CIVIL RIGHTS AND CIVIL LIBERTIES PROTECTION

GUIDANCE

Requirement

The Information Sharing Environment (ISE) Privacy Guidelines, at Section 1(b), state that they "apply to information about United States citizens and lawful permanent residents that is subject to information privacy or *other legal protections* under the Constitution and Federal laws of the United States ('protected information')." (Emphasis added.) Section 2 of the ISE Privacy Guidelines, entitled "Compliance with Laws," states as follows:

a. *General*. In the development and use of the ISE, all agencies shall, without exception, comply with the Constitution and all applicable laws and Executive Orders relating to protected information.

b. *Rules Assessment*. Each agency shall implement an ongoing process for identifying and assessing the laws, Executive Orders, policies, and procedures that apply to the protected information that it will make available or access through the ISE. Each agency shall identify, document, and comply with any legal restrictions applicable to such information. Each agency shall adopt internal policies and procedures requiring it to:

   (i) Only seek or retain protected information that it is legally permissible for the agency to seek or retain under the laws, regulations, policies, and executive orders applicable to the agency; and

   (ii) Ensure that the protected information that the agency makes available through the ISE has been lawfully obtained by the agency and may be lawfully made available through the ISE.

Purpose

This document does not create new or modify existing policy but, rather, provides guidance interpreting the above ISE Privacy Guidelines requirements and outlines possible methods or "best practices" to assist agencies in implementing this requirement. This guidance will be supplemented as the ISE matures and other technological recommendations are implemented.

General

As envisioned by the Intelligence Reform and Terrorism Prevention Act and stated in Homeland Security Presidential Directives 6 and 11, it is "the policy of the United States Government to share terrorism information to the full extent permitted by law" to support a wide range of prevention and disruption activities across the federal, state, local, territorial, tribal, foreign government, and private sector spectrum in a manner consistent with the provisions of the Constitution and applicable laws, including those protecting the rights of all Americans. The

drafters of the ISE Privacy Guidelines recognized the importance of ensuring that ISE participants protect civil rights and civil liberties (CR/CL) (as well as privacy rights) in the ISE by developing appropriate policies and procedures. This Guidance paper is designed to serve as a vehicle to assist agencies in identifying the range of potential CR/CL issues that may arise in the ISE, provide recommendations to ISE participants regarding the manner in which they may address these issues through the development of ISE CR/CL policies and procedures, and discuss the legal basis for the recommendations. This will be especially important in developing a common understanding among the various parties that are expected to be ISE participants now and into the future.

By definition, the ISE is an approach that facilitates the sharing of terrorism-related information and does not prescribe rules or standards for the initial collection (acquisition) of protected information. However, any information shared in the ISE must have been lawfully collected by the acquiring agency. Nevertheless, the manner and the purpose for which information is collected, retained, and used by ISE participants may impact individual civil rights and civil liberties. Therefore, when developing policies and procedures governing ISE operation, participating agencies should ensure that civil rights and civil liberties are protected.

This Guidance is not meant to cover every possible CR/CL issue that may arise in the ISE. ISE participants are required to produce a written ISE privacy protection policy and are strongly encouraged to have policies and procedures that protect civil rights and civil liberties, consistent with mission requirements and tailored to the agency. Because there are some issues that will be common to many ISE participants, possible approaches to those issues are addressed in this Guidance.

This Guidance will not address individual states' CR/CL laws and state constitutional limitations (which in many cases may impose different and sometimes higher standards than federal laws and the U.S. Constitution). In developing their policies and procedures for sharing information in the ISE, state, local, and tribal entities should consult their respective legal counsels or privacy and civil liberties officers to ensure consideration of such limitations when sharing, receiving, and using protected information.

Core Elements

Agency civil rights and civil liberties staff should address the following core elements in each agency's ISE privacy protection policy:

a. A description of the existing agency legal and policy framework for the protection of CR/CL.

b. A description of policies, procedures, and personnel dedicated to identifying and addressing CR/CL issues pertaining to information acquisition, access, retention, production, use, management, and sharing.

c. A description of policies and procedures (as needed) developed and implemented for protecting CR/CL in the ISE that are not otherwise covered by existing policies and procedures.

