National Identity Cards: Fourth and Fifth Amendment Issues

By

Daniel J. Steinbock*

---

* Harold A. Anderson Professor of Law and Values, University of Toledo College of Law; B.A., J.D., Yale University. The author is grateful to Professors David. A. Harris and Rebecca Zietlow for their thoughtful comments on an earlier draft.

I. INTRODUCTION

In the frenzied days and weeks following September 11th many observers called for serious consideration of a national identity system whose centerpiece would be some form of national identity card. Such a system was seen mainly as a tool against terrorists, but also as a useful response to illegal immigration, identity theft, and electoral fraud. As yet, no member of Congress has introduced legislation to establish a formal national identity system or require a national identity card,[1] and the "war on terrorism" has turned to other concerns. Nevertheless, the past two years have seen the most serious and detailed consideration of a national identity

[1] Testimony of Katie Corrigan, "National ID Card Proposals by Another Name" "Does America Need a National Identifier?" at 114, 118

system in a generation,[2] and we are probably just one domestic terror attack away from its implementation in some form.[3]

A national identity system raises a host of policy and legal issues. Among the former, the most important issue is what the purpose of such a system would be and whether it would be worth the inevitable financial and social costs. The answer to that question would help determine such subsidiary questions as who would be required to carry an identity card, what data would be linked to the card, who would have access to that data, and what uses would be made of it. There are many possible "national identity systems" and myriad kinds and uses of a national identity card.

Scholarly and popular commentary on the possibility of national identity cards has tended to focus on their effect on individual privacy, or, as some have put it, the right to anonymity. Obviously, this is an extremely important issue, because a national identity card has the potential to alter some fundamental aspects of American life. It would undoubtedly enhance governmental access to information about each person's activities, interests, and contacts. Imposing identity checks would in all likelihood vastly increase the frequency of interactions with government agents. Although the possible Fourth and Fifth Amendment ramifications of a national identity system have often been acknowledged, they have not been explored in any great depth.[4] While the impact on these constitutional rights would of course depend on the particular features of the

---

[2] See e.g. ALAN M. DERSHOWITZ, WHY TERRORISM WORKS: UNDERSTAND THE THREAT, RESPONDING TO THE CHALLENGE 200-201 (2002) (a national identity card is "an issue that deserves careful consideration"); The Century Foundation Homeland Security Project, The Debate Over a National Identification Card 1 (2003) ("[P]roposals for creating a national identification card have gained new attention."). See also, id. at 8-9 (listing proposals for enhancements to identity documents and identification requirements).

[3] The Century Foundation Homeland Security Project, The Debate Over a National Identification Card 10 (2003)("[I]t is likely that some sort of more extensive identification system will eventually be established in the United States").

[4] Computer Science and Telecommunications, National Research Council, IDs – Not That Easy 7 (200!) ("Clearly, an examination of the legal . . . framework surround identity systems . . . would be essential.")

system, because of their centrality to any likely national identity system it is worth examining these issues even in the absence of a concrete proposal.[5]

Part II of this Article describes the features of a national identity system which most observers regard as essential. The main point of identity checking is to make a connection between the identified individual and a collection of data. To be effective, a national identity system would therefore need to insist that people provide identification at certain times or places. This would almost certainly produce new interactions between the populace and law enforcement personnel – a subject regulated by the Fourth Amendment only when it amounts to a seizure of the person. One Fourth Amendment question, then, concerns the occasions on which state agents could demand to see a person's identity card. As the law stands now, the police may *request* to see identification of anyone at any time, in a so-called consensual encounter that does not involve seizure of the individual. On the other hand, the *demand* to see identification usually turns the encounter into an investigative detention, which generally requires that the police have reasonable suspicion of criminality. In addition, however, the Supreme Court has approved the use of suspicionless identification checkpoint stops for certain purposes like border control.

The creation of a duty to carry and present identification at certain times would presumably take place against this background, while moving some of these doctrines into new territory. Could, for example, every person subjected to an investigative stop be compelled, on pain of prosecution, to show identification? If so, would a national identity system create an incentive to make more stops, particularly for moving violations. When could compulsory identity checkpoints be sustained under the Fourth Amendment administrative search rationale?

---

[5] NRC Report, supra note 4, at 29 ("The constitutional limitations on an agent's ability to require presentation of IDs . . . should be explored before any such enactment to avert the costs of imposing the system and then having to revise or abandon it in the face of its unconstitutionality, to say nothing of its effects on civil liberties."

Moreover, would there be Fifth Amendment self-incrimination objections to any of these identification requirements? Part III addresses the constitutional questions raised by governmental demands, in a number of contexts, that a person present her identity card.

An identity check can generate new data as well as draw on existing databases. The Fourth and Fifth Amendments are also potentially implicated by the surveillance and monitoring of a person's movement and activities through such data collection and retention. This is particularly true of governmental collection of data generated in circumstances in which there might otherwise be some legitimate expectation of privacy, such as information provided to health care or educational institutions or in other registration procedures. Would this be a search under the Fourth Amendment and, if so, would it be a reasonable one. As to more public encounters, law enforcement personnel may generally observe a person while she is in a public place, and may even use common technological aids to do so. So some data collection attendant on identity checks would seem exempt from Fourth Amendment scrutiny. Would the national identity system's frequent and thorough monitoring of movement and activities be so unlike more common police surveillance, though, that it constitutes a search and is therefore regulated by the Fourth Amendment? If so, at the very least it could not be done as a matter of course. A potential source of compelled self-incrimination inheres in this data generating aspect of a national identity system: the requirement that certain self-reported information be conveyed to official databanks. Part IV explores the Fourth and Fifth Amendment issues raised in the potential data collection and retention features of a national identity system.

This Article is not concerned with the efficacy of a national identification system or whether its benefits, however measured, would outweigh its costs – in other words, whether it is a "good idea." The findings of this Article are not completely divorced from that question,

however. As this Article will demonstrate, to some degree the Fourth Amendment will reduce the potential benefits of a national identification system by standing in the way of practices that system might otherwise employ. In particular, random identification stops would fly in the face of Fourth Amendment jurisprudence. "Terrorist" profiling checkpoints probably do not pass Fourth Amendment muster, either, though they might in certain circumstances. Identification demands in the course of registration procedures, traffic or investigative stops, or arrests, however, are all acceptable. Nor does the Fourth Amendment stand in the way of requesting – rather than demanding -- identification of any person at any time. On the information gathering side of the process, there are substantial Fourth Amendment questions raised by mandated reporting of personal information that people produce in the course of everyday life. Though this practice should be regarded as a search, it may not be an unreasonable one, up to a point. In contrast to the substantial questions that arise under Fourth Amendment, the Fifth Amendment presents little serious obstacle to the most probable national identity system practices.

Whether all of this leaves the glass of a national identity card half full or half empty depends on one's perspective. What is fairly clear is that while the constitution might bar certain practices, and block others depending on their purpose, it would be possible to have a constitutional national identity card system of a fairly comprehensive type. Even where such an identity system would not strictly run afoul of the Fourth and Fifth Amendments, an analysis of the interests those provisions are designed to protect provides an insight into the price in privacy and liberty a national identity card would exact. This Article will also indicate how these effects might be somewhat mitigated in the system's design. In that sense, this Article hopes to illuminate not only what kind of national identity system the U.S. lawfully could have, but how it might be designed, and, implicitly, whether we want to have one at all.

II. FUNCTIONS AND FEATURES OF A NATIONAL IDENTITY SYSTEM

A. Generally

The basic function of a national identity system would be "to link a stream of data with a person."[6] "[H]uman identification is the association of data with a particular human being."[7] Once that connection is made, official reaction can take a variety of forms, depending of course on what the data show and the legal consequences of that knowledge. Our current database of outstanding arrest warrants,[8] for example, authorizes the arrest of the individual linked with such information.[9] In protecting against terrorists, in general once the link between an individual and a certain record was established, the aim would be that "[i]f there were risk factors, the appropriate measure could be taken to ensure safety."[10] In a similar way, the association between a given person and a body of data can be used for purposes other than crime prevention and enforcement. A national identity system, it has been suggested, can "aid in fraud prevention (for example, in the administration of public benefits), catch 'deadbeat dads,' enable electoral reforms, allow quick background checks for those buying guns or other monitored items, and prevent illegal aliens from working in the United States."[11]

Any such system depends on two major features: the database (or databases) containing information about particular individuals and a means to connect a given person with that

---

[6] Roger Clarke, Human Identification in Information Systems: Management Challenges and Public Policy Issues," 7 Information Technology & People, (No. 4) 6, 8 (1994).
[7] Roger Clarke, Human Identification in Information Systems: Management Challenges and Public Policy Issues," 7 Information Technology & People, (No. 4) 6, 8 (1994).
[8] **Cite needed**
[9] See, e.g., Arizona v. Evans, 514 U.S. 1 (1995) (holding the exclusionary rule inapplicable to a search resulting from the arrest of a suspect erroneously listed in a database as having an outstanding arrest warrant).
[10] Sobel, Demeaning, at 334. See also, statement of Tim Hoescht, Oracle, , "Does America Need a National Identifier?" at 140, 141-42.
[11] NRC, supra note 1, at 6.

information.[12] One way to store information about a person is on a card or other physical token in human readable or machine-readable form.[13] Alternatively, information may be stored in computer databases elsewhere, in which case there will likely be points in time at which information about the individual would be accessed, or input, or both. "[A] card would likely be one component of a large and complex nationwide identity system, the core of which could be a database of personal information on the U.S. population."[14] What data to collect, who would have access to that data, and what uses would be made of it are major issues in the design of any prospective national identity system.[15] As is discussed below, these decisions will directly affect the degree to which the system creates searches or seizures in the Fourth Amendment sense.

In addition to this information cache, any national identity system must have a means of establishing identity, in the sense of recognizing an individual as being a specified person. Roger Clarke has produced a thorough review of the various means of identifying a person in order to associate data with that person. These include appearance, social behavior, names,

---

[12] This is no easy task. For an indication of some of how much work would need to be done to construct a standard national database, see Government Accounting Office, *Terrorist Watch Lists Should be Consolidated to Promote Better Integration and Sharing*, GAO-03-322 (April 15, 2003) at 1-2 ("Generally, the federal government's approach to developing and using terrorist and criminal watch lists in performing its border security mission is diffuse and nonstandard, largely because these lists were developed and have evolved in response to individual agencies' unique mission needs and the agencies' respective legal, cultural, and technological environments."); Government Accounting Office, *Border Security: New Policies and Procedures Are Needed to Fill Gaps in the Visa Revocation Process*, GAO-03-798 (June 2003). In September 2003 the federal government established a new Terrorist Screening Center, to consolidate terrorist watchlists and used the results in screening by consuls, border agents, and other federal officials, as well as some private industries. Homeland Security Presidential Directive/Hspd-6 (September 16, 2003) *reprinted in* 80 Interpreter Releases 1322 (September 22, 2003); Dan Eggen, *Plan for Counterterror Database Unveiled*, WASH POST A02 (September 17, 2003).

[13] NRC, supra note 1, at 22.

[14] NRC at 5.

[15] See NRC, supra note 1, at 22-28.

codes, knowledge, tokens, bio-dynamics, natural physiology, and imposed physical characteristics.[16]

In any potential national identity system codes, tokens, and physiology – or some combination of all three – will likely be the most important means of identification. Codes are usually a set of numbers, such as the Social Security number. Their major advantages over names are that they are unique, they do not change, and their issuance can be controlled.[17] A "token" is a tangible item that a person has in his or her possession. These are often documents, though they do not have to be; "memory" or "smart" cards with encoded data can also serve as identity tokens. Documentary tokens currently in common use include birth certificates, passports, drivers' licenses, and social security cards.[18]

Biometrics are identification techniques based on some unique physiological and difficult-to-alienate characteristic.[19] Current forms of identification often rely on such relatively primitive biometrics as skin, hair, and eye color, physical markings, gender, and facial hair.

---

[16] Roger Clarke, *Human Identification in Information Systems: Management Challenges and Public Policy Issues*, 7 INFORMATION TECHNOLOGY & PEOPLE, No. 4, 6, 10 (1994). Clarke gives an interesting account and capsule history of each. He also gives the following shorthand summary:

1. appearance – or how the person looks;
2. social behaviour – or how the person interacts with others;
3. names – or what the person is called by other people;
4. codes – or what the person is called by an organization;
5. knowledge – or what the person knows;
6. tokens – or what the person has;
7. bio-dynamics – or what the person does;
8. natural physiography – or what the person is;
9. imposed physical characteristics – or what the person is now.

[17] Clarke, supra note 16, at 13.

[18] For a detailed specification of documents establishing employment authorization and identity for purposes of verifying authorization to work in the U.S., see Immigration and Nationality Act §274A(b)(1), 8 U.S.C.A. §1324a(b)(1) (identity established by U.S. passport, resident alien card, driver's license).

[19] Clarke, supra note 16, at 17.

These are often portrayed in a photograph or list of physical characteristics, as, for example, on a driver's license. More discriminating physiological features that can also be used to establish identity include fingerprints, DNA patterns, and iris patterns.[20] Such biometrics serve to link the token on which the biometric information is contained to the person to whom it is supposed to relate.[21] Biometrics can also be associated directly from the person to the identification, as with computerized face recognition or iris scans.[22]

Codes and biometrics can be combined on a token, and present-day engineering can make this token hard to duplicate. The National Research Council Committee on Authentication Technologies and Their Privacy Implications has sketched out one example.[23] Another proposal made, and retracted, recently includes an enhanced and standardized state drivers license.[24] It must be recognized, however, that "the best that any system of authentication can do is provide a

---

[20] Clarke, supra note 16, at 19.
[21] Clarke, supra note 16, at 17.
[22] **Cite needed**
[23] NRC, supra note 1, at 38-39:

> Another possibility is a memory card (or storage card), which would hold more information and be more expensive than the magnetic-stripe cards of the previous example. These cards contain memory as well as some security logic to prevent unauthorized reading or tampering with their data. The information contained on them could be digitally signed (that is, a number would be associated with that information that is dependent on a secret known only to the signer as well as on the data itself) to prevent easy counterfeiting. The correspondence between the user and the card (along with the information on the card and in the database) could be ascertained through biometric authentication, which would be undertaken using special equipment – such as a reader for fingerprints or iris scans – in addition to presentation of the card. An additional possibility is to use smart card technology that permits computation (such as digital signatures and encryption) to take place on the card itself.
>
> Though successful attacks have taken place, these cards are even harder to counterfeit than memory cards. They might have a name, photo, number, and biometric data, all of which could be cryptographically signed. The data would be backed up in a database to enable checking when reissuing a card and checking for duplicates when the card is first issued. A card of this sort could engage in a real-time, cryptographic exchange with an online system to verify a user's identity – possibly without exposing details of that identity to the organization performing the data capture – for example, an airline or a retail establishment.

[24] See, Sobel, supra note 10, at 336-37 (The American Association of Motor Vehicle Administrators called for linking driers' license records with Social Security, immigration, and law enforcement databases.) See also, Richard Edwardson, *National Identification Systems and Privacy Right,* UCLA J. OF LAW & TECHNOLOGY 4 (2002).

compelling connection with some previous verification of identity."[25] In other words, identity documents or other tokens are only as good as the "breeder" documents that produced them; "[t]he accuracy of each layer of identification depends on the accuracy of the preceding layers."[26] While this may mean that no identification system can ensure completely that a given individual is who she claims to be, this problem goes more to the efficacy of a national identity system than to any question of legality.

This capsule summary of the functions and broad features of a national identity system may sound familiar to anyone living in early 21st century America because identification linked to information is already part of daily life. Some would conclude that we already have a national identity system, based primarily on the social security number.[27] Richard Sobel, for example, contends that even prior to September 11th a national identity system "was developing from the combination of government databanks and ID requirements," due to several pieces of federal legislation that combine a demand for identification with computerized records.[28] Other proposed legislation would move the U.S. in the direction of a national identity system, without

---

[25] NRC, supra note 1, at.

[26] Lynn M. Lopucki, *Human Identification Theory and the Identity Theft Problem*, 80 TEX.L.REV. 89, 98 (2001); U.S. General Accounting Office Testimony of Robert J. Cramer, Counterfeit Identification and Identification Fraud Raise Security Concerns (Sept. 9, 2003) (Senate Committee on Finance) (government officials generally did not recognize counterfeit documents in General Accounting Office attempts to obtain genuine driver's licenses).

[27] See e.g., Rick S. Lear & Jefferson D. Reynolds, *Your Social Security Number or Your Life: Disclosure of Personal Identification Information by Military Personnel and the Compromise of Privacy and National Security*, 21 B. U. INTL. L. J 1, 13-14 (2003).

