CREATING A VIRAL FEDERAL PRIVACY STANDARD

A. Michael Froomkin*

Abstract: National identification ("ID") cards appear increasingly inevitable. National ID cards have the potential to be repressive and privacy-destroying, but it is also possible to design a system that captures more benefits than costs. Because the United States currently lacks a single, reliable credential, private businesses have trouble authenticating their customers and matching data among distributed databases. This Article argues that the desire for reliable ID creates a window of opportunity for the federal government to strike a bargain: offer private businesses the use of a reliable credential in the form of a national ID card, on the condition that they abide by a privacy standard set and owned by the United States. But the government must act quickly—the Real ID Act of 2005, which sets up a national standard for the issuance of state driver's licenses, is poised to become effective in May 2008. This law does not provide for privacy protections, and once it goes into effect the opportunity to leverage such protections on a national ID card will be greatly reduced.

Introduction

There is a narrow window of opportunity for the creation of a simple federal identification ("ID") standard that, if properly designed, could have substantial privacy-enhancing properties for private sector uses of personal information. If we hurry, the government's standard-setting powers can be used to enhance privacy protections for holders of a hypothetical enhanced (and even mandatory) national ID card. The key to this apparent paradox is a bargain enforced by legislation: the government issues a secure credential and takes on the substantial effort of initially verifying the identity of applicants. It produces a card or other token with standardized and easily-verified identifiers, and assigns each person an identifier—a government-standard index number akin to a Social Security number ("SSN"). Businesses will find the authenticating features of the card

 Professor, University of Miami School of Law. I would like to thank Caroline Bradley and the participants in the 2006 *Boston College Law Review* Owning Standards symposium for their thoughtful comments.

attractive, and—at least until private-sector data management techniques improve—should find the opportunity to use the index number to organize and share data about consumers attractive as well.

By keeping ownership and control of the identification standard,[1] and especially the unique ID numbers, the government would be able to set privacy-enhancing conditions on the private sector's use of the card. No one would be required to participate, but only those firms agreeing to abide by a set of federally-determined national privacy rules would be allowed to use these authenticating, taxpayer-funded credentials, and in particular to store the new ID number or to use it to organize their customer data. Furthermore, participating firms would only be allowed to share any data ever assembled or organized with the aid of that index number with other firms who had agreed to be bound by the same national privacy rules—in effect, a viral privacy provision.

If any privacy-enhancing federal standard is to be effective, it needs to be adopted soon. Otherwise, we risk ending up with the worst of both worlds: mandatory ID cards and less privacy. Already, we face two onrushing deadlines, one from the market and one from the states and Congress. Competing market-based standards are slowly emerging, and sooner or later the almost inevitable network effects will create an entrenched user base whose market and political clout would make change via a new credential even more unlikely. Meanwhile, Congress has already laid the groundwork for an unhappy result by passing the REAL ID Act of 2005 ("REAL ID")[2] while giving little if any thought to how the credentials it mandates will likely be used in the private sector, much less to the long-run effects on personal privacy.

This Article's inquiry into the use of government power to mandate pro-privacy ID card standards is part of a larger project on the possible uses and abuses of national ID cards. Thus, it may be helpful to begin by summarizing the most relevant parts of the overall argument of which the claims in this Article form a part.[3] National ID

---

[1] Who should own and control both the data on the card and the data associated with the card are separate questions.

[2] The REAL ID Act of 2005 was enacted as part of the 2005 Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief. Pub. L. No. 109-13, div. B, 119 Stat. 231, 302 (codified in scattered sections of 8 and 49 U.S.C.A.); *infra* notes 115–134 and accompanying text.

[3] My object in providing this summary is less to persuade the reader of the accuracy of what may seem to be controversial claims—a task I plan to undertake elsewhere—than it is to provide context that may explain why I believe that, far from being as dry and hypothetical as they may seem, national ID card standards are actually an important, even urgent, issue.

cards are a surprisingly emotional subject for many, conjuring mental images of black-and-white movies featuring jack-booted soldiers with fierce dogs and large guns moving down the aisles of trains and saying "papers, please" in Hollywood German accents. I should start, therefore, by stating that I am not arguing that national ID cards are inherently good, but nor do I find them inherently evil. My claim is that given the forces pushing for them, some form of national ID is likely to emerge soon (and that a "virtual ID card" almost exists already)[4] and that if we are going to have a debate about them it should be informed by a richer understanding of their potential costs and benefits. Furthermore, the extent to which any national ID card regime is, on balance, a good or bad thing depends critically on how it is designed. It is clearly possible to design national ID cards that are privacy-destroying and can be enlisted in a program of national repression. With care, however, it may be possible to design a system that captures more benefits than costs.

Evaluating the overall costs and benefits of ID cards, especially as regards their effects on freedom and privacy, requires careful attention to several factors beyond the scope of this paper, among them the interactions between public and private uses of ID cards, who has authority to use or demand an ID card, who determines what data is on the card, how it is secured, and who can access that data. One must also be sensitive to what one selects as a baseline for comparison. In a privacy nirvana, ID cards would have no place. If, however, one takes the baseline to be current practices rather than what one wishes current practices were, it may be possible that the right sort of ID cards would, on balance, contribute to personal privacy. Both the possible public and the possible private uses of a national ID card raise tough questions. Proposals for a national ID card often focus on the (alleged) advantages to law enforcement, prevention of terrorism, public benefits, voter authentication, public health, and the delivery of various other public services. Each of these applications raises complex and controversial issues.

This Article, however, addresses a key element of the private sector issues. Although these issues are not easily resolved, they are refreshingly straightforward by comparison to some of the public sector applications.

---

[4] *See* A. Michael Froomkin, The Uneasy Case for National ID Cards 18–27 (Mar. 2004) (unpublished manuscript, *available at* http://personal.law.miami.edu/~froomkin/articles/ID1.pdf) (arguing that the ability to link distributed databases of personal information, such as credit ratings, driver's licenses, SSNs, and even DNA, has already created a patchwork version of a national ID).

I. Some Context

A discussion of the costs and benefits of a standardized national ID card begins with a clear understanding of current conditions, the baseline for comparing the merits of any proposal. As described further below, the United States currently uses a mix of identity documents, each of which has serious flaws and limitations.[5] These limitations cause difficulties for firms seeking to authenticate customers, as well as for those trying to do data matching among distributed databases. The very confusion those firms experience is itself a limited privacy-enhancing feature of the system. It seems inevitable, however, that data matching will continue to improve in ways that make it unwise to put much faith in these transaction costs as the basis for long-term data privacy protection.

Although national ID cards are common in many parts of the world,[6] it is an article of faith in many quarters that the United States does not have one. In fact, rather than one ID card we have many: notably, voter ID cards, SSNs, driver's licenses, and credit cards, to name only the most common. Each type of ID was created for a limited purpose, and each is significantly flawed or insecure. As businesses and government have felt a greater need to find a way to authenticate individuals and associate them with existing records, the private sector has come to rely on existing forms of government-issued identification. In particular, SSNs and driver's licenses have gradually become semi-official national identity documents; the other major civilian federal identity credential, the passport, is rarely if ever used for private transactions other than oc-

---

[5] *See infra* notes 21–26 and accompanying text.

[6] *See* Julia Scheeres, *ID Cards Are* de Rigueur *Worldwide*, Wired News, Sept. 25, 2001, http://www.wired.com/news/conflict/0,2100,47073,00.html (quoting Privacy International director Simon Davies as saying, "It's safe to say that the majority of countries have some kind of national identification system"); *see also* Privacy International, Identity Cards: Frequently Asked Questions, http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-61881&als[theme]=National%20ID%20Cards (last visited Oct. 23, 2006) (listing countries with ID cards).

casionally to demonstrate citizenship status for employment.[7] Indeed, fewer than one in three U.S. citizens has a passport.[8]

Although perhaps not formally mandatory, SSNs are necessary if one wishes to take paid employment or participate in the banking system. Cars are a practical necessity for most Americans who live outside the largest urban areas, making a driver's license a practical necessity for most as well. A government-produced ID is currently demanded for travel not only behind the wheel of a car, but also as a passenger on airlines, trains, intercity buses, and even local buses.[9] Although such demands are increasingly common, their legal status remains debated. In 2006, in *Gilmore v. Gonzales*, a panel of the U.S. Court of Appeals for the Ninth Circuit rejected a claim that the enactment and enforcement of the U.S. government's airline passenger identification policy violate the constitutional right to travel and the First and Fourth Amendments.[10] The court rejected the petitioner's claim "because the Constitution does not guarantee the right to travel by any particular form of transportation."[11] The panel also observed that "the identification policy's 'burden' is not unreasonable."[12] Importantly, however, the panel reached this conclusion only after characterizing the regulatory scheme as one that "requires that airline passengers *either* present identification *or* be

---

[7] U.S. employers must complete an INS Form I-9, Employment Eligibility Verification Form, for every new hire, verifying that they have checked that the new employee is eligible to work in the United States. *See* Verification of Employment Eligibility, 8 C.F.R. § 274a.2 (2006), *amended by* Electronic Signature and Storage of Form I-9, Employment Eligibility Verification, 71 Fed. Reg. 34,510 (June 15, 2006); *see also* 8 U.S.C. § 1324a(a)(1)(B), (b) (2000) (prohibiting employers from hiring workers without verifying their identity and authorization to work in the United States). A U.S. passport is one of the forms of ID employers may use to satisfy that duty. § 1324a(b)(1)(B)(i).