Additional Considerations

a. Identify record-keeping practices and objectives that will ensure protection of CR/CL in the ISE.

b. Identify training needs for agency staff to protect CR/CL in the ISE.

BACKGROUND AND COMMENTARY[1]

Background and Purpose

This Background and Commentary will consider how ISE participants' information collection and subsequent use and sharing activities may implicate a person's civil rights and civil liberties (CR/CL). This analysis will begin with definitions of the key terms *civil rights* and *civil liberties* and explore what steps may be needed to protect federal statutory and constitutional rights while simultaneously enhancing information sharing to combat terrorism. It will also provide guidance on and examples of common CR/CL issues that might be encountered by both federal and state, local, and tribal (SLT) ISE participants.

Understanding the Terms—Civil Rights and Civil Liberties

Although the full scope of the terms *civil rights* and *civil liberties* is subject to debate, participants in the U.S. Department of Justice's Global Justice Information Sharing Initiative have defined the term *civil liberties* as follows:

> The term *civil liberties* refers to fundamental individual rights such as freedom of speech, press, or religion; due process of law; and other limitations on the power of the government to restrain or dictate the actions of individuals. They are the freedoms that are guaranteed by the Bill of Rights—the first ten Amendments—to the Constitution of the United States. Civil liberties offer protection to individuals from improper government action and arbitrary governmental interference….[2]

For purposes of this paper, the term *civil liberties* also includes any rights and privileges not specifically delegated to the federal government by the people. This includes common law rights and "unenumerated rights" derived from a general presumption of freedom of individual action (i.e., action that is permissible unless expressly prohibited by law). Influential framer of the Constitution, Alexander Hamilton, believed these rights did not need to be expressly protected by the Bill of Rights because they were so self-evident that they did not need to be addressed in detail.[3] The general concept of individual liberty and the limitations on the federal government's powers that were expressly stated in the Constitution ("enumerated powers") were recognized in the Ninth Amendment, which provides that the people retain rights beyond those specifically protected by the Constitution. When evaluating the impact of the ISE on civil liberties, it is important to keep in mind the legal and cultural importance of civil liberties in American life.
For purposes of this paper:

---

[1] The Background and Commentary section is provided as a resource concerning the general principles applicable to each ISE Privacy Guidelines requirement addressed. This section neither establishes policy under the ISE nor is binding on any department or agency participating in the ISE. It is not a binding interpretation of law, regulation, or policy.

[2] *National Criminal Intelligence Sharing Plan* (NCISP), p. 5. This definition was also adopted in the U.S. Department of Justice's Global Justice Information Sharing Initiative, *Privacy, Civil Rights, and Civil Liberties: Policy and Templates for Justice Information Systems*, February 2008, at p. 2, http://www.it.ojp.gov/documents/Privacy_Civil_Rights_and_Civil_Liberties_Policy_Templates.pdf.

[3] Alexander Hamilton, "Federalist No. 84," in *The Federalist Papers*, at http://www.constitution.org/fed/federa84.htm.

> The term *civil rights* refers to those rights and privileges of citizenship and equal protection that the state is constitutionally bound to guarantee all citizens regardless of race, religion, sex, or other characteristics unrelated to the worth of the individual. Protection of civil rights imposes an affirmative obligation upon government to promote equal protection under the law. These civil rights to personal liberty are guaranteed to all United States citizens by the Thirteenth and Fourteenth Amendments and by acts of Congress. Generally, the term *civil rights* involves positive (or affirmative) government action to protect against infringement, while the term *civil liberties* involves restrictions on government.[4]

How Civil Rights and Civil Liberties Issues Might Arise in the ISE

As noted above, CR/CL issues commonly arise in the acquisition of information (e.g., illegal search) and in its retention or use for unlawful or improper purposes (e.g., collection of First Amendment information that is not linked to criminal or national security activity). However, dissemination of information through the ISE is also a potential source of CR/CL violations as described below. Agencies should be mindful of these risks and seek to limit potential adverse consequences caused by the sharing of such information. Agencies should also be aware they may be subject to court order or agency policy requiring them to expunge or redact illegally or improperly acquired or retained information.