[28] Sobel, supra note 10, at 323-32 (The five basic parts of an incipient national identification system are the Immigration Reform and Control Act of 1986 ("IRCA"); Immigration Reform and Control Act of 1986, Pub. L. No. 99-603, 100 Stat. 3359 (1986) hereinafter IRCA; the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 ("IIRIRA"); Illegal Immigration Reform and Immigrant Responsibility Act of 1996, Pub. L. No. 104-208, 110 Stat. 3009-546 to 3009-724 (1996) hereinafter IIRIRA; the Personal Responsibility and Work Opportunity Reconciliation Act of 1996 ("Welfare Reform Act"); Personal Responsibility and Work Opportunity Reconciliation Act of 1996, Pub. L. No. 104-193, 110 Stat. 2105 (1996) hereinafter Welfare Reform Act; the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"); Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996) hereinafter HIPPA; and the Federal Aviation Administration ID requirement and Computer Assisted Passenger Screening system ("CAPS"); Id at 323. Sobel also mentions educational databanks. Id. at n. 13. A social security number is used by the military, appears on military identity cards, and must be given to captors by service members. Lear & Reynolds, supra note 27, at 4-8.

formally establishing one.[29] One object of a true national identity system would be to allow access to information contained in several unrelated databases through one centralized system.[30]

B. Demands for Identification

Any system that depends on linking an individual with a certain identity, and hence to a body of data, must require that the person identify herself at some point or points in time, whether that identification is made by way of codes, tokens, biometrics, or some other means.[31] In theory, participation in an identification system can be voluntary or mandatory. An example of a "voluntary" program is the proposal for a "trusted traveler" card, which would exempt airline passengers from certain pre-flight inspections.[32] While possession and use of such a card would be voluntary,[33] the need to present it to gain the benefits of the program would not. Virtually any true national identity system requires mandatory participation, both in the sense of having an identity within the system and in presenting identification when required.[34] This is certainly true for a system whose object was discovery of undocumented migrants; some means of proof of lawful presence in the U.S. would seem to be a *sine qua non* of its operation.

---

[29] Testimony of Katie Corrigan, "Does America Need a National Identifier?" at 123 "National ID Card Proposals by Another Name" ("No member of Congress has introduced legislation that would implement a national ID system or ID card. Instead there are several proposals that would establish a national ID card or system through the 'backdoor' of other proposed legislation.") See sources supra note 2.

[30] Testimony of Katie Corrigan, "Does America Need a National Identifier?" at 120

[31] See TAN 16

[32] See e.g. David Jones, *What's Your "Risk Score"?*, In These Times (June 23 2003), at 17 (A trusted traveler program "would allow travelers to speed through airport security if they voluntarily agree to undergo an extensive background check and carried a card with a digital fingerprint or other biometric identifier." Alan M. Dershowitz, *Why Fear National ID Cards?*, NY TIMES OCT. 13, 2001, at A23 (optional identity card would be allowed to pass through security "more expeditiously"). See also, Sarah D. Scalet, *Who Do You Trust?*, CIO Magazine (referring to a trusted traveler program as the "post-9/11 version of first class").

[33] Cf., NRC, supra note 1, at 28 ("[E]ven when a system is nominally voluntary, attention should be paid to whether the large inconveniences of nonparticipation make it effectively mandatory.")

[34] NRC, supra note 1, at 28.

Realistically, demands for presentation of identification are inherent in any national identity system that would be worth having. [35]

Observers fear, however, that these "identification encounters" will have several inevitable effects. First, people would be required to carry the identification card or other token, and present it at designated interactions.[36] Second, at least some of these encounters would entail involuntary stops to present the identity token, and would thus interfere with free movement, as well as imposing dignitary harms. "Day-to-day individuals could be asked for ID when they are walking down the street, applying for a job or health insurance or entering a building."[37] There is also some fear that these identification checks would be disproportionately directed at members of minority groups.[38]

None of these apprehensions is without precedent. Even today, Belgium has a comprehensive national identity system and police officers can ask to see the identity card of any person found in public.[39] When the British used identity cards for commodity rationing during and after World War II, police demanded to see the cards at other times, leading to protests and ultimately the end of the program in 1952.[40] Identity cards were essential to South Africa's apartheid system. They also proved very helpful to Nazi and Rwandan genocidal killers, who used them to identity and locate members of their target ethnic groups.[41]

---

[35] NRC, supra note 1, at 28 ("In general, any attempt to ascertain that an individual does not possess an unwanted attribute (for example, malicious intent) requires a complete knowledge of behaviors related to that attribute, and hence mandatory checks.")
[36] Sobel, supra note 10. at 338-39, 363.
[37] Testimony of Katie Corrigan, "Does America Need a National Identifier?" at 113
[38] Testimony of Katie Corrigan, "Does America Need a National Identifier?" at 114, 118
[39] Testimony of Rudi Veestraeten, Identity Cards and National Register in Belgium, in "Does America Need a National Identifier?" at 129, 131 ("Although such request on behalf of a law enforcement agency does not need to be [so] motivated, it mostly occurs only when there is a particular reason for a police officer to so do (suspicious behavior, events, security reasons)." Id. at 131.
[40] Sobel, supra note 10, at 347.
[41] Sobel, supra note 10, at 343-49.

In addition to the burdens of carrying identification and producing it on demand, required presentation of identity tokens might have other effects on individuals' freedom from unreasonable search and seizure. One is the monitoring of individual movement and activity. Each identification encounter would be an occasion to add information to the central database, facilitating government surveillance of movement and activity.[42] In any high-integrity identifier scheme, it is feared by some, "[a]ll human behaviour would become transparent to the state and the scope for non-conformism and dissent would be muted to the point envisaged by the anti-Utopian novelists."[43]

Conversely, each identification encounter would contain the potential for the resulting information, rightly or wrongly, to cause a further interference with personal mobility. This effect depends, of course, on what the information is and how it is used. Historically, some identity cards have served in effect as internal passports. "Under the most repressive regimes, such as those in Communist Eastern Europe, inhabitant registration schemes were instrumental in the prevention of unauthorized movement both within the country and out of it."[44]

The Transportation Security Administration (and its forerunner) has had a computer-based airline passenger screening in place since the late 1990's, and is currently testing an updated version called CAPPS II.[45] The CAPPS II system collects passengers' personal information such as name, address, birth date and credit card number. It then checks this information against databases, including criminal history records, to produce a passenger

---

[42] Testimony of Katie Corrigan, "Does America Need a National Identifier?" at 113

[43] Roger Clarke, Human Identification in Information Systems: Management Challenges and Public Policy Issues," 7 Information Technology & People, (No. 4) 6, 34 (1994).

[44] Roger Clarke, Human Identification in Information Systems: Management Challenges and Public Policy Issues," 7 Information Technology & People, (No. 4) 6, 27 (1994). This was also true in a more rudimentary form for slaves in the antebellum South. Sobel, supra note 10, at 343.

[45] Joe Sharkey, *A Safer Sky or Welcome to Flight 1984?*, N.Y. TIMES, March 11, 2003, at C9.

security code of green, yellow, or red.[46] According to the Transportation Safety Administration, this will "allow dynamic targeting on a real-time basis."[47] Those passengers receiving a rating of red will be denied boarding, something that has happened under the existing CAPPS system.[48]

In sum, it is almost inevitable that any national identity system, whether total or partial, will require individuals to present identification at certain times and places because "[t]he absence of the power to demand evidence of identity weakens the integrity of a general-purpose identification scheme."[49] Just what occasions would require an identification check is an important issue in the system design. At present, individuals must provide specified forms of identification to prove employment authorization at the time of hire,[50] to obtain a passport,[51] or to board an airplane.[52] The provision of a social security number (often without actual production of the card) attends other transactions.[53] Increased demands for identification, probably through presentation of a token or some other identification mechanism, are almost inevitable if a

---

[46] Joe Sharkey, *A Safer Sky or Welcome to Flight 1984?*, N.Y. TIMES, March 11, 2003, at C9. See also, Matthew L. Wald, *U.S. Agency Scales Back Data Required On Air Travel*, N.Y. TIMES, July 31, 2003, at A16 (Transportation Safety Administration "will not use information of a passenger's credit, like a returned check or an unpaid bill, nor any health records.") Larry Abramson, *Plans to step up security screening for airline passengers have been derailed*, Morning Edition, National Public Radio, August 1, 2003 (Lexis).

[47] Wald, supra note 46 ("The risk assessment function . . . will determine the likelihood that a passenger is a known terrorist , or has identifiable links to known terrorists.") There are also plans eventually to identify people for whom there are warrants for violent crimes. Ricardo Alonso-Zaldivar, *Critics Wary of New Traveler Profile System*, LOS ANGELES TIMES (August 26, 2003).

[48] Jones, supra note 32

[49] Roger Clarke, Human Identification in Information Systems: Management Challenges and Public Policy Issues," 7 Information Technology & People, (No. 4) 6, 27 (1994).

[50] See supra note 18.

[51] U.S. Dept. of State, How to Apply for in Person for a U.S. Passport, http://travel.state.gov/passport_obtain_text.html (visited September 29, 2003) (previous U.S. passport; naturalization certificate; certificate of citizenship; or current, valid driver's license or government or military identification; plus a social security number).

[52] Sobel, supra note 10, at 325. (Since October 1995, the Federal aviation Administration ("FAA") has required airlines to ask passengers to identify themselves with government-issued identification.")

[53] Sobel, supra note 10, at 324-27.

national identity system is established. Moreover, once the system was in place the tendency would be to use it, and over time to expand its use.[54]

III. IDENTITY CARD REQUESTS AND DEMANDS

The Fourth Amendment bars "unreasonable seizures," including seizures of the person. Evaluating the effect of the Fourth Amendment on demands for identification involves determining first whether the demand is a "seizure;" if not, the Fourth Amendment inquiry is at an end. If the encounter does entail a "seizure" the second question is whether it is one that is "reasonable." All manner of state-citizen interactions are potentially implicated by identity card checking, and the Fourth Amendment analysis will be similarly varied. This Part proceeds by both applying existing Fourth Amendment principles to the kinds of situations in which a national identity card would likely be requested or demanded and evaluating what effects a widespread national identity system would have on the law itself.

A. Consensual Interactions

Not every demand for identification involves a "seizure." For reasons of her own, an individual may choose to interact with a state agent requesting her identification, and the additional action of producing identification will usually not convert the voluntary encounter to a seizure. There are however, degrees of voluntariness. Moreover, an intrusive national identity system would, itself, probably affect how people perceive identity checks, and how they react to them.

At present one occasion for mandatory identification occurs when individuals must give identification information over the phone, over the internet, or by mail. This is usually some

[54] Roger Clarke, Human Identification in Information Systems: Management Challenges and Public Policy Issues," 7 Information Technology & People, (No. 4) 6, 27 (1994). ("It is only to be expected that various pressure groups will seek to increase the impositions as time goes by, in response to such problems as illegal immigration, perceived worsening of law and order, epidemics, natural disasters, national security emergencies, etc."). In addition, there is the real possibility of abuse of whatever system results. See TAN infra.

combination of name, code (e.g., social security or credit card number), and knowledge-based identifier (e.g. PIN, mother's maiden name).[55] Nothing even remotely approaching a seizure is involved in this kind of exchange because there is no personal restraint.

At the level of personal interaction, identification is currently required during what may be described as registration procedures. These include registration for drivers' licenses, medical services, schools, and flights, as well as employment eligibility verification. Airport check-in is the paradigm, and now necessitates government-issued photo identification.[56] All of these tasks may require the customer to "stop" to register, and while the display of identification tokens may slightly lengthen the process, it is unlikely that those additional moments would convert it to a state-mandated seizure.

The Supreme Court has refused to find a seizure in governmental questioning and identification requests of people already in confining circumstances. In *INS v. Delgado*, for example, immigration agents moved through a factory, questioning workers and then asking for immigration papers from those who appeared not to be citizens.[57] These requests for identification were held not to be seizures, because, in the Court's view, the workers had no reasonable fear that they could not continue working or moving about the factory.[58] INS agents also took positions near the factory exits. The Court rejected the claim that the entire workforce was therefore seized because "[o]rdinarily, when people are at work their freedom to move about has been meaningfully restricted, not by the actions of law enforcement officials, but by the workers' voluntary obligations to their employers."[59] The Court has followed this approach in

---

[55] See supra note 16.
[56] See supra note 52.
[57] 466 U.S. 210, 212-13 (1984).
[58] Id. at 220-21.
[59] Id. at 218.

two cases upholding police requests for permission to search the luggage or persons of interstate bus travelers, finding that although the passengers' freedom of movement had been limited the restriction flowed not from police conduct but from being passengers on a bus.[60] This reasoning easily applies to identification requests that are ancillary to other required interactions, such as the registration procedures described above, and strongly suggests that a national identity system could mandate the display of identification at other registration points, such as hotel or car rental check-ins, without creating any "seizure" of the person, so long as the registration would, by itself, ordinarily restrict movement.

Moreover, similar reasoning allows law enforcement agents to approach people and ask for identification even when their freedom of movement is not already limited by their own actions or decisions; in other words, as they go about their business in public. As long as a reasonable person would feel free to "terminate the encounter" in the circumstances, then the person has not been seized;[61] instead, she is participating in what the Court has called a "consensual encounter."[62] A request for identification documents falls within the scope of a consensual encounter.[63] The Court has recently stated, "Even when law enforcement officers have no basis for suspecting a particular individual, they may pose questions [and] ask for

---

[60] Florida v. Bostick, 501 U.S. 429, 436 (1991); see also United States. v. Drayton, 536 U.S.194, 201-02 ((2002).
[61] *Bostick*, 501 U.S. at 434-36.
[62] Florida v. Royer, 460 U.S. 491, 504 (1983); INS v. Delgado, 466 U.S. 210, 221 (1984). The Court's conclusion that a "reasonable person" would truly feel free to decline law enforcement requests for conversation, identification, travel documents, and permission to search has been criticized as an unrealistic characterization of how people actually react to these tactics. See Janice Nadler, *No Need to Shout: Bus Sweeps and the Psychology of Coercion*, 2002 SUPREME COURT REV. 153, 164-206 (2002); Stephen A. Saltzburg, *The Supreme Court, Criminal Procedure and Judicial Integrity*, 40 AM. CRIM. L. REV. 133, 135-141 (2003); Daniel J. Steinbock, *The Wrong Line Between Freedom and Restraint: the Unreality, Obscurity, and Incivility of the Fourth Amendment Consensual Encounter Doctrine*, 38 SAN DIEGO L. REV. 507, 521-35 (2001).
[63] United States v. Mendenhall, 446 U.S. 544, 552 (1980). If the individual declines to answer questions or requests for identification, "and the police take additional steps . . . to obtain an answer," however, then a detention has occurred. *Delgado*, 466 U.S. at 217.

identification . . . provided they do not induce cooperation by coercive means,"[64] a holding that reiterates statements in earlier cases. [65]

This doctrine has important implications for any national identity system. Law enforcement agents could approach individuals on the street and request to see a national identity card at any time, without any prior suspicion of criminality or other illegality. In a sense, an American national identity system could resemble the present Belgian one[66] as long as the interactions were requests and not commands. Simple requests for identification would probably produce compliance in the large majority of cases.[67] This raises, however, one of the dangers of law enforcement use of consensual encounters. Because the Fourth Amendment does not govern them, they can be initiated for no reason or for any reason at all, including the "racial stereotyping that is, unfortunately prevalent in every area of unregulated police discretion."[68] As a means of identity checking, then, consensual encounters run the risk of being employed on the basis of apparent race, ethnicity, or national origin, or appearing to be. In fact, since September 11, the debate on profiling understandably has shifted to role of racial, ethnic, national, religious profiling in preventing terrorism. Given that this would presumably be the principal goal of any national identity system, the role of profiles could easily figure in its design and use. Airline checking and immigration enforcement, to name two contexts, have already been criticized for

---

[64] United States v. Drayton, 536 U.S. 194, 201 (2002).
[65] See *Delgado*, 466 U.S. at 216, citing Florida v. Royer, 460 U.S. 491 (1983).
[66] See supra note 39
[67] Illya D. Lichtenberg, *Voluntary Consent or Obedience to Authority: An Inquiry Into the "Consensual" Police-Citizen Encounter* 199 (1999) (unpublished Ph.D. dissertation, Rutgers University (on file with author)) (89% of motorists acceded to police requests to search their vehicles).
[68] Steinbock, supra note, 62, at 509. DAVID COLE, NO EQUAL JUSTICE: RACE AND CLASS IN THE AMERICAN CRIMINAL JUSTICE SYSTEM 47 52 (1999). The Court has made clear on several occasions that an officer's subjective motivation for an otherwise lawful practice, even one based on racial or ethnic factors, is irrelevant to its legality under the Fourth Amendment. Bond v. United States, 529 U.S.334, 338 (2000); Whren v. United States, 517 U.S. 808, 816 (1996).

the use of ethnic and national criteria,[69] but some have contended that this is a rational response to the current terrorism threat.[70] Because the constitution puts so little restraint on racial, national, and ethnic profiling in areas such as consensual encounters, it is especially important that the issue be addressed in the drafting of any such system.