[8] An adult passport is valid for ten years, a child's for five years. Bureau of Consumer Affairs, U.S. Department of State, Frequently Asked Questions: Passports and Citizenship Documents, http://travel.state.gov/passport/fri/faq/faq_1741.html (last visited Nov. 2, 2006). During the last ten years, the United States issued between 5.5 and 10.1 million passports per fiscal year. Bureau of Consumer Affairs, U.S. Department of State, Passport Statistics, http://travel.state.gov/passport/services/stats/stats_890.html (last visited Nov. 2, 2006). Even if all of those passports were issued to adults, the number would still total less than one-third of the U.S. population. *Cf.* Phil Gyford's Website, http://www.gyford.com (Jan. 31, 2003, 17:14 EST) (describing the difficulty of estimating the number of U.S. passports in circulation).

[9] *See* PapersPlease.org, United States v. Deborah Davis, http://www.papersplease.org/davis/facts.html (last visited Nov. 2, 2006) (recounting demands by Denver police for ID from passengers on a municipal bus route that crosses the Denver Federal Center).

[10] 435 F.3d 1125, 1136–39 (9th Cir. 2006); *see* U.S. CONST. amend. I, IV; Shapiro v. Thompson, 394 U.S. 618, 629–31 (1969) (recognizing a constitutional right to interstate travel), *overruled in part on other grounds by* Edelman v. Jordan, 415 U.S. 651 (1974).

[11] *Gilmore*, 435 F.3d at 1136.

[12] *Id.* at 1137.

subjected to a more extensive search."[13] Thus, whether the government can require ID as a condition of air travel is still an open question. At present, however, the question remains somewhat academic, as few passengers are prepared to endure significant hassle, delay, and even possible arrest for failing to show ID when asked.

Many private-sector transactions, particularly those that involve the creation of an ongoing relationship or obligation, also involve the exchange of identification data, including name, address, telephone number, and SSN or driver's license number. Together, these data ordinarily permit the merchant to link a customer to transaction and credit histories maintained by commercial data brokers such as Experian and ChoicePoint.[14] Merchants' reasons for requesting ID often depend on the nature of the transaction. For example, by associating a consumer with a set of records such as a credit history, a business can estimate the likelihood of current or future payment. Verifying address and employment information provides some guarantee of recovery by suit or garnishment if payments stop. And, in other types of transactions, the firm may be required to do a records check to comply with regulatory requirements such as "know your customer" rules in financial transactions.[15] In the absence of a regulatory duty, the firm's primary motive may be to enable demographic analysis of the customer database, or to permit future targeted marketing.

The databases maintained by private firms on U.S. persons are remarkably large. Experian, for example, brags that its "North America databases contain more than 65 terabytes (65 trillion bytes) of data" including "credit information on approximately 215 million U.S. consumers and more than 15 million U.S. businesses" and "demographic information on approximately 215 million consumers in 110 million living units across the United States."[16]

---

[13] *Id.* (both emphases added).

[14] ChoicePoint describes itself as "the nation's leading provider of identification and credential verification services." ChoicePoint Home Page, http://www.choicepoint.com (last visited Nov. 2, 2006).

[15] *See, e.g.*, 12 U.S.C. § 1818(s) (2000) (requiring federal banking agencies to prescribe regulations requiring depository institutions to establish and maintain procedures reasonably designed to ensure and monitor compliance with the Currency and Foreign Transactions Reporting Act, 31 U.S.C.A. § 5311 (2006)); Financial Record-Keeping and Reporting of Currency and Foreign Transactions, 31 C.F.R. § 103 (2006).

[16] Experian, Corporate Fact Sheet, http://www.experian.com/corporate/factsheet.html (last visited Nov. 2, 2006).

These large databases contain many inaccuracies.[17] And from a firm's perspective, the process of matching a given person with the right set of records can be quite difficult, especially if the person has a common name.[18] There are many John Smiths in the United States. Between data entry errors, and inconsistent methods of data acquisition, firms' records can get mixed up.[19] Pulling together an accurate set of data regarding a given person becomes even more difficult when dealing with distributed databases.[20] In theory, as data storage gets cheaper and electronic communication becomes almost costless, it should be easy to tie together disparate sets of records to produce a single, giant, virtual dossier about each of us. But in fact it is not easy, which is why firms like Experian and ChoicePoint have something valuable to sell.

The authentication problem exists in part because there is not at present a particularly reliable identity credential. The existing Social Security cards, U.S. driver's licenses, and even passports are known to have been issued in a manner that does not provide enormous reliability. SSNs are easy to share and to fake; the most recent study, now almost a decade old, estimated that 10 million of the 269 million valid SSNs in use were duplicates, often due to fakery or human error.[21]

---

[17] *See* Colin Beasty, *Cleaning a 75 Million Name Database*, DESTINATIONCRM.COM, Dec. 1, 2005, http://www.destinationcrm.com/articles/default.asp?ArticleID=5596&TopicID=4 ("With 75 million customers, Meredith Corp., a provider of magazines, books, television broadcasting, and integrated marketing, was bound to have duplicate and inaccurate customer information in its customer database—a problem, especially when trying to cross- and up-sell products.").

[18] *See* GEOFF HOLLOWAY & MIKE DUNKERLEY, THE MATH, MYTH AND MAGIC OF NAME SEARCH AND MATCHING 11–12 (5th ed. 2004).

[19] *See id.* at 51.

[20] *See id.*

[21] SOC. SEC. ADMIN., PUBL'N NO. 12-002, REPORT TO CONGRESS ON OPTIONS FOR ENHANCING THE SOCIAL SECURITY CARD (1997), http://www.ssa.gov/history/reports/ssnreport.html; *see* IDS—NOT THAT EASY: QUESTIONS ABOUT NATIONWIDE IDENTITY SYSTEMS 36–37 (Stephen T. Kent & Lynette I. Millet eds., 2002) [hereinafter IDS—NOT THAT EASY]. The percentage of shared SSNs could be lower today, although the fraction due to fraud is certainly higher. Although the Social Security Administration (the "SSA") has never issued the same number to two wage earners as a practice, the SSA in the past sometimes used the same number—often with the suffix "A" attached—to identify both the wage earner and a relative (such as a spouse or child) who had never worked but was receiving benefits due to the wage earner's work record. *See* Yigal Rechtman, Social Security Administration & Genealogy (July 2001), http://members.aol.com/rechtman/ssafaq.html. This practice ended in the mid-1970s, *id.*, but those numbers inevitably lived on in both public and private record systems; as those beneficiaries die out, the major cause of nonfraudulent number sharing should die with them.

The SSA collects $17 billion per year in payroll tax payments for which valid SSNs cannot be found, *see* Latino Pundit, http://www.latinopundit.com (Mar. 12, 2006, 19:24 EST), which suggests that there are many fake numbers used by undocumented aliens.

Currently, providing a domestic birth certificate, a registration fee, and some evidence of a local address is more than enough to acquire a driver's license in most states; providing a driver's license, another fee, and a certified birth certificate suffices for a passport.[22] Although modern practices are improving, birth certificates have traditionally been anything but standardized, issued by hospitals with no federal and usually little state regulation.[23] As a result, a person (or machine) presented with a birth certificate is hard put to tell if it is authentic, much less if it is accurate; like driver's licenses and passports, birth certificates are not standardized, so that determining whether a particular certificate is authentic requires substantial research.[24] Nor are these documents strongly linked to the owner, which enables several people to present one ID as their own.[25] What is more, ID-issuing agencies do not guard very heavily against counterfeiting.[26]

The authentication problem is particularly important in certain sectors, such as the financial sector, where the consumer takes on a long-term obligation of some sort. It also matters in employment relationships where the employee requires a special degree of trust or a background check, such as daycare. For many firms, however, particularly those whose primary interest in personal data is to enhance their marketing efforts, the data-matching problem is the key. For these firms, the authentication problem is that even when consumers identify themselves, they do not do so in a consistent manner.[27]

Difficult as it may be to do a high-quality job, there is clearly a lot of data matching occurring in the United States. Experian, for example, "provides address information for more than 20 billion promotional mail pieces to more than 100 million households every year," and total sales exceed $1.3 billion per year.[28] And, at present, it is happening without much privacy protection for the people whose information is being sorted and traded. There are very few national limits on the sharing of private transactional data collected by persons not classified as professionals. Perhaps the most important are the Health Insurance

---

[22] *See* Bureau of Consumer Affairs, U.S. Department of State, How to Apply in Person for a Passport, http://travel.state.gov/passport/get/first/first_830.html (last visited Nov. 2, 2006).

[23] Office of the Inspector Gen., U.S. Dep't of Health & Human Servs., Birth Certificate Fraud 2 (2000), *available at* http://oig.hhs.gov/oei/reports/oei-07-99-00570.pdf.

[24] *Id.*; *see* IDs—Not That Easy, *supra* note 21, at 30.

[25] IDs—Not That Easy, *supra* note 21, at 30.

[26] *Id.*

[27] On authentication generally, see Who Goes There? Authentication Through the Lens of Privacy 33–54 (Stephen T. Kent & Lynette I. Millett eds., 2003).

[28] Experian, *supra* note 16.