If information acquired in the ISE is not properly vetted and protected and its proper use controlled, then its dissemination to ISE partners may affect the CR/CL of individuals identified in that information. Information shared in the ISE includes terrorism information, homeland security information, and law enforcement information ("terrorism-related information").[5] Given the national imperative to share terrorism-related information quickly and broadly, there may be times when such information is later determined to be inaccurate, incomplete, untimely, or irrelevant. As a result, its dissemination may contribute to an agency's action that violates CR/CL and, the wider the distribution, the greater the risk of harm. Individuals identified or misidentified in the information may be subject to adverse action from a government agency or private sector entity, which disrupts their lives.

To examine in more detail how ISE sharing may implicate CR/CL, it may be helpful at this point to describe the primary liberties at issue under the constitutional provisions that preserve them.

[4] This is a modified version of the definition contained in the *National Criminal Intelligence Sharing Plan* (NCISP), pp. 5–6.

[5] Definitions for these terms can be found in the *Privacy and Civil Liberties Implementation Guide for the Information Sharing Environment* (September 2007).

First Amendment

The First Amendment prohibits Congress from passing any law that prohibits the free exercise of religion or abridges freedom of speech, freedom of the press, the right of the people to assemble peaceably, or the right to petition the government for redress of grievances. The Supreme Court and the inferior courts have made it clear that this prohibition extends beyond legislation and includes the official acts of government officials, including the acts of agencies participating in the ISE. Although the courts have approved restrictions that limit the exercise of these rights as to time, manner, and place, any government act that has the effect of infringing any of these freedoms, absent a valid law enforcement or other mission-related purpose, is prohibited.

Allegations of First Amendment violations usually arise from direct contact between persons exercising those rights and law enforcement or regulatory authorities. However, sharing information through the ISE concerning the exercise of First Amendment rights could give rise to such a claim as well. If, for example, information is collected by an ISE participating agency identifying persons who participate in an antiwar protest group that appears to pose no threat to the national security, the mere act of sharing that information in the ISE, absent a legitimate law enforcement or national security purpose, may violate the First Amendment rights of those protestors. As another example, an agency collects a membership list of a religious or political organization that poses no national security or criminal threat. If the agency shares that information, the affected organization could reasonably claim that its First Amendment rights had been violated where the public disclosure of the information results in public derision or leads to regulatory restrictions that result in a significant drop in membership.

The foregoing is not intended to suggest that each dissemination in these examples was unlawful or unjustified. It does suggest, however, that because First Amendment violations can occur as a result of sharing information, ISE participating agencies should have explicit policies that prohibit the sharing of information in the ISE based solely on the exercise of rights guaranteed by the First Amendment and should require clear documentation of a valid mission purpose whenever information affecting these rights is shared in the ISE.[6]

Fourth Amendment

As a general rule, courts have held that dissemination of information from one federal agency to another does not implicate rights under the Fourth Amendment because the dissemination itself is neither a "search" nor a "seizure."[7] There are, however, two significant potential ramifications resulting from the sharing of protected information in the ISE that could affect an individual's rights under the Fourth Amendment. ISE participants should be aware of these issues when formulating information sharing policies and procedures.

[6] Subsection (e)(7) of the Privacy Act of 1974 is an example of a federal law that expressly limits the maintenance of records regarding the exercise of First Amendment rights, providing that: "Each agency that maintains a system of records shall…(7) maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity…."

[7] *See Jabara v. Webster*, 691 F.2d 272 (6th Cir. 1982), *cert. denied*, 464 U.S. 863 (1983).

First, sharing information about an individual that is subsequently determined to be materially inaccurate or misleading may indirectly implicate that individual's Fourth Amendment rights if he or she is seized or his or her property is searched as a consequence of the erroneous information. This could occur, for example, when an individual is detained based on erroneous information or misidentification (e.g., at an airport or pulled over by a police officer on the public highways). For this reason, agencies that share information should make reasonable efforts to ensure that the information is accurate, complete, timely, and relevant prior to dissemination.[8] In those instances where it is later determined that the information is erroneous, agencies that share information should employ timely notice and corrective procedures.

