CENTER FOR
DEMOCRACY
&
TECHNOLOGY
Working for Civil Liberties on the Internet

1634 I Street, NW Suite 1100
Washington, DC 20006
202.637.9800
fax 202.637.0968
http://www.cdt.org

CDT Analysis of Privacy Guidelines for the Information Sharing Environment for Terrorism Information

February 2, 2007

On December 4, 2006, the President approved privacy guidelines for the Information Sharing Environment (ISE), the Congressionally-mandated system or framework for sharing terrorism-related information among federal agencies and with state and local governments and the private sector.[1] The guidelines reflect months of complex and probably intensive inter-agency deliberation; it is a tribute to the dedication and negotiating abilities of their lead drafters that they were issued at all.

However, the guidelines do not address in adequate detail key issues posed by expanded cross-agency sharing of sensitive personally-identifiable information. Accordingly, the guidelines do not provide a sufficient framework for sharing information in the ISE in a manner that protects privacy and other civil liberties. They could serve as a framework for the process of developing the needed guidelines. The reports of the Markle Foundation Task Force on National Security in the Information Age and other expert sources offer recommendations as to what such guidelines should include. Meanwhile, there is ground for serious concern that implementation of the ISE is proceeding without the privacy guidelines contemplated by Congress.

Guidelines Are Needed to Clarify What Privacy Is - These Guidelines Do Not Even Try to Define Privacy

To understand the limits of the new ISE guidelines, it is useful to consider why privacy guidelines are needed in the first place. The answer is two-fold. First, guidelines are

---

[1] Section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 directed the President to establish an Information Sharing Environment (ISE). Pub. L. 108-458, 118 Stat. 3638, 3664 (December 17, 2004), codified at 6 U.S.C. 485. Implementing the ISE is a complex and challenging task. In December 2005, the President issued a memorandum setting certain guidelines and requirements in support of the ISE. http://www.fas.org/sgp/news/2005/12/wh121605-memo.html. In November 2006, the ISE Program Manager issued the Information Sharing Environment Implementation Plan. http://www.ise.gov/docs/ISE-impplan-200611.pdf. The privacy guidelines are online at http://www.ise.gov/portfolio.html.

needed because "privacy" is a broad and a widely misunderstood concept. The word "privacy" means different things in different contexts. In the context of the ISE, government officials who are required by statutes and Presidential orders to protect "privacy" need to understand the concept as it relates to the sharing of information that is already lawfully in the possession of the government or readily available to it from commercial entities.[2] (Indeed, some of the information at issue is actually public.)

"Privacy" in this context of information sharing is largely about due process: How do you use information to make fair and reliable decisions about people? In the counterterrorism context, the consequences to individuals of being mistakenly designated as a terrorist or an associate of terrorists can be devastating and can include arrest or detention, deportation, loss of a job, more intrusive inspection or investigation, damage to reputation and a cloud of suspicion. Some of these consequences can be imposed with little or no opportunity for redress or correction of errors. Increasingly, the Executive Branch has claimed the authority to impose serious consequences on individuals outside the normal criminal justice or administrative due process systems, heightening the risk of serious adverse consequences from mistake. In addition, false leads also have serious consequences for national security, diverting resources from true threats.

There is a framework for using information to make fair and reliable decisions about people. The framework is called the "Fair Information Practices," a much more meaningful term than "privacy." There is no single authoritative statement of Fair Information Practices (FIPs), even though they were developed in the 1970s by an Advisory Committee to the US Department of Health, Education and Welfare and since have become globally recognized. CDT uses the following framework, the elements of which can be found in the Privacy Act, which is generally applicable to all U.S. government systems of records:

1. Notice (or openness) -- the government should state when it is collecting data, through a published notice and wherever possible on an individual basis - Privacy Act, subsection (e)(2), (3) and (4). Sometimes notice is discussed in conjunction with choice or consent, the principle that individuals should have control over when data is collected and how it is used, unless a certain standard is met for the compulsory collection of data (such as with a warrant or subpoena).
2. Purpose specification -- the government should specify the purpose for which it is collecting data - Privacy Act, subsection (e)(3).
3. Collection limitation – collect no more than relevant and necessary for the specified purpose (minimization) – see Privacy Act subsections (e)(2) and (7).