In a true consensual encounter, no person could be *compelled* to produce her identity card, however. After all, the whole premise of a consensual encounter is voluntariness on the part of the citizen, so individuals have a perfect right to say no.[71] While consensual encounters are not at all uncommon as an investigative technique, particularly for drug interdiction,[72] they are not currently imposed on large segments of the U.S. population, as would be the case if they became an integral part of identity-checking. If a true cross-section of the American population were routinely asked to show their identity cards by government agents, the incidence of compliance might decline drastically.[73] A national identity system that depended on voluntary responses to requests for identification thus runs the risk of perfectly legal, and possible

---

[69] See e.g., Leti Volpp, *The Citizen and the Terrorist*, 49 UCLA L. Rev. 1575, 1576-86 (2002) (describing the profiling of those who appeared "Middle Eastern, Arab, or Muslim" after September 11); David A. Harris, *Racial Profiling Revisited: "Just Common Sense" in the Fight Against Terror?*, 17 Criminal Justice 36, 40-41(2002) (describing immigration enforcement and questioning directed against persons from the Middle East).

[70] See e.g., Stephen J. Ellmann, *Racial Profiling and Terrorism*, 22 N.Y.L.S. L .REV. 675, 698 (2003) ("So long as our adversaries tend to be members of definable groups, in principle we should be able to find them if we take group membership into account, not as either a necessary or a sufficient factor, but as a relevant one."); DERSHOWITZ, supra note 2, at 208 ("It is foolish . . . to misallocate our resources in the fight against suicide bombers by devoting equal attention to searching an eighty-year-old Christian woman from Maine and a twenty-two-year-old Muslim man from Saudi Arabia>"). See also, U.S. Department of Justice, Fact Sheet: Racial Profiling, (June 17, 2003) at 5-6, http://www.usdoj.gov/opa/pr/2003/June/racial_profiling_fact_sheet.pdf (race and ethnicity may be used in terrorist identification to the extent permitted by the nation's law and the constitution).

[71] Steinbock, supra note 62, at 540-42.

[72] Nadler, supra note , at 159 ("[L]aw enforcement agencies capitalized on the *Bostick* decision by stepping up their efforts to root out drug trafficking on interstate buses.)

[73] DAVID COLE, NO EQUAL JUSTICE: RACE AND CLASS IN THE AMERICAN CRIMINAL JUSTICE SYSTEM 8 (1999).("[P]olice officers routinely used method of investigation and interrogation against members of racial minorities and the poor that would be deemed unacceptable if applied to more privileged members of the community."),

organized, civil disobedience.[74] It is unlikely, therefore, that a national identity system could rely solely, or mainly, on consensual compliance as a means of identity verification.

B. Investigative Stops

In contrast to a consensual encounter, the compelled detention of a person for investigation, including a demand for identification, constitutes a seizure under the Fourth Amendment. Though the real life factual differences between them can be quite small, an investigative stop is thus conceptually quite different from a consensual encounter. Under *Terry v. Ohio*[75]and its numerous Supreme Court progeny,[76] such seizures can be conducted only on "specific and articulable facts which, taken together with rational inferences from those facts, reasonably warrant [the] intrusion."[77] These facts and inferences can relate to an ongoing crime or a past felony. The level of evidence need for a lawful stop is often called "reasonable" or "articulable" suspicion, and can be distinguished from "inarticulable hunches"[78] or "inchoate and unparticularized suspicion,"[79] which are not sufficient to compel a person to halt for investigation.

Therefore, persons could not involuntarily be seized on a random or individual basis for identity checks in the absence of reasonable suspicion. The Supreme Court so held in *Brown v. Texas*, in which an officer stopped Brown for the sole reason of discovering his identity.[80] Because the officer lacked any basis for believing Brown to be involved in criminal activity, the

---

[74] Cf., municipal resolutions of noncompliance with Patriot Act.
[75] 392 U.S. 1 (1968).
[76] See, e.g., Florida v. J.L., 529 U.S. 266 (2000); Illinois v. Wardlow, 528 U.S. 119, 124-25 (2000); United States v. Sokolow, 490 U.S. 1, 7-8 (1989; United States v. Cortez, 449 U.S. 411, 417-18 (1981).
[77] Terry, 392 U.S. at 21.
[78] Id. at 22.
[79] Id. at 27.
[80] 443 U.S. 47, 52 (1979).

seizure violated the Fourth Amendment.[81] The Supreme Court similarly has barred the suspicionless stopping of motor vehicles to check license and registration[82] or for questioning about the travelers' citizenship.[83] These cases obviously constitute an obstacle to the effectiveness of any national identity system that depends on more than spot checking of the already suspicious, though, as we shall see below, not necessarily an insurmountable one.[84]

In those cases where reasonable suspicion to stop a person *is* present, mandatory possession of an identity card or other identity token would greatly enhance the utility of the investigative stop – as well as the possibility of abuse. As things stand now, the officer may demand identification and may even in some cases search for it,[85] but without a statute criminalizing noncompliance,[86] the officer has no way of securing it. Even then, addressing a statute requiring "'credible and reliable'" identification that carries a 'reasonable assurance' of its authenticity," *Kolender v. Lawson*, the Court found the law void for vagueness.[87] In the

---

[81] Id.
[82] Delaware v. Prouse, 440 U.S. 648 (1979).
[83] United States v. Brignoni-Ponce, 422 U.S. 873 (1975). This holding does not apply at the border or its functional equivalents. Id. at 876.
[84] See TAN infra.
[85] Generally, the warrantless seizure and search of a defendant's wallet during an investigatory stop or Terry stop for purposes of identification constitutes an unreasonable search and seizure. *Schraff v. State*, 544 P.2d 834 (Alaska 1975); *Baldwin v. State*, 418 So.2d 1219 (Fla. Dist. App. 1982); *State v. Newman*, 637 P.2d 143 (Or. App. 1981); *State v. Biege*, 787 P.2d 577 (Wash. App. 1990); *State v. Miller*, 1994 WL 246072 (Minn. App. Jun. 7, 1994); *State v. Webber*, 694 A.2d 970 (N.H. 1997); *Commonwealth v. Briscoe*, 2001 WL 1830019 (Va. Cir. Ct. Jun. 13, 2001); *State v. Beegle*, 2003 WL 21652737 (Wash. App. Div. 3 Jul. 15, 2003). However, a California Court of Appeals found that the seizure of a defendant's wallet for the purpose of identifying the defendant was within the scope of an investigatory detention. *People v. Loudermilk*, 195 Cal App.3d 996 (Cal. App. 1987). Also, the United States Court of Appeals, Fifth Circuit, held that the search of a defendant's wallet during an investigatory stop was reasonable when border patrol agents had reasonable suspicion that the defendant was an illegal alien and the defendant refused to disclose his identity or citizenship status. *United States v. Garcia*, 942 F.2d 873 (5th Cir. 1991).

[86] See e.g. Tex. Penal Code Ann., Tit. 8, §38.02 (a) ("A person commits an offense if he intentionally refuses to report or gives a false report of his name and residence address to a peace officer who has lawfully stopped him and requested the information.") quoted in *Brown*, 443 U.S. 47, 49 n.1.
[87] Kolender v. Lawson, 461 U.S. 352 (1983). (statute requiring citizen "who loiters or wanders upon the streets . . . . without apparent reason or business" to provide a "credible and reliable identification" and to account for their presence. Id. at 353 n. 1, 356.

Court's opinion, this standard gave excessive discretion to the police, opening the possibility of discriminatory enforcement.[88]

The vagueness problem in *Kolender* could presumably be remedied by a careful specification of just what kind of identity documentation the law requires.[89] A standard and relatively secure identity token would seem to be an essential feature of any national identity system,[90] and it would be surprising if such an identity card did not satisfy the vagueness objections voiced in *Kolender.* In other words, the specification of a national identity card as adequate (or necessary) proof of identity would remove uncertainty about what constitutes proper identification.

That would still leave two issues not decided by the Supreme Court in *Kolender*: whether either the Fourth or Fifth Amendments stand in the way of requiring that someone stopped on reasonable suspicion identify herself.[91] The Fourth Amendment argument, as made by Justice Brennan in two nonmajority opinions, seems to be that because it is conducted on less than probable cause, a *Terry* stop assumes a relatively low level of intrusion on personal privacy and mobility.[92] A demand for identification infringes on the right of a person stopped on reasonable suspicion to refuse to answer police questions,[93] and, overall, imposes on the suspect more than the seizure alone, and, overall, more than reasonable suspicion can justify. The Ninth Circuit has

---

[88] Id. at 360-61.
[89] See e.g., employment authorization documents supra note18.
[90] See TAN supra.
[91] *Kolender,* 461 U.S. at 355; see also. *Brown,* 443 U.S. at 53 n. 3 (Court stated it "need not decide whether an individual may be punished for refusing to identify himself in the context of a lawful investigatory
[92] *Kolender,* 461 U.S. 362-69 (Brennan, J. concurring); Michigan v. DeFillippo, 443 U.S. 31,41-46 (Brennan, J. dissenting).
[93] Id. at 366 ("[U]nder the Fourth Amendment, police officers with reasonable suspicion that an individual has committed or is about to commit a crime may detain that individual, using some force if necessary , for the purpose of asking investigative questions. They may ask their questions in a way calculated to obtain an answer. But they may not *compel* an answer, and they must allow the person to leave after a reasonably brief period of time unless the information they have acquired during the encounter has given them probable cause sufficient to justify an arrest.") (emphasis in original)(citations omitted).

accepted these arguments and found criminal punishment for refusal to give identification during a *Terry* stop to violate the Fourth Amendment, at least where identification is not needed as part of the investigation.[94] Most other courts, on the other hand, have upheld arrest and conviction for obstructing police business or for violation of statutes specifically requiring a suspect to give identification on request.[95]

As the Supreme Court has repeatedly stated, the purpose of an investigative stop is to confirm or dispel the suspicion that caused it.[96] The officers may use reasonable means to do so, including briefly detaining, demanding identification, and directing questions to the person. If everyone was compelled to carry an identity card pursuant to a previously enacted national identity system, would it be "reasonable" to demand to see that identification of those persons stopped on reasonable suspicion? The answer probably depends on two issues: 1) whether official knowledge of the person's identity (and associated data) would assist in the investigation, and 2) how long, or otherwise inconvenient, that process would be.

On the first issue, once the police have articulable suspicion that a person is committing or planning a crime, there is a reasonable likelihood that an identity check, especially one that tapped into criminal history and law enforcement databases, would produce useful information. For example, if the reasonable suspicion concerned drug sale or possession, access to a criminal history for that or related crimes would at least intensify the investigation. Similarly, data might confirm a suspect's story – that, for example, she works in an isolated area -- and thus dispel suspicion. There are myriad ways in which access to the suspects' identity would further the investigation. Probably the most significant effect of database-linked identity checks would be

---

[94] Id.; Martinelli v. City of Beaumont, 820 F. 2d 1491 (9th Cir 1987); Lawson v. Kolender 658 F. 2d 1362 (9th Cir. 1981).
[95] See e.g. Risbridger v. Connelly, 275 U.S.565 (6th Cir. 2002) (reviewing cases).
[96] United States v. Sharpe, 470 U.S. 675, 687 (1985); Royer, 460 U.S., at 500.

the discovery of outstanding warrants, which themselves would provide a basis for the suspects's arrest.[97] In short, a national identity card would make investigative stops more efficient and effective.

It is hard to see how these uses would materially increase the intrusiveness of the stop itself. While there would also be some circumstances in which requiring the suspect's identity card would not advance the investigation, merely asking for or reading it does not seem to add appreciably to the stop's intrusiveness. Moreover, it would be silly and unworkable to ask the officer on the street to distinguish between stops where identification would help and those where it would not. Rather, this would seem an area where a "bright-line" rule would make good sense.[98]

On the other hand, if the suspect was detained for an appreciable period of additional time, moved, or placed in a more confined area in connection with the identity check, then the process might be more intrusive than a *Terry* stop allows.[99] This could happen, for example, if the identity information had to be transmitted to a database and a reply took a long time to arrive. While in theory this could be accomplished in the time it takes to authorize a credit card transaction, a glitch in database access or communication is certainly possible. It is debatable

---

[97] If a national visa database could also be accessed, it is likely that a fair number of allegedly undocumented aliens would be identified.

[98] United States v. Robinson, 414 U.S. 218, 235 (1973) (stressing police officers' need to make quick *ad hoc* judgments). See also, Dunaway v. New York, 442 U.S. 200, 213-14 ("A single familiar standard is essential to guide police officers, who have only limited time and expertise to reflect on an balance the social and individual interests involved in the specific circumstances they confront.").

[99] A stop, the Court has said, may last as long as is reasonably necessary to conform or dispel the officer's suspicions. United States v. Sharpe, 470 U.S. 675, 686 (1985). At some point a stop cannot be justified on the basis of reasonable suspicion but becomes tantamount to an arrest and thus requires probably cause. *Id.* at 685. In United States v. Place, 462 U.S. 696 (1983), the Court held that a ninety-minute detention alone rendered the search unreasonable. *Id.* At 709-10. Otherwise, the Court has assessed the issue as one of overall reasonableness. Important factors in this assessment include the duration of the stop, whether the police diligently pursue the investigation, *Sharpe*, 470 U.S. at 686, and whether the suspect is moved during the detention, Florida v. Royer, 460 U.S. 491, 504-05 (1983).

whether a prolonged detention pending the outcome of a database search would be a "reasonable" incident of an investigative stop.[100]

The last objection to requiring an identification token on pain of criminal prosecution is that if the police may arrest a person for failing to identify herself during a *Terry* stop, then identification statutes "bootstrap the authority to arrest on less than probable cause."[101] There is very little to this argument. If the state can legitimately require people to carry identity cards and they fail to produce them at statutorily specified moments, then there is now probable cause to arrest for that crime even if probable cause to arrest for the circumstances that produced the stop never developed. Perhaps the fear is that the police would demand identification only, or mainly, from those whom they wanted to arrest for the underlying offense, but could not. If a national identity system was in existence, this tactic might actually succeed in producing an arrest for failure or refusal *less* frequently, because more people would be able easily to supply identification. In any event, it is hard to see how the possibility that an otherwise lawful stop might lead to an arrest for an unrelated crime somehow makes the stop itself, based upon independent grounds, questionable under the Fourth Amendment.[102]

Nor does the Fifth Amendment self-incrimination clause, by itself or in conjunction with the Fourth Amendment, bar officers from demanding identity cards from those stopped on reasonable suspicion. Ordinary questioning of a suspect during an investigative stop has been held not to bear the kind of psychological "compulsion" to self-incriminate that would trigger

---

[100] Traffic stops, a possible analogy, can generally last no longer than necessary to process the citation or warning. See e.g. United States v. Fernandez, 18 F 3d 874 (10th cir. 1994); People v. Cox, 782 N.E. 2d 275 (Ill. 2002).
[101] Carey v. Nevada Gaming Control Board , 279 F. 3d 873, 880 (9th Cir. 2002).
[102] *Terry* stops can, for example, lead to assaults on the officers or obstruction of police business in ways unrelated to the reason for the stop, and the validity of these charges is beyond question.

Miranda warnings.[103] A demand for identification, however, *does* involve compulsion, because a refusal -- often now, and certainly under a national identity system -- would likely involve some criminal penalty.[104] A suspect would thus face the choice between complying with a directive to produce her identity card or face arrest and prosecution. Thus, though *Miranda* warnings presumably do not have to be given, other core Fifth Amendment issues are potentially involved in demands for identification.

