July 31, 2003

Docket Management Facility (USCG-2003-14749)
U.S. Department of Transportation, room PL-401
400 Seventh Street, SW.
Washington, DC 20590-2251

RE: Docket Number USCG–2003–14749
Comments on Interim Vessel Security Regulations

## I. Introduction

Americans have a long history of opposing national identification systems.[1] As more and more everyday activities require identification, our rights to travel freely and conduct our affairs privately are violated. Though the Department of Homeland Security and others assume that pervasive identification checking will increase security and reduce terrorist threats, there is no evidence or analysis to support that assumption. Indeed, over-reliance on identification systems could make it easier for sophisticated terrorists to evade detection using forged identification documents. Meanwhile, the risk to our privacy and civil rights is a pressing concern. Such rights are the foundation of a free society and should be abridged only when the security gains are clear and significant and only to the extent necessary to effect those gains.

The new Coast Guard port security regulations are flawed because they create the strong potential for violation of passengers' and maritime workers' civil rights. Passengers' and workers' constitutional rights to privacy, travel and association are at risk of being violated by the screening and identification checking requirements of the new regulations. These regulations open the door to invasive and ubiquitous ID checks, moving this country one step closer to a national ID system.

Specifically, the interim regulations may violate passenger and worker civil rights because 1) ID checks unsupported by terrorist watch lists or profiling are unwarranted invasions of privacy lacking any proven security benefit; 2) ID checks supported by terrorist watch lists or profiling further invade privacy by enabling extensive monitoring of passengers' activities, while increasing the risk of personal information being abused and facilitating identity theft in a manner that may reduce security; 3) physical searches of passengers authorized by the regulations may exceed the scope of what is constitutionally permissible; 4) the regulations impermissibly impair the constitutional rights to travel and associate freely; 5) passengers and workers may be denied access to information about them that is collected by the government, in a manner inconsistent with fair information practices, and 6) the regulations force port workers to submit to invasive biometric identification measures of dubious effectiveness.

For these reasons the interim regulations must be withdrawn.

## II. Passenger Rights

*A. Regulatory Background*

The new vessel security regulations allow vessel operators to inspect all entering persons' (passengers or crew) identification as well as other documents related to the reason for entry.[2] Vessel operators can inspect joining instructions, passenger tickets, boarding passes, and work orders, pilot orders, or surveyor orders.[3] The regulations give no guidelines on how such documents should be interpreted by facility personnel, nor do they specify whether and to what extent ID and travel information may be retained or used in the future. The regulations also fail to prohibit detaining, screening, or interrogating persons based solely on protected characteristics such as race, country of origin or political beliefs.

The regulations further authorize vessel operators to search or "screen" all persons seeking to board.[4] The regulations vaguely define "screening" as a "reasonable examination of persons, cargo, vehicles or baggage."[5] Passengers who refuse to submit to these invasive procedures will be denied access to the vessel.

Even after they have boarded, passengers must consent to even further screening or inspection,[6] and authorization to be on board can be revoked if they refuse additional requests for ID.[7]

As Maritime Security (MARSEC) Levels increase (MARSEC levels are calibrated to the national terror alert levels set by the Department of Homeland Security) the Coast Guard recommends increased screening frequency in addition to ID checks.[8] The regulations allow some vessels to use alternative security measures such as patrols and surveillance instead of ID checks and screening.[9] However, cruise ships must screen all persons and baggage and check all IDs at every MARSEC level.[10]

*B. ID Checking is Ineffective as a Security Measure*

1. ID Checking Alone

The regulations fail to show how identification checking alone will increase security. While there seems to be an assumption in law enforcement as well as the general populace that checking IDs will reduce terrorism, these regulations offer no proof that this is indeed the case. ID checks, for the sake of ID checks, offer little to no increased security. Unless IDs are checked against a narrowly defined watch list of those persons known to pose a risk to maritime travel, ID checks are nothing more than a hassle to passengers, serving as a political band-aid to make them feel safer despite the lack of any demonstrated security gains. The new vessel security regulations do not provide for the use of watch lists. Nor do they mention the use of databases and profiling software to catch "high risk" travelers. Without these resources, ID checks are an unwarranted invasion of privacy.