---

[2] There are huge unresolved issues about the standards for government collection of digital information from the oceans of business records and transactional data we generate in the course of modern life. These include questions as fundamental as what is a "search and seizure" for Constitutional purposes. Collection issues (Fourth Amendment issues) are beyond the scope of the guidelines and this memo.

4. Retention limitation – retain (or "maintain") no longer than necessary for the specified purpose –the Privacy Act does not require record disposal, but see subsections (e)(1), (2) and (5).
5. Use and disclosure limitation –limits on secondary use without consent– Privacy Act subsection (b).
6. Data quality – timely, accurate, complete – Privacy Act subsection (e)(5).
7. Security – Privacy Act subsection (e)(10).
8. Access to one's own records – Sometimes referred to as "individual participation," access is a right in and of itself, but also it is a precursor to exercising the right to insist on the correction of mistakes – Privacy Act subsections (c), (d) and (f).
9. Redress – Sometimes combined with the "individual participation" principle, this refers to the right to challenge inaccurate data, preferably before adverse decisions are made, and to correct mistakes and obtain redress for abuse – Privacy Act subsections (e) and (d).
10. Accountability- audit, enforcement – Privacy Act subsections (e)(9) and (10), (g) and (i).[3]

Clearly, not all of these concepts can be implemented in the counterterrorism context in the same way they are applied in the government benefits context. Nevertheless, they define the key questions that should be asked in designing even counterterrorism information systems, including: What information is being collected, for what purpose, with whom will it be shared, how long will it be retained, how accurate and reliable is the information, how will the data be secured against loss or unauthorized access, and will individuals know the basis for decisions affecting them and be able to respond to mistakes.[4]

In the intelligence context, "privacy" is also used to refer to the important First Amendment principle that individuals should be able to oppose government policies or engage in other political activities without the government collecting information about

---

[3] *See, for example,* Department of Justice, Office of Justice Programs, Global Justice Information Sharing Initiative ("Global"), "Fusion Center Guidelines: Law Enforcement Intelligence, Public Safety, and the Private Sector" (2006) http://it.ojp.gov/documents/fusion_center_guidelines.pdf, Guideline 8, pp. 41-42, which sets forth a slightly different formulation. The DNI guidelines draw, appropriately, from the Global guidelines, but unlike the DNI guidelines, the Global guidelines begin with a comprehensive summary of the privacy framework. In other respects, the Global Guidelines also suffer from a lack of specificity. See also Global's "Privacy Policy Development Guide and Implementation Templates" (October 2006) http://it.ojp.gov/documents/Privacy_Guide_Final.pdf, Section 4 and Appendix A (the "templates"), pp 2-3.

[4] *See* James X. Dempsey and Lara M. Flint, "Commercial Data and National Security," *The George Washington Law Review*, Vol. 72, No. 6 (August 2004).

them. Investigation by secretive counterintelligence agencies, even if those agencies take no adverse action, can have a chilling effect on the exercise of First Amendment rights. Therefore, our national policy has been to limit carefully what the primary domestic intelligence and counterintelligence agency, the FBI, can do inside the US and to generally prohibit other intelligence agencies, such as the CIA and the NSA, from operating inside the US or collecting information about US citizens at all. Most importantly, we limit the government's collection of information about the exercise of citizens' First Amendment rights, even if the exercise of those rights is public.