Assuming it is compelled, is a response to an identification demand also testimonial? The individual is saying "XY is my name," or "ABC is my address." The suspect is being "asked for a response requiring him to communicate an express or implied assertion of fact or belief," and the answer therefore contains a testimonial component.[105] Because a false answer could also result in criminal penalty,[106] and a truthful answer could sometimes serve to incriminate, the "cruel trilemma" of self-accusation, perjury, or punishment could potentially be present.[107] Similarly, someone who hands over an identity card is implicitly stating, "The information on this card pertains to me." The communication implicit in that act of production makes testimonial a response to a command to supply identification.[108]

For *Miranda* purposes, at least, even where there is compelled testimony, questions "normally attendant to arrest and custody"[109] are exempt from the usual interrogation rules. Eight Justices have concluded that responses to these "booking questions," designed to obtain

---

[103] Berkemer v. McCarty, 468 U.S. 420 (1984) (*Miranda* warnings not required during traffic stop).
[104] See TAN supra (criminal penalties under specific statutes requiring the production of identification during lawful stops or under obstruction of justice statutes). In contrast to other documents whose production may later be required because they were voluntarily and independently created, e.g. Andresen v. Maryland, 427 U.S. 463 (1976); United States v. Doe, 465 U.S. 605 (1984), a person presumably would have been compelled to participate in "creation" of the identity card.
[105] Pennsylvania v. Muniz, 496 U.S. 582, 597 (1990)
[106] 18 U.S.C. §1001; see e.g. the Texas statute in *Brown*, supra note .
[107] Murphy v. Waterfront Comm'n of New York Harbor, 378 U.S. 52, 55 (1964).
[108] Fisher v. United States, 425 U.S. 391 (1976); United States v. Doe, 465 U.S. 605 (1984).
[109] Rhode Island v. Innis, 446 U.S. 291, 301 (1980).

biographical data for police administrative purposes, are an exception to the *Miranda* rules.[110] It would not be surprising for the Court to extend this administrative question exception to "core" Fifth Amendment compulsion. The Court might be encouraged to do so by the fact that ordinarily a response to an identification demand would not be incriminating. Although under Fifth Amendment case law it does not take much for a person to establish the requisite possibility of incrimination,[111] the usual identity check is not likely to provide "a link in the chain of evidence needed to prosecute." [112] If an identity check produces any useful information at all it is likely to be the name and other data about a hitherto unknown person against whom evidence of a crime already exists. This is not the kind of testimonial incrimination against which the Fifth Amendment protects.[113] It of course is possible that in some exceptional case presenting an identity card will constitute compelled self-incrimination. It is even more possible that the police, having received compliance with their identification demands, will proceed to interrogate outside of the "booking questions" or the simple command to produce an identity card. Neither of these possibilities, however, makes the ordinary identity check incriminating as a general matter. Importantly, because this is a case-specific question, no blanket injunction against a national identity system on Fifth Amendment grounds could succeed.

Finally, even where an identification request nevertheless did appear to implicate the Fifth Amendment, the recent decision in *Chavez v. Martinez* calls into question whether a Fifth

---

[110] *Muniz*, 495 U.S. at 601.(questions regarding name, address, height, weight, eye color, date of birth, and age). Id. at __. Four Justices (Rehnquist, C. J., White, Blackmun, Stevens) consider the answers non-testimonial. (Brennan, O'Conner, Scalia, Kennedy) found the answers to be testimonial but to constitute an exception to *Miranda* rules.
[111] Hoffman v. United States, 341 U.S. 479 (1951); Ohio v. Reiner, 532 U.S. 17 (2001).
[112] Hoffman, 341 U.S. at 486.
[113] California v. Byers, 402 U.S. 424, 431 (1971) ("Disclosure of name and address is an essentially neutral act."). See also, id. at 433 ("Although identity, when made know, may lead to inquiry that in turn leads to arrest and charge, those developments depend on different factors and independent evidence.") (upholding California "hit and run statute which made criminal the failure of a driver involved in an accident to stop and give his or her name and address).

Amendment violation would occur if the suspect's responses were never introduced at trial.[114] If the required production of identification resulted in compelled testimonial incrimination, under *Chavez*, unless and until the statements or information (or evidence derived therefrom) were used at trial there would be no constitutional claim. This would raise questions about what evidence was "the fruit of the poisonous" identification; that is, what causal connection need be shown between the compelled self-identification and the trial evidence, and to what degree doctrines like independent source and inevitable discovery would come into play.[115] It is almost certain that identity could be independently proved at trial and that associated data could be shown likely to be inevitably discovered.[116]

In summary, identification checks would involve compelled testimonial communication. Courts would thus have to decide whether the disclosure of personal data would nevertheless fall outside the Fifth Amendment's coverage under a doctrine like the "booking question" exception to *Miranda*. Moreover, the ordinary identity check would rarely reveal incriminating information, and even more rarely directly lead to tainted, and thus suppressible, courtroom evidence. As a general matter, the Fifth Amendment self-incrimination clause, therefore, appears to present no insuperable barrier to required identity checks.

C. Arrests and Citations

All the reasons permitting law enforcement personnel to demand identification from those stopped for investigation, and one more, apply to persons being arrested or given a traffic

---

[114] 123 S.Ct. 1994 (2003). (Four of the Justices (Thomas, Rehnquist, O'Connor, and Scalia) maintain that the Fifth Amendment cannot be violated unless the evidence is actually introduced against the defendant. Two others (Souter and Breyer) maintain that this is the general rule and is certainly true in this case.)
[115] Murray v. United States.; Nix v. Williams, 467 U.S. 431 (1984) (exclusionary rule does not apply to information that ultimately or inevitably would have been discovered by lawful means).
[116] United States v. Crews, 445 U.S. 463 (1980).

citation. These people have already been seized on an allegation of probable cause,[117] so a demand for identification imposes no additional restraint. Identification is even more necessary for the processing of the arrest or traffic citation than for an investigative stop.[118]. An arrest will usually lead to an arraignment on a criminal charge, and courts will often refuse to arraign an individual whose identity is unknown.[119] Before an arrestee is released on bail it is important to know whether or not she is wanted for other offenses. A traffic citation also requires some assurance that the person cited will respond or face the consequences

The Supreme Court held in *U.S. v. Whren* that the officers' motivation for a traffic stop is irrelevant to its reasonableness under the Fourth Amendment; in other words, a driver cannot object to a stop on the ground that it was a "pretext" for the officers to perform one of the many investigation measures attendant on a traffic stop[120] Because identification verification is always part of a traffic law enforcement,[121] police officers could, consistent with Supreme Court precedent, pull drivers over to check that identification so long as they had first observed a traffic violation. They would simply have to follow the driver until she committed the moving violation that almost all drivers eventually do.[122] None of the restraints on police discretion to target

---

[117]United States v. Watson, 423 U.S. 411 (1976) (probable cause justifies arrest); Whren v. United States, 517 U.S. 808, 810 (1996)("As a general matter, the decision to stop an automobile is reasonable where the police have probable cause to believe that a traffic violation has occurred.")

[118] Illinois v. Lafayette, 402 U.S. 640, 640 (1983) (noting the importance of ascertaining or verifying arrestee's identity); Smith v. United States, 324 F. 2d 879, 882 (routine identification processes are part of custodial arrest).

[119] **cite needed**

[120] Whren, supra note 117 ; Arkansas v. Sullivan, 532 U.S. 769 (2001) (valid traffic stop not rendered unreasonable by officers' subjective aim to search for evidence of crime.). See also David A. Harris, *The Stories, the Statistics, and the Law: Why "Driving While Black" Matters*, 84 Minn. L. Rev. 265, 311-18 (1999).

[121] David A. Harris, *Car Wars: The Fourth Amendment's Death on the Highway*, 66 Geo. Wash. L. Rev. 556, 568 (1998) (The traffic stop gives the officer the opportunity to walk to the driver's side window and . . . request license and registration . . . ").

[122]David A. Harris, *Car Wars: The Fourth Amendment's Death on the Highway*, 66 Geo. Wash. L. Rev. 556, *559-66 (1998) ("Vehicle codes, which exist in every state, contain an almost mind-numbing amount of detailed regulation. There are, of course, the usual "moving violations," such as speeding, failing to obey stop signs, and changing lanes without signaling. But these violations only begin the catalog of possible offenses. There are traffic infractions for almost every conceivable aspect of vehicle operation, from the distance drivers must signal before

individuals on the basis of race or other appearance-based factors that the Supreme Court has imposed with checkpoints apply in this context.[123] The history of traffic enforcement against minority motorists proves that law enforcement officers are perfectly willing to take advantage of this opportunity.[124]

Traffic stops therefore present a powerful and dangerous tool for any national identity system. Powerful because with enough law enforcement desire and effort, virtually any driver could be made to stop and present an identity card; dangerous because of the unlimited official discretion this practice allows. In the context of a national identity system, *Whren* opened more of a Pandora's Box than the Court knew. For this reason, statutory restraint on the use of traffic stops as a means of identity checking should be considered as part of any national identity scheme, though it must be acknowledged that such limitations would be difficult to define and enforce.[125] There are, of course, legitimate reasons to stop people for traffic violations. How

---

turning, to the times of day and weather conditions that require drivers to turn on their lights.") are not even clearly defined, giving officers the discretion to stop drivers who are operating vehicles in ways and under conditions that are not "reasonable and prudent." And if regulation of driving is pervasive, legal requirements concerning vehicle equipment may be even more so. For example, state traffic codes mandate the kind of lights each vehicle must have and the distance from which these lights must be visible, the types of license plates and regulatory stickers vehicles must carry, how loud an exhaust system may be, and even how deep the tread on a car's tires must be. The upshot of all this regulation is that even the most cautious driver would find it virtually impossible to drive for even a short distance without violating some traffic law. A police officer willing to follow any driver for a few blocks would therefore always have probable cause to make a stop under Whren."). See also, David A. Harris, *""Driving While Black" and All Other Traffic Offenses: The Supreme Court and Pretextual Traffic Stops*, 87 J. OF CRIM. L. & CRIMINOLOGY 544, 557-58 (1997).

[123] See TAN infra. For this reason David Moran has contended that "Atwater and Sullivan effectively rendered irrelevant the Court's other major vehicle search case from the 2000-2001 Term, City of Indianapolis v. Edmond, in which the Court held that the police could not set up roadblocks for the primary purpose of catching motorists transporting narcotics. If an officer may stop any car she observes committing any traffic or equipment violation, arrest the motorist and search the car, there is no need to set up roadblocks. Indeed, it would obviously be much more efficient and productive for the police to single out "suspicious" motorists, stop and arrest them for trivial violations . . . . .") David A. Moran, *The New Fourth Amendment Vehicle Doctrine: Stop and Search Any Car at Any Time*, 47 Vill. L. Rev. 815, 832 (2002).

[124] Harris, Stories, Statistics, etc.

[125] Cf., U.S. Department of Justice, Fact Sheet: Racial Profiling, supra note 70 ("[T]he officer may not use race or ethnicity as a factor in deciding which motorists to pull over."); but see id. at 5-6. (race and ethnicity may be used in terrorist identification to the extent permitted by the nation's law and the constitution).

could police be dissuaded from doing so for the "wrong" reasons? It would be possible, for example, to bar identity card demands during traffic stops for certain minor infractions. This would result in some missed connections to valuable data, but it might be necessary in order to discourage stops made for the primary purpose of identity checks. Official inducement to stop vehicles for minor offenses in order to demand national identity cards is one major disadvantage of an identity system.

D. Checkpoints

Checkpoints entail the stopping all persons or vehicles (or a pre-designated subset) passing a particular location. They are a potentially important method of identity determination for any national identity system, both because they could reach large numbers of people and because they could be placed at or around sensitive locations. From an efficiency standpoint they do not rest on the voluntary compliance of consensual encounters; nor do they depend upon the reasonable suspicion of illegal behavior required for investigative stops. Checkpoints, in short, are both compulsory and total in their potential coverage. Roadblock-type checkpoints have already been employed for immigration enforcement, sobriety checking, drug interdiction, and other national security and law enforcement objectives, and there is therefore a fairly substantial body of case law on their legality under the Fourth Amendment. If a national identity system did employ checkpoints, they would likely be applied to pedestrians as well, a use not yet addressed by the Supreme Court.

1. Program Purpose

Forcing people, in vehicles or on foot, to stop at checkpoints constitutes a seizure under the Fourth Amendment.[126] The question then becomes under what circumstances such suspicionless seizures are reasonable. In answering that question the Supreme Court has distinguished between checkpoints whose primary purpose is to "detect evidence of ordinary criminal wrongdoing" and those that serve some "special need" other than the general interest in crime control.[127] The case creating this distinction, *Edmond v. City of Indianapolis*, held that a checkpoint whose primary purpose was to apprehend persons carrying illegal drugs fell in the former category.[128] Any checkpoint whose primary purpose is to "advance the general interest in crime control" violates the Fourth Amendment's ban on seizing people without some individualized indication of criminality and is *per se* unreasonable.[129] On the other hand, checkpoints "aimed primarily at purposes beyond the general interest in crime control"[130] can be permissible under the Fourth Amendment and are evaluated for reasonableness on the basis of a three-pronged test discussed below.[131] Using this test, the Supreme Court has upheld immigration and sobriety checkpoints, and in dicta has indicated approval of roadblock-type stops for highway license and registration checks,[132] at government buildings or airports,[133] or to "thwart an imminent terrorist attack or to catch a dangerous criminal who is likely to flee by way of a particular route."[134]

---

[126] Martinez-Fuerte v. United States, 428 U.S. 543, 556 (1976); Michigan Dept. of State Police v. Sitz, 496 U.S. 444, 450 (1990); City of Indianapolis v. Edmond, 531 U.S. 32, 40 (2000).
[127] *Edmond*, supra note 126, at 37-8, 41. See also Ferguson v. City of Charleston, 532 U.S.67 (2001).
[128] *Edmond*, supra note 126.
[129] Id. at 44, n. 1.
[130] Id. at 48.
[131] TAN infra.
[132] Prouse, supra note 82 , at 663.
[133] Edmond supra note 126, at 48-49.
[134] Edmond supra note 126, at 49. See also Lidster v. Illinois, -- U.S. – (May 5, 2003) (granting certiorari on a case involving an "informational" roadblock being used to distribute flyers and look for witnesses to a hit and run accident in that area exactly a week before).

Whether national identity system checkpoints would have as their primary purpose the "detect[ion of] evidence of ordinary criminal wrongdoing," would depend, of course, on the origins and contours of the program, but it seems unlikely that general crime detection would be the primary purpose of such a system. Given the deep-seated national reluctance to adopt a national identity card, it would probably not be put into use unless there was a substantial threat to national security, possibly in the form of more terrorist attacks. If so, the purpose would be the prevention of further attacks. While such attacks would obviously be serious crimes, the fact that the harm is also the subject of the criminal law would not necessarily keep these checkpoints from serving a predominantly "non-criminal" purpose. The immigration checkpoints in *Martinez-Fuerte* and the drunk driving roadblocks in *Sitz* sought to prevent harms (the presence of undocumented aliens and inebriated drivers) that are also the object of criminal penalties.[135]

On the other hand, it could be argued that "terrorism" encompasses a variety of crimes, and indeed is just crime with a particular motivation and/or target.[136] Anti-terrorism checkpoints would stretch the rationale of "special needs"/"non-criminal purpose" searches to its limit, if not beyond. It is likely, however, that courts would find anti-terrorism checkpoints to be distinguishable from general crime fighting, particularly in the face of the enormous public pressures that would probably lie behind their creation.[137] Lower courts that have considered the permissibility of checkpoints on open military bases in the wake of *Edmond* have distinguished

---

[135] Cite dissent in Edmond.

[136] On the varying definitions of terrorism see e.g. James A.R. Nafziger, *The Grave New World of Terrorism: A Lawyer's View*, 31 DENVER J. OF INT'L. L. AND POLICY 1, 8-10 (2003).

[137] Indeed, if the Supreme Court found itself unable to classify prevention of terrorism as a "special need," it would, I suspect, abandon *Edmond* (a 5-4 decision) before it would strike down suspicionless identity checks under a legislatively established national identity system.

national security protection from society's general interest in crime control, and have upheld the practice.[138]

Congress could virtually insulate identity checkpoints from an *Edmond* challenge by making immigration enforcement a major, if not primary, purpose. Emphasizing the importance of border control, the prevalence of illegal alien presence in the U.S., and the difficulty of interdicting those from Mexico, the Supreme Court in *Martinez-Fuerte* upheld a challenge to vehicle roadblocks, each located approximately 65 miles from the Mexican border, in California and Texas.[139] The *Edmond* Court was careful to distinguish and preserve *Martinez-Fuerte*, invoking again the special need to police the border.[140] Checkpoints under a national identity system would likely be distributed around the country and not necessarily be located within a short drive of an international border as in *Martinez-Fuerte*.[141] They would, in all likelihood, be designed to identify not only illegal border crossers from Mexico but any noncitizens unlawfully present in the U.S.[142] A broader-gauged immigration focus would not, however, convert their purpose to one of general law enforcement. In short, checkpoints whose principal purpose is the identification and apprehension of noncitizens illegally present in the U.S. would certainly fall outside of *Edmond's* limited ban on suspicionless checkpoint seizures.

2. Reasonableness Determination

---

[138] United States v. Green, 293 F. 3d 855, 859 (5th Cir. 2002); United States v. Hawkins, 249 F. 3d 867, 873 (9th Cir. 2001).

[139] *Martinez-Fuerte*, supra note 126, at 545-50.

[140] *Edmond*, supra note 126, at 38-40, 47.

[141] A national identity system that relied on identification checkpoints might also differ from the *Martinez-Fuerte* roadblocks by their use with pedestrian as well as vehicle traffic. This difference would not seem to have any bearing on whether the checkpoint was for general criminal enforcement rather than for immigration control, however, though it might affect the balancing used to determine their legality. See TAN infra.

[142] See TAN infra for a description of the nature of the problem and the need for checkpoints as a means to combat it.