Second, if it is determined that information that has been shared was acquired in violation of an individual's rights under the Fourth Amendment, the information may become the subject of an expungement order which, depending on the jurisdiction of the court issuing the order and the contents of the order, could apply broadly throughout the ISE (as discussed above). Such a determination could result from a suppression hearing in a criminal trial or an agency's internal response to a complaint from the affected party. Information may also be determined to be erroneous or deficient, either from the time collected or due to changing factual circumstances. In any case, the aggrieved party may obtain an order to have the information expunged from agency records, and therefore, agencies may be under a legal or policy-driven obligation to provide notice of this consequence to other agencies with which the information has been shared. Agencies are encouraged to have in place robust data quality measures to facilitate compliance with court orders and to correct data errors when detected.

Fifth and Fourteenth Amendments—Due Process

The due process rights conferred by the Fifth and Fourteenth Amendments could be implicated if erroneous information about an individual is shared in the ISE and, as a result, leads to the denial of that individual's entitlements, benefits, status, privileges, or rights granted by statute. This result may occur wherever a background check or other investigation is conducted prior to granting some benefit to the individual. Due process concerns may arise when the individual is not allowed to challenge the facts underlying the adverse action. This may occur when an individual is denied the freedom to travel or when the individual loses or is denied employment by an employer who receives and then acts upon the erroneous information. The process that is due such an individual may include the right to access information that may be used to his or her detriment and the right to request correction of that information if the individual believes the information is not accurate, relevant, timely, or complete. (See Footnote 11.) In those situations where information access is not available, an after-the-fact redress process, as discussed in the following section, may be necessary (See ISE Privacy Guideline, Section 8, and Redress Guidance, Privacy and Civil Liberties Implementation Manual, Key Issues Guidance at www.ise.gov). Due process issues involving the ISE may also arise when end users, relying on information shared in the ISE, deny individual rights.

[8] Subsection (e)(6) of the Privacy Act of 1974 requires that "Each agency that maintains a system of records shall …(6) prior to disseminating any record about an individual to any person other than an agency, unless the dissemination is made pursuant to subsection (b)(2) [FOIA] of this section, make reasonable efforts to assure that such records are accurate, complete, timely, and relevant for agency purposes…." It is significant that this is one Privacy Act provision from which an agency may not exempt a system of records.

Federal agencies sharing information that could be used to deny constitutional rights should not rely on access and correction procedures as the only protective mechanism for minimizing the risk that action may be taken against persons based on inaccurate information. Redress should be part of the solution as a matter of policy—this is consistent with other rights, protections, and strategies that reduce agency liability. This is particularly true in the ISE, where many ISE participants are not subject to certain federal statutory disclosure requirements. Some information, for instance, may be classified or otherwise exempt from disclosure and individuals' access to information about them, and correspondingly, their ability to contest the agency action will be severely limited.

If the quality of information shared in the ISE is not accurate or reliable, there is a risk that some individuals will mount broad challenges to security measures and information sharing activities. This may have a negative operational impact on ISE participants and end users. ISE participants are, therefore, encouraged to consider policies and procedures that define what reasonable efforts are appropriate to ensure that acquired information shared with other ISE participants is accurate, complete, timely, and relevant and to adopt redress procedures as discussed above.