However, even when backed by watch lists or profiling databases, ID checks raise serious security issues, in addition to threatening privacy.

2. Watch Lists

There are also a number of problems generated by the use of watch lists designed to keep known terrorists from traveling.

First is the problem of accuracy. An example serves to illustrate this problem. Many men named David Nelson report being repeatedly stopped at airports in recent months.[11] They are subject to interviews, searches, and background checks by the Transportation Security Administration (TSA). Apparently the name David Nelson, or one similar, is on the "no-fly" list kept by the TSA. Airlines, who have access to the no-fly list, have stopped travelers and referred them to the TSA for further investigation because their names share common letters with suspected terrorists. To clear their names passengers must provide extensive personal information to complete a "passenger identification verification form."[12] Even then, there is no guarantee that falsely stopped passengers will not continue to be inconvenienced and embarrassed at airport security stations.

Use of watch lists to keep people from boarding ships poses even greater problems than air travel. If an air traveler misses his flight he may well be able to take a later flight. However if a cruise passenger is denied access to the ship, he has been denied his vacation. He may be left behind by friends and family, or friends and family may be forced to forego their vacations.

3. Profiling and Databases

An assumption that profiling and databases will be used when checking IDs and travel documents raises many unresolved questions. What sources of data will be used to determine whether someone is a high security risk? Will that data be retained by the government? If so, how long will it be stored? Who will be authorized to see that data, and what security measures will be taken to protect it? How will it be used in the future? Before a profiling system in conjunction with ID checks can be implemented, all of these questions must be answered, and answered with passengers' security and privacy in mind.

A major reason that ID checks that use profiling and databases will not be useful for their intended purposes is that the data used will likely have very high error rates. A recent Public Interest Research Group (PIRG) study illustrated that records on individuals kept by even the highly regulated credit reporting industry have up to a 70% error rate – and 30% of those errors are serious enough to prevent an individual form obtaining credit.[13] Given those statistics, it is very likely that data collected by the government from unregulated data-aggregators, companies that aggregate data from government records, credit reports and criminal histories, will contain substantially more errors than data collected by credit bureaus.

Vessels may use risk assessments generated from the information in the databases. Information in risk assessment reports is divided into two categories: the risk assessment report, and the data that was used to make the risk assessment.

With regard to the use of risk assessment reports, several questions arise. What are the criteria used to decide whether someone is a security risk, who evaluates the criteria, and are there any guidelines in place that will eliminate human bias or error? Again, these questions need to be answered while citizens' rights are considered and addressed.

Similar questions arise regarding the data that are used to populate the risk assessment report. What kinds of activities constitute "risky" behavior? Data that has been scooped up by law enforcement in the past include such activities as those who like to scuba[14] and those who like to order pizza via credit card.[15] In addition, police often target specific groups for extra surveillance and inject their own biases into their reports. For example, such law-abiding political organizations as the "American Friends Service Committee, the Rocky Mountain Peace and Justice Center and NARAL" have been listed as "extremist" organizations in police files.[16]

Considering the accuracy problems inherent in both watch lists and profiling schemes, it is possible that they may create more security risks than they prevent. While security personnel and resources are wasted on scrutinizing passengers profiled as "high risks" based on faulty information or on "David Nelsons" incorrectly watch-listed, actual security threats may go unnoticed.

The risks and problems created by ID checking, with or without attendant use of profiling or watch lists, are especially troubling in light of the immense cost of these new security measures. In this case, the security gains are undemonstrated and the cost high. The Coast Guard estimates that the cost of implementing the new vessel security measures will total $1.4 billion over the next ten years.[17] This cost does not even consider the economic impacts to small ports of call that depend on revenues generated when cruise ships dock there for short periods of time. The cost of the new measures is potentially astronomical, while the threat to privacy is all too real.

4. Security and Privacy Issues Related to Storage and Use of Personal Information

As mentioned above, the vessel security regulations fail to state whether and to what extent personal information and travel details will be collected as a result of passenger ID checking. As a result, some travelers may be reluctant to disclose accurate travel information, knowing that this information may be compiled in a government database for unspecified future investigative purposes; this may actually lead to a situation less secure than the current one. Other persons, concerned that every time they travel, myriad personal details about their lives will be acquired and reviewed by the government in the process of risk-profiling, may choose not to travel at all.