For checkpoints whose primary purpose is not general law enforcement, the Supreme Court determines reasonableness (and thus compliance with the Fourth Amendment) using a three-pronged balancing test. The Court balances 1) the government's interest in preventing the relevant harm, 2) the extent to which the checkpoint system can be said to advance that interest, and 3) the degree of intrusion on those persons who are stopped.[143] The following subsections discuss how this balance might apply to checkpoints employed in a national identity system.

a. Interest in Prevention

In assessing the degree of the problem it addressed, much would turn on the circumstances behind national identity checkpoints and the aims they were designed to achieve. It is hard to imagine, for example, that prevention of identity theft or election fraud, or the need to assure that government benefits are delivered correctly, would count as substantial government interests for widespread identity checkpoints. On the other hand, as indicated above, a national identity system directed at a real and present danger of terrorist attacks or the illegal presence of millions of noncitizens would almost certainly suffice. In *Sitz* the Court measured the magnitude of the drunk driving problem by its annual death and personal injury toll and amount of property damage.[144] In the period after September 11th there would have been no question about the scope and seriousness of the threat of domestic attack. The absence of additional attacks thus far would probably not lower significantly the governmental interest, though, particularly in light of the subsequent apprehension and conviction of several people for

[143] *Sitz*, supra note 126, at 455. See also, *Martinez-Fuerte*, supra note 126, at 555. **Brown v. Texas?**
[144] Sitz, supra note 126, at 451 (citing 25,000 deaths, one million personal injuries, and five billion dollars in property damage per year).

supporting or planning terrorist activity, as well as the elevated threat levels during the past two years.[145]

As for immigration enforcement, what the Court said in 1976 *Martinez-Fuerte* is still true: despite (or perhaps because of) the national policy to limit immigration, "large numbers of aliens seek illegally to enter or to remain in the U.S." [146] What is different now is that a much smaller percentage of undocumented migrants than *Martinez-Fuerte's* estimate of 85% is from Mexico.[147] Also, comparatively more undocumented migrants are now likely to be people who overstayed their visas than people who entered the country surreptitiously.[148] These people can be anywhere in the country, pointing toward a greater necessity of enforcement activity in the nation's interior.

Unlawful alien presence is not an unmitigated harm, and the costs and benefits are subject to vigorous debate.[149] The undocumented population was assumed to be a serious national problem in *Martinez-Fuerte*, however, and Congress would be entitled to find it to be so if it created an immigration-focused national identity system.[150] Moreover, to the extent that a

---

[145] **Need data on DHS threat levels since they began.** . Ellmann, supra note 70, at 683 ("[P]reventing terrorism presents an *especially* compelling interest. . . . Terrorism is a danger to huge numbers of people, and perhaps to the nation itself, in a way that each individual crime of violence can hardly ever be." (emphasis in original).

[146] *Martinez-Fuerte*, supra note 126, at 551. The Court mentioned a possible 10-12 million aliens illegally in the country. Id.

[147] See Eduardo Porter, Illegal Immigrants May Total 8.5 Million, Wall St. J. August 14, 2001 at A4 (estimating that 4.5 million of 8.5 million undocumented migrants, or 53%, are from Mexico) cited in STEPHEN H. LEGOMSKY, IMMIGRATION AND REFUGEE LAW AND POLICY 1112 (3d ed. 2002). Over 80% of undocumented immigrants are from the Western Hemisphere, however. T. ALEXANDER ALEINIKOFF ET AL, IMMIGRATION AND CITIZENSHIP 601 (4TH ed. 1998).

[148] About 41 per cent of the total undocumented population in 1996 were "overstays" who entered legally on temporary visas but failed to leave. Aleinikoff, supra note 148, at 601, and the percentage seems to be increasing. See James A.R. Nafziger, *The Grave New World of Terrorism: A Lawyer's View*, 31 DENVER J. OF INT'L. L. AND POLICY 1, 6 (2002) ("For many foreign visitors, visa overstaying has become the immigration procedure of choice.")

[149] For a discussion of the several ways of measuring the impact, and summaries of and some selection from the vast literature on the subject, see Aleinikoff et al., supra note 147, at 610-20; Legomsky, supra note 147, at 1111-13. For a more anecdotal account, see ERIC SCHLOSSER, REEFER MADNESS: SEX, DRUGS, AND CHEAP LABOR IN THE AMERICAN BLACK MARKET 75-108 (2003) (describing costs and benefits of undocumented agricultural labor).

[150] This is particularly so because of Congress' traditional plenary power over immigration. *See e.g.* Harisiades v. Shaughnessy, 342 U.S. 580, 588-89 (1952). To what extent this doctrine still exists, and its extent is the subject of

terrorism threat comes from persons who are not U.S. citizens, especially those here without permission, the governmental interests in preventing terrorist attack and illegal migration reinforce each other.[151] All of this suggests that the nature of the immigration problem may have changed in the twenty-five years since Martinez-Fuerte, but its severity has not diminished and may actually have increased.

b. Effectiveness

The second factor in the balance, the extent to which checkpoints advance the identified interest, also depends on the problem or problems the checkpoints are designed to address. Let us assume that these are prevention of terrorist attack and mitigation of illegal alien presence, or some combination of the two. Checkpoint effectiveness can be measured in several different ways: 1) the *absolute number* of suspects apprehended, 2) the *rate* of apprehensions (the number of suspects divided by the number of individuals stopped); or 3) *relative effectiveness* compared to other methods of prevention and enforcement. The Supreme Court has considered all three outcomes in evaluating checkpoints, though not in any systematic way. The following discussion applies these measures to hypothetical immigration and anti-terrorism identification checkpoints.

As noted above, the country and the Court already have substantial experience with immigration checkpoints in the form of roadblocks on major highways leading from the border. The San Clemente checkpoint, located 66 miles north of the Mexican border on Interstate 5, the

---

long-standing debate. *See e.g.* Peter J. Spiro, *Explaining the End of Plenary Power*, 16 GEO. IMM. L.J. 339 (2002); T. Alexander Aleinikoff, *Detaining Plenary Power: The Meaning and Impact of Zadvydas v. Davis*, 16 GEO. IMM. L.J. 362 (2002). Whatever its contours, a deference to Congressional conclusion that unlawful immigration was a serious problem would seem to be an unexceptionably mild use of the doctrine.

[151] On the pros and cons of using immigration enforcement as a weapon against terrorism, see e.g. Victor C. Romero, *Decoupling "Terrorist" from "Immigrant": An Enhanced Role for the Federal Courts Post 9/11,* 7 J. Gender Race & Just. 201,202-06 (2003).

principal highway between San Diego and Los Angeles, resulted in the apprehension of 17, 000 undocumented aliens in 1973.[152] In fiscal year 2000, the San Clemente and Temecula checkpoints in California produced slightly less than 10,000 arrests.[153] In absolute terms, then, highway checkpoints can be quite effective, at least when they straddle a well-traveled Interstate in the vicinity of the border.

Of greater concern, however, is that the San Clemente checkpoint relied on referring some motorists for a "secondary inspection" of three to five minutes, at which they would be questioned about their citizenship or immigration status. These referrals, the Court assumed, "are made largely on the basis of apparent Mexican ancestry."[154] It is hard to see how secondary referrals would work outside of the factual context of the Mexican border. Could other ethnic groups be pulled aside for secondary inspection on the basis of their "apparent [fill in] ancestry"? Putting aside the indignity of this of ethnic targeting,[155] it is wildly inefficient. Under a national identity system, however, presumably, *every* person would have to present a national identity card to verify lawful presence in the U.S. Longer detention and more thorough questioning would be necessary only for those who lacked proof of citizenship or lawful presence. This form of "secondary" inspection eliminates the discretionary and profiling aspects of past checkpoints.[156] It does, to some degree however, correspondingly increase the inconvenience

---

[152] Martinez-Fuerte, supra note 126, at 554. The Court's projection of the data for 1974, based on eight days of operation at issue in the case, was 33,000 arrests. Id.

[153] United States Border Patrol San Diego Sector, Press Release (September 13, 2000) (on file with author).

[154] Martinez-Fuerte, supra note 126, at 563. The dissent in Martinez-Fuerte focused most of its ire on this aspect of the immigration roadblocks. ("Every American citizen of Mexican ancestry and every Mexican alien lawfully in this country must know after today's decision that he travels the fixed checkpoint highways at the risk of being subjected not only to a stop, but also to detention and interrogation.") (Brennan, J., dissenting) Id. at 572.

[155] Kevin R. Johnson, *The Case Against Race Profiling in Immigration Enforcement*, 78 WASHINGTON U. L. Q. 675, 726-28 (2000).

[156] Dershowitz, supra note 2, at 203 (national identity card eliminates justification for racial and ethnic profiling). It would be analogous to the requirement that all prospective employees present proof of citizenship or other work authorization, regardless of their appearance, attire, or "native" English speech. INA §274A(a)(1)(B).

for everyone.[157] Moreover, the discretionary aspects of checkpoint placement would, presumably, remain, raising the possibility of placement in ethnically selected target areas.[158]

Measuring as it does *rate of success,* the ratio between the number of persons stopped and the number apprehended is certainly an important factor in the reasonableness balance.[159] Existing checkpoints impact an enormous number of vehicles and the success rate is relatively low. In *Martinez-Fuerte* the Court found that .12% (or 12 of every 10,000) vehicles contained deportable aliens. (In *Sitz* it approved a 1.6% success rate for sobriety checkpoints.[160]) While the Court has upheld immigration enforcement roadblocks with a miniscule rate of success, more general use of checkpoints would probably test even those numerical limits. On the other hand, the Court in *Sitz* explicitly cautioned the judiciary against "a searching examination" of checkpoint effectiveness.[161]

The success rate of a national identity system designed to discover undocumented migrants is integrally tied to the third method of assessing effectiveness: *relative effectiveness* compared to other methods of prevention and enforcement. In other words, are checkpoints effective and necessary compared to available alternatives? The Court accepted roadblocks on major highways leading from the border in *Martinez-Fuerte* partly because "the flow of illegal

---

[157] See TAN infra.
[158] While perhaps legal, this would be profoundly unwise, creating, as it would, apartheid-type enclaves subject to special "border" controls.
[159] Prouse, supra note 82, at 659-60 (striking down random motor vehicle license and registration checks as unreasonable seizures under the Fourth Amendment).
[160] Sitz, supra note 126, at 455 (noting that nationally sobriety checkpoints result in drunk driving arrests of 1% of motorists stopped). But see id. at 461 (0.3% success rate at 125 Maryland checkpoints). The difference between the *Martinez-Fuerte* and *Sitz* balancing test and the *Edmond* primary purpose test is illustrated by the fact that the Indianapolis drug enforcement roadblock's 9% rate of producing arrests for some offense, drug related or not, was irrelevant under the latter approach.
[161] *Sitz*, supra note 126, at 454 (Effectiveness evaluation is "not meant to transfer from politically accountable officials to the courts the decision as to which among reasonable alternative law enforcement techniques should be employed to deal with a serious public danger.") Id. at 453.

aliens cannot be controlled effectively at the border" itself.[162] If roadblocks were more widespread they would probably catch additional undocumented aliens, particularly if they were set up at other restricted access transportation routes or nodes. It is likely, however, that their success rate would be even less than border region checkpoints because of the lower concentration of undocumented aliens away from border areas. In addition, if checkpoints were used with pedestrian traffic, ways to circumvent them would probably be available. The checkpoints could be avoided unless they were mobile enough that the undocumented migrants were taken by surprise or the checkpoints were situated so that there was no way around them. If these speculations are correct, the more widespread checkpoints became, and the more they were used against pedestrians, the lower their success rate is likely to be, though the total numbers of apprehended aliens would go up.

With *relative effectiveness*, too, the Court urges deference to governmental preferences. "[F]or purposes of Fourth Amendment analysis, the choice among . . . reasonable alternatives remains with the governmental officials who have a unique understanding of, and a responsibility for, limited public resources . . . ."[163] Moreover, parties objecting to checkpoints have the burden of proving that "the particular law enforcement needs served by checkpoints could be met without reliance on routine checkpoint stops."[164]

Despite the passage of numerous immigration law amendments designed to discourage illegal entry and presence since 1976, including employer sanctions, expedited removal, new

[162] *Martinez-Fuerte*, supra note 126, at 556. The dissent in Sitz saw this as an important distinction between immigration and sobriety checkpoints.
[163] Sitz, supra note 126, at 453-54.
[164] Martinez-Fuerte, supra note 126, at 557 n. 12.

inadmissibility grounds, restrictions on public benefits, and enhanced border enforcement, [165] the continued presence of millions of undocumented migrants makes it hard to imagine that a court would find checkpoints relatively unnecessary.[166] This is true even though checkpoints are no panacea for illegal immigration. They are as likely to drive the undocumented further underground – off thoroughfares and locations where checkpoints may be placed -- as to greatly increase apprehensions. On the other hand, they may have some deterrent effect, by adding one more burden to illegal presence in the U.S.[167] In sum, an expanded use of checkpoints in conjunction with a national identity card to enforce the immigration laws would seem to pass the "effectiveness" threshold of the current Fourth Amendment balancing test.

To the extent that checkpoints would be employed to identify potential "terrorists" other than undocumented aliens, the various measures of efficacy come out differently. Presumably, checkpoints would be used either to catch individuals already identified as terrorism suspects or to single out previously unknown persons who met some kind of "terrorist" profile.[168] The closest current analogy to the latter method is the CAPPS system used to screen airline

---

[165] See generally, Legomsky supra note 147 at 1109-1117; U.S. COMMISSION ON IMMIGRATION REFORM, U.S. IMMIGRATION POLICY: RESTORING CREDIBILITY 9-179 (1994)

[166] In Martinez-Fuerte, supra note 126 at 556-57 the Court held "maintenance of a traffic-checking program in the interior is necessary because the flow of illegal aliens cannot be controlled effectively at the border." Indeed, dissenting in Sitz, supra 126 at 475 , Justice Stevens differentiated immigration from sobriety roadblocks on the ground that the former produce "thousands of otherwise impossible arrests."

[167] Surprisingly, in upholding checkpoints, Supreme Court majorities have not chosen to rely on their deterrent effect, which, while not measurable statistically, should exist to some degree. The dissent in Sitz, supra note 126, at 470-71 does speak approvingly of the possibility that sobriety checkpoints might deter drunk driving, while noting the absence of data on the issue. ("There is, obviously, nothing wrong with a law enforcement technique that reduces crime by pure deterrence without punishing anybody; on the contrary, such an approach is highly commendable.") For an example of an immigration enforcement effort that caused some undocumented immigrants to depart the U.S. on their own, see e.g., Susan Sachs, *U.S. Crackdown Sets Off an Unusual Rush to Canada*, N.Y. TIMES Feb. 25, 2003, at A1 (Pakistanis unlawfully in U.S. flee to Canada rather than undergo special registration).

[168] The latter effort is designed to address the problem that potential terrorists "have no visible markers." David Cole *Enemy Aliens*, 54 STANFORD L. REV. 953, 985 (2002)

passengers.[169] What effects would flow if checkpoints similar to those used at airports were installed in other public spaces?

Preventing terrorism is certainly a powerful national goal,[170] but it seems likely that the absolute number of suspects apprehended through extensive identification checkpoints would be very small and the success rate would be miniscule.[171] To begin with, the number of terrorism suspects seems to be tiny, and the group of those who are not also in the U.S. illegally is even smaller. Moreover, given what a crude instrument terrorist "profiling" is, the likelihood of mistaken "hits" is substantial. Indeed, though statistics are not available, anecdotal reports suggest that false positives – the singling out of innocent travelers -- occur fairly regularly under the present version of CAPPS[172] and are a concern in the design of CAPPS II.[173] In short, the rate of success would be relatively low and the rate of error relatively high.

In theory at least, the more information available to terrorist profiling software like CAPPS, the greater the chances for accurate prediction. This produces the paradox that the more intrusive the data collection and search, the greater its effectiveness is likely to be.[174] Thus, from the point of view of efficacy, tying a national identity card to as many databases as possible is a good thing. Obviously, however, this encourages the collection and storage of more and more

---

[169] See TAN infra.
[170] See TAN supra.
[171] See Ellmann, supra note 70, at 699-700, n. 65-70 for an attempt to estimate the number of Al Qaeda terrorist within the United States and the relative hit rate of a program that tried to profile them. Recognizing that we "simply do not know what the true number [of such terrorists] is" and that no profile is completely accurate, he assumes that a hit rate of even 1 in 10,000 would be a "plausible basis for action." Id. at n. 65-66. He also notes that a profiling program's effect in deterring attacks adds to the measure of its usefulness. Id. at n. 63. On profiling's effectiveness in general, see DAVID A. HARRIS, PROFILES IN INJUSTICE: WHY RACIAL PROFILING CANNOT WORK (2002).
[172] See TAN infra.
[173] See Wald, supra note 46 ("The goal of CAPPS II, the department says, is to 'significantly reduce the number of passengers who are misidentified as potential threats to passenger of airline security . . . .'").
[174] Hence the controversy over the number and kinds of data sources that CAPPS II will tap into and the use that will be made of them. See Wald, supra note 46 (reporting a reduction in both the scope of information collected on air travelers and on the use of credit and medical records).

personal data and the linking of identity cards to greater numbers of databases, leading to a greater potential impact on privacy.