None of this is explained in the guidelines. Nowhere do the guidelines or accompanying material ever actually say what privacy is. The title and text of the guidelines refer to "other legal protections," but never explain what those are either. The guidelines never mention the First Amendment or free speech. The word "privacy" is repeated numerous times, but never defined. The cover memorandum to the ISE guidelines includes one reference to Fair Information Practices, and the guidelines themselves contain some of the FIPs. However, there is no engagement with the challenges of applying the Fair Information Practices in the terrorism context. Government officials confused about what "privacy" means in the counterterrorism context will receive no guidance from these guidelines.

Guidelines Are Needed to Fill the Gaps in Privacy Law – These Guidelines Do Not Even Acknowledge the Gaps

The second reason why guidelines are needed is because the existing "privacy" rules are inadequate, incomplete, fragmented and full of exceptions. Currently there is both too much privacy law and too little. The interagency working group that drafted the guidelines tried to catalogue existing privacy rules and gave up after its count reached 108 different sets of privacy rules. The working group found it impossible to harmonize the various rules. Instead, it directed all agencies to comply with all "applicable" privacy rules. Guidelines should provide a clear path through this confusion, but the December 2006 guidelines do not. Officials reading these guidelines might still conclude that it is impossible to comply with confusing and conflicting privacy requirements, in which case they might fail to share or they might seek to evade privacy principles entirely.

Moreover, existing privacy laws are full of exceptions.[5] The Privacy Act, for example, is the core privacy law for federal government agencies, including law enforcement and intelligence agencies. As noted above, it embodies all of the Fair Information Practices. However, it is replete with exceptions:

- Law enforcement and intelligence agencies can exempt their records from the collection limitation principle (Privacy Act subsection (e)(1)), which requires agencies to collect only such information as is "relevant and necessary" to

[5] CDT prepared a chart outlining the exceptions to the sectoral privacy laws: http://www.cdt.org/security/guidelines/final_government_matrix.shtml.

accomplish an authorized purpose of the agency.

- The CIA and law enforcement agencies can exempt themselves from the Act's requirement (subsection (c)(4)) that an agency inform other agencies when it makes a correction to, or notes a dispute regarding the accuracy of, a previously disseminated record.
- Law enforcement and intelligence agencies can exempt their records from the access principle (Privacy Act subsections (d), (e)(G) - (H), and (f)), which is a foundation of the redress principle (if you cannot access records about you, it will be hard to challenge their accuracy or seek redress for their misuse).
- The CIA and law enforcement agencies can exempt their records from the accuracy principle (Privacy Act subsection (e)(5)).
- The Act's statement that agencies may maintain "no record describing how any individual exercises rights guaranteed by the First Amendment" (subsection (e)(7) has an exception for collection "within the scope of an authorized law enforcement activity," which the courts have interpreted to include intelligence activities unrelated to the investigation of a crime.
- Any agency can redisclose information and use it for secondary purposes, if it claims that such use is "compatible" with the purpose for which the information was collected and therefore "routine."
- Counterintelligence activities and law enforcement investigations are exempt from the Act's provisions on computer "matching."
- The CIA and law enforcement agencies can partially avoid the enforcement principle, by exempting themselves from the Act's provisions affording civil remedies and judicial review (subsection (g)).

In this context, the statement in the guidelines that "all agencies shall, without exception, comply with the Constitution and all applicable laws and Executive Orders relating to protected information" is meaningless, since the laws themselves are full of exceptions.[6] If the guidelines meant that the exceptions of the Privacy Act could not be invoked for data to be shared through the ISE, that would be an extraordinary achievement – but it seems highly unlikely that any agency will read the guidelines as taking away the Privacy Act exemptions "without exception."[7]

---

[6] A direction to comply with the Constitution and all laws is especially meaningless in an Administration where the President claims that he has the power under the Constitution to disregard statutes. This is not to state a position on the Constitutional debate over Presidential powers. We are simply noting that, today, an admonition to follow the Constitution and "all applicable laws" offers absolutely no guidance to front line officials struggling with the hard issues.