Fourteenth Amendment—Equal Protection Under the Law

The Fourteenth Amendment provides that "No State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws." Under the Equal Protection Clause, it has been held that U.S. government employees and agencies are prohibited from engaging in invidious discrimination against individuals on the basis of race, ethnicity, national origin, or religious affiliation. This is further reflected and implemented for federal law enforcement in the U.S. Department of Justice's *Guidance Regarding the Use of Race by Federal Law Enforcement Agencies* (DOJ Guidance). The standard articulated in the DOJ Guidance (and one that has a well-established basis in case law) is that investigative and intelligence information collection activities must not be based *solely* on race, ethnicity, national origin, or religious affiliation. In the ISE context, sharing information about an individual solely because he or she is of a certain race, ethnicity, or national origin or practices a certain religion would violate that individual's constitutional right to equal protection. For this reason, agencies should consider adopting robust policies to ensure that information about individuals is collected for valid mission purposes (i.e., not solely due to those factors). Moreover, if it is later discovered that information was collected and subsequently retained solely on that basis, that it is not disseminated to other agencies in the ISE, and that if it has been disseminated, the originator should make reasonable efforts to ensure that recipients of the information are notified of the improper collection and delete or refrain from using the information. Given the complexity of equal protection law, agency personnel should seek legal guidance when questions relating to race, ethnicity, national origin, or religious affiliation, or related practices arise.

Investigations involving national security, race, ethnicity, national origin, or religious affiliation often provide links to individuals who pose terrorist threats. ISE participating agencies are urged to develop policies to ensure that information shared with other ISE participants that draws such a connection is well-founded and based on reasonable inferences.

Other Individual Rights Issues

Unenumerated Rights

As noted above, the concept of civil liberties is much broader than those freedoms specifically enumerated in the Constitution. It includes the general presumption of freedom of action and the commonly recognized rights protected by federal statutory law, common law, and state law. Civil liberties may include a right to travel, to seek and retain employment, privacy, nondiscrimination in housing, and many other rights and freedoms that people take for granted. Even when the inconvenience or constraint imposed on a person's activities does not amount to an infringement of constitutional rights, the sharing of inappropriate or inaccurate information in the ISE can have a consequential effect on an individual's unenumerated rights. For instance, when erroneous information is shared and subsequently relied on by end users, an individual's ability to travel or conduct lawful business may be impaired. Agencies participating in the ISE are urged to consider the potential unintended consequences on innocent individuals and to develop policies that minimize those consequences.

Statutory Rights—Personal Information Held by Third Parties

Certain types of information are lawfully retained by third parties and are regulated by statutory schemes that prohibit unauthorized disclosure. These include financial records subject to the Right to Financial Privacy Act, 12 U.S.C. § 3401; credit information subject to the Fair Credit Reporting Act, 15 U.S.C. § 1681; tax information subject to the Internal Revenue Code, 26 U.S.C. § 6300; telephone and Internet service records subject to the Electronic Communications Privacy Act, 18 U.S.C. § 2701; school records subject to the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g; and medical records subject to federal regulations issued pursuant to the Health Insurance Portability and Accountability Act, 45 C.F.R. Parts 160, 164. Although the Supreme Court has made it clear that there is no reasonable expectation of privacy in information disclosed to third parties,[9] federal law restricts the U.S. government's and some other governmental and private entities' access to, and use and disclosure of such information. ISE participating agencies are encouraged to develop policies that treat this information as sensitive and to protect it from unlawful disclosure. Practices commonly used to safeguard sensitive information include physically or electronically securing sensitive information, limiting physical access to such information to those with a need to know the information, sound personnel security practices, and audit capability and implementation.

Building In Corrective Measures That Apply Specifically to Civil Rights and Civil Liberties

Data Quality

One of the most important steps that should be taken by participants in the ISE to protect civil rights and civil liberties is the implementation of robust data quality policies and practices. Data quality matters because erroneous data can negatively affect individuals who are subsequently investigated, stopped, or seized by law enforcement agencies acting in reliance on flawed data.

[9] *See United States v. Miller*, 425 U.S. 435 (1976).

Section 5 of the ISE Privacy Guidelines establishes three requirements to ensure data quality. First, federal agency ISE participants must implement policies and procedures designed to ensure the accuracy of data prior to sharing it in the ISE. Second, when protected information is identified that may be erroneous, the agency must inform the originating agency of the potential error. Third, participants must, consistent with legal authorities and mission requirements, adopt policies and procedures that protect individuals' personally identifiable information. These include (1) steps to ensure that data-merging operations do not incorrectly merge one individual's data into another person's information, (2) procedures for timely investigation and correction of alleged errors and deficiencies, and (3) retaining protected information only so long as it is relevant and timely. In this instance, civil liberties interests are squarely aligned with operational interests because improving the integrity and quality of data relied upon by end users will ultimately improve their operational effectiveness.