With respect to the usefulness of other alternatives, much depends on the circumstances that would prompt widespread use of identification checkpoints. Since September 11th the federal government has enacted and assumed a wide range of powers to protect domestic security. The best known is the USA PATRIOT Act of 2001,[175] but there are a host of others, including the creation of special military tribunals and the indefinite detention of "unlawful combatants."[176] It is hard to know just how effective they have been, both because the government releases scant information about its anti-terrorism activities,[177] and because no one really knows the extent of the threat. In light of the deference given by the Court to the political choice of crime prevention methods, and the additional deference accorded the government in protecting national security in and preventing terrorism,[178] if checkpoints were deployed in the wake of another domestic attack it seems highly unlikely the judiciary would find other alternatives to be so effective as to render checkpoints constitutionally unnecessary.

---

[175] United and Strengthening American By Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

[176] See e.g., STEPHEN J. SCHULHOFER, THE ENEMY WITHIN (2002) (passim) (summarizing steps taken to identify and apprehend terrorists within the U.S.); Sean D. Murphy, *Terrorist Attacks on World Trade Center and Pentagon,* 96 A.J. INT'L L 237, 238-43 (2002); Andrew E. Taslitz, *Terrorism and the Citizenry's Safety,* 17 CRIMINAL JUSTICE 4, 4-5 (2002); **Padilla**

[177] Amy Goldstein, *Fierce Fight Over Secrecy, Scope of Law,* WASH. POST at A1 (September 8, 2003) (Patriot Act bans disclosures about its use, and there is little information publicly available about its effectiveness.)

[178] See e.g.,Zadvydas v. Davis, 533 U.S. 678, 696 (2001)(referring to the "heightened deference to the judgments of the political branches with respect to matters of national security."); Center for National Security Studies, v. U.S. Dept. of Justice, 331 F. 3d 918, *27 (D.C. Cir. 2003) (upholding Dept. of Justice refusal to release the names of persons detained in the wake of September 11 attacks and granting deference to governmental assessment of impact on national security) ("American faces an enemy just as real as its former Cold War foes, with capabilities beyond the capacity of the judiciary to explore."); Samuel Issacharoff & Pildes, *Between Civil Libertarianism and Executive Unilateralism: An Institutional Process Approach to Rights During Wartime,* **[publication] [page]** ("Times of heightened risk to the physical safety of their citizens inevitably cause democracies to recalibrate their institutions and processes, and to re-interpret existing legal norms, with greater emphasis on security, and less on individual liberty, than in "normal" times.) **[page 1]** (noting that "[i]n terms of actually defining first-order claims of rights, American courts show great reticence to engage the permissible scope of liberties in direct, first-order terms" but rarely endorse the position that the executive can make these deviations unilaterally.). **[pages 7,5]**

c. Degree of Intrusion

The third factor in the Supreme Court's assessment of roadblocks has been the degree of intrusion experienced by stopped motorists. The Court speaks in terms of "objective" and "subjective" intrusions, with "objective" referring to physical interference with movement and "subjective" referring to concern or fright caused to those stopped by the roadblock.[179] In the cases involving immigration and sobriety checkpoints, the Court found neither form of intrusion particularly weighty.

The "objective" intrusion obviously depends on how a checkpoint is operated. Hypothetical checkpoints under a national identity system would most likely involve stopping each motorist or pedestrian, a demand for presentation of her identity card, and a "swipe" of the card through a reader linked with computerized records.[180] The individual effectively would be detained both while this occurred as well as pending the electronic reply from the database. If this sequence of events took no longer than an ordinary credit card authorization, it is doubtful the Court would find the objective intrusion to differ significantly from that of immigration or sobriety checkpoints, which the Court has characterized as "quite limited"[181] and "slight."[182] A "positive" response to the identity check, in the form of an outstanding warrant, an indication of unlawful presence in the U.S., or some other adequate ground, can justify further detention, but

[179] Sitz, supra note 126, at 451-53; Martinez-Fuerte, supra note 126, at 558-59.
[180] See TAN infra.
[181] Martinez-Fuerte, supra note 126, at 557-58 ("The stop does intrude to a limited extent on motorists' right to 'free passage without interruption, and arguably on their right to personal security. But it involves only a brief detention of travelers during which all that is required of the vehicle's occupants is a response to a brief question or two and possibly the production of a document evidencing a right to be in the U.S.") (internal quotations and citations omitted)
[182] Sitz, supra note 126, at 451).

that additional seizure must have its own independent basis.[183] In fact, the use of terrorist profiling raises separate Fourth Amendment issues of how much indication of "terrorist" potential, as revealed at the identification checkpoint, would be necessary to justify taking measures against a person, be it delayed or denied air travel, additional questioning or search, or even arrest. [184]

Even for stops that do not result in a "hit", circumstances could easily cause people to be detained or delayed to an extent that would weigh heavily against the practice. The average delay occasioned by the sobriety checkpoints in *Sitz* was approximately 25 seconds,[185] but checkpoints requiring an individual to remove an identity card from her pocket or purse, to have it read, and then to await clearance would probably take considerably longer. This would be particularly true if the database scan took some length of time. Moreover, anyone who has passed through airport security since September 11 knows that checkpoints can produce long waiting lines, interfering significantly with free passage. Any of these entirely likely possibilities would significantly increase the objective intrusion and distinguish identity checkpoints from those upheld by the Supreme Court so far.

The "subjective" intrusion, however, can be seen as greater than that of current immigration and sobriety checkpoints. In one way an identification checkpoint would be less intimidating, because the checking would be limited to asking for a clearly designated piece of identification. This is much less open-ended than looking for signs of intoxication, for example,

---

[183] See TAN supra (secondary inspections); Whren v. U.S. . ; Cf. Bob Herbert, *Jailing Immigrants,*, N.Y. TIMES, August 4, 2003, at A17 (describing the lawful, if unnecessary, detention of an alien after a computer check following a traffic stop revealed his undocumented status).

[184] Unless the law of search and arrest is going to be drastically revamped for terrorism suspects, the answers would seem to be the usual measures of reasonable suspicion for investigative stops and probable cause for extended detention, **Dunaway**, **Sokolow** search. Treating persons identified by a terrorism profile as unlawful combatants would obviously negate some of these rules**. Padilla**

[185] Id. at 448.

at sobriety checkpoints. Fear of facing unknown questions on unknown topics would thereby be reduced (assuming the officers stationed at the checkpoints restricted themselves to inspecting identification). Although the Court has yet to consider pedestrian checkpoints, it seems unlikely that it would find them more invasive than vehicle checkpoints as a general matter.[186] In fact, being forced to stop while on foot is in some ways less startling, and certainly less dangerous, than approaching a roadblock by car.[187]

Being checked against a database is probably much more frightening, though, than the checkpoint screening in *Martinez-Fuerte* or *Sitz* – even for an innocent person.[188] The individual has no way of knowing the contents of the database against which her identification is being run, whether they are accurate or not, or what further impositions might be triggered by the information. This uncertainty will turn every identification demand into cause for apprehension.

The purpose of the checkpoint matters less perhaps, in terms of "fear and surprise" than whether the checkpoint is anticipated or not. Clearly there will more fright for even an innocent traveler[189] on encountering an unexpected demand to show identification than from a permanent checkpoint akin to an airport security gate.[190] The Court upheld, however, even temporary checkpoints in *Sitz*. Nevertheless, this distinction is not meaningless, and checkpoints at permanent, known locations do carry less of a subjective impact.

---

[186] At one point in *Martinez-Fuerte*, the Court adverted to the general principle of lesser expectation of privacy in automobiles, ___ U.S. at _)__, but in context of the entire case the holding does not seem to turn on this factor.
[187] On the other hand, the individual lacks the "protective shell" of her automobile.
[188] Normally the Supreme Court only accounts for the reaction of a reasonable *innocent* person when determining Fourth Amendment issues. See e.g. Florida v. Bosticle, 501 US at 438. Arnold H. Loewy, *The Fourth Amendment as a Device for Protecting the Innocent*, 81 MICH, L. REV. 1229 (1983).
[189] "Fear and surprise" relate to the "innocent" traveler, and not the trepidation produced in a person who fears legitimate apprehension at the checkpoint. Sitz, supra note 126, at 451-52.
[190] Sitz, supra note 126, at 463 ("A driver who discovers an unexpected checkpoint on a familiar local road will be startled and distressed.") (dissent of Stevens, J).

Identification checkpoints, it may be argued, have an additional subjective effect, on a grand scale: the psychic harm to a free people of having to "show your papers," even if only at certain designated locations.[191] Not only would people forced to go through identity checkpoints experience some degree of fear and surprise, but, knowing that this has become a permanent part of the social fabric, their sense of liberty would be diminished.[192] This feeling is not mitigated – indeed, it may be enhanced – by the knowledge that other people are also being stopped and asked for identification.[193] Supreme Court majorities have not yet taken this subjective effect into account, and may never, but it is certainly real even if it cannot be measured quantitatively.

Finally, the degree of intrusion must be considered in light of its frequency. In its evaluation of the burden imposed by highway roadblocks, the Court has tended to describe and consider the interference with *one individual's* freedom. The more relevant fact in passing on the reasonableness of a methodology that depends on stopping everyone, however, is the *collective* burden.[194] This imposition is a function of the intrusiveness of each individual stop multiplied by the number of stops the system will entail. Looked at this way – admittedly, an approach the majority of the Court has avoided – national identity card checkpoints carry a very high cost. If a national identity system were to involve checkpoints at all, it is likely to require

---

[191] See e.g., Edmond v. Goldsmith, 183 F. 3d 659, 662 (7th Cir. 1999) (referring to checkpoints as "methods of policing associated with totalitarian nations") (Posner, J.).

[192] Cf. Andrew E. Taslitz, *The Fourth Amendment in the Twenty-First Century: Technology, Privacy, and Human Emotions*, 65 Law & Contemp. Probs. 125, 131 (Spring 2002) (arguing for an "affective" definition of privacy that takes into account peoples' emotional reactions to surveillance).

[193] Compare United States v. Ortiz, 422 U.S. 891, 895 ("At traffic checkpoints the motorist can see that other vehicles are being stopped, he can see visible signs of the officers' authority, and he is much less likely to be frightened or annoyed by the intrusion."), cited in Martinez-Fuerte, supra note 126, at 558.

[194] The dissents in Martinez-Fuerte and Sitz did pay some attention to the *collective* effects of highway roadblocks. See Martinez-Fuerte, supra note 126, at 571 ("[C]heckpoints . . . detain thousands of motorists, a dragnet-like procedure offensive to the sensibilities of free citizens.) (Brennan, J., dissenting); Sitz, supra note 126, at 472 (describing sobriety checkpoints as "a program that produces only a handful of arrests which would be more easily obtained without resort to suspicionless seizures of hundreds of innocent citizens.") (Stevens, J., dissenting). Cf. Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 367 (1974) (contrasting the "atomistic" view of the Fourth Amendment as a protection for isolated individuals with a conception of the Fourth Amendment as a regulator of governmental conduct as a whole).

lots of them. Otherwise, there is little point in having them; the few that did exist could be easily circumvented. Thousands upon thousands of people would experience recurring delays and some degree of distress in connection with the number of checkpoints likely in any national identity system that used them.

d. Striking the Balance

Ubiquitous or even common demands for identity cards at stationary checkpoints would change the nature of American life, and judicial determination of their constitutionality would be a momentous event. All aspects of the three-part equation for assessment of their reasonableness under the Fourth Amendment depend in great part on the checkpoints' purpose, how they are structured, and the conditions that produced them. For that reason, it is impossible to given any definitive answer in the abstract to the question of identity checkpoints' constitutionality. The fact-laden nature of the constitutional analysis, however, may run up against judicial reluctance to second-guess political choice in times of national danger. This seems particularly true for measures receiving both executive and legislative endorsement, [195] as would almost certainly be the case for any comprehensive national identity system.

That said, some tentative conclusions about national identity system checkpoints are possible. First, those aimed mainly at undocumented aliens would seem to have a good chance of being upheld, principally because of the seriousness of the problem and the nation's inability to solve it despite decades of legislative and enforcement efforts. To the extent that potential terrorists lurk among the undocumented, there is an additional justification. It seems likely, too, that such identity checkpoints would have a reasonable rate of success, at least initially, as measured by the Court's undemanding standard. Unlike "terrorism" checkpoints, those that

[195] Issacharoff & Pildes, supra note 191.

focused on immigration offenders would be less likely to have "false positive" results (identifying U.S. citizens or lawful aliens as unlawful aliens), and would thereby keep unfounded seizures resulting from identity checks to a minimum.[196]

This assumes that immigration checkpoints would require identity cards of all persons passing through, not just those who "look" or "sound" foreign.[197] The absence of police discretion in who is exposed to an initial stop, particularly in contrast to roving patrols, [198] was an important reason the Court upheld the checkpoints in *Martinez-Fuerte*.[199] In that case, though, the Court did approve two other forms of official discretion: the choice of checkpoint locations[200] and the referral for secondary inspection of persons of "apparent Mexican ancestry."[201] As noted above, the use of a national identity card at immigration-focused checkpoints eliminates the second type of discretion. Freedom to choose checkpoint location would remain, however, and make possible troubling ethnic selection. In theory checkpoints designed to catch illegal immigrants from Mexico, for example, could then be put in and around Mexican neighborhoods, or those aimed at "terrorists" from the Middle East placed near Arab population centers. Establishing, as they would, ethnic enclaves subject to border control, such decisions would be profoundly unwise, even if legal.

---

[196] At first glance this, might seem like another example of what David Cole has described as a "sacrifice of the liberties of noncitizens in furtherance of the citizenry's purported security." David Cole *Enemy Aliens*, supra note 168, at 957 (2002). Even if imposed principally to apprehend undocumented aliens, though, checkpoints would impact all people equally. In that sense they do not involve profiling or targeting of noncitizens. Immigration focused checkpoints would be a law enforcement technique aimed at enforcing a body of law that affects only those who could not prove lawful presence.

[197] The absurdity of the latter category is illustrated by the fact that it would include two 2003 candidates for California's governorship.

[198] Compare Prouse, supra note 82 and Brignoni, supra note .

[199] Martinez-Fuerte, supra note 126, at 558-59 (**insert quote)**

[200] Id. at 559.

[201] See note supra.

Apart from immigration enforcement, checkpoints directed at catching potential terrorists would, and should, mainly fail to pass muster under the Fourth Amendment. Huge numbers of people would need to be stopped in the hopes of locating a very small collection of previously identified individuals. The profiling of potential terrorists is at a very rudimentary stage, and its coupling with identification checkpoints would in all likelihood yield a low rate of success and a large number of wrongful investigative detentions. Despite the obvious importance of preventing further domestic attacks, these likely results should stand in the way of finding such general anti-terrorism identity card checkpoints to be reasonable seizures under the Fourth Amendment. The outcome would probably be different, however, at especially sensitive locations like airports, monuments, public buildings, or so-called national special security events.[202]

E. Summary:

Existing Fourth Amendment law, then, would allow a fair amount of identity checking, but forbid certain important techniques. Nothing in the Fourth Amendment bars official requests for identification from any person at any time, as long as the person is not "seized" in the process. This means that people could be required to present identification whenever they are already stopped, as for example at registration procedures, and could be asked, but not compelled, to present identification at other times under the so-called "consensual encounter" doctrine. These two kinds of interactions alone would encompass a fairly large amount of identity checking. In addition, when grounds to stop an individual already existed, as for

---

[202] When an event is designated a National Special Security Event, the Secret Service becomes the lead agency for the design and implementation of the operational security plan. http://www.secretservice.gov/nsse.shtml. In 2002 these included the Winter Olympics, Super Bowl, World Economic Forum, and State of the Union Address. http://www.dhs.gov/dhspublic/display?theme=30&content=55. See also, Florida v. J.L., 529 U.S. 266, (2000) (Fourth Amendment expectations of privacy diminished in certain places, including airports). **check Lafave on the law in this area.**

example, in the relatively unusual instances when there was probable cause or reasonable suspicion of criminality, under Court precedent there is no Fourth Amendment objection to official demands for the person's identity card. In fact, the requirement that people carry an identity card would be useful in the investigation of those stopped on suspicion and in the processing of arrestees. There is a real danger, however, that the desire to run an identity check would add one more temptation for police to perform traffic stops for ulterior purposes.