Portability and Accountability Act of 1996 ("HIPAA")[29] and the Fair Credit Reporting Act.[30] HIPAA creates a new regime of privacy regulations, including a requirement that patients specifically agree to releases of their medical information.[31] The Fair Credit Reporting Act, in addition to having rules designed to make credit reports more accurate, also has a few rules prohibiting credit bureaus from making certain accurate statements about aged peccadilloes, although even this statute of limitations does not apply to reports requested for larger transactions.[32] There are a few other federal data privacy protections. The Cable Communications Policy Act of 1984 forbids cable operators and third parties from monitoring the viewing habits of subscribers.[33] Cable operators must tell subscribers what personal data is collected and, in general, may not disclose it to anyone without the subscriber's consent.[34] The "Bork Bill," formally known as the Video Privacy Protection Act of 1988, also prohibits most releases of customers' video rental

---

[29] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified in scattered sections of 26, 29, and 42 U.S.C.).

[30] Fair Credit Reporting Act, 15 U.S.C. § 1681 (2000 & Supp. III 2003).

[31] The revised HIPAA regulations can be found at 45 C.F.R. §§ 160, 164 (2006). Two works can provide to the reader a useful introduction to HIPAA. *See* Diane Kutzko et al., *HIPAA in Real Time: Practical Implications of the Federal Privacy Rule*, 51 DRAKE L. REV. 403, 410–36 (2003); Susan T. House & John R. Price, HIPAA: How Ill Are My Documents, and Whom May I Tell About It?, Presentation Before the American College of Trust and Estate Counsel in San Antonio, Texas 1–4 (Mar. 11, 2004), *available at* http://d2d.ali-aba.org/_files/thumbs/rtf/01-House-HIPAA_thumb.pdf.

Many parts of HIPAA are enormously controversial and have faced a wide range of critiques. *See generally* Sharona Hoffman & Andy Podgurski, *In Sickness, Health, and Cyberspace: Protecting the Security of Electronic Private Health Information*, 48 B.C. L. REV. (forthcoming Mar. 2007); Meredith Kapushion, Comment, *Hungry, Hungry HIPAA: When Privacy Regulations Go Too Far*, 31 FORDHAM URB. L.J. 1483 (2004); David R. Morantz, Comment, *HIPAA's Headaches: A Call for a First Amendment Exception to the Newly Enacted Health Care Privacy Rules*, 53 U. KAN. L. REV. 479 (2005); Marie C. Pollio, Note, *The Inadequacy of HIPAA's Privacy Rule: The Plain Language Notice of Privacy Practices and Patient Understanding*, 60 N.Y.U. ANN. SURV. AM. L. 579 (2004).

[32] See 15 U.S.C. § 1681c(a), which prohibits reporting of bankruptcies that are more than ten years old; reporting of "[c]ivil suits, civil judgments, and records of arrest that, from date of entry, antedate the report by more than seven years or until the governing statute of limitations has expired, whichever is the longer period"; reporting of tax liens paid seven or more years earlier; and reporting of other noncriminal adverse information that is more than seven years old. None of the prohibitions apply if the transaction for which the report will be used exceeds $150,000, or the job on offer pays more than $75,000 per year. *Id.* § 1681c(b); *see also id.* § 1681k(a)(2) (requiring that consumer credit reporting agencies have procedures in place to verify the accuracy of public records containing information adverse to the data subject).

[33] *See* Cable Communications Policy Act of 1984, 47 U.S.C. § 551(b) (2000 & Supp. III 2003).

[34] *Id.* § 551(a)(1), (c).

data.[35] There are also an increasing number of state data privacy rules, notably rules requiring disclosure of breaches after they occur.[36]

Meanwhile, four complementary developments are creating a virtual national ID system. First, a number of legislative initiatives have required the creation of (ostensibly) special-purpose databases, each of which covers a substantial fraction of the population.[37] Second, increased use of credit and debit cards, store loyalty cards, web-based marketing, and other private initiatives has allowed retailers and financial intermediaries to amass great amounts of data on consumers.[38] 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.[39] Fourth, advances in computer storage and networking technology have made it vastly cheaper to store, search, and share the gigabytes of data resulting from these developments.[40] The result is a hybrid public-private system in which a very great amount of information about almost every U.S. resident is available for a small fee. Much of this information is currently distributed on separate networks, but the technology to tie them together exists.[41]

II. Enlisting the Government's Standards-Making Power to Create Viral Privacy

Any future national ID card will be driven, in the main, by governmental aims. The justifications offered at various times include: (1) the hope that a secure credential would make it easier to validate citizenship and visa status and thus make undocumented immigrants unemployable, which in turn may reduce the incentive to enter the

---

[35] Video Privacy Protection Act of 1988, 18 U.S.C. § 2710(b) (2000). The Act allows videotape rental providers to release customer names and addresses to third parties wishing to market their products to customers so long as there is no disclosure of titles purchased or rented. *Id.* Customers can, however, be grouped into categories by the type of film they rent. *See id.* § 2710(b)(2)(D)(ii).

[36] *See* Satish M. Kini & James T. Shreve, *Notice Requirements: Common Themes and Differences in the Regulatory and Legislative Responses to Data Security Breaches*, 10 N.C. Banking Inst. 87, 92–103 (2006) (identifying, comparing, and contrasting state laws).

[37] *See* A. Michael Froomkin, *The Death of Privacy?*, 52 Stan. L. Rev. 1461, 1472–73 (2000) (discussing government databases).

[38] *See id.* at 1474.

[39] *See id.* at 1476–82.

[40] *See id.* at 1468–69.

[41] *See id.*

country illegally;[42] (2) claims that ID cards would help the fight against terrorism;[43] (3) improved delivery of government services, notably transfer payments and other government benefit programs;[44] (4) improved voter registration and identification;[45] and (5) assistance to

---

[42] *See, e.g.*, John J. Miller & Stephen Moore, *A National ID System: Big Brother's Solution to Illegal Immigration*, CATO POL'Y ANALYSIS No. 237 (Cato Inst., Washington, D.C.), Sept. 7, 1995, at 1 (noting that, without national ID cards, a national computer worker registry system would not work); Stuart Taylor, Jr., Op-Ed., *Hidden America*, LEGAL TIMES, Apr. 10, 2006, at 60 (arguing that Congress should create a more reliable ID card system and enforcement mechanisms to prevent employers from hiring illegal immigrants).

[43] *See, e.g.*, Ben Quarmby, iBrief, *The Case for National DNA Identification Cards*, 2003 DUKE L. & TECH. REV. 2, ¶¶ 24–25, http://www.law.duke.edu/journals/dltr/articles/2003dltr0002.html ("At times like these, it is therefore crucial not only for the law enforcement authorities and the government, but also for private entities such as commercial airlines, public transport companies, weapons retailers, and others, to be able to accurately identify all individuals."); Charlie Savage, *Congress Set to Impose ID Card Rules—States Would Need to Verify Papers*, BOSTON GLOBE, May 5, 2005, at A1 (noting that the REAL ID Act was "[t]outed as an antiterrorism measure").

In fact, the claim that ID cards help fight terrorism is highly debatable. *See* Marc Rotenberg, *REAL ID, Real Trouble?*, COMM. OF THE ACM, Mar. 2006, at 128, 128 ("Systems of identification remain central to many forms of security. But designing secure systems that do not introduce new risks is proving more difficult than many policymakers had imagined."); Bruce Schneier, Op-Ed., *A National ID Card Wouldn't Make Us Safer*, STAR TRIB. (Minneapolis), Apr. 1, 2004, at A17 ("[E]verything I've learned about security over the last 20 years tells me that once it is put in place, a national ID card program will actually make us less secure."); Chad Vander Veen, *Papers Please*, GOV'T TECH., Nov. 2005, http://www.govtech.net/magazine/story.php?id=97147&issue=11:2005 ("[O]f the 9/11 terrorists, as many as seven carried Florida drivers' licenses and at least four carried Virginia drivers' licenses, which obviously calls into question the effectiveness of those states' driver's license security measures prior to Sept. 11, 2001.").

[44] *See* U.S. GEN. ACCOUNTING OFFICE, ELECTRONIC BENEFITS TRANSFER: USE OF BIOMETRICS TO DETER FRAUD IN THE NATIONWIDE EBT PROGRAM 9–10 (1995) (recommending electronic fingerprint identification as a condition for receipt of government benefits); Amy Mulzer, Note, *The Doorkeeper and the Grand Inquisitor: The Central Role of Verification Procedures in Means-Tested Welfare Programs*, 36 COLUM. HUM. RTS. L. REV. 663, 664–65 (2005) (noting the importance of computer matching to detect benefit fraud); Amitai Etzioni, Op-Ed, *You'll Love Those National ID Cards*, CHRISTIAN SCI. MONITOR, Jan. 14, 2004, at 11 (arguing that national ID cards would greatly curtail tax and welfare fraud); Samantha Maiden & James Riley, *ID Card Plan for Health, Welfare,* AUSTRALIAN, Mar. 27, 2006, at Local 1 (reporting on Australian government proposal to issue "a health and welfare smart card to save on postage and prevent billions of dollars being lost to fraud and identity theft"); Stephen O'Brien, *Outrage over ID Cards to Beat Welfare Fraud*, SUNDAY TIMES (Ireland), Aug. 14, 2005, *available at* http://www.timesonline.co.uk/article/0,,2091-1734736,00.html (reporting Ireland's Social Affairs Minister as saying ID cards would be "designed to combat up to £600m a year in welfare fraud").

