ID card (or number), especially in its early days.

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

⁹⁵NRC REPORT, *supra* note 1, at 30-31.

⁹⁶The problem is equally real with a national ID system that lacks a card, but is easier to visualize with a tangible example.

⁹⁷So named after *Terry v. Ohio*, 392 U.S. 1 (1968).

card.⁹⁸ If others, such as airlines, are allowed to access this information, the government may be able to plead that it should not be responsible for the consequences. I return to the critical issue of the government's ability to take or burden the ID in Part IV below.

While there may be difficulties in sanctioning people for information in their dossiers, there are likely to be considerably fewer barriers to making a 'clean' record a precondition for permits or benefits. Lest this seem far-fetched, consider that "[f]ifteen states now link driver's licenses with school attendance and performance."⁹⁹ 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 that can be summarized in a chart:

Type of Danger..	From Government Actors	From Private Actors
Risks from legal use of accurate info	Virtual 'general searches' on data / data mining TIPS (e.g. risk of anonymous denunciations) Profiling (danger of false positives, stigmatizing) Efficient stigmatization (mega-Megans laws) Function creep Moral/psychological costs to free society.	Profiling, legal types social/political discrimination More perfect price discrimination Aids enforcement of Digital Rights Management (DRM) Threat to anonymity Accidental or intentional release of embarrassing facts.

⁹⁸Allegedly, frequently buying a pizza with a credit card is one of the factors that 'predicts' likely terrorists. See Bard, *supra* note (quoting Larry Ponemon, CEO of consulting firm Privacy Council).

⁹⁹Robert 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
<p>Risks from illegal use of accurate info</p> <p>Risk of reliance on false information (whether created intentionally or not)</p>	<p>"J. Edgar Hoover problem" (abuses by malign officials, in high positions and low)</p> <p>Unsanctioned snooping, by government employees</p> <p>Totalitarian roundups made easier</p> <p>ID's only as good as data used to generate them</p>	<p>Profiling, illegal types social/political discrimination</p> <p>Blackmail [already illegal]</p>
<p>Risk of over-dependance on some feature of the system (completeness of database, ubiquity of card or other token)</p>	<p>Transparency issues</p> <p>Greater harm from identity theft; system likely "fails badly"</p> <p>Threat of removal (or addition of notation) becomes powerful sanction</p> <p>Desire to collect maximum information 'just in case'</p> <p>Function creep</p> <p>Threat to anonymity</p>	<p>Transparency issues</p> <p>Greater harm from identity theft; system likely "fails badly"</p>

D. Searching for Design Safeguards

The 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 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, 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 a 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.¹⁰⁰ 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.¹⁰¹

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.

Fundamentally, the idea of a centralized national ID system is inimical to individual control over all 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.

A national ID system threatens anonymous and pseudonymous speech and commerce. The threat to anonymous speech impacts a valuable constitutional right -- one need most by persons least able to speak out for it, since they are the ones who have a legitimate fear of retaliation.¹⁰² 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 and also for multiple pseudonyms.¹⁰³

¹⁰⁰See generally Roger Clarke, *Chip-Based ID: Promise and Peril* (1997), <http://www.anu.edu.au/people/Roger.Clarke/DV/IDCards97.html>.

¹⁰¹Id.

¹⁰²It may also make whistle blowing more difficult and dangerous.

¹⁰³Roger 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
(continued...)

Good error handling is essential. There needs to be a way 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.¹⁰⁴

IV. The (Very?) Uneasy Case

Part III suggests that 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 very little difference of degree. The only substantial¹⁰⁵ 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.

The real issue is the collection and use of personal data.¹⁰⁶ The primary importance of a

¹⁰³(...continued)

- 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 100.

¹⁰⁴See, 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>

¹⁰⁵There 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.

¹⁰⁶See, 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*, (continued...)

physical national ID card is its symbolic effect and political consequences.¹⁰⁷ Other than the possible psychological effect, ID Cards matter not because they are ID cards, but because their introduction becomes an excuse, or a shorthand, for greater scope or greater centralization of national databases. 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.¹⁰⁸

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.

¹⁰⁶(...continued)

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.mvca.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).

¹⁰⁷There 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 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.

¹⁰⁸See Fromkin, *supra* note 6.

A. 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 Rotenberg, "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."¹⁰⁹ The "OECD Guidelines," or more formally the 1980 Organization for Economic Co-operation and Development issued its Recommendations Concerning and Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data,¹¹⁰ 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:

- 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."¹¹¹
- 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".¹¹²
- 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.¹¹³
- Individuals should have a means of enforcing rules protecting their data privacy.¹¹⁴

Whole-hearted application of these principles to the public sector¹¹⁵ 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.

¹⁰⁹Marc 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) .

¹¹⁰OECD, 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> [hereinafter OECD Guidelines]

¹¹¹OECD Guidelines ¶ 7.

¹¹²Id. at ¶ 8.

¹¹³Id. at ¶¶9-12.

¹¹⁴Id. at ¶ 19.

¹¹⁵Many of these principles are already found in the Privacy Act.