Besides acting as a deterrent to travel, ID checking can create other problems. Although

the government or vessel operators may claim not to use any information gathered from ID checking, they cannot guarantee that unscrupulous government or vessel employees will not improperly view or use the personal information contained in IDs and travel documents. Furthermore, the regulations fail to mention whether additional security measures will be put in place to protect the personal information that is collected about travelers.

For example, identity theft is a huge problem and growing exponentially.[18] Required ID or background checks increase the risk of identity theft by increasing the number of people who have access to personal information. Not only do people who check IDs pose a risk, but any person who has access to information in the databases poses a security risk. When combined with a lack of safeguards, ID checks and storage of personal information can lead to unscrupulous individuals taking advantage of their privileged ability to access this information. According to testimony to the U.S. Senate Judiciary Subcommittee on Technology, Terrorism, and Government Information, Beth Givens, Director of the Privacy Rights Clearinghouse testified that many cases of identity theft are "inside jobs."[19]

An example illustrates why this could become a serious problem. Recently the Transportation Security Administration (TSA) recommended that air travelers leave their checked baggage unlocked. Since then passengers have been complaining of increased thefts.[20] Two TSA employees in Miami were charged with stealing from checked baggage.[21] Yet passengers are often left with no relief as the TSA and airlines argue over who is liable for the thefts.[22] The implications these thefts have are more serious in the context of the new vessel security regulations. Losing valuables or even your luggage is far less serious a problem than having your bank account drained by an identity thief or losing time and money trying to clear your criminal or credit record.

ID checks also make the lives of identity theft victims much more difficult. The more ID checks a victim is subjected to, the more times she will be stopped because of discrepancies in her record. A growing number of identity thefts are for the purpose of committing crimes in the victim's name.[23] Criminals are able to give police false identities when arrested or charged. Such falsely created criminal records are sure to cause problems for these victims as they go about their normal lives, e.g., while riding ferries or vacationing on cruise ships. These victims may be unable to travel by ship or by air, and are left with little recourse as they attempt the difficult task of clearing their records. Conversely, potential terrorists may be masquerading under stolen identities that are unblemished by any criminal record or other threat-indicator.

The new regulations fail to take into account these *increased* security risks created by ID checking. Considering that there is no evidence that ID checking enhances security, and no mention of the possible risks, the new regulations fail to achieve their stated purpose: improved security.

*C. The Interim Regulations Would Violate Passenger Privacy by Allowing Extensive Monitoring and Almost Unbounded Searches of Travelers*

In addition to the privacy concerns outlined above, ID checking of travelers also makes it far easier for the government to monitor people's movement and personal or business relationships. Assurances that the government will not monitor citizens, though possibly sincere, do nothing to prevent such monitoring from becoming commonplace in the future. Systems and methods naturally come to be used for previously uncontemplated uses (this progression is often described as "function creep.") A good example of function creep is the expanded use of Social Security Numbers as a form of national ID. The Social Security Administration originally promised that the SSN would not be a national identifier. Now a person needs a SSN to get a driver's license, open a bank account, or enroll in school. Similarly, ID checks can, and probably will, be used by government and law enforcement to monitor citizens, innocent or not. Each vessel and port will be able to collect extensive time, place and destination information on every traveler.

Furthermore, just as the police are not allowed to arrest a person without certain minimum criteria (probable cause), neither should the government be able to submit someone to identity verifications, baggage and body screenings and interrogations without evidence of behavior that constitutes, or at the very least suggests, criminal activity. Although warrantless searches of air travelers have been allowed by many courts, such searches must be no greater in scope than is necessary to prevent weapons and explosives from being carried onto a plane, and are only valid to the extent that travelers can choose to avoid them by not boarding.[24] However, the regulations at issue articulate no limits to the scope of the allowed screening, nor does the authorization of discretionary searches after passengers have already boarded serve to prevent weapons or explosives from being carried onto the vessel in the first place. Nor can passengers aboard a vessel in transit, who have already been forced to consent to an initial screening when boarding, elect to debark in order to avoid another such search.