[45] *Cf.* Ind. Democratic Party v. Rokita, No. 1:05-CV-0634-SEB-VSS, 2006 U.S. Dist. LEXIS 20321, at *114–83 (S.D. Ind. Apr. 14, 2006) (rejecting constitutional and statutory challenge to Indiana law requiring that most voters present valid, government-issued photo ID card in order to vote); Common Cause/Georgia v. Billups, 406 F. Supp. 2d 1326, 1376–77 (N.D. Ga. 2005) (granting preliminary injunction precluding Georgia from enforcing its statutory

law enforcement.[46] There has been discussion of both the purported government benefits and the concomitant risks, ranging from various losses of liberty right up to the creation of an Orwellian state—although I think that neither side has been sufficiently rigorous.[47]

In light of the fact that businesses have used SSNs and driver's licenses to identify and index consumers for decades, it would be foolish to ignore how the private sector will use any new national identification credential. Indeed, it would be sensible to try to design that credential in a way that met as many of the private sector's reasonable requirements as possible while at the same time trying to provide some systematic protection for personal privacy.

In the private sector, the advantages of a strong and reliable national identity credential most likely will fall in these areas: fraud prevention, medical care,[48] e-commerce, and the linking of databases with personal information about consumers. Excluding the special circumstances surrounding health care data,[49] the things many firms will most likely want to do relating to commercial transactions are identify customers, learn a lot about them, and market to them. Reconciling these market-oriented objectives with the protection of personal privacy may sound like a contradiction in terms. But if we act quickly it need not be.

Firms seeking to correlate distributed data and use them to learn more about their customers face three problems. First, they need to *authenticate* customers—to establish that customers are in fact who they say they are. Indeed, in cases where the firm's primary goal is fraud prevention, authentication may be more important than any-

---

photo ID requirement in future elections), *motion to stay preliminary injunction denied sub nom.* Common Cause/Georgia v. Cox, No. 05-15784-G (11th Cir. Oct. 27, 2005), *available at* http://moritzlaw.osu.edu/electionlaw/litigation/documents/11thCircuitDenial.pdf.

[46] *See* N.Y. State Dep't of Motor Vehicles, Photo Licenses and ID Cards: Secure Proof for Drivers and Non-Drivers (2006), http://www.nydmv.state.ny.us/broch/c-33.htm (touting New York State photo ID on the grounds that it "may provide increased identification security for you, plus law enforcement and driver safety advantages for everyone").

[47] *See* Froomkin, *supra* note 4, at 4–17, 27–44.

[48] In its original version, HIPAA contemplated a unique patient identifier to help organize disparate medical records. That idea was scrapped and the issue remains controversial. *See* Nancy Ferris, *Patient ID Is Trouble Spot for Commission*, Gov't Health IT, Aug. 11, 2005, http://governmenthealthit.com/article89870-08-11-05-Web.

[49] The medical care area presents special problems of both access and regulation. If an ID card is going to carry information useful to first responders and especially emergency medical caregivers, then that information needs to be accessible to a large and unpredictable population, raising issues qualitatively different from the market-oriented issues discussed in this paper. Furthermore, HIPAA has occupied the field of privacy regulation of medical data, however unartfully.

thing else. Second, firms need to *distinguish* that person from other persons in the database who have the same[50] (or a similar)[51] name or who have (or had) the same address. For example, the first time I checked my credit history some employment data had bled in from a Michael Froomkin in Ohio, a person previously unknown to me. Third, when trying to tie distributed databases together, firms need a way to ensure that the records they are linking are about the same person: they have to make sure that each set of records is distinguished in a compatible manner. In the case of an unusual name like "Froomkin" this may not be too difficult, but there are many John Smiths in the United States, not all of whom have or use middle initials, and many of whom may live on Main Streets. In any case, the merchant's (or data broker's) goal is to automate every step in the process to keep the costs down.

A. *The U.S. Government and the Power of Standards*

The federal government has been in the standard-setting business since the early days of the Republic. The Constitution, after all, gives Congress the power to "fix the Standard of Weights and Measures,"[52] which no less an authority than Joseph Story explained was "for the sake of uniformity, and the convenience of commerce."[53] Thus, in addition to market-based standards, whether set by first movers, competitive victors, regulated or de facto monopolists, cartels, anti-trust exempted industry bodies, or volunteers operating under

---

[50] *See* Lisa Friedman, *Paying for a Name: David Nelsons Draw Red Flags Getting Through Airport Security*, L.A. Daily News, June 15, 2003, at N1 ("Throughout Southern California and across the country, men named David Nelson report they have been harassed, questioned by FBI agents, pulled off airplanes, searched and then searched again when attempting air travel. Apparently caught up in a nationwide dragnet for a terrorist by that name, David Nelsons everywhere are being told their names raise red flags on airline screening software.").

[51] The U.S. government's well-publicized difficulties in running the "do not fly" list demonstrate the nature of the problem. *See, e.g.*, Sally B. Donnelly, *You Say Yusuf, I Say Youssouf . . .*, Time.com, Sept. 25, 2004, http://www.time.com/time/nation/article/0,8599,702062,00.html ("[The incident where] the former Cat Stevens was denied entry into the U.S. when federal officials determined he was on the government's 'no-fly' antiterror list, started with a simple spelling error."); Leslie Miller, *Babies Caught Up in "No-Fly" Confusion*, sfgate.com, Aug. 16, 2005, http://www.sfgate.com/cgi-bin/article.cgi?file=/n/a/2005/08/15/national/w115806D06.DTL ("Infants have been stopped from boarding planes at airports throughout the U.S. because their names are the same as or similar to those of possible terrorists on the government's 'no-fly list.'").

[52] U.S. Const. art. I, § 8, cl. 5.

[53] Joseph Story, 3 Commentaries on the Constitution of the United States § 1117, at 20 (Fred B. Rothman Publ'ns 1991) (1883).

conditions of near-Habermasian discourse,[54] there is a variety of ways in which the government itself enforces standards.

Modern government standard setting encompasses much of the modern regulatory state, including health and safety rules, disclosure requirements, licensing laws, and much more. Sometimes the government adopts privately drafted industry standards as its own;[55] sometimes it writes on a blank slate. Similarly, if the government defines a "safe harbor" as part of a regulatory scheme—for example, as presumptively meeting a standard of care—this may in practice become a standard.

But not all government standard setting is by mandatory rule. Sometimes the government sets de facto private standards through the exercise of its market power: when the government, acting either by accident or design, sets a standard for its own volume purchases, it can have a knock-on effect for private purchasers. Manufacturers wanting to sell to the government produce goods that comply with the standard. If the government purchases are large, and if the production function for the good is one characterized by declining marginal costs, the effect of the volume sales to the government is a lower market price for the government-standard goods as compared to similar but nonconforming products. The lower price makes the government-standard goods more attractive to private buyers, and—so long as there is not a significant quality disadvantage—a de facto private sector standard emerges.

A great deal of both private and governmental standard setting is likely to increase consumer welfare.[56] A standard can make families of devices interoperable in ways that increase social welfare by promoting competition.[57] "Interface" standards permit products made by different manufacturers to work together;[58] infrastructural standards such as railroad gauges or electricity voltages and cycles per second enable entire industries.[59] A safety standard can provide a minimum

---

[54] *See generally* A. Michael Froomkin, *Habermas@discourse.net: Toward a Critical Theory of Cyberspace*, 116 Harv. L. Rev. 749 (2003).

[55] *See generally* Mark A. Lemley, *Intellectual Property Rights and Standard-Setting Organizations*, 90 Cal. L. Rev. 1889 (2002) (surveying interactions, between standard-setting organizations and firms that claim ownership of industry standards, that occur in the shadow of patent and antitrust laws).

[56] *Id.* at 1896–97.

[57] *Id.* at 1897.

[58] *Id.* at 1893.

[59] *See id.* at 1897.

level of assurance and safety to the public, especially in circumstances where information may be costly to acquire.[60]

Nevertheless, it is important to understand that the economic benefits of a federally imposed standard cannot be assumed. For example, there is substantial literature examining cases in which incumbents have "captured" the regulatory process and persuaded the government to use its standard-setting powers in ways that advantage the incumbents and make entry difficult and expensive for competitors with a new technology.[61] Arguably, the current push for government-mandated "digital rights management" technologies, already backed by the creation of paracopyright interests in the copy-protection technologies,[62] is another form of capture-driven standards policy in which incumbents are trying to stifle disruptive technologies that threaten their business models.[63]

Additionally, even if it is not following an agenda driven by special interests, the government's interest in making a standard may have little to do with the sort of consumer welfare measured by economists. For example, in the mid-1990s, the federal government sought to stem the spread of strong cryptography by creating a de facto standard around the Clipper Chip, a device that could be used to encrypt telephone conversations with a cipher that was orders of magnitude stronger than the increasingly vulnerable ciphers then

---

[60] *See* Lemley, *supra* note 55, at 1897–98.

[61] For a compelling account of a contemporary misuse of standards to stifle competition, see generally Susan P. Crawford, *The Ambulance, the Squad Car, & the Internet*, 21 Berkeley Tech. L.J. 873 (2006), which demonstrates how incumbent telecommunications carriers persuaded the Federal Communications Commission to institute rules under the guise of safety standards, disadvantaging VoIP-based competitors.

[62] "Paracopyright" refers to copyright-like legal protections created in the Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998), that sanction content users who defeat anticircumvention devices deployed by copyright owners in order to prevent the reproduction of digital copies of their content. *See* 3 Melville B. Nimmer & David Nimmer, Nimmer on Copyright § 12A.18[B], at 12A-185 (2004); *see also* Stefan Bechtold, *Digital Rights Management in the United States and Europe*, 52 Am. J. Comp. L. 323, 338 (2004) (describing the traditional role of copyright as "react[ing] to significant changes in technology").

