

Balancing Privacy & Security: The Role of Privacy and Civil Liberties in the Information Sharing Environment

IAPP Conference 2010



*Samuel P. Jenkins
Director for Privacy, Defense Privacy & Civil Liberties Office,
U.S. Department of Defense*



*Alexander Joel
Civil Liberties Protection Officer,
Office of Director of National Intelligence*



About Our Organizations



DoD, Defense Privacy & Civil Liberties Office (DPCLO)

- DPCLO located within Office of the Secretary of Defense
- Oversees programs and develops policy to protect privacy and civil liberties of more than 2.3 million U.S. Military service members (Active, Reserve, and Guard), 700,000 Civilian employees, military installations, hospitals, and schools, as well as the private citizens and organizations with whom DOD interacts
- Defense Privacy Office established in 1970s; currently standing up and conjoining a civil liberties functional area pursuant to Section 803 of the Implementing Recommendations of the 9/11 Commission Act



ODNI, Civil Liberties Protection Officer

- Established by Intelligence Reform and Terrorism Prevention Act of 2004, and stood up in 2005 to oversee coordination and integration of Intelligence Community (IC) personnel, expertise, and capabilities
- IC includes such agencies as the CIA, FBI, National Security Agency (NSA), National Reconnaissance Office (NRO), and National Geospatial Intelligence Agency (NGA)
- Ensures the protection of civil liberties in development and implementation of an Information Sharing Environment construct.



Overview



- Challenge of National Security in a Nation Built on Freedom
- Implications of Shifting from a “Need to Know” Philosophy to a “Need to Share” Approach
- Agency-Level Privacy Protections as a Safeguard & Support Structure for the ISE
- Balancing National Security with Respect for Privacy and Civil Liberties



Key Points of Focus



- Information sharing is an imperative to maintain our nation's security, but to be successful, it will require both a renewed emphasis on existing vehicles and a shift in long-held intelligence practices.
- With adherence to time-tested fair information practice principles and respect for constitutionally guaranteed civil liberties, non-intelligence agencies' and private sector programs can help the IC conserve valuable human and technological resources.
- Non-intelligence agencies' adherence to privacy and civil liberties engenders trust in the government's deliberative processes, and builds faith in the ISE to conduct lawful and legitimate intelligence analysis.
- Once non-intelligence agencies share information within the ISE, it is incumbent upon the IC to institute its own institutional protections that maintain a proper balance between intelligence practices and individuals' liberty interests.



The Challenge of National Security



"Respect my privacy!!!"

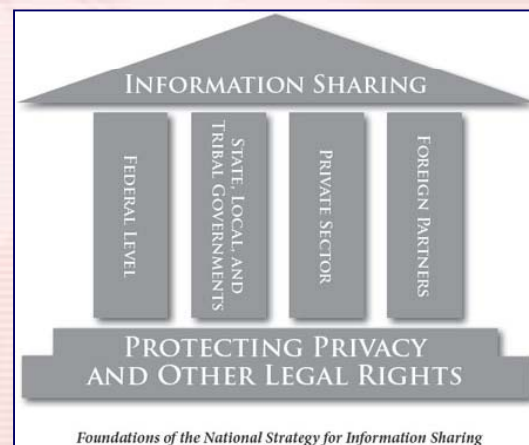
"Keep me safe!!!"



Information Sharing Environment



- **Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004 – Sec. 1016(b)(1)(A):** “The President shall create an information sharing environment for the sharing of terrorism information in a manner that is consistent with national security and with applicable legal standards relating to privacy and civil liberties.”
- **Executive Order 13388, Further Strengthening the Sharing of Terrorism Information to Protect Americans, October 25, 2005 – Sec. 1(b):** “To the maximum extent consistent with applicable law, agencies shall, in the design and use of information systems and in the dissemination of information among agencies...protect the freedom, information privacy and other legal rights of Americans in the conduct of activities [relating to the detection, prevention, disruption, preemption, and mitigation of the effects of terrorist activities, including the sharing of terrorism information among agencies and appropriate State, local, and tribal government authorities.”