Measures like ID checking or repeated, discretionary searches treat everyone like a criminal. More importantly, these measures are costly and unproven. Curtailment of privacy rights may be warranted where the benefits are great and the cost minimal. As we showed earlier, the benefits of the new port security regulations are assumed and intangible and the cost very high.

*D. The Interim Regulations Impermissibly Impair the Right to Travel*

Given the lack of any empirical justification for passenger ID checking, and considering the unreasonable requirement that passengers consent to any and all screening at the vessel operator's discretion, the new maritime security regulations unreasonably burden the fundamental right to travel or move freely. The Supreme Court has held that the privileges and immunities clause of Article IV of the Constitution protects the right to travel freely between states.[25] As the Court has recently stated, "the constitutional right to travel from one State to another is firmly embedded in our jurisprudence" and is "a

virtually unconditional personal right, guaranteed by the Constitution to us all."[26] By requiring passengers to show ID and be repeatedly "screened," or be otherwise subject to heightened surveillance in order to travel by ship, the regulations here unduly restrict several aspects of the right to travel: the right to pass through a state;[27] the right to visit another state;[28] and the right to free movement.[29] "The right to move freely about one's neighborhood or town, even by automobile" is "implicit in the concept of ordered liberty" and "deeply rooted in the Nation's history."[30] Because of the vagueness of the screening requirements ("reasonable" search of persons and baggage) and the fact that each facility may have different requirements, citizens will have no way of knowing when they might be searched and how. Ship travel becomes inconvenient at the very least, humiliating and more costly at the most.

We emphasize that ID checking and passenger screening is becoming the rule for multiple modes of travel; every air traveler today expects to be asked for ID and to undergo security screening before being allowed to board. Thus, while courts have held that "burdens on a single mode of transportation do not implicate the right to travel,"[31] the burden of ID checking and security screening is no longer limited to a "single mode of transportation." It is our understanding that ID checking is becoming the norm for much rail and bus travel as well.

The rapidly spreading federal practice of ID checking is an unreasonable burden on the right to travel precisely because, as we observe above, there is no reason to believe that ID checking is an effective means of providing security.

*E. The Interim Regulations Compromise the First Amendment Right of Association*

To the extent that ID checks enable monitoring of travelers' social and political activities, deter them from traveling in order to engage in such activities, or target them based on their political affiliations, those travelers' First Amendment right to associate freely is threatened. Where state action causes people to decide not to join political groups or to end their memberships to such groups, their right of association has been violated and the state action is subject to strict scrutiny.[32] The state action must be narrowly tailored using the least restrictive means to further the purported state interests.[33] Security procedures that target members of certain political or religious groups may severely curb innocent citizens' desire to join those groups and to express their views. Considering the level of discretion left to vessel operators in implementing the new regulations, and the irrational level of fear many feel towards Islamic persons and organizations in light of the September 11th attacks, such targeting is a very real possibility. Citizens may fear being detained or prevented from traveling when attempting to board cruise ships or vessels because of their political associations. They are faced with a choice between not traveling and not participating in social and political groups. This Hobson's choice is exactly what the Constitution forbids. When the lack of empirical support of these new security measures is taken into account, it is unlikely that a court will hold that they are narrowly tailored as well as the least restrictive methods available.

*F. Minorities Will be Disproportionately Affected*

Identity checks and screening will have an affect on all travelers. However, minorities and underrepresented groups are likely to be especially affected. Increasingly tough immigration laws have lead to higher rates of deportation.[34] Immigrants, even legal ones, may not travel knowing that their identification may be checked, thereby increasing their risk of deportation. Individuals of Arab descent may decide not to travel for fear of being harassed at security checkpoints. It is likely that their fears will not be unfounded. A report issued by the Department of Justice Office of the Inspector General described how many immigrants were detained and later deported for minor immigration violations.[35] The report further states that many immigrants were held without bond based on their ethnicity or religious beliefs.[36]

The government, of course, may not plan to use ID checking and screening to discriminate, but political pressures can build over time to override weak safeguards. The McCarthy hearings, or the use of census records to round up Japanese citizens for internment during World War II, are good examples of the kinds of effects strong political pressures can have on fundamental constitutional rights.