[63] *See* Brief of Amici Curiae Sixty Intellectual Property and Technology Law Professors and the United States Public Policy Committee of the Association for Computing Machinery in Support of Respondents, Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 545 U.S. 913 (2005) (No. 04-480), *reprinted in* 20 Berkeley Tech. L.J. 535, 559 (2005) (accusing "petitioners and certain *amici*" of advocating rules under which "copyright holders could effectively approve or deny new technologies that are disruptive to, or merely competitive with, their business models").

available for export.[64] Previously, the government had objected to strong encryption on the grounds that it would stymie law enforcement agencies (and intelligence agencies) with legitimate reasons to eavesdrop on communications.[65] With the Clipper Chip, the government offered the private sector a bargain: strong cryptography with a built-in back door.[66] The government would keep a copy of the keys—the unique codes belonging to each chip—thus allowing it to retain the ability to intercept every message sent using it.[67] The safeguards against the U.S. government would be purely legal, not technological.[68] As part of its effort to encourage the private sector to adopt Clipper as its standard for secure communications, the U.S. government proposed to buy substantial numbers of Clipperized phones for its own use, thus jump-starting production.[69] The hope was that once there were enough Clipperized telephones in use, network effects would take over; Clipper would become the de facto standard and every business interested in secure communications would think it had no other choice.[70] The political resistance was so great that only one manufacturer announced it would produce the phones, and in fact that one company, AT&T, made very few of them.[71]

---

[64] *See* A. Michael Froomkin, *The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. Pa. L. Rev. 709, 752–64 (1995). There were no rules limiting the strength of domestic cryptography, but the export control regime had prevented a standard from emerging.

[65] *See id.* at 743–44.

[66] *See id.* at 752.

[67] *See id.*

[68] The government set out relatively elaborate procedures that it said would reduce the risk that the keys would be released to law enforcement agencies without legally sufficient justification, such as a valid wiretap authorization. *See* U.S. Dep't of Justice, Authorization Procedures for Release of Encryption Key Components in Conjunction with Intercepts Pursuant to FISA (Feb. 4, 1994), *available at* http://www.epic.org/crypto/clipper/doj_key_escrow_procedures.html; U.S. Dep't of Justice, Authorization Procedures for Release of Encryption Key Components in Conjunction with Intercepts Pursuant to State Statutes (Feb. 4, 1994), *available at* http://www.epic.org/crypto/clipper/doj_key_escrow_procedures.html; U.S. Dep't of Justice, Authorization Procedures for Release of Encryption Key Components in Conjunction with Intercepts Pursuant to Title III (Feb. 4, 1994), *available at* http://www.epic.org/crypto/clipper/doj_key_escrow_procedures.html.

[69] *See* Froomkin, *supra* note 64, at 769–70.

[70] *See id.* at 769.

[71] *See* Jared Sandberg & Don Clark, *AT&T, VLSI Technology to Develop Microchips That Offer Data Security*, Wall St. J., Jan. 31, 1995, at A3 (noting that AT&T had originally supported the Clipper Chip but was now abandoning it).

The Clipper Chip never really got off the ground,[72] but that failure was due to an unusually determined public opposition at home and deep suspicion abroad. Non-U.S. users in particular did not want to commit themselves to communications that could be acquired by the U.S. government (and not their own).[73] Ironically, the very importance of an international standard that had allowed the United States to use export control to influence domestic standards helped doom the government's attempt to impose Clipper by market means. But for these extraordinary circumstances, Clipper could have become a standard. And there may be a lesson there.

Unlike encrypted communications, a national ID standard is by definition purely domestic,[74] vastly increasing the power of the government to impose a standard. Indeed, at present the state and national governments remain the sole possible suppliers of identity credentials likely to be widely accepted in the marketplace; as discussed below, the only serious competition for any federal ID card will come from the new standardized state driver's licenses that will come into production at some uncertain point in the next few years.[75]

B. *The Carrot*

National data privacy policies arguably could be enforced directly by federal statute. There are, however, two reasons why we should not rely on Congress to do so. First, Congress has shown no inclination to enact a broad, meaningful, and non-sectoral privacy statute. As noted above, the United States has a few targeted national privacy rules,[76] but otherwise the federal policy is most often one of lip service[77]

---

[72] The Pentagon did announce plans to order a large quantity of its cousin, the CAPSTONE card, for the Defense Messaging System, *see* Ellen Messmer, *NIST Acknowledges Patent Infringement*, NETWORK WORLD, July 25, 1994, at 20, but it is not clear how many were actually purchased or deployed. *See* Bill Murray, *12 Years, $1.6 Billion and Counting*, FCW.COM, Mar. 5, 2001, http://www.fcw.com/article72901 (noting the disarray of the Defense Messaging System and Department of Defense's increased reliance on software encryption).

[73] *See* A. Michael Froomkin, *It Came from Planet Clipper: The Battle over Cryptographic Key "Escrow,"* 1996 U. CHI. LEGAL F. 15, 34–35.

[74] If the credential were to double as a passport, then a number of international rules would apply. There are also some international standards regarding the use of ID for visa applications, but these do not affect the argument in the text.

[75] *See infra* note 131 and accompanying text (noting that REAL ID will become effective in May 2008, but that many states have made it clear that this deadline is unrealistic).

[76] *See supra* notes 29–35 and accompanying text.

[77] For instance, the United States endorsed the 1980 Organisation for Economic Cooperation and Development data privacy guidelines twenty years ago. *See* Robert M. Gell-

combined with unconvincing claims that state law and industry self-regulation provide adequate privacy protection.[78] Indeed, for more than thirty years Congress has avoided enacting any wide-ranging data privacy protections, especially as regards data in private hands.[79] Recent laws, such as the much-touted privacy provisions of the Gramm-Leach-Bliley Financial Modernization Act, are, in practice, weak.[80] If Congress cannot be persuaded to mandate a national data privacy regime, the likely introduction of a new ID provides an occasion for a bargain: give firms something valuable in exchange for their agreement to comply with stiffened data privacy rules. Second, although it

---

man, *Can Privacy Be Regulated Effectively on a National Level? Thoughts on the Possible Need for International Privacy Rules*, 41 VILL. L. REV. 129, 154–55 (1996) (noting endorsement by the United States, but criticizing it as mostly lip service); *infra* notes 104–111 and accompanying text. Indeed, a U.S. government agency issued one of the first reports on the need for more attention to the privacy implications of computerized records. *See* SEC'Y'S ADVISORY COMM. ON AUTOMATED PERS. DATA SYS., U.S. DEP'T OF HEALTH, EDUC. & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS 48–50 (1973).

[78] *See* Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45,666, 45,667 (July 24, 2000). Numerous works describe the United States-European Union ("EU") safe harbor negotiations. *See, e.g.*, Barbara Crutchfield et al., *U.S. Multinational Employers: Navigating Through the "Safe Harbor" Principles to Comply with the EU Data Privacy Directive*, 38 AM. BUS. L.J. 735, 781 (2001) (warning that compliance with EU privacy rules "will require substantial changes in the way [U.S. firms] do business"); Sean D. Murphy, *Contemporary Practice of the United States Relating to International Law*, 95 AM. J. INT'L L. 132, 156 (2001) (noting that "European negotiators resisted the U.S. proposal for private sector self-regulation, proclaiming it to be little more than the 'fox guarding the hen-house,' while U.S. negotiators resisted increased U.S. government monitoring of the private sector"); David A. Castor, Note, *Treading Water in the Data Privacy Age: An Analysis of Safe Harbor's First Year*, 12 IND. INT'L & COMP. L. REV. 265, 289–90 (2002) (praising U.S. privacy legislation for lacking the scope of European rules); *see also* Ryan Moshell, Comment, . . . *And Then There Was One: The Outlook for a Self-Regulatory United States Amidst a Global Trend Toward Comprehensive Data Protection*, 37 TEX. TECH L. REV. 357, 388–432 (2005) (surveying data-protection schemes in other nations, and arguing that the United States should take a more active role in data protection rather than relying on self-regulation); David Raj Nijhawan, Note, *The Emperor Has No Clothes: A Critique of Applying the European Union Approach to Privacy Regulation in the United States*, 56 VAND. L. REV. 939, 958–75 (2003) (arguing that an EU-style data-protection scheme would not work in the United States). *But see* Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 1, 55–88 (2000) (arguing that U.S. privacy standards have become tougher due to pressure from the EU).

[79] First Amendment limits on preventing persons from sharing what they know are one constraining factor. *See generally* Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049 (2000) (discussing the First Amendment implications of information privacy speech restrictions).

[80] Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 (2000); *see* Eric Poggemiller, Note, *The Consumer Response to Privacy Provisions in Gramm-Leach-Bliley: Much Ado About Nothing?*, 6 N.C. BANKING INST. 617, 628–35 (2002) (discussing possible explanations for why the privacy provisions in the Gramm-Leach-Bliley Act have not been very effective).

is clear that Congress has substantial power to regulate the commercial use of personal data,[81] there may be some First Amendment limits to Congress's power to regulate the repetition of true statements.[82]

If we cannot rely on Congress to act directly, and if there are also First Amendment doubts about Congress's power to make sufficiently broad rules, then perhaps it would be better to try a carrot and stick approach, one in which firms' participation in a national data privacy regime is formally voluntary. In order to persuade firms to buy into a formally voluntary scheme, however, there must be a carrot—something that firms want badly enough to buy into an enhanced set of privacy rules.