Although quite sweeping, the OECD Guidelines have been criticized as insufficient,¹¹⁶ 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.¹¹⁷ While there are a number of federal privacy laws, only the federal Privacy Act of 1974¹¹⁸ 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.¹¹⁹ For example, the Federal Wiretap Act¹²⁰ imposes limits on wiretaps. The Electronic 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.¹²¹ 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.¹²²

In the absence of any reason to believe that technological solutions will be adopted in the marketplace,¹²³ 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

¹¹⁶See, e.g. Gary T. Marx, *Ethics for the New Surveillance* in VISIONS OF PRIVACY 39 (Colin J. Bennett & Rebecca Grant, ed.s 1999).

¹¹⁷See Fromkin, *supra* note 6.

¹¹⁸Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (codified as amended at 5 U.S.C.A. § 552a

¹¹⁹Cf. Fred H. Cate, *The EU Data Protection Directive, Information Privacy, and the Public Interest*, 80 IOWA L. REV. 431, 438 (1995).

¹²⁰18 U.S.C.A. § 2518 (2000)

¹²¹ECPA. See Steve Jackson Games.

¹²²See, 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)

¹²³A good discussion of the (un)likelihood of this is Rotenberg, *supra* note 109.

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.¹²⁴

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.

It seems fair to assume that any new federal ID numbering system would be adopted by the private sector. The private sector makes routine use of the SSN despite its known security and uniqueness flaws; a new number that promised (whether or not it actually provided) uniqueness, full coverage, and greater security, undoubtedly would 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.

A more centralized national information system, or even a decentralized one that relied on a common identifier, would allow incorrect information to propagate more widely, which is harmful. But it would also allow corrections to catch up more quickly. Which effect would predominate seems a fundamentally empirical question.

The simplest way of conditioning the use of a new ID number by third parties on adherence to fair information practices would be to have the government retain ownership of the ID number and any associated card, following the passport model,¹²⁵ and to issue appropriate regulations. As the legal history of the passport teaches us, this strategy is dangerous because it also opens the door to regulations that might substantially effect the freedom of anyone who used the number or card.¹²⁶

¹²⁴On privacy enhanced digital cash, see generally A. Michael Froomkin, *Flood Control on the Information Ocean*.

¹²⁵See *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)

¹²⁶Another 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...

In the 1956 case of *Kent v. Dulles*,¹²⁷ 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.¹²⁸

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.¹²⁹ 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 suggest the person seeks to leave the country to avoid unpleasant legal consequences.¹³⁰ 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

¹²⁷357 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).

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

¹²⁹*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).

¹³⁰For 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

of the United States."¹³¹

A national ID system that allows the government to suspend what might easily become the cornerstone of a citizen's transactional identity (and might interfere with the right to travel if used in tolls) cannot be left to the uncertainties of a legal regime that might or might not distinguish it from a passport. A better model would be to vest ownership of the number and any associated card in the person to whom it refers. Giving individuals ownership of their number means that due process unquestionably attaches to governmental attempts to regulate their use and enjoyment of it.

Arguably, this property right ought to extend to some of the data also. The case for having people own at least part of the data the government held about them is that it would more clearly invoke the warrant requirement before the government 'searched' the data as part of a data-mining operation. Here, however, the picture is murkier. The government could probably work around any such limit by buying access to commercial databases -- subject only to whatever OECD Guideline limits had been imposed on private data by statute (a week reed since the OECD Guidelines contemplate exceptions for law enforcement). Furthermore, as Jessica Litman has argued, commodified data is information that is prepared to be traded,¹³² and it seems odd to organize a privacy regime around data that is packaged in a legal form ready to be sold.

B. Centralizing the Politics of ID Cards

As noted above, since the relative success of the Privacy Act of 1974 that regulates data held by the federal government, privacy advocates in the US have enjoyed only sectoral, and sometimes limited success in their attempt to secure federal protection for data privacy. The privacy provisions of the Gramm-Leach-Bliley Financial Modernization Act of 1999 are a case in point: they are, in practice, quite weak.¹³³ 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 a mixed blessing, for not only would it allow privacy campaigners to focus on one debate, but so too would it allow interests that tend to oppose restrictions on the use of personal data to unite their lobbying efforts.

¹³¹Id.

¹³²See, e.g. Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283 (2000).

¹³³See Poggemiller, *supra* note 11, 132.

There are reasons to believe that a centralized system, especially one that relies on physical cards, would greatly increase the 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 experience in Japan, not a nation known for protest, supports this.¹³⁴ The UK is currently engaged in a consultation exercise on so-called "Entitlement Cards"¹³⁵ that has also caused protests.

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."¹³⁶ While not justifying the enterprise, a privacy agency might be an additional silver lining.

V. Summary

A fair evaluation of the likely privacy costs of a national ID regime requires a proper understanding of the privacy baseline. A key part of the argument that the marginal cost to privacy of national ID cards may be less than it seems is the claim that the data privacy picture is worse than most people realize, and that the odds are it will continue to get worse quickly.

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. Defining the number as the property of the data subject would be a means of beginning to address this danger.

¹³⁴Japan 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).

¹³⁵ 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).

¹³⁶Rotenberg, *supra* note -, at 94-95.

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 the numbering system would be very attractive to businesses, they would have an incentive to adopt it, and the fair information practices obligations with it.