## III. Worker Rights

*A. Regulatory Background*

The Maritime Transportation Security Act (MTSA), which mandates the new vessel security regulations at issue, also requires background checks and issuance of a biometric transportation security card in order for a person to be admitted to secure areas as designated by the port's security plan.[37] Biometrics refers to the automatic identification or identity verification of living persons using their enduring physical or behavioral characteristics such as fingers, hands, faces, or eyes. Maritime employees who apply for the security card must submit to background checks that not only include looking into criminal histories but extends to "review of any other national security-related information or database identified by the Attorney General for purposes of such a background records check."[38] This language allows investigation into practically any information the Attorney General has access to, including credit reports, purchase profiling information, or medical information.

*B. Background Checks and Biometric IDs May Not be Effective Ways to Increase Security*

As with passenger ID checking, the MTSA and the regulations it authorizes, make no mention of exactly how background checks and biometric IDs will increase security. The new regulations may even make it easier for a dedicated terrorist to gain access to sensitive areas. Where security rests on ID checks, IDs are heavily emphasized to the exclusion of other security methods. A terrorist may simply have to work to overcome one hurdle (getting an ID) instead of having to overcome a broader less predictable range of security measures.

*C. Criteria are Vague and Allow for Discrimination*

All people who access secure areas of the ports must apply for a transportation ID. The Secretary can deny someone an ID because the applicant "poses a terrorism security risk to the United States."[39] This definition is extremely vague. It is also subjective – each person designated to review the profiles and backgrounds of applicants (itself a risk to the applicant's privacy) may use different criteria. In addition, there is no safeguard that protected characteristics (race, country of origin, religion) will not be considered.

*D. Personal Information is Not Secure*

The MTSA specifies that background information will not be made available to the public or employers. However, neither the MTSA nor the new port regulations require safeguards that protect individuals from dishonest government employees who may sell personal information or even use it themselves to steal identities and commit other crimes. The MTSA and regulations also fail to require, much less acknowledge the need for security measures that protect sensitive information from, for example, hackers. Indeed, the new security regulations lack even an acknowledgement of identity theft much less ways of preventing it.

Furthermore, the MTSA and security regulations have no provision allowing individuals to view the records or risk assessments made from those records. The MTSA includes an appeal process for those denied IDs but does not describe details. Access to information is an essential component of the Fair Information Practices developed by the Department of Health and Welfare.[40] These model practices were the basis of the Privacy Act of 1974,[41] which generally provides individuals with the ability to view records that the government keeps on them.

As the Department of Justice has stated, "the purpose of the Privacy Act is to balance the government's need to maintain information about individuals with the rights of individuals to be protected against unwarranted invasions of their privacy stemming from federal agencies' collection, maintenance, use, and disclosure of personal information about them."

Moreover, the Act's historical context is important to understanding its remedial purposes: "In 1974, Congress was concerned with curbing the illegal surveillance and investigation of individuals by federal agencies that had been exposed during the Watergate scandal; it was also concerned with potential abuses presented by the government's increasing use of computers to store and retrieve personal data by means of a universal identifier--such as an individual's social security number."

The MTSA and corresponding regulations lack specific provisions implementing these model practices and allowing individuals to access their records and to correct them if they contain errors.

*E. Biometrics are Not a Magic Bullet to Increase Security*

The MTSA requires issuance of a transportation security card that includes a biometric identifier.[42] There are a number of privacy and security issues raised by the use of biometrics identifiers:

- **Biometric technology is inherently individuating and interfaces easily to database technology, making privacy violations easier and more damaging.** To avoid privacy violations, privacy must be designed into biometric security systems from the beginning, as it is hard to retrofit complex systems for privacy.
- **Biometrics are no substitute for quality data about potential risks**. No matter how accurately a person is identified, identification alone reveals nothing about whether a person is a terrorist. Such information is completely external to any biometric ID system.
- **Biometric identification is only as good as the initial ID.** The quality of the initial "enrollment" or "registration" is crucial. Biometrics are as vulnerable as present ID systems to fraudulent enrollment, as they will likely be based on exactly the document-based methods of identification upon which biometrics are supposed to improve.
- **Biometric identification is often overkill for the task at hand.** It is not necessary to identify a person (and to create a record of their presence at a certain place and time) if all you really want to know is whether they're entitled to do something or be somewhere. For example, when in a bar, customers use IDs to prove they're old enough to drink, not to prove who they are, or to create a record of their presence.
- **Some biometric technologies are discriminatory.** A nontrivial percentage of the population cannot present suitable features to participate in certain biometric systems. Many people have fingers that simply do not "print well." For example, the elderly often have fingerprints that are too “weak” to be read by scanners because fingerprints tend to fade as we age. This is a significant portion of the population. Even if people with "bad prints" represent 1% of the population, this would mean massive inconvenience and suspicion for that minority. The INS, for example, handles about 1 billion distinct entries and exits every year. Even a seemingly low error rate of 0.1% means 1 million errors, each of which translates to INS resources lost following a false lead.
- **Biometric systems' accuracy is impossible to assess before deployment.** Accuracy and error rates published by biometric technology vendors are not trustworthy, as biometric error rates are intrinsically manipulable. When subjected to real-world testing in the proposed operating environment, biometric systems frequently fall short of the performance promised by vendors.
    - A study conducted by a Japanese researcher showed that finger print scanners could be fooled 80% of the time by using gelatin to make a mold of a fingerprint.[43] The researcher used commonly available tools to make the fake fingerprints. He could even make a functioning fake from a fingerprint left on glass.[44] He tested eleven commercially available scanners and fooled all of them (including some with “live finger detection” features).

- A test conducted at Palm Beach International Airport of face recognition technology showed that the face scanners failed to match faces to the database pictures in 503 out of 958 test attempts (53%). The report found that eye-glasses interfered with correct matching, that face angle had a significant effect on accuracy, and that the subjects needed to be well lit and had to stand perfectly still.[45]

- **The cost of failure is high.** If you lose a credit card, you can cancel it and get a new one. If your biometric is somehow compromised, you've lost it for life. Any biometric system must be built to the highest levels of data security, including transmission that prevents interception, storage that prevents theft, and system-wide architecture to prevent both intrusion and compromise by corrupt or deceitful agents within the organization.

**IV. Conclusion**

There are fundamental problems created by the new security regulations. ID checks violate the fundamental right to move freely, and invade the privacy and security of travelers. ID checks threaten important constitutional values.

Not only do these new regulations threaten fundamental constitutional rights, they also fail a simple cost/benefit analysis. ID checks, biometric identifiers and repeated discretionary screenings are unproven and expensive security measures. Invasions into citizens' personal lives should only be tolerated when the resulting security benefits are clear and the financial and moral costs are clearly outweighed by those benefits. Because the new security measures violate important rights and fail a cost benefit analysis, they should be removed from the new security regulations until further studies confirm that they work and work well.

Sincerely,

Beth Givens
Privacy Rights Clearinghouse

Mike Stollenwerk
Advisor to the Privacy Rights Clearinghouse

Edward Hasbrouck
Travel writer and consumer advocate
Author, The Practical Nomad

Kevin Bankston
Attorney & Equal Justice Works Fellow
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110

Lee Tien
Senior Staff Counsel
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110

Deborah Pierce
Executive Director
PrivacyActivism
452 Shotwell Street
San Francisco, CA 94110