Improved national ID cards would offer firms two things they value: the prospects of solving both the authentication problem and the distinction problem.[83] The existence of an ID card is strong evidence that the government believes it authenticated the person to whom it issued the credential. For downstream users, the authentication provided by the card is at best as good as the quality of the evidence that

---

[81] Although the Driver's Privacy Protection Act of 1994 (the "DPPA") provides a model of what federal regulation might look like, it is important to note that it is directed at state agencies, not at the private sector. 18 U.S.C. § 2721 (2000); *see* Reno v. Condon, 528 U.S. 141, 143 (2000) (rejecting federalism challenge to the DPPA). Furthermore, the DPPA contains numerous exceptions. States may release information for:

- Legitimate government agency functions, § 2721(b)(1);
- Use in matters of motor vehicle safety, theft, emissions, and product recalls, *id.* § 2721(b)(2);
- Motor vehicle market research and surveys, *id.*;
- "Legitimate" business needs in transactions initiated by the individual to verify accuracy of personal information, *id.* § 2721(b)(3);
- Use in connection with a civil, criminal, administrative or arbitral proceeding, *id.* § 2721(b)(4);
- Research activities and statistical reports, so long as personal information is not disclosed or used to contact individuals, *id.* § 2721(b)(5);
- Insurance activities, *id.* § 2721(b)(6);
- Notice for towed or impounded vehicles, *id.* § 2721(b)(7);
- Use by licensed investigators or security services, *id.* § 2721(b)(8);
- Use by private toll transportation facilities, *id.* § 2721(b)(10);
- Response to requests for individual records if the state has obtained express consent from the individual, *id.* § 2721(b)(11);
- Bulk marketing distribution if the state has obtained express consent from the individual, *id.* § 2721(b)(12);
- Use by any requester where the requester can show written consent of the individual, *id.* § 2721(b)(13); and
- Any other legitimate state use if it relates to motor vehicle or public safety, *id.* § 2721(b)(14).

[82] *See* Volokh, *supra* note 79, at 1080–122.

[83] *See supra* notes 17–28 and accompanying text.

the government required to issue the ID. Subsequent possession of the card suggests a link between the holder and the person to whom it was issued, but the level of reliance that one is justified in placing on this proffer depends on several factors, among them the ease with which cards can be duplicated or altered. Unless the card is tamper-resistant and hard to counterfeit, it will not be of much use to anyone.

A national ID card with biometric authentication offers a solution to the authentication problem. Similarly, a new national identity credential offers the enticing possibility of a new numbering scheme that could replace the nearly ubiquitous SSN with something harder to fake and very likely to be unique.[84] What is more, if the card is government-mandated, then all the costs of original verification of the information and the production of a secure card will be borne by the card holder, either directly as a fee or indirectly as taxes. Either way, neither the merchant nor the data broker has to pay, a price point that both are likely to find pleasing. All other things being equal, one would expect merchants and others to embrace the new card.

As one recent study of national identification systems stated:

> A nationwide identity system, depending on its implementation, 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, the system's use would be free to other segments of society unless measures (technical, legal, or otherwise) are taken to prevent unauthorized use. Second, unless private parties are prevented by law (or restrictions on technology) 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

[84] By using cryptographic techniques, the government can digitally sign not just the number but also some fact about the card holder, such as a digitized photo. This will make it very difficult to counterfeit or alter. If the information used in conjunction with the number is something that could be known only to the genuine card holder or that is biometrically unique to that person, the chance that a card could be forged or altered is minute unless the entire encryption system for all cards is broken.

> and/or identity within the system. The information in these commercial databases may not be as strongly protected (legally or technologically) as, presumably, is the information in the nationwide identity system's own databases.[85]

Businesses will want to use a national ID card—the only questions are what they will put up with to get it, and whether there will be close substitutes that might do instead. The next two sections address these questions.

C. *The (Viral) Stick*

If firms find it beneficial to use a national ID card for authentication and especially for data indexing and matching, they should be willing to accept a degree of expense or constraint regarding the way that they manage the information created, verified, and indexed thanks to this new technology. Thus, it should be politically feasible to condition the use of the new national index number on adherence to national data protection and privacy rules. The ownership and dissemination of private sector data would remain a matter of contract and state law as it is today,[86] but would be constrained by the third party's duty to adhere to government-defined data protection rules when using the federally owned ID number to index data, or even when using any data that had been so indexed.[87]

Meaningful privacy rules restricting the use of indexing information, and the information indexed with it, will have to be set nationally. Although this creates a focal point for regulation, it also inevitably creates a single point of policy failure, and a large target waiting for capture by industries that will want the minimum restrictions on their ability to process and share personal information. This is undoubtedly a risk, but it is one that should be weighed against the "virtual" ID card world currently being built, one in which the locations at which privacy-destroying decisions occur are scattered and often invisible.[88] Centraliz-

---

[85] IDs—Not That Easy, *supra* note 21, at 30–31.

[86] As a general matter, and absent duties of confidentiality that fall primarily on professionals such as lawyers and doctors, the facts of an economic transaction belong jointly and severally to the parties. *See* Froomkin, *supra* note 37, at 1502.

[87] The obligation to comply with data protection rules would thus run with the data, as do the obligations under the European Data Protection Directive. *See generally* Paul M. Schwartz & Joel R. Reidenberg, Data Privacy Law (1996) (discussing the Directive); *infra* note 94 (same).

[88] *See* Froomkin, *supra* note 37, at 1468–501; *see also* Office of Tech. Assessment, U.S. Congress, Making Government Work: Electronic Delivery of Federal Services 144

ing 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.

The linchpin of this approach is to have the government own both the national ID numbers themselves and the standard by which the information is readable from the card. Admittedly, this ownership interest in the numbers is not easy to characterize under existing law. As an intangible form of property, the numbers might seem to be a form of intellectual property, but this is at best a very imperfect fit.[89] Under current law, even unique ID numbers would not be patentable,[90] copyrightable,[91] or trademarkable,[92] nor would they qualify as trade secrets.[93] Moreover, the much-debated idea of database copyright does not provide a useful model. In the United States, copyright law cannot be used to block access to raw data contained in a database unless the underlying data is entitled to copyright protection on its own.[94] The

---

(1993) (warning that "extensive computer matching can lead to a 'virtual' national data bank, even if computer records are not physically centralized in one location").

[89] *See generally* Pamela Samuelson, *Questioning Copyrights in Standards*, 48 B.C. L. Rev. 193 (2007) (discussing whether Internet standards should be eligible for copyright protection).

[90] In 1994 Roger Schlafly obtained U.S. Patent 5,373,560 on two prime numbers. U.S. Patent No. 5,373,560 (filed Aug. 4, 1993) (issued Dec. 13, 1994). *See generally* Paul Horowitz et al., *The Law of Prime Numbers*, 68 N.Y.U. L. Rev. 185 (1993) (surveying law relating to prime numbers). ID-related numbers would not be patentable, however, because if nothing else they lack originality. *See* 35 U.S.C. § 101 (2000) ("Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title."). In any case, patents lapse; this project would require the government's interest to last indefinitely.

[91] It would be difficult to characterize an ID number, or even 300 million of them, as "original works of authorship." *See* 17 U.S.C. § 102(a) (2000).

[92] To be protected as a trademark, a mark must be used in "connection with the sale, offering for sale, distribution, or advertising of any goods or services." *See* 15 U.S.C. § 1114(1)(a) (2000). To the extent that the ID number would be used to identify people, it runs up against the fact that people are not commodities. Data about people can certainly be a commodity, but it is hard to characterize an ID number used to authenticate or index data as being used to "distinguish[] from the goods of others" as meant in 15 U.S.C. § 1052.

[93] For starters, the ID number will not be secret.

[94] *See* Assessment Techs. of WI, LLC v. WIREdata, Inc., 350 F.3d 640, 644 (7th Cir. 2003) (holding that copying unoriginal data, however extracted from a database, is not an infringement of copyright); *see also* Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 348 (1991) (stating that a database is copyrightable only if it "features an original selection or arrangement" that "possesses at least some minimal degree of creativity").

In 1996, the European Community adopted a Database Directive giving copyright protection to databases. Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the Legal Protection of Databases, 1996 O.J. (L 77) 20. The Directive thus conferred a new "sui generis" database right even on unoriginal compilations of facts. *See id.*

U.S. Court of Appeals for the Third Circuit has even held that numbers, by their nature, are too small to be copyrightable.[95]

But even if no existing property rule fits, there is no reason why Congress cannot create a regulatory obligation, either by fiat or by recognizing a new sui generis property right in the government's—or the card holder's—interest in the index number created for an ID card. Without such a rule, be it regulatory or property-based, the only thing that would prevent the private sector from making full use of the number would be technological protections encoded on the card. It would be possible, for example, to make the card hard to read, or to encrypt the data on the card (including the index number) in a manner that makes it difficult for unauthorized persons to read. In fact, however, although these protections are technically feasible, they are unlikely to be part of any foreseeable national ID card because they would require special equipment to read the cards. That equipment would have to be available to all the state and federal agencies relying on the card, and would greatly complicate the use of the card for governmental purposes. Furthermore, this equipment would have to be available to airlines, other transportation businesses, and any other businesses that would be required to check ID under law. It is far more likely that the government will define a standard, perhaps attempting to ensure that it has a monopoly on writing data to the card, but allowing anyone to read the data.