Redress

ISE participants are required to provide some form of redress, in a manner that is compatible with legal authorities and mission requirements, to persons whose CR/CL may have been affected in the ISE. As the term is used in the ISE Privacy Guidelines, *redress* requires that each ISE participant develop and implement procedures to address complaints regarding protected information shared in the ISE. This includes not only complaints related to privacy rights (one of many civil liberties) but also complaints involving other CR/CL protected by the U.S. Constitution or other law. Potential requests for redress regarding important CR/CL issues might include complaints related to the failure to remove information from the ISE that has been expunged by a court of law or is determined to have been collected in violation of law or the U.S. (or a state) Constitution. It may at times also include requests for redress when erroneous information results in impairment of an individual's ability to travel or conduct business. To the extent that a redress complaint is related to a terrorist watchlist issue, the Memorandum of Understanding on Terrorist Watchlist Redress Procedures (executed September 2007) would apply for those agencies that are signatories to that memorandum of understanding. Redress Guidance for information privacy and CR/CL issues has been developed by the ISE Privacy Guidelines Committee.[10]

Expungement

If administrative measures such as redress do not prove satisfactory, a complainant may take his or her case to court, and the agency may find itself in receipt of a judicial order to expunge the records in question. Most states allow individuals who have not been convicted of a crime to have arrest records expunged under certain conditions. Some states also permit offenders to apply for expungement (a.k.a. erasure, destruction, sealing, setting aside, expunction, and purging) of certain criminal offense records after the expiration of a specific amount of time following the completion of their sentences. Grants of clemency and pardons may have similar effects on the individual's criminal or arrest records.

[10] ISE Redress Guidance is provided in Key Issues Guidance of the Privacy and Civil Liberties Implementation Manual (PM-ISE, 2007).

Federal agencies may honor state court orders for expungement (and vice versa).[11] For example, it is the practice of the FBI's Criminal Justice Information Services Center (the entity that operates the National Crime Information Center [NCIC]) to honor state court orders or other authorized requests to expunge records. If, however, an ISE participant receives arrest record information from a state (and incorporates it in a terrorism-related information database) and a court in that state later expunges the record, ISE participants should have procedures in place for determining how federal agency recipients of the information will be notified of the order, ensure the expungement of the information from its records and, in turn, notify any other ISE participants with which it has shared the information.

Under federal law, there is a statutory remedy (18 U.S.C. § 3607(c)) for expungement of the disposition records of an individual found guilty of an offense under Section 404 of the Controlled Substances Act, 21 U.S.C. § 844. Although this is the only federal statute that expressly addresses expungement, federal judges exercising their equitable powers often grant this relief to individuals who have been arrested and later found to be innocent of any crime, provided they can also show that they have suffered significant adverse consequences because of the criminal record. In most jurisdictions, expungement is not limited to situations in which a constitutional violation or arrest was the result of unlawful action. *See United States v. Paul Van Wagner,* 746 F. Supp. 619 (E.D. Va. 1990). It is appropriate any time "the dangers of unwarranted adverse consequences to the individual outweigh the public interest in maintenance of the records." (*Diamond v. United States,* 649 F.2d 496, 499 (7th Cir. 1981)). In order to ensure compliance with a federal court order expunging information shared in the ISE, agency information dissemination would need to be tracked (via manual log or an electronic audit trail, metatagging, or similar mechanism) in order to ensure compliance with the expungement order.

[11] The Privacy Act of 1974, 5 U.S.C. § 552a, provides in Subsection (d) for individuals to have access to records about them contained in a system of records and to request amendment (correction) of such records that are not accurate, relevant, timely, or complete.