[7] Indeed, it seems impossible that the Privacy Act could apply to the ISE without invoking some of the Act's exceptions. Exceptions are not necessarily bad. They may be necessary accommodations to conflicting policy objectives. We are making two separate points here: (i) The exceptions in the Privacy Act have become gaping holes. (ii) The guidelines make no effort to establish a reasonable balance; they leave agencies torn

In recent years, agencies have been increasingly bold in claiming the Privacy Act's exemptions. In 2003, over the strenuous objection of public interest organizations, the DOJ exempted the National Crime Information Center from the accuracy requirement of the Privacy Act.[8] In 2005, the Department of Homeland Security granted its Operations Center blanket exemption from major provisions of the Privacy Act.[9] The Privacy Act notice for Secure Flight claimed sweeping exemption from the Act.[10] Most recently, Customs and Border Protection claimed that data collected on American citizens under the Automated Targeting System (ATS) would be shared with a wide range of agencies for a variety of uses, under a particularly expansive interpretation of the Privacy Act's "routine use" exception.[11] Last year, the Senate Intelligence Committee approved a provision that would amend the Privacy Act to exempt all agencies from the redisclosure and secondary use provision of the Privacy Act for purpose of sharing with intelligence agencies.[12]

The guidelines and accompanying materials make no reference to these exceptions, yet all of the systems at issue are, we presume, part of the ISE. For example, will information in the NCIC be able to be shared through the ISE even though the NCIC no longer complies with the Privacy Act's accuracy requirement? The guidelines did not heed the advice of the Markle Task Force in its third report: ""There inevitably will be ambiguities or unanswered questions; these should be addressed expliclty, not ignored or exploited to avoid the law's requirements."

There are other gaps in the Privacy Act that could be ameliorated in part by administrative action, but which the guidelines do not address. Notably, the Act does not apply to existing private sector databases. Therefore, when the government accesses commercial databases, it need not ensure (or even evaluate) the accuracy of the data; it need not allow individuals to review and correct the data; and the government is not limited in how it interprets or characterizes the data. Agencies are increasingly using commercial databases for counter-terrorism purposes. In October 2005, the Department

---

between applying the Privacy Act without exception or driving a Mack truck through all of the Act's exceptions.

[8] http://www.epic.org/privacy/ncic/.

[9] http://epic.org/privacy/homeland/dhs_hsocd_final.pdf.

[10] Transportation Security Administration, Notice of Privacy Act System of Records, 68 Fed. Reg. 2101 (January 15, 2003).

[11] Department of Homeland Security, Notice of Privacy Act System of Records, 71 Fed. Reg. 64543 (November 2, 2006).

[12] Section 310 of the Intelligence Authorization Act for FY 2007, S. 3237 (109th Cong.).

of Homeland Security's privacy advisory board recommended that the Department abide by the Privacy Act when it obtains information about citizens from private third party data aggregators.[13] To our knowledge, the recommendation has not been implemented. The ISE guidelines, which could have adopted the DHS privacy board recommendation, do not even mention the issue. The guidelines' definition of "protected information" seems to exclude commercial data accessed by the federal government for counter-terrorism purposes.

Neither the Guidelines nor Any Other Element of the ISE Framework Resolves Questions About Roles and Missions

The privacy guidelines do not address the question of agency roles and missions, nor do other materials issued in connection with the ISE Implementation Plan. This is a serious gap in the ISE framework.[14] The development of a process for better sharing terrorism-related information while also better protecting civil liberties requires a clarification of what agencies are permitted to make what "authorized uses" of information about individuals. That in turn requires careful consideration and definition of the appropriate roles and missions of agencies and offices engaged in counterterrorism. The question of roles and responsibilities is addressed neither in the ISE Implementation Plan nor in the Privacy Guidelines. Those questions include: Which agencies have which missions? Who is responsible for the collection of intelligence information, particularly inside the United States or against U.S. persons? What is the role of the military in domestic intelligence? What does domestic intelligence mean? Until those questions can be answered, they will be left to the assertions of individual agencies, with the risk not only of civil liberties intrusions but also duplication of effort, the expenditure of resources on non-productive forms of information gathering and analysis, and ongoing conflicts between agencies.[15]