On the other hand, the Fourth Amendment does not allow random, suspicionless identity checks. To that extent the specter of law enforcement officers asking for "your papers, please" on an individual discretionary basis is barred by the constitution. Moreover, identity checkpoints could not be established willy-nilly. They would, though, probably be constitutionally reasonable for certain purposes in certain circumstances. If the Supreme Court follows its own roadblock precedents in an intellectually honest way, the outcome will very much depend on the scope of the problem checkpoints are designed to address, their effectiveness in doing so, and the degree of interference with free movement they entail. On these factors, general checkpoints (outside of sensitive locations) designed to "profile terrorists" should probably be found to be unreasonable.

IV. DATA GENERATION, COLECTION, AND RETENTI ON

At the same time the checking of identity cards taps into existing databases, it can also generate new data by inputting the location and activity of the person whose identification token is being read. For example, everyone is now required to present an identity card or other token while checking in for a flight. In addition to indicating whether that person was a flight risk (or perhaps an undocumented alien or wanted criminal), the same readable token could easily create new data, such as the location, time and date the token was read, and even the flight and itinerary. The database would now contain information about the person's location and activities

it did not previously have. This information could be used not only in subsequent identity checks but also potentially for more general law enforcement or other purposes.[203]

Clearly, the compelled collection of this data would impact personal privacy and what might be called the right of anonymity.[204] People would know that the government has information about their movements and activities, some of a private or even intimate nature. They might change their behavior, not for fear of being caught doing something illegal, but because they were reluctant to contribute to a permanent, government-held record of their actions.[205] The issue here, though, is not simply whether identity checks would compromise individual privacy but whether they would do so in a way as to constitute a "search" under the Fourth Amendment.[206] This Part will evaluate the potential information generation, collection, and storage aspects of a national identity system under current Fourth Amendment law, and indicate how such a system might cause the law to change. As with seizures, the answers to these questions depend on the circumstances, as well as the nature of the information itself.

A. Registration Procedures

---

[203] See ABA Standards for Criminal Justice, Electronic Surveillance (3d ed. 1999), Section B: Technologically-Assisted Physical Surveillance, Commentary to Standard 2-9.1(d) (vii) (p. 43) ("[T]he results of tracking operations . . . can be preserved well after the surveillance ends, in theory indeterminately. This capability raises the specter of extensive libraries that retain information on vast numbers of individuals in perpetuity.")

[204] The United States Supreme Court obliquely recognized this threat in Whalen v. Roe, 429, U.S. 589, 605 (1977) as it was upholding a statute requiring the reporting to a state agency, with patients' names, of controlled substances prescriptions. ("We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files."); See also, Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 Miss. L. J. 213, 237-52 (2002) (advocating recognition of a right to anonymity).

[205] Id. at 251 ("People who know they are under government surveillance will act less spontaneously, more deliberately, less individualistically, and more conventionally; conduct on the streets that is outside the mainstream, susceptible to suspicious interpretation, or merely conspicuous – even if perfectly harmless – will diminish and perhaps even be officially squelched.").

[206] There are arguments that data collection through identity checks would also compromise First Amendment freedoms of speech and association and freedom of movement, but this Article will not address them. See ABA Standards for Criminal Justice, Electronic Surveillance (3d ed. 1999), Section B: Technologically-Assisted Physical Surveillance, Standard 2.9-1 ("Law enforcement use of technologically-assisted physical surveillance can . . . diminish . . .freedom of speech, association, and travel . . . ."). Cf., Slobogin, supra note 204, at 252-63.

As mentioned above, in registration procedures an individual provides personal information to a public or private entity, often, but not always, in person.[207] There are a surprising number of registration occasions in modern American life. If a national identity number was used in these procedures, the data could end up in a database linked to that number and be accessible for government use. This, in fact, is true already of a great deal of personal information through its association with social security numbers.[208] A centralized national database would only fill in more of the picture of a person's life.[209]

Deciding whether official access to such information is a "search" under the Fourth Amendment, therefore requiring a warrant, probable cause, or some other evidentiary basis, would put to the test a series of cases in which the Court has applied a concept of assumption of the risk of surveillance. The Fourth Amendment aspects of government mandated data generation were first raised in *California Bankers Assn. v. Shultz*, a case challenging various aspects of the Bank Secrecy Act of 1970.[210] The Act authorized the Secretary to require banks to retain, with identifying information, their customers' financial records, including copies of checks over $100. These "record keeping" requirements, plaintiffs contended, constituted an illegal search and seizure. The Court curtly dismissed this claim on the ground that neither the Act nor the implementing regulations "require that any information contained in the records be

---

[207] See TAN infra (giving as examples registration for drivers' licenses, medical services, schools, and flights, or employment eligibility verification).

[208] See TAN infra.

[209] ALEXANDER SOLZHENITSYN, CANCER WARD 192 (Nicholas Bethell & David Burg trans., Modern University Library 1995 (1968) cited in United States v. Kincade, - F 3d -, 2003 U.S. App. Lexis 20133 n. 35 (October 2, 2003).

> As every man goes through life he fills in a number of forms for the record…. A man's answer to one question on one form becomes a little thread…. There are hundreds of little threads radiating from every man, millions of threads in all. If these threads were suddenly to become visible, the whole day would look for a spider's web.

[210] 416 U.S .21 (1974).

disclosed to the Government; both the legislative history and the regulations make specific reference to the fact that access to the records is to be controlled by existing legal process."[211]

However, when in *United States v. Miller* a depositor complained that the prosecution obtained his bank records by defective process, the Supreme Court held that bank customers had no expectation of privacy in their account records maintained by their banks.[212] A depositor such as Miller, the Court held, "takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."[213] It continued: "This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."[214] The Court has upheld the installation of pen registers, which record telephone numbers dialed, for the same reason: the caller assumes the risk that the phone company will divulge these numbers, and therefore has no expectation of privacy in that information.[215] This theory would encompass just about all information "voluntarily" conveyed to third parties in course of one's activities.[216]

---

[211] Id. at 52. The Court went on to hold that as to information the banks obtain from a customer "simply because the Government wants it" the information is sufficiently described and limited, and sufficiently related to commerce clause power as the withstand a Fourth Amendment challenge made by the *banks.* Id. at 67. It never reached *depositors'* Fourth Amendment claims in this regard, concluding that the plaintiffs lacked standing. Id. at 68.
[212] 425 U.S.435 (1976).
[213] Id. at 443.
[214] Id., citing cases involving government informants being sent, without judicial authorization, to converse with suspects and report, record, or transmit the suspect's statements.
[215] Smith v. Maryland, 442 U.S. 735, 743 ("When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and "exposed" that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed.")
[216] Certain statutory protections now exist for personal financial records, Right to Financial Privacy Act, 12 U.S.C. §3401 (1978) (permitting depositors to challenge subpoenas for their financial records except where notifying them would "seriously jeopardize the investigation"), and Electronic Communication Privacy Act, 18 U.S.C. §3121 (1987) (court approval required for government access to telephone records). It is not clear whether the existence of the statute would be found to create an expectation of privacy under the Fourth Amendment. Cf. California v.

There are serious conceptual and practical problems with the approach, however. Conceptually, when applied to information supplied under some assurance of confidentiality, as with bank records, an individual cannot realistically be said to have assumed the risk of divulgence; most people's assumption would be the opposite. Furthermore, why should disclosure to one person or entity be equated with disclosure to the entire world, and particularly to law enforcement personnel?[217] Privacy expectations do not need to be all or none, and are not in real life.[218] After all, the fact that one opens one's home to social guests does not mean that one has no expectation of privacy as against the police.[219] Practically, the holdings above present citizens with a Hobson's choice of participating in many of the fundaments of modern life or giving up the confidentiality of their personal information. These cases might be described as adopting the "hermit" theory of privacy expectations: a person only has an expectation of privacy in what she keeps totally to herself.[220]

Beyond these objections, the theory falls of its own weight when applied to information *required* to be passed to the government, as would be the case if a national identity card was needed for certain registrations and the information was then, by statutory mandate, transmitted to the system's computers. The risk of disclosure would be imposed, not assumed, and would not

---

Greenwood, 486 U.S. 35 (1988) (state right to privacy in garbage left at the curb does not create a reasonable expectation of privacy for Fourth Amendment purposes).

[217] See Brian J. Sen, *Great Expectations of Privacy: A new Model for Fourth Amendment Protection*, 73 MISS. L. REV. 583, 604 (1989) ("Simply because individuals have, to a limited degree, exposed an activity to public view, the Court should not conclude that they have completely relinquished all Fourth Amendment protection.")

[218] The Supreme Court recently acknowledged as much in Ferguson v. City of Charleston, 521 U.S. 67, 78 (2001) ("The reasonable expectation of privacy enjoyed by the typical hospital patient undergoing diagnostic tests in a hospital is that the results of those tests will not be shared with nonmedical personnel without her consent.").

[219] Indeed, not only does the homeowner retain her expectation of privacy, but her social guest may share in it. Minnesota v. Olson, 495 U.S. 91 (1990).

[220] Smith v. Maryland, supra note 215, at 750 ("[U]nless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance.") (Marshall, J., dissenting).

be a risk at all but a certainty.[221] These differences distinguish the bank records and telephone pen register cases.[222] The two requirements that information be linked to a national identity number and transmitted to the government for inclusion in its identity system database make all the difference, even if the information itself would have been generated anyway in the registration transaction. In addition, many occasions for registration involve activities that are central to a free and full life, like education, medical care, and travel.[223] Together these factors obviate the fictions of voluntary third-party disclosure and assumed risk, and should cause governmentally mandated collection and transmission of personal data to be found to be a search under the Fourth Amendment.[224] Whether the Court would reach this conclusion is not so clear-cut in light of its record.[225]

If it did conclude that such compelled data collection was a search, that finding would not end the inquiry. The Court would then need to address the reasonableness of the practice. Given

---

[221] This would be analogous to Justice Marshall's hypothetical of an official announcement that henceforth mail or private phone conversations would be randomly monitored, forcing citizens to "assume the risk" of government intrusion. *Smith*, supra note 215, at 750.

[222] But official constraint on choice was not enough to save the homeowner who was compelled by ordinance to leave his garbage at the curb from being held to have assumed the risk that "animals, scavengers, children, and snoops" – along with police – would go through that garbage. *Greenwood*, supra note , at

[223] As pointed out by Justice Marshall in dissent in *Smith*, supra note 215, at 749, this distinguishes the consensual monitoring cases on which risk assumption analysis is built, because one can certainly live a full life without speaking to a given individual. In other words, talking to an unreliable auditor is truly a risk one "assumes," while engaging in these other activities is not. On the other hand, the Court has characterized the disclosures of private medical information to doctors, hospitals, insurance companies and public health agencies as "an essential part of modern medical practice." Whalen v. Roe, 429 U.S 589, 602 (1977).

[224] In a dissent in *California Bankers Assn.,* supra note 210, at 84, that neatly anticipates the kind of data collection possible in a national identity system, Justice Douglas wrote: "It would be highly useful to governmental espionage to have. . . reports from all our bookstores, all our hardware and retail stores, all our drugstores. These records [in addition to financial records] might be 'useful' in criminal investigations . . . [Doctors, lawyers, creditors, political allies, social connections, religious affiliation, educational interests, papers and magazines read] are all tied to one's social security number; and now that we have the data banks, these other items will enrich that storehouse and make it possible for the bureaucrat – by pushing one button – to get in an instant the names of the [millions of] Americans who are subversives or potential and likely candidates."

[225] The majority in *Smith*, supra note 215, at 740-41 n 5, was at least willing to entertain the possibility of using a "normative inquiry" rather than risk analysis to determine the applicability of the Fourth Amendment in some circumstances. See also United States v. White, 401 U.S. 745, 786 (1971) ("[since] it is the task of the law to form and project, as well as mirror and reflect, we should not . . . merely recite . . . risks without examining the desirability of saddling them upon society.") (Harlan, J., dissenting)

what could be characterized as the non-criminal purpose of such data collection,[226] the analysis used for other administrative searches would probably be applied. As with regulatory seizures, this methodology balances "the government's need to search against the invasion the search entails**."**[227] Using this approach the Court has upheld health and safety inspections of homes without any indication of individual wrongdoing, as well as a host of other suspicionless "special needs" searches.[228]

On the other hand, it has never upheld the kind of blanket invasion of personal privacy that the transmission of registration information into national databases would involve. While it is true that such personal information would be used to further important government interests,[229] this practice would appear to lack many other attributes of the administrative searches the Court has sustained. For example, as a novel expansion of data collection, it would not carry the "long history of judicial and public acceptance" that home health and safety inspections have had.[230] Even though amassing personal information in comprehensive databases might ultimately increase their usefulness, the marginal utility is uncertain if not completely speculative. An enormous amount of data about virtually every person in the United States would have to be collected and retained in the hope that some of it might give some hint of terrorist or other illegal activity. The absolute effectiveness of terrorist profiling using a wide array of personal data has yet to be demonstrated.[231] There can thus be no claim that no "other technique would achieve acceptable results."[232]

---

[226] Cf., TAN infra.
[227] Camara v. Municipal Court of the City and County of San Francisco, 387 U.S. 523, 537 (1967).
[228] Wayne Lafave, Search and Seizure
[229] See TAN supra.
[230] *Camera*, 387 U.S. at 537. In fact, on the federal level, Congress has imposed protection for data privacy in a number of instances. **add**
[231] For an argument that this kind of data mining will be ultimately be productive, see John M. Poindexter, *Finding the Face of Terror in Data*, NY. Times A25 (September 10, 2003)((“The only way to detect . . . terrorists is to look

With respect to the degree of intrusion, much would turn on how long the information was retained, what parties had access to it, and the purposes for which it would be used. These factors figured in the Court's assessment in *Whalen v. Roe* of New York's centralized filing system for controlled substances prescriptions, identifiable by patient name.[233] Challenged by doctors and patients on right to privacy grounds,[234] this mandatory reporting program was upheld by a unanimous Court. The program contained limitations on who could access the data and made unauthorized disclosure a crime; no instances of unauthorized use had occurred in the first twenty months of the program's operation.[235] These and other features of the New York drug prescription library in *Whalen* point the way for designing a mandatory data collection system that could pass as a reasonable search. Limited disclosure is essential.[236] Because a national identity system's more extensive database would potentially be useful in civil or criminal cases, additional restrictions, such as barring the use of database contents in litigation in a manner akin to a privilege, might also be advisable.[237]

In a national identity system, limiting retention of registration records would conflict with compiling the fullest picture of a person's movements and activities. Obviously, the longer records were retained the more complete that picture, though older data is usually less informative than more recent. Record retention has surfaced as an issue in the design of CAPPS

---

for patterns of activity that are based on observations from past terrorist attacks as well as estimates about how terrorists will adapt to our measures to avoid detection.").

[232] Compare id; Martinez-Fuerte, supra note , at .

[233] 429 U.S. 589 (1977).

[234] While the Court did not have before it pure Fourth Amendment claim, it rejected a Fourth Amendment based right to privacy argument. Id. at 604, n. 32.

[235] Id. at 593-94, 600-01.

[236] Cf., Even a nondisclosure policy can be violated, however, as happened when JetBlue breached its own privacy policy and gave 5 million passenger itineraries to a defense contractor that used the information as part of a study of how to identify "high risk" airline customers. Greg Schneider and Keith L. Alexander, *Plan to Screen Air Travelers Hits Bump*, WASH. POST. A13 (September 25, 2003).

[237] For example, data collected at hotel or car rental registrations could easily be relevant in a criminal conspiracy prosecution or even a divorce action.

II. At first the Department of Transportation proposed to retain data about certain individuals for up to 50 years. In response to a flood of negative comments, the Department (now of Homeland Security) currently proposes to retain information about U.S. citizens and permanent resident aliens only for a matter of days after completion of travel.[238] The Court in *Whalen* noted with approval that New York destroyed its stored prescription records after five years, and it seems likely that the shorter the retention period the more reasonable a records database will appear.

In sum, although mandatory reporting to government databases of the kind of "registration data" that is an incident of twenty-first century American life should be found to be a "search" under the Fourth Amendment, it might well pass as a reasonable one. The outcome of the reasonableness balance would depend in part on the purpose of the data collection as well as the its effectiveness in achieving that purpose. But even where the success rate was low, as it undoubtedly would be in "terrorist" profiling, restrictions on use, retention, and disclosure might well tip the balance toward Fourth Amendment acceptability, at least during its experimental phase.[239]

Governmental collection of registration data would also withstand Fifth Amendment self-incrimination challenge, even if some of the information might provide a "link in the chain of evidence used to prosecute." [240] Suppose, for example, a flight school was obligated to transmit personal data about its students, including the fact of enrollment, to a governmental database,

---

[238] 68 FR 45265 (August 1, 2003) (record retention for non-resident aliens is still under consideration; furthermore, for all persons existing government records will be retained for up to three years, or until superseded).
[239] See e.g., ABA Standards for Criminal Justice, supra note 203, at §2-9.1(d)(vi) and (vii). (recommending disclosure of technologically assisted physical surveillance for designated lawful purposes only and disposition of records no longer required). See also case law upholding DNA collection from persons convicted of federal crimes under the DNA Analysis Backlog Elimination Act of 2000, 42 U.S.C. § 141350, and state analogues, United States v. Kincade, - F. 3d – 2003 U.S. App. Lexis 20123 (October 2, 2003) (summarizing and distinguishing cases).
[240] Hoffman, supra note 112.

and that this data helped trigger a terrorist profile or was used in a criminal prosecution.[241] The main answer to a Fifth Amendment objection is that the government did not "compel" production of the information; the person voluntarily supplied it when she registered with the school.[242] As the Court said in *Fisher v. United States,* "the Fifth Amendment protects against compelled self-incrimination, not the disclosure of private information."[243] "It follows that the self-incrimination privilege is not available to a customer, patient, or client of a third party [required] to produce its records relating to that person."[244] Most, if not all, database material would probably come from third parties; if so, no Fifth Amendment self-incrimination rights would be affected.