Resources and Tools

Federal Agencies That Address CR/CL Issues (this list is not exhaustive)

U.S. Commission of Civil Rights, http://www.usccr.gov/

Office of the Director of National Intelligence, Civil Liberties Protection Officer,
http://www.dni.gov/aboutODNI/organization/CivilLiberties.htm

U.S. Department of Justice, Privacy and Civil Liberties Office
http://www.usdoj.gov/pclo/index.html

U.S. Department of Justice, Civil Rights Division,
http://www.usdoj.gov/crt/crt-home.html

U.S. Department of Homeland Security, Office for Civil Rights and Civil Liberties,
http://www.dhs.gov/xabout/structure/editorial_0371.shtm

U.S. Department of State, Office of Civil Rights, http://www.state.gov/s/ocr/

U.S. Department of Agriculture, Director, Office of Adjudication and Compliance,
http://www.ascr.usda.gov/complaint_filing_program.html

U.S. Department of Health and Human Services, Office for Civil Rights,
http://www.hhs.gov/ocr/howtofile.pdf

U.S. Department of Transportation, Departmental Office of Civil Rights,
http://www.dotcr.ost.dot.gov/

U.S. Department of Labor, Civil Rights Center,
http://www.dol.gov/oasam/programs/crc/crcwelcome.htm

U. S. Department of the Treasury, Office of Civil Rights and Diversity,
http://www.treas.gov/offices/management/hr/oeod/civil-rights/

U.S. Commission on Civil Rights has six regional offices. Contact information for each office can be found at http://www.usccr.gov/regofc/rondx.htm

U. S. Department of Commerce, Office of Civil Rights,
http://www.osec.doc.gov/ocr/contact.html

U.S. Department of Education, Office of Civil Rights,
http://www.ed.gov/about/offices/list/ocr/index.html?src=oc

U. S. Department of the Interior, Office of Civil Rights,
http://www.doi.gov/diversity/

U.S. Environmental Protection Agency (EPA), Office of Civil Rights (OCR),
http://epa.gov/civilrights/index.html

Federal Aviation Administration, Office of Civil Rights,
http://www.faa.gov/about/office_org/headquarters_offices/acr/

General Services Administration, Office of Civil Rights,
http://www.gsa.gov/Portal/gsa/ep/contentView.do?contentType=GSA_OVERVIEW&contentId=11553

Key Federal CR/CL Statutes, Regulations, and Policies

Confidentiality of Identifiable Research and Statistical Information, 28 CFR Part 22,
http://ojjdp.ncjrs.org/funding/confidentiality.pdf

Criminal Intelligence Systems Operating Policies, 28 CFR Part 23,
http://www.iir.com/28cfr/pdf/ExecOrder12291_28CFRPart23.pdf

Criminal Justice Information Systems, 28 CFR Part 20, http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&tpl=/ecfrbrowse/Title28/28cfr20_main_02.tpl

Privacy Act of 1974, 5 U.S.C. § 552a and Computer Matching and Privacy Act of 1988, 5 U.S.C. § 552a(b),
http://www.usdoj.gov/oip/privstat.htm

Executive Order 12333,
http://www.archives.gov/federal-register/codification/executive-order/12333.html

USA PATRIOT Act, Pub. L. 107–56,
http://fl1.findlaw.com/news.findlaw.com/cnn/docs/terrorism/hr3162.pdf

USA PATRIOT Act, Pub. L. 109–177,
http://www.usdoj.gov/olp/pdf/usa_patriot_improvement_and_reauthorization_act.pdf

U.S. Department of Justice Guidance on the Use of Race by Federal Law Enforcement Agencies; Religious Profiling,
http://www.usdoj.gov/crt/split/documents/guidance_on_race.htm

Memorandum of Understanding on Terrorist Watchlist Redress Procedures,
http://www.fbi.gov/terrorinfo/counterrorism/redress_mou.pdf

State, Local, and Tribal Laws and Regulations

It is important for state, local, and tribal governments to recognize that their own laws and regulations may impose higher standards regarding the protection of privacy and other civil rights and civil liberties than current federal law. It may be useful within the ISE to share

information on best state practices that are consistent with federal law and which advance federal CR/CL interests concurrently.