To be sure, it is not the role of privacy guidelines to clarify agency roles and missions. The point here is that the ISE, if it is to respect individual rights, must be conducted within a framework in which it is clear what agencies are responsible for collecting and acting upon information about US citizens. The current statement of roles and missions is classified, but we suspect it is vague. Even the best privacy guidelines will be inadequate to protect against adverse due process and First Amendment effects of the ISE until domestic roles and missions, especially of the DoD, are publicly clarified.

---

[13] http://www.cdt.org/privacy/20051027dhsdatareport.pdf.

[14] The Markle Task Force, in its third report, stated, "We urge our government to engage in a public debate, to the extent possible while maintaining national security, about the guidelines and rules that govern information sharing. This debate should also seek to clarify agency missions and address the requisite civil liberties and privacy protections."

[15] Eric Lichtblau and Mark Mazzetti, "Military Expands Intelligence Role in U.S.," *New York Times* (January 14, 2007) p. A1.

Name Match Reliability (Entity Disambiguation)

One of the many challenges facing the government as it seeks to identify terrorists and control their movements is to reliably identify a person in the first place, to distinguish that person from all other individuals with the same or similar names, and to associate with that person all of his aliases. The government's terrorist watchlists contain hundreds of thousands of names, but no one knows how many of those entries represent unique individuals. This poses an extremely difficult set of challenges. When a new piece of intelligence is acquired concerning J. Doe, should it be added to the file of (associated with the existing record of) John Doe or to the file of Jasper Doe or should a new file be created on J. Doe? Similarly, when someone bearing identification documents in the name of Edward M. Kennedy shows up at the airport, should he be subjected to more intensive scrutiny because there is an Edward or Ted or Eddie Kennedy watchlisted as a suspected terrorist?

The issue of accurate name matching illustrates how little the guidelines offer. The guidelines simply state that agencies shall, "Take appropriate steps when merging information about an individual from two or more sources to ensure that the information is about the same individual." Presumably, agencies were already taking steps to improve their ability to match information about individuals. More fundamentally, however, the guidelines do not offer any guidance about how agencies can actually improve their practices. So the guidelines tell TSA to be careful when matching Ted Kennedy on the terrorist watch list with Sen. Ted Kennedy on the flight to Massachusetts, but they did not begin to tell TSA or any other agency how to actually go about doing that.

In contrast, the guidelines developed by the Global Information Sharing include at least a somewhat more precise framework for the merging of data:

> (a) Information about an individual or organization from two or more sources will not be merged unless there is sufficient identifying information to reasonably conclude that the information is about the same individual or organization.
>
> (b) The set of identifying information sufficient to allow merging will consist of [specify a standard or set of information or characteristics that are considered adequate to allow merging of information].
>
> [Consider adding the following subsection to allow tentative matching of information from more than one source: (c) If the matching requirements are not fully met but there is a strong partial match, the information may be associated if accompanied by a clear statement that it has not been adequately established that the information relates to the

same individual or organization.][16]

This is not sufficient either, but it is closer to the kind of detailed guidance that agencies need.

Audit

To take another example, the guidelines appropriately say that each agency shall implement adequate review and audit mechanisms to ensure compliance with the guidelines. Sound information management requires no less, and subsection (e)(10) the Privacy Act already requires agencies to establish "appropriate administrative, technical and physical safeguards to insure the security and confidentiality of records" and to protect against their misuse. The Privacy Act already requires agencies to keep an accurate accounting of all disclosures of records to other agencies. But the guidelines add nothing to these Privacy Act requirements. The guidelines do not have any specificity as to what is an adequate audit, what agencies should be auditing for, who should be audited, or who should have access to the audits. The Markle Task Force, in its third report on pages 67 through 70, gave some concrete recommendations as to how auditing should be conducted, not only at the agency level but at the individual level and what are some of the technologies for carrying out auditing.[17]