Common Privacy Concerns



What information is being shared?

Can I see my information before they share it?

With whom is that information being shared?

What are they doing with my information?



Using Existing Vehicles to Ensure Early Safeguards within the ISE



- **U.S. Constitution**

- First Amendment prevents government interference with exercise of free speech, free assembly, free religious exercise, among others
- Recording of protected activity could result in “chilling effect” and violate civil liberties, Privacy Act, and agency requirements.

- **Privacy Act of 1974 (as amended), codified at 5 U.S.C. § 552a**

- Requires government agencies to show an individual any records kept on him or her
- Requires agencies to follow fair information practices when gathering and handling personal data
- Places restrictions on how agencies can share an individual's data with other people and agencies
- Lets individuals sue the government for violating its provisions

- **DoD Directive 5400.11, Defense Privacy Program**

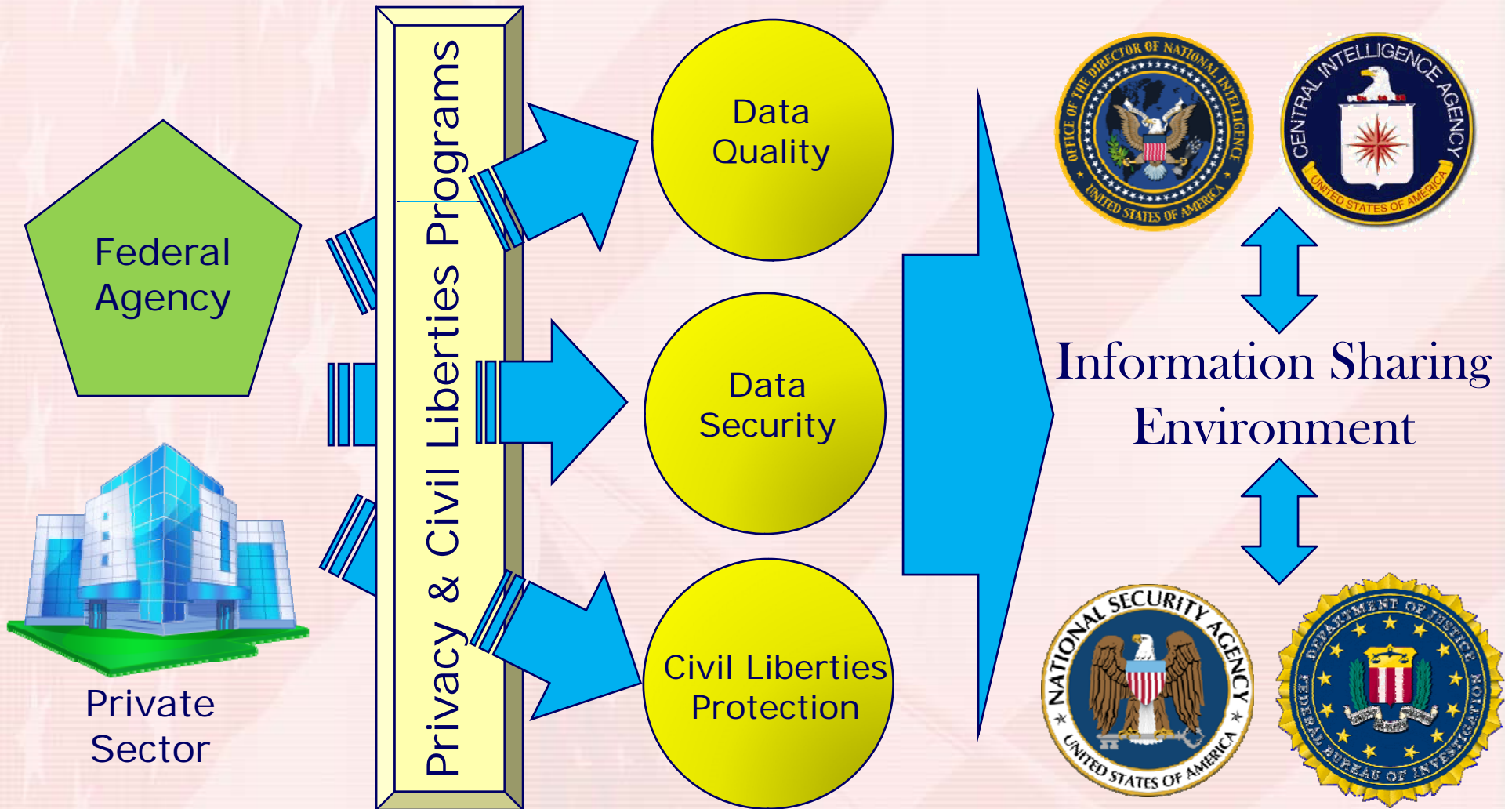
- Requires balancing of need to collect, maintain, use, or disseminate personal information about individuals with individual's right to be protected against unwarranted invasion of privacy
- Ensures checks for relevancy, timeliness, completeness, and accuracy
- Limits recording information relating to the exercise of First Amendment rights