If the holders' personal data is not protected by technical means, it will either have legal protection or it will have none at all.[96] By creating a sui generis property interest that it would hold, the government would give itself the leverage for a deal: firms that wished to avail themselves of the cost-saving benefits that using and relying on the new cards might bring them would have to agree to be bound by specific data privacy rules, and at the very least would also have to agree to share their data only with firms that had agreed to be bound by the same rules. Preferably, the duty to observe the privacy rules

---

[95] *See* Southco, Inc. v. Kanebridge Corp. (*Southco III*), 390 F.3d 276, 282, 285 (3d Cir. 2004) (en banc) (holding that the petitioner's product numbers were not copyrightable because they were not "original"—in other words, because each number was rigidly dictated by the rules of the petitioner's system, and they were "analogous to short phrases or the titles of works"). *But see* Justin Hughes, *Size Matters (or Should) in Copyright Law*, 74 Fordham L. Rev. 575, 591–600 (2005) (suggesting that other courts have muddied the waters on this issue).

[96] Contractual protection is a theoretical possibility but not a practical one. For an argument that consumers likely suffer from privacy myopia, which causes them to undervalue their personal data, see Froomkin, *supra* note 37, at 1501–05.

would be made "viral"—it would run with the number. Ordinary licenses that permit sublicensing commonly require licensees to pass on limits in their licenses to the sublicensees. A "viral" license differs from an ordinary sublicense provision in that, in addition to the sublicensor passing on the obligations to future users, the terms of the viral license purport to run with the subject of the license without the need for actual consent by either the licensee or the sublicensee.[97]

It could be objected that creating a sui generis property right for the government in ID numbers is an inefficient means to achieve data privacy, and one that poses the risk of creating a lousy precedent.[98] Why not, the argument goes, simply legislate the privacy rules directly? And why take the risk of creating (another)[99] sui generis right, thus further emboldening those who seek to enclose the information commons? These arguments, legitimate as they are, underestimate the obstacles that need to be overcome to secure information privacy. Undoubtedly, direct privacy legislation, whether free-standing or grafted onto REAL ID, would have many advantages over the market-driven and voluntary scheme advocated here—immediate universal coverage chief among them. But despite years of effort by the privacy community, the odds of direct legislation remain low—and due to REAL ID, time is running out.

Worse, any direct legislation that sought to compel rather than entice compliance would have to overcome a substantial constitutional obstacle. Although the issue is not free from doubt, there are substantial reasons to believe that the First Amendment could pose a significant obstacle to any wide-reaching data privacy law enforced via compulsion.[100] As Eugene Volokh and others have noted, data privacy law blocks truthful speech about information lawfully acquired, in-

---

[97] *Cf.* Margaret Jane Radin, *Humans, Computers, and Binding Commitment*, 75 IND. L.J. 1125, 1132–33 (2000) (discussing viral contracts). Professor Boyle warns that some people find the term viral "offensive," James Boyle, *The Second Enclosure Movement and the Construction of the Public Domain*, 66 LAW & CONTEMP. PROBS. 33, 45 (2003), but I think the metaphor fits.

[98] Indeed, a number of people, notably Michael Carroll, did object to the idea when I presented an earlier draft of this Article at the Boston College symposium.

[99] Previous sui generis intellectual property rules include the creation of rights in the word "Olympics," *see* S.F. Arts & Athletics, Inc. v. U.S. Olympic Comm., 483 U.S. 522, 530 (1987), and the anticircumvention rules of the Digital Millennium Copyright Act of 1998, *see, e.g.*, CRAIG JOYCE ET AL., COPYRIGHT LAW § 9.04[A], at 813 (6th ed. 2003); Dan L. Burk, *Anticircumvention Misuse*, 50 UCLA L. REV. 1095, 1102–10 (2003).

[100] *See generally* Volokh, *supra* note 79 (applying several free speech doctrines to proposed information privacy laws).

formation that may relate to the speaker's own experience.[101] In contrast, promises not to reveal information—including, presumably, the viral agreements proposed here—are "eminently defensible under existing free speech doctrine."[102]

Precisely what the content of the national privacy protections should be will be hotly debated. Defining the ID number as the property of the government, or as jointly but not severally owned with the citizen, might cut off private sector attempts to demand that citizens waive their data protection rights, which I think would plug a major gap in most existing privacy protection regimes under which consent, even expressed in a standard form contract, usually vitiates all. More generally, a sensible national data privacy plan would seek to buy into a full-blown set of Fair Information Practices.[103] My personal preference is to require, at a minimum, that the United States commit itself to an updated and improved version of the 1980 Organisation for Economic Co-operation and Development privacy guidelines (the "OECD Guidelines").[104] The OECD Guidelines set out recommendations for nations concerned about data privacy to "take into account in their domestic

---

[101] *See id.* at 1050–51; *see also* Will Thomas DeVries, *Protecting Privacy in the Digital Age*, 18 Berkeley Tech. L.J. 283, 308 (2003) (discussing "[t]he perceived conflict between informational privacy and free speech"); Daniel J. Solove, *The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure*, 53 Duke L.J. 967, 974 (2003) ("[P]rivacy protections against disclosure, when analyzed in light of our longstanding tradition of protecting free speech and a free press, seem quite problematic.").

[102] Volokh, *supra* note 79, at 1057; *see* Cohen v. Cowles Media Co., 501 U.S. 663, 672 (1991) (holding that the First Amendment does not prohibit a plaintiff from recovering damages from a newspaper for breach of a promise of confidentiality).

[103] *See* Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. Ill. L. Rev. 357, 358, 368–82; *see also* Fed. Trade Comm'n, Privacy Online: A Report to Congress 7–10 (1998) (noting that contemporary Fair Information Practice codes all contain five core principles of privacy protection: (1) Notice/Awareness, (2) Choice/Consent, (3) Access/Participation, (4) Integrity/Security, and (5) Enforcement/Redress).

[104] Org. for Econ. Co-operation & Dev., Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (1980) [hereinafter OECD Guidelines], *available at* http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html. On the OECD Guidelines, see Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 Stan. Tech. L. Rev. 1, ¶¶ 44–47, http://stlr.stanford.edu/STLR/Articles/01_STLR_1/index.htm.

The OECD is a group of thirty countries that, among other things, issues publications and statistics on economic and social issues and produces internationally agreed-upon instruments, decisions, and recommendations. *See* Organisation for Economic Co-operation & Development, About OECD, http://www.oecd.org/about/0,2337,en_2649_201185_1_1_1_1_1,00.html (last visited Nov. 2, 2006).

legislation," subject only to the minimum limits necessary to preserve national security.[105] The OECD Guidelines require, in part, the following:

- Data should be collected with the knowledge or consent of the data subject;[106]
- Data should only be collected when relevant to the purpose for which the data are being used;[107]
- The purpose for which data are collected should be stated at the time of collection, and the data should only be used for that stated purpose;[108]
- When retained, data should be kept accurate, up-to-date, and protected by reasonable security safeguards;[109]
- Persons have the right to know who holds data about them, and to inspect it;[110] and
- Persons have the right to challenge data as inaccurate and "if the challenge is successful to have the data erased, rectified, completed or amended."[111]

Although they are far more demanding than most current national privacy practices, the OECD Guidelines have been criticized as too weak.[112] And, indeed, in some ways they are showing their age. One right that surely needs to be added today is the right to know when data held about a person has been compromised—hacked, leaked, lost, or stolen. An increasing number of states have rules requiring disclosure of data security breaches,[113] rules needed to allow people to take steps to protect themselves against identity theft.[114]

---

[105] *See generally* OECD Guidelines, *supra* note 104.

[106] *Id.* ¶ 7.

[107] *Id.* ¶ 8.

[108] *Id.* ¶¶ 9, 10.

[109] *Id.* ¶¶ 8, 11.

[110] OECD Guidelines, *supra* note 104, ¶¶ 12, 13.

[111] *Id.* ¶ 13(d).

[112] *See* Gary T. Marx, *Ethics for the New Surveillance*, *in* Visions of Privacy: Policy Choices for the Digital Age 39, 41–42 (Colin J. Bennett & Rebecca Grant eds., 1999).

[113] The original and, in many ways, model law is California's. *See* Cal. Civ. Code § 1798.29 (West 2006).

[114] *Cf.* Quinn Norton, *Porn Biller Says It Was Framed*, Wired News, Mar. 9, 2006, http://www.wired.com/news/technology/0,70380-0.html (reporting that a private data security firm uncovered the stolen consumer records of 18 million individuals, originally thought to be customers of iBill, an online payment company).

III. REAL ID on the Horizon—Setting the Wrong Standard

Without much thought about the consequences for privacy (or for several other things), last year Congress passed the REAL ID Act of 2005, which set up a national standard for the issuance of state driver's licenses.[115] Unless the statute is amended (or struck down as an unfunded mandate),[116] the state identity documents produced as a result of this command will be better authenticated and contain more personal data than any previous general-use government-issued credential in U.S. history.[117] These new REAL ID-compliant cards will probably become de facto national ID cards. At present, there is no sign that the private sector will be prevented from using the cards for authentication or data indexing. Thus, even if the new cards do not become full national ID cards, businesses will find these new cards to be such close substitutes for national ID cards as to close any existing window for an ID/privacy deal. Once these cards are ubiquitous, businesses will have access to a credential that provides strong authentication, and an index number, without having to commit to any improvement in their privacy practices.