Case Law on Dissemination of Personal Information

The following briefly summarizes constitutional and statutory treatment of civil claims arising from the dissemination of personal information by government agencies. This summary is intended to serve as a tool to assist agencies in identifying the types of civil liberties issues that may arise in the Information Sharing Environment (ISE). Its only purpose is to stimulate ideas regarding these issues and is not intended to be an in-depth coverage of the relevant subject areas or the case law.

The Privacy Act of 1974, at 5 U.S.C. § 552a (e)(6), prohibits the dissemination outside of the federal government of inaccurate or misleading information to any person and provides no authority for an agency to exempt itself from this prohibition.[12] While adverse characterization of a group in agency records is not actionable absent a showing of harm, some courts have found that federal law enforcement agencies have a duty to take reasonable steps to ensure the accuracy of records they disseminate. *See New Alliance Party v. FBI*, 858 F. Supp. 425 (S.D.N.Y. 1994) (describing national political party as a "cult"). For example, in a case decided before the Privacy Act of 1974 became law, the court in *Tarlton v. Saxbe*, 507 F.2d 1116 (D.C. Cir. 1974) found that the FBI's failure to exercise a reasonable standard of care with respect to the accuracy of its records may implicate due process rights.

Similarly, dissemination of adverse information to local law enforcement or to the media that harms a group's reputation and interferes with its ability to recruit new members or raise funds may violate the group members' rights to speech, assembly, and to petition the government under the First Amendment. *See Philadelphia Yearly Meeting of the Religious Society of Friends v. Tate*, 519 F.2d 1335 (3d Cir. 1975); *Socialist Workers Party v. Attorney General*, 642 F. Supp. 1357 (S.D.N.Y. 1986); and *Alliance to End Repression v. City of Chicago*, 407 F. Supp. 115 (N.D. Ill. 1975). In addition, dissemination of an employee's personal information concerning the exercise of First Amendment rights to his employer that leads to termination may be actionable. *See Clark v. Library of Congress*, 750 F.2d 89, 94 (D.C. Cir. 1984) (protecting government employees' right to lawfully associate without the "potential for subtle coercion of the individual to abandon his controversial beliefs or associations"); *Paton v. La Prade*, 524 F.2d 862, 869–71 (3d Cir. 1975) (in case involving a First Amendment challenge to the collection and maintenance of records, court denied motion for summary judgment on mere potential that investigative record—in which student was cleared of wrongdoing—would lead to difficulty landing a job). Likewise, dissemination by U.S. Department of Defense investigators of records showing political activity by employees to their employers at an overseas military base was

[12] Subsection (e)(6) of the Privacy Act of 1974, 5 U.S.C. § 552a, expressly requires that: "Each agency that maintains a system of records shall…(6) prior to disseminating any record about an individual to any person other than an agency, unless the dissemination is made pursuant to subsection (b)(2) [FOIA] of this section, [the agency must] make reasonable efforts to assure that such records are accurate, complete, timely, and relevant for agency purposes…."

found to violate the employees' First Amendment rights. (*Berlin Democratic Club v. Rumsfeld*, 410 F. Supp. 144 (D.C. Cir. 1976)).

Finally, in *Hobson v. Wilson*, 737 F.2d 1 (D.C. Cir. 1984), the Circuit Court for the District of Columbia found expungement to be a proper remedy for ensuring First Amendment protection when personal information was collected and maintained in FBI records in violation of the Privacy Act of 1974, notwithstanding the FBI's argument that it needed to retain the records for present and future litigation defense purposes. In *Doe v. Webster*, 606 F.2d 1226 (D.C. Cir. 1979), to remove the mere possibility of inappropriate dissemination, the court directed the FBI to physically remove the record of a juvenile offender for an offense that a court had set aside under the Federal Youth Corrections Act and to respond in the negative to any and all inquiries concerning the set-aside conviction.

This case law summary will be updated, as necessary, to inform agencies of developments that may affect information sharing in the ISE.

Template for Civil Liberties Policy Development

This document is under development by the DHS Office of Civil Rights and Civil Liberties and will be included as a resource for agencies participating in the ISE when it is completed.