---

[1] National ID Cards, http://www.epic.org/privacy/id_cards/.
[2] § 104.265(e)(3), Vessel Security, 68 Fed. Reg. 39,292, 39,308 (proposed Jul. 1, 2003) (to be codified at 33 C.F.R. pt. 104).
[3] Id.
[4] Id. at § 104.265(e)(1), 68 Fed. Reg. 39,292, 39,307.
[5] § 101.105, Implementation of National Maritime Security Initiatives, 68 Fed. Reg. 39,239, 39,279 (proposed Jul. 1, 2003) (to be codified at 33 C.F.R. pt. 101, 102).
[6] § 104.265(e)(2)(i), 68 Fed. Reg. 39,292, 39,308.
[7] Id. at § 104.265(e)(4), 68 Fed. Reg. 39,292, 39,308.
[8] Id. at § 104.265(f), 68 Fed. Reg. 39,292, 39,308.
[9] Id. at § 104.292(b), 68 Fed. Reg. 39,292, 39,310.
[10] Id. at § 104.295, 68 Fed. Reg. 39,292, 39,311.
[11] Rex Huppke, Security screeners 'nab' David Nelsons, Seattle Times, Jul. 1, 2003, at A2.
[12] Id.
[13] See http://www.pirg.org/reports/consumer/mistakes/page1.htm for more details.
[14] See Electronic Frontier Foundation Media Release, Electronic Frontier Foundation Helps Dive Shop Resist Feds, October 21, 2002 (available at http://www.eff.org/Privacy/Surveillance/20021021_eff_pr.html).
[15] See Erik Baard, Buying Trouble: Your Grocery List Could Spark a Terror Probe, The Village Voice, July 24-30, 2002 (available at http://www.villagevoice.com/issues/0230/baard.php).
[16] Katha Pollitt, They Know When You Are Sleeping, The Nation, Jan. 9, 2003, at No. 3 Vol. 276 p. 9.
[17] Vessel Security, 68 Fed. Reg. 39,292, 39,298.
[18] Matt Canham, Utah task force tackles mounting identity theft, Salt Lake Tribune, Jul. 14, 2003.
[19] See Jay Mathews, Identity Theft [is] More Often an Inside Job: Old Precautions Less Likely to Avert Costly Crime, Experts Say, The Washington Post, Dec 3, 2002, at A1 (available at http://www.privacyrights.org/ar/id_theft.htm).
[20] Sara Kehaulani Goo, Travelers reporting thefts from luggage; Belongings vanish from

unlocked bags, The Washington Post, Jun. 29, 2003, at A18.
[21] Id.
[22] Id.
[23] See Privacy Rights Clearinghouse's Criminal Identity Theft page (available at http://www.privacyrights.org/fs/fs17g-CrimIdTheft.htm).
[24] See e.g. U.S. v. Davis, 482 F.2d 893, 908-11 (9th Cir. 1973).
[25] Saenz v. Roe, 526 U.S. 489, 498 (1999) (internal quotations and citations omitted).
[26] Id. (internal quotations and citations omitted).
[27] United States v. Guest, 383 U.S. 745 (1966).
[28] Baldwin v. Fish & Game Commission, 436 U.S. 371 (1978).
[29] Kent v. Dulles, 357 U.S. 116, 126 (1958).
[30] Lutz v. City of New York, 899 F.2d 255, 268 (3rd Cir. 1990).
[31] Miller v. Reed, 176 F.3d 1202, 1205 (9th Cir. 1999).
[32] NAACP v. Alabama, 357 U.S. 449, 463 (1958).
[33] Roberts v. United States Jaycees, 468 U.S. 609, 623 (1984).
[34] See Gregg Krupa, Immigration Crackdown Changes Lives; Tighter Federal Rules Can Separate Families, Detroit News, Nov. 18, 2002, at 1A.
[35] United States Department of Justice Office of the Inspector General, A Review of the Treatment of Aliens Held on Immigration Charges in Connection with the Investigation of the September 11 Attacks (2003) (available at http://www.usdoj.gov/oig/special/03-06/index.htm).
[36] Id.
[37] 46 U.S.C. § 70105.
[38] Id. at § 70105(d)(2)(D).
[39] Id. at § 70105(c)(1)(D).
[40] The Fair Information Practices are available at http://www.privacyrights.org/ar/fairinfo.htm.
[41] See 5 USC § 552a.
[42] Id. at § 70105(b)(1).
[43] See T. Matsumoto, H. Matsumoto, K. Yamada, S. Hoshino, "Impact of Artificial Gummy Fingers on Fingerprint Systems," Proceedings of SPIE Vol. #4677, Optical Security and Counterfeit Deterrence Techniques IV, 2002 (cited at http://www.counterpane.com/crypto-gram-0205.html#5).
[44] Id.
[45] See Palm Beach International Airport's Facial Recognition Test (Phase I) Summary (available at http://archive.aclu.org/issues/privacy/FaceRec_data.pdf).