Under REAL ID, starting on May 11, 2008, "a Federal agency may not accept, for any official purpose, a driver's license or identification card issued by a State to any person unless" that state credential complies with technical standards issued by the Department of Homeland Security.[118] Although it will not be federally issued, the new federally defined ID card will become a practical necessity for anyone wishing to "travel on an airplane, open a bank account, collect Social Security payments, or take advantage of nearly any government service."[119]

REAL ID requires that states comply with extensive rules about how they issue driver's licenses, and defines in some detail what in-

---

[115] REAL ID Act of 2005, Pub. L. No. 109-13, div. B, 119 Stat. 231, 302. Title II of REAL ID, "Improved Security for Drivers' Licenses and Personal Identification Cards," lays out requirements for new state ID cards. *See* div. B, tit. II, 119 Stat. at 311 (codified at 49 U.S.C.A. § 30301 note (2006)).

[116] *See* Suzanne Gamboa, *Senator Slams New Driver's License Rules*, SFGATE.COM, May 10, 2005, http://www.sfgate.com/cgi-bin/article.cgi?f=/n/a/2005/05/10/national/w155857D84.DTL (noting that the National Governors Association is considering a challenge to REAL ID on the ground that it is an unfunded mandate).

[117] *See generally* REAL ID Act.

[118] *Id.* § 202(a), 119 Stat. at 312. The Secretary of Homeland Security may extend this deadline. *Id.* § 205(b), 119 Stat. at 315. And he will.

[119] Declan McCullagh, *FAQ: How REAL ID Will Affect You*, CNET NEWS.COM, May 6, 2005, http://news.com.com/2102-1028_3-5697111.html.

formation those licenses must contain.[120] Before issuing a driver's license that will qualify as valid under REAL ID, the states will have to require and verify the applicant's documentation[121]—either a photo identity document or a non-photo identity document that contains both the applicant's full legal name and date of birth.[122] States must verify the applicant's name, primary address, date of birth and SSN (or proof of Social Security ineligibility).[123] What is more, REAL ID obliges states to verify the correctness and uniqueness of the SSN.[124] States may not accept any foreign document other than an official passport.[125] And they can only issue driver's licenses to citizens, permanent residents, certain asylum seekers, and the holders of particular types of visas.[126]

When issued, the license must contain the holder's actual addresses (rather than a post office box), full legal name, date of birth, gender, signature, and driver's license number, and it also must contain a digital photo of the person's face.[127] In addition, the card will have to include physical security features (to be defined by the Department of Homeland Security), designed to prevent tampering, counterfeiting, or

---

[120] *See* REAL ID Act of 2005, Pub. L. No. 109-13, § 202(b)–(d), 119 Stat. 231, 312–15.

[121] *Id.* § 202(c)(1), (d)(4), 119 Stat. at 312–13, 314. The statute also imposes substantial record-keeping requirements on the states:

- States must retain digital images of identity source documents in electronic storage in a transferable format, *id.* § 202(d)(1), 119 Stat. at 314;
- States must retain paper copies of source documents for a minimum of seven years or images of source documents for a minimum of ten years, *id.* § 202(d)(2), 119 Stat. at 314; and
- States must maintain a state motor vehicle database that contains: (A) all data fields printed on driver's licenses and IDs issued by the state; and (B) motor vehicle drivers' histories, including motor vehicle violations, suspensions, and points on license. *Id.* § 202(d)(13), 119 Stat. at 315. This database must be shared with other states. *Id.* § 202(d)(12), 119 Stat. at 315.

[122] *Id.* § 202(c)(1)(A), 119 Stat. at 313.

[123] *Id.* § 202(c)(1)(B)–(D), 119 Stat. at 313.

[124] *See id.* § 202(c)(3)(A), 119 Stat. at 314. In the event an SSN already is registered to or associated with another person to whom any state has issued a driver's license or ID, the state shall resolve the discrepancy and take appropriate action. *Id.* § 202(d)(5), 119 Stat. 314.

[125] *Id.* § 202(c)(3)(B), 119 Stat. at 314.

[126] *See* REAL ID Act of 2005, Pub. L. No. 109-13, § 202(c)(2)(B), 119 Stat. 231, 314. The list of visa classes that qualify for a driver's license is noticeably shorter than the list of visa types that permit long-term residence and even employment in the United States. *See* 8 C.F.R. §§ 204, 205, 212, 214, 244 (2006). This is likely to cause serious problems.

[127] REAL ID Act § 202(b), (d)(3), 119 Stat. at 312, 314.

duplication.[128] REAL ID also tries to ensure that driver's licenses will be a unique credential. If a person presents an out-of-state driver's license as ID, the issuing state will have to confirm that the out-of-state license is being terminated before issuing a new one.[129]

For most states, REAL ID means a significant, and expensive,[130] change from current procedures. And the states have claimed that REAL ID's May 2008 deadline is unrealistic.[131] The Department of Homeland Security has the power to waive that deadline for cause, but it is unclear how willing the Department will be to use it.[132] In any event, whether the effective date is 2008 or a few years later, it seems very likely that once enough states start issuing REAL ID-compliant credentials, the IDs will become at least very close substitutes for a national ID card.

Worse, REAL ID specifies that licenses will have to be machine-readable by a "common machine-readable technology"—a technology that has not yet been defined by the Department of Homeland Security.[133] It is likely, however, that this technology will be available to the private sector as well as to governmental users.[134] And because the IDs will become standardized around one mandated technology, the cost of license-reading technology will decrease, thereby lowering the cost barrier to the collection and storage of the holders' personal data by private parties. Once this takes off, whatever hope there may be to leverage even a moderately benign privacy rule off the creation of a standardized national ID card will evaporate.

---

[128] *Id.* § 202(b)(8), 119 Stat. at 312; *see id.* § 205(a), 119 Stat. at 315 (granting the Secretary of Homeland Security the authority to issue regulations under REAL ID).

[129] *Id.* § 202(d)(6), 119 Stat. at 314.

[130] Estimates of the total cost for all states together range from $100 million to $260 million. *See* Jared Joyce-Schleimer, Current Development, *The State of the REAL ID Act of 2005*, 19 Geo. Immigr. L.J. 611, 612–13 (2005).

[131] § 202(a)(1), 119 Stat. at 312; *see* Nat'l Governors Ass'n et al., The REAL ID Act: National Impact Analysis 2 (2006), *available at* http://www.nga.org/Files/pdf/0609REALID.pdf.

[132] *See* REAL ID Act of 2005, Pub. L. No. 109-13, § 205(b), 119 Stat. 231, 315.

[133] *Id.* § 202(b)(9), 119 Stat. at 312.

[134] This is already being criticized:

> This will, of course, make identity theft easier. Assume that this information will be collected by bars and other businesses, and that it will be resold to companies like ChoicePoint and Acxiom. It actually doesn't matter how well the states and federal government protect the data on driver's licenses, as there will be parallel commercial databases with the same information.

Schneier on Security, http://www.schneier.com/blog (May 9, 2005, 09:06 EST).

Conclusion

Some form of national ID card now seems inevitable, be it a "virtual" card, REAL ID-based driver's license, or federally issued document.[135] At present, we are on track for cards that both lack privacy protections and fail to address the ways in which the cards will be integrated with new and existing databases. Most likely, these new cards will be used not only for authentication but also as the index around which databases of personal data will be organized. Once a standard becomes dominant in the marketplace, it will be hard to change; experience suggests it will also be hard to regulate.

The time for new legislation—or an amendment to REAL ID—is now, before other standards become entrenched in the marketplace. We live in a last, brief moment of opportunity: absent fairly unlikely legislation forbidding the use of alternatives, privacy rules can successfully piggyback on a national ID system only if private sector data users decide that it is in their economic interest to use the new credential. A single reliable identifier should be of considerable interest to most private sector data users, as the alternatives that exist today are unreliable because of data quality problems and because the data is difficult to sort reliably, at least without expense. At present, the economics may still allow an opportunity for a deal. It seems all but certain that five years from now this will no longer be true.

The introduction of a new standard REAL ID has created an opportunity for the federal government to use its power creatively. The carrot of lower transaction costs dangled by easy, secure, reliable, and cheap identification might suffice to create market-based incentives for businesses to accept the stick of adherence to substantive privacy conditions. By defining a standard for data access and numbering, and by retaining ownership of the standard and especially the data, the government could give itself the leverage to offer a deal to firms desiring to take advantage of the new credential. A ubiquitous and reliable numbering system should be very attractive to businesses, and they might be willing to accept the obligations of Fair Information Practices as the price of admission. Making the privacy program formally voluntary, in the sense that only those who used the new cards or the new numbers would be required to follow the privacy standard, would also make it more likely to be politically acceptable.

---

[135] As I noted at the outset, a full weighing of the costs and benefits of national ID cards requires looking at the public sector uses of the card as well.

One important consequence of this proposal is that it would centralize and nationalize the data privacy debate. Although there have been successes, the explosion of privacy-destroying technologies within the last two decades suggests pretty strongly that standards and practices unfriendly to data privacy are being set more quickly and in more places than the privacy community can handle. A perverse advantage of a centralized national ID regime would be that it would create a very visible, single target for debate about privacy regulation. This is only a mixed blessing, for centralization also allows the interests that tend to oppose restrictions on the use of personal data to unite their lobbying efforts in one massive push for the goldfish bowl society.[136]

An invitation to a debate, by definition, offers only an uncertain outcome. But without this debate, at present the outcome seems all too certain, and it will be ugly.

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