Redress

The guidelines call for redress mechanisms to be put in place to address complaints from persons regarding protected information about them that is under an agency's control. Again, however, the guidelines offer no further details on how to go about setting up a redress mechanism. In particular, they don't address the threshold problem, which is that some agencies won't even tell you in the first place whether they have information about you. How can you exercise a redress right if you don't know what information exists about you? For example, it has been revealed recently that the Department of Homeland Security through Customs and Border Protection Bureau is conducting risk assessments of all people entering and leaving the country, including citizens. The Privacy Act notice for those risk assessments specifically purports to exempt the records from the Privacy Act's rule that a person has the right to see information about himself, a right upon which redress normally hinges. Of course, there will be circumstances in which the government cannot tell a person what it knows about him, but in those circumstances there has to be some alternative redress mechanism. The guidelines offer no guidance on how to reconcile the tension between secrecy and redress.

---

[16] Global's "Privacy Policy Development Guide and Implementation Templates" (October 2006) http://it.ojp.gov/documents/Privacy_Guide_Final.pdf, Appendix A (the "templates"), Section B.6.20.

[17] "Mobilizing Information to Prevent Terrorism: Accelerating Development of a Trusted Information Sharing Environment" http://www.markle.org/downloadable_assets/2006_nstf_report3.pdf.

At the very least, it seems possible to outline in more detail a redress system for screening programs like the airline passenger screening system and ATS. A review of redress systems under the Fair Credit Reporting Act and other laws applicable to the private sector suggests the following core elements of a redress system:

- Notice of the fact of the adverse decision and the procedure for challenging it;
- Access to the information on which the decision is based, which is premised on the ability to trace information to its source for verification;
- An opportunity to correct erroneous information and an obligation to correct or delete information that is erroneous;
- Procedures for ensuring that erroneous information does not re-enter the system;
- Obligations on data furnishers to respond to requests for reconsideration of data and to take corrective action when justified;
- Independent administrative or judicial review and enforcement.

Purpose Specification

Agencies must still operate within their assigned missions; the CIA and the DoD should not engage in the collection or analysis of domestic intelligence. The Markle Task Force recommended that guidelines should permit information to be shared with an agency only if the purpose for the sharing is within the assigned role and mission of the receiving agency. The ISE guidelines, however, say that each agency's access to and use of information available through the ISE should be consistent "with the authorized purpose of the ISE." But the ISE has the very broad purpose of promoting the sharing of information relevant to terrorism. What the guidelines should say is that agencies must ensure that the sharing and receipt of information is consistent with the authorized purpose and mission *of the receiving (or requesting) agency.* Something like this is found under Section 2.b, "Rules Assessment," which requires each agency to adopt internal rules and procedures requiring it to only seek or retain protected information that is legally permissible for the agency to seek or retrieve. However, in the absence of clear determination of which agency is permitted to do what, this provision will likely have little effect.

The Markle Task Force on National Security in the Information Age,[18] which conducted an extensive inquiry on information sharing and privacy, did not find it necessary lower standards on collection of U.S. person data. Nor did it find it necessary to expand agency missions to permit targeting of U.S. persons by agencies traditionally focused overseas. The ISE privacy guidelines likewise accept current collection standards and are premised upon the principle that U.S. person data merits special treatment.

[18] The non-partisan task force was comprised of former senior officials from Democratic and Republican administrations as well as business leaders, technology experts and civil liberties advocates. CDT President Jerry Berman and Policy Director Jim Dempsey were members of the Task Force.