- **ISE Privacy Guidelines**

- Protected information may be shared through the ISE only if it is terrorism information, homeland security information, or law enforcement information.
- Requires appropriate physical, technical, and administrative measures to safeguard protected information



Privacy Spheres of Influence





Fair Information Practice Principles



- The Fair Information Practice Principles will enhance **not only the privacy protection** of the ISE, **but also the ISE's effectiveness and functionality.**
- Strong privacy & civil liberties programs across government and private organizations can accomplish **two objectives**:
 - 1: Protect the Public
 - 2: Protect the Intelligence Community



Fair Information Practice Principles



Information Limitation

- Keep and collect only that information which is necessary
- Ensure that information shared is relevant and necessary

Data Quality

- Ensure data is accurate, up-to-date, and complete
- Provide a more clear and accurate picture to the IC when sharing information.



Fair Information Practice Principles



Accountability

- Identify an official responsible for each data collection to ensure its accuracy and protection
- Provide the IC with easily understood contacts for information requests.

Security

- Strong administrative, physical, and technical safeguards are essential to protect the public
- Data loss can compromise government secrets and bolster criminals, terrorists, and other foreign powers



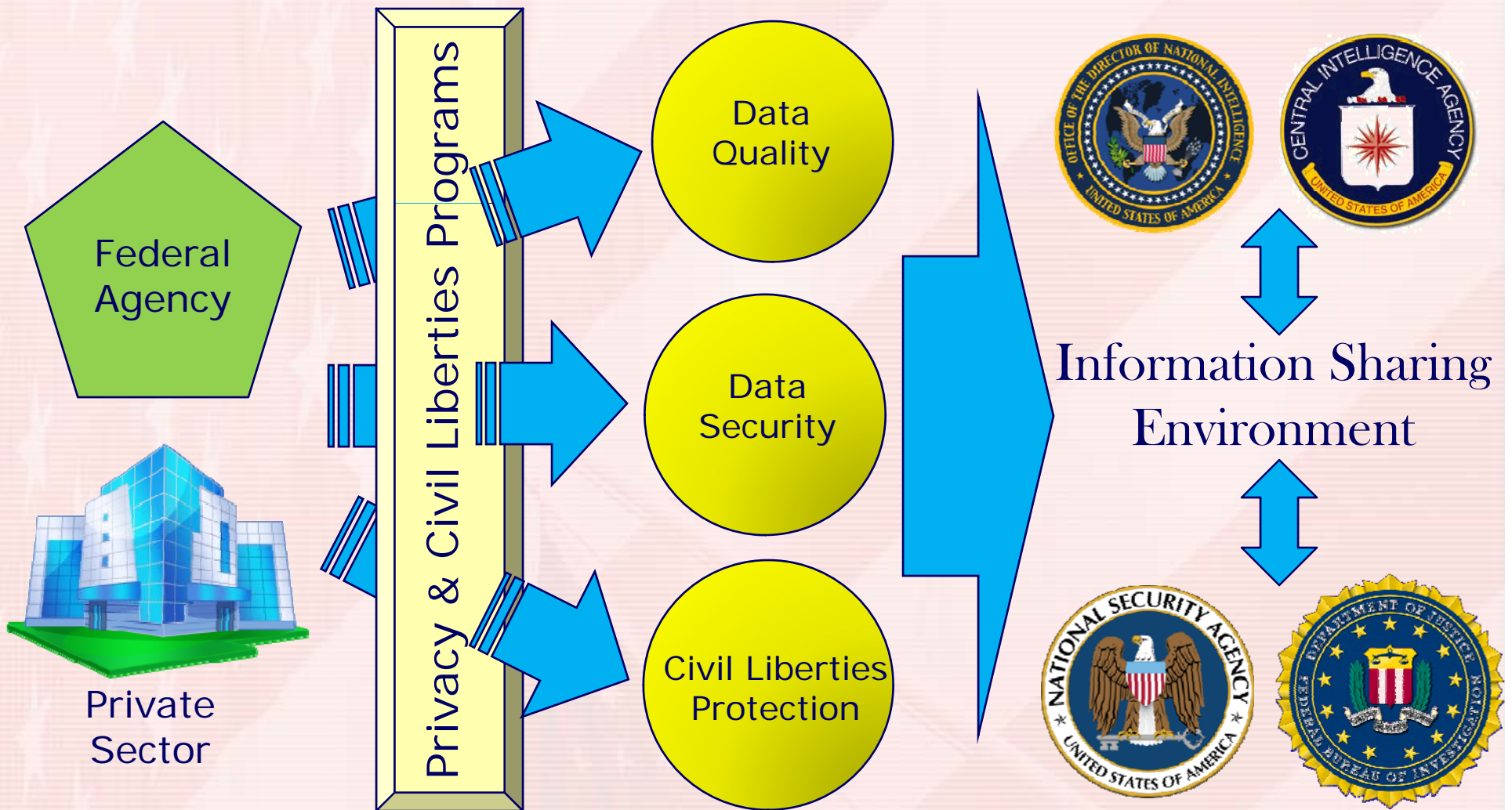
DoD Application of Pre-Sharing Safeguards



- **Increased Use of System of Record Notices (SORNs)**