Because a national identity system would probably not require an individual to report her own whereabouts or private activities directly to a government database, the discussion of this form of data collection will be fairly summary. One reason for its unlikelihood is that the permissibility of a self-reporting scheme under the Fifth Amendment is much less clear-cut than reporting by third parties. An analysis of the self-incrimination issue would necessitate a choice between a line of cases barring self-reporting obligations which produce clearly incriminating communications[245] and those where the likelihood of self-incrimination is less and/or the reporting is more directly linked to a noncriminal regulatory scheme.[246] Significantly, among the

---

[241] This example is meant to illustrate a "real and appreciable" likelihood of self-incrimination. Brown v. Walker, 161 U.S. 591, 599 (1896). But see Chavez v. Martinez, supra note 114, suggesting that no Fifth Amendment issue arises unless and until the compelled information is offered in a criminal prosecution.
[242] Couch v. United States, 409 U.S. 322 (1973); Fisher v. United States, 425 U.S. 391 (1976).
[243] Fisher, 425 U.S. at 401. (internal quotation marks omitted).
[244] WAYNE R. LAFAVE ET AL., 3 CRIMINAL PROCEDURE 247, n. 47 (2d. ed. 1999).
[245] Marchetti v. United States, 390 U.S. 39 (1968) (requiring gamblers to identify themselves and pay occupational tax) ; Grosso v. United States, 390 U.S. 62 (1968)(same); Haynes v. United States, 390 U.S. 85 (1968) (requirement to register illegally possessed firearm) , Albertson v. United States, 382 U.S. 70 (1965) (requiring registration of members of the Communist Party).
[246] California v. Byers, 402 U.S. 424 (1971) (motor vehicle accident report), Baltimore City Dept. of Soc. Services v. Bouknight, 493 U.S. 549 (1990) (order to produce child).

latter category is *California v. Byers*, in which the Court narrowly upheld a "hit and run" statute requiring any driver involved in an accident to stop and provide his or her name and address.[247] The resolution of the conflict between these lines of authority would depend on the precise contours of the self-reporting demanded by the national identity system, as well as any restrictions on the information's use.[248] It is possible that self-reporting could be structured in a way as to avoid offending the Fifth Amendment. Barring the information's use in a criminal prosecution would certainly suffice, and would not greatly interfere with employing the information in profiling for further surveillance. As a practical matter, though, self-reporting would surely be far less reliable and complete than mandated data reporting by third parties. For those reasons alone a national identity system could not sensibly depend on individuals providing information about their own activities. Avoidance of any substantial Fifth Amendment self-incrimination problems suggests the same course.

B. Consensual Encounters, *Terry* Stops, Citations, and Arrests

In contrast, data generation and collection associated with consensual encounters, stops, and arrests does not fall afoul of the Fourth Amendment ban on unreasonable searches, though for slightly different reasons in each case.

1. Consensual Encounters

---

[247]Byers, supra note 246. In this concurrence Justice Harlan advanced an argument for rejecting a self-incrimination challenge that resonates with proposed data collection in a national identity system: "Technological progress creates an ever-expanding need for governmental information about individuals. If the individual's ability in any particular case to perceive a genuine risk of self-incrimination is to be a sufficient condition for imposition of use restrictions on the government in all self-reporting contexts, then the privilege threatens the capacity of the government to respond to societal needs with a realistic mixture of criminal sanctions and other regulatory devices." Id. at 452

[248] Use for a noncriminal, regulatory purpose would certainly enhance prospects for acceptance, and that in turn, might depend on whether a terrorist apprehension program was deemed to be regulatory, criminal, or military. See TAN infra.

The same consent that prevents certain encounters from being classified as seizures under the Fourth Amendment should keep their attendant production of information from constituting searches. Suppose, for example, a person pauses and presents her identity card in response to a request for that card. Suppose, too, that data showing the card was checked at that particular time and place is added to the government database while her identification is being "run" against that database. The database would now contain additional information about this person: that she was at place X at time Y and that she voluntarily presented her identity card. It might very well also record the fact that her identity check showed nothing unusual.

For two related reasons, this does not amount to a search. First, to the extent she knew the workings of the system, a fairly likely possibility if a national identity system were in place, having voluntarily stopped and presented her identification card, she has consented to having this information included. Second, even if she was unaware of its implications, here, unlike the registration procedures above, she has truly assumed the risk of this data collection and storage. The person who has viewed her card now knows her identity, and of course also knows the time and place the card was read. That person is free to report, record, or transmit that information, and the fact that this is done surreptitiously, or electronically, has no bearing, the Court has held, on the individual's expectation of privacy.[249]

2. *Terry* Stops

Investigative stops, of course, do not contain this element of consent. The question here is whether the same reasonable suspicion that justifies stopping a person and demanding identification in the first place also justifies recording and retaining that information with a date, time, and location stamp. This data collection and retention clearly adds to the imposition of a

[249] United States v. White, 401 U.S. 745 (1971)

Terry stop. Now instead of the "brief intrusion" described by the Court, the individual has a "brief intrusion" plus an endless record, not only of having been in a particular place at a particular time, but also perhaps of having generated reasonable suspicion of criminal activity. Because *Terry* was decided by balancing the governmental need for investigative stops against their degree of individual intrusion, this additional imposition upsets *Terry's* balance.

It is a close question, but the Court would nevertheless probably permit this practice, for several reasons. One is that the observations underlying this newly recorded data ordinarily are of the person in a public place, a law enforcement action not usually subject to Fourth Amendment regulation.[250] Second, the individual is not being forced to provide any information beyond her identification, an incident of a *Terry* stop the Court has already upheld.[251] The additional information transmitted to the database – time, place, and even the reason for the stop and its outcome – is all created by the officer; in other words, there is no search involved in discovering these facts. Third, access to such stored information may serve the purposes of investigative stops in general: confirming or dispelling the suspicion of criminality. A person who claims to be "lost" in the vicinity of high-value theft targets, for example, is less believable if he was "lost" there before.

There is no question that retaining data from a stop adds to its intrusiveness when that data is linked to a particular person.[252] This is especially true when the investigative stop does not lead to arrest; an individual could acquire a police "record" for activities that were not criminal enough to produce an arrest, much less a conviction.[253] Whether that extra weight on

---

[250] TAN infra.
[251] TAN supra.
[252] **Harris' writings on data collection re: traffic stops.**
[253] **FOIA case on arrest records.** For that reason, constraints on the use of this data should be built into any system that collected and retained it. See TAN infra.

the *Terry* scale would cause the Court to bar this practice, or insist on a higher level of criminal probability for its use, is much less clear.

3. Traffic Citations and Arrests

Recording and storing data associated with traffic citations and arrests is unexceptionable. As with *Terry* stops, other than the identification supplied by the suspect, the information would have been observed and recorded by the officer. Moreover, here there is probable cause for detaining and processing the individual. It is not possible to adjudicate traffic citations and arrests without collecting data about their circumstances. The widespread practice of gathering and storing this data attests to its acceptance.[254] Arrest records are now used for charge, bail and sentencing decisions**,** and in connection with the grant of certain licenses**.**[255] There is thus a demonstrated need for the collection and retention of arrest data, and no apparent Fourth Amendment objection to doing so. This is true even though aggregation of arrest data in one database, or several linked ones, is qualitatively different from the maintenance of discrete public records in the originating jurisdictions.[256]

C. Checkpoints

Identification checkpoints present another opportunity for collecting, and then storing, information about the location of a particular individual at a particular time. Ordinarily, official surveillance of a person in public, even targeted surveillance, does not amount to a search under

---

[254] See e.g. 28 U.S.C. § 534 (requiring U.S. Attorney General to "acquire, collect, classify, and preserve identification, criminal identification, crime and other records" and make them available for official use by state and federal agencies).

[255] Williams v. New York, 337 U.S. 241 (1949) (arrests not resulting in convictions may be considered for sentencing purposes); Tatum v. Rogers, 1979 U.S. Dist. LEXIS 14351 (S.D.N.Y. 1979) (use of arrest records by prosecutors and judges in charge and bail decisions and by licensing authorities).

[256] United States Department of Justice v. Reporters Committee for Freedom of the Press, 489 U.S. 749, 764 ("[T]here is vast difference between the public records that might be found after a diligent search of courthouse files, country archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information.") (upholding Freedom of Information Act exemption for rap sheets as involving an unwarranted invasion of personal privacy).

the Fourth Amendment.[257] In *United States v. Knotts* the Supreme Court applied this principle to the tracking of a beeper that government agents had installed in a can of chloroform, a chemical used to manufacture methamphetamine.[258] With the assistance of a monitoring device placed in a helicopter, agents tracked the vehicle carrying the can to a particular cabin, and included this discovery in a search warrant application for the cabin. Responding to defendant's argument that this was search, the Court stated, "A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another," the Court stated.[259] It continued, "[t]he fact that the officers in this cased relied not only on visual surveillance, but on the use of the beeper . . . does not alter the situation. Nothing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed on them at birth with such enhancement as science and technology afforded them in this case."[260] In *Knotts*, then, the Court placed official surveillance of public movement, and the use of technological aids to do so, outside the purview of the Fourth Amendment. No longer could a person rely on her wiles or the vagaries of human physical and mental abilities to preserve her public "anonymity."[261] *Knotts*, it might be said, ended the "sporting chance" age of public surveillance and moved us into the era of big game hunting.[262]

---

[257] The classic statement of this point comes from the majority opinion in Katz v. United States, 389 U.S. 347, 351 (1967): "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection." See also Justice Harlan's concurrence: "[O]bjects, activities, or statements that [a person] exposes to the 'plain view' of outsiders are not 'protected' because no intention to keep them to himself has been exhibited." Id. at 361.

[258] 460 U.S. 276 (1980).

[259] Id. at 281.

[260] Id. at 282.

[261] See Taslitz, supra note 192, at 143 (radio transmitter much more effective and difficult to detect than human observer).

[262] In Kyllo v. United States, 533 U.S. 27 (2001), a majority of the Court found the use of thermal imaging to detect heat patterns in the home to be a search under the Fourth Amendment. That decision does not seriously undermine *Knotts*, because, as the Court emphasized repeatedly, Kyllo involved surveillance of a home, "the prototypical . . . area of protected privacy." Id. at 34. Furthermore, Kyllo's expectation of privacy depended also on the fact that the

Knotts thus poses a major obstacle to any claim that information garnered in a checkpoint stop would be the fruit of an unconstitutional search. If the government can follow (or stop) people traveling in public, presumably it can also record what it learns. With enough checkpoints, though, it could virtually track everyone's movements. Knotts himself raised the specter of "twenty-four hour surveillance of any citizen," eliciting this response from the Court: "[I]f such dragnet type law enforcement practices . . . should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable."[263] The use of identification checkpoints to generate a database of individual activities would certainly bring that day closer, but the constitutional outcome would very much depend on the nature and extent of such public surveillance. It is possible to imagine degrees of checkpoint data collection that would fall well within the Supreme Court's tolerance level.

D. Summary

National identity cards could be the fulcrum for a massive exercise in government data collection. At the least, the resulting databases would cause many people to experience a loss of privacy and a fear of the use (or misuse) of their personal information. Whether such governmental collection, use, and retention of personal data would constitute an unreasonable search is far less certain. As reviewed above, under present law the state can view and record a fair amount of publicly observable activity, and can collect data on police-citizen interactions that are otherwise justifiable. These instances involve few real Fourth Amendment concerns. Mandatory reporting of personal information raises the toughest Fourth Amendment issue because, this section contends, it should be regarded as a governmental search. Nevertheless, it

---

technology in question "is not in general public use." Id. This is probably not the case with tracking devices, and certainly not the case for checkpoint surveillance and record keeping.

[263] Knotts, 460 U.S. at 283-84.

is likely that some measure of collection of data that has already been generated in daily life would be tolerated under the case law permitting non-criminal administrative searches. Comprehensive restrictions, particularly on disclosure and use, as well as on the duration of information retention, would help this practice pass constitutional muster. On the other hand, before the United States came close to becoming a "total information society" one would hope the Supreme Court call a halt to its previous acceptance of mandated reporting. Just when that line would be crossed is impossible to predict. Fifth Amendment self-incrimination objections would not arise in governmental gathering of information given to third parties.

V. CONCLUSION

The United States may never have or use a national identity card. Since September 11, however, the possibility has become real enough that it is not too soon to attempt to evaluate the constitutionality under the Fourth and Fifth Amendments of the kinds of practices a national identity system might employ. It would be pointless and unwise to design a system blatantly conflicting with these provisions. Given the expense and effort entailed in creating any national identity system, costs and benefits should be evaluated at an early stage of its consideration. To the extent that the constitution would stand in the way of a particular national identity card uses, the projected benefits will be correspondingly reduced, decreasing its overall desirability. In addition, if there is going to be a national identity system, it is advisable to consider the Fourth and Fifth Amendment issues in advance of its design so as to minimize civil liberties intrusions and maximize the prospects for judicial acceptance.

This Article has attempted to indicate what those constitutional obstacles and issues might be, as well as what practices present little or no problem. With respect to the Fourth Amendment seizures that might be implicated in official demands for an identity token, a wide

range of identification occasions would not present much constitutional difficulty. These include demands for identification during registration procedures and during investigative and traffic stops and arrests, and requests for identification during consensual encounters. There is one outright prohibition on official insistence on presentation of an identity card, and two important caveats. Suspicionless stops to check identity cards would be unreasonable seizures. One caveat concerns the use of checkpoints for terrorist profiling. Unless extraordinary circumstances develop, or there is a quantum leap in the effectiveness of this technique, checkpoint stops to link people to a database in order to profile potential terrorists should be held to be unreasonable seizures. On the other hand, checkpoints designed to identify unauthorized migrants or known suspects seem likely to receive judicial acceptance. The second caveat about the design of a national identity system is the danger it poses for drastically increasing pretextual traffic stops of motorists: stops for genuine traffic violations undertaken not to enforce the law but for the purpose of checking identification. This practice is lawful under the Fourth Amendment, but, in the absence of a wholesale reinterpretation of the pretextual stop doctrine, legislation for a national identity system should attempt to discourage it.

A review of the Fourth Amendment issues in government-mandated data collection, retention and use shows that recording public encounters, including those in normal investigative stops and arrests, as well as those at checkpoints, would be unlikely to raise serious objection. Recording investigative stops would probably be upheld despite considerable grounds for finding them to upset the carefully constructed balance sustaining the constitutionality of seizures based upon reasonable suspicion. Government acquisition of personal data that was already supplied in connection with some ordinary service poses the most serious Fourth Amendment issue. This procedure should be treated as a search, but it may be a reasonable one, at least until it reaches

some indefinable level of societal surveillance. Thus far the Supreme Court seems willing to accept a certain amount of government database creation by way of gathering information already in existence.

Where this leaves the prospects for a national identity system is hard to say, particularly because a definitive judgment about its constitutionality can only come after its features are defined, and even then only the litigation necessary to resolve many of the close questions identified in this Article. Clearly, the Fourth Amendment stands in the way of the kind of total surveillance and the anytime identification demands that would allow such a system to operate at maximum efficiency. On the other hand, there is still a fair amount the government could do in both areas that would withstand Fourth Amendment challenge. Moreover, the Fifth Amendment presents no significant obstacle to the primary functions of a national identity system.

This review of the Fourth and Fifth Amendment issues should serve to demonstrate to proponents of an identity card that there are both limits and dangers to its use. It should also make clear to those who see a national identity system as an Orwellian nightmare that while the constitution stands somewhat athwart its path, it does not make such a system impossible. Whether the kind of national identity system that could operate lawfully is worth the financial, administrative, and social costs, would ultimately be a policy, not a legal, judgment. Much of the policy assessment, though, involves a balancing of the government's need for a national identity card, its effectiveness, and its imposition on privacy and free movement. To a large degree, these are the same factors on which the constitutionality of a national identity system turns. The legal analysis thus gives a useful window on the desirability as well as the constitutionality of adopting a national identity card.