The Task Force gave considerable attention to purpose specification in its third report (2006). The Task Force's third report recommended the adoption of an "authorized use" standard for sharing and accessing U.S. person information that has been lawfully collected by or is available to the U.S. Government. According to the Markle Task Force, "authorized uses" are mission or threat-based permissions to access or share information. These permissions would be determined beforehand for each agency, each unit, and possibly each personnel position, so that each agency and each employee was clear on what was permitted. The Task Force report provided some examples of how an authorized purposes standard would work. For example, the CIA is generally prohibited from collecting intelligence inside the United States. However, if particular U.S. person data collected by another agency is relevant to an overseas activity of the CIA, such as the tracing of terrorist financing overseas, then under the proposed authorized purposes standard it would be appropriate to share that U.S. person related data with the CIA, not for the purpose of the CIA operating domestically but for the CIA to use in its mission to investigate terrorist financing overseas.

The Concept of Sharing

Just as the guidelines do not offer a clear definition of privacy, they do not seem to be based on a clear sense of what information sharing is. The Markle Task Force recommendations and Section 1016 of the IRTPA were based on the premise that information sharing would be most effective from a national security standpoint *and* most protective of privacy if it did not involve the wholesale transfer of information between departments. Rather, the Markle recommendations and Section 1016 left databases at the agencies where they were created, so they could be more readily updated corrected and so their use could be more easily controlled and audited. Achieving information sharing while letting data reside where it was created requires the establishment of data directories containing key attributes for searching (metadata) and pointers to data, In addition, important oversight and control mechanisms could be implemented through the data directories.

While the guidelines do not seem to fully understand the importance of decentralization, they get close to the issue in Section 4, on page 3. This potentially useful provision requires each agency to identify its data holdings that contain U.S. person data that might be shared through the ISE and to identify specifically the rules within the agency that govern the use and sharing of that information. This catalogue of information could be very helpful to the agency privacy officers, the President's Privacy Oversight Board, the program manager for the ISE, the DNI, Congress, and even the agencies themselves, so they can get a sense of what their counterpart agencies hold. We wish the catalogue of data holdings had been coupled with a clear explanation of the role of directories in finding information within those holdings without having to open them to browsing by other agencies.

The Guidelines' Procedural Elements

The guidelines have a number of useful procedural elements. The gudielines establish an ISE privacy governance structure for deconfliction, compliance, and continuous development of privacy guidance. They provide a consistent framework for identifying information that is subject to privacy protection and for identifying and assessing applicable privacy rules. These procedures are important, but they are not a substitute for comprehensive, consistent substantive rules.

Conclusion

The development of detailed privacy guidelines was supposed to be a predicate for development of the Information Sharing Environment. Moving forward with the ISE on the basis of the guidelines issued in December 2006 poses a serious risk to privacy and national security.

The issuance of these guidelines should be the beginning of a process that would take the hard issues – such as data accuracy, entity resolution or watch list fidelity, and auditing -- and develop more detailed guidance, leading to a set of accompanying appendices or directives. The ISE guidelines, as a framework, contemplate that process, but so far, the Administration has not indicated whether that process has begun; there is no indication it will involve public consultation.

In its third report, the Markle Task Force stressed that guidelines such as these will have to be developed incrementally. The Markle Task Force called for careful monitoring and oversight of the implementation and actual uses of the Information Sharing Environment. Specifically, the Task Force said,

> "In an area this complex and dynamic and so affected by evolving threats and rapidly changing technologies, the guidelines should be revisited at regular intervals to determine what is working, what is not, what needs to be changed or improved. There inevitably will be ambiguities or unanswered questions. These should be addressed explicitly, not ignored or exploited to avoid the laws' requirements."

CDT fully appreciates how difficult it is to define a set of standards that work across a range of agencies and situations. (In some areas, like auditing and security, the challenge is choosing among a welter of existing industry and government standards.) CDT hasn't come up with such a set of detailed guidelines either. However, CDT remains committed to working with the Administration to draft the kind of specific guidelines contemplated by Section 1016 of the IRTPA.

For more information, contact Jim Dempsey, (202) 365-8026, jdempsey@cdt.org