 - Increased completion rate of public notices from 57% to 95% over the past year; over 1,300 DoD SORNS currently in existence
 - Creates greater transparency in records held on individuals
- **Implementation of Required Quarterly Reporting**
 - Previously, DoD Components reported only once per year
 - Quarterly reporting requires Components to conduct more regular reviews of policy, data, and systems
 - Supports Federal Information Sharing and Management Act reporting
- **Formalization of DoD Civil Liberties Program & Revision of DoD Privacy Regulations**
 - DoD Privacy Regulations will codify Fair Information Practice Principles
 - Increase and strengthen awareness of privacy and civil liberties policies
- **Conduct Privacy and Civil Liberties Impact Assessments**
 - Allows early detection of privacy and civil liberties implications of proposed policies, programs, or operations



Privacy Spheres of Influence



INSERT ALEX JOEL SLIDES

FOUO

15



Revisiting Key Points



- As the ISE facilitates a shift from “need-to-know” to “need-to-share”, each agency and private sector privacy and civil liberties program must renew its commitment to applying existing safeguards to the information it collects.
- The Fair Information Practice Principles provide a helpful roadmap for ensuring that our privacy and civil liberties programs are adequately preparing collected information for potential sharing within the ISE, if and when such an authorized need arises.
- By holding our respective privacy and civil liberties programs to a higher standard, we can strengthen the ISE’s ability to achieve the critical balance between privacy and national security.