Securing Our Borders:
Citizen Protection vs. Citizen Privacy Protection

Version 1.0
January 2006

For more information, please contact:

Lynn Ann Casey
Chief Executive Officer
Arc Aspicio LLC
3318 Lorcom Lane
Arlington, VA 22207

1.0 THE GLOBAL PRIVACY CHALLENGE

As governments globally increase the use of information to secure their borders following the attacks in the United States (U.S.), Madrid, and London, citizens are raising concerns over governmental use and storage of their personally identifiable information.

As new government programs seek to implement border security solutions, it is possible to protect the privacy of citizens' information while using information and intelligence to identify high-risk individuals. Security and privacy are not mutually exclusive. Border management programs dealing with the use and distribution of information must build privacy solutions internally from the beginning while effectively managing public perceptions externally. Chief Privacy Officers (CPOs) must work together with Chief Information Officers (CIOs) to conduct early and routine Privacy Impact Assessments (PIAs) to verify that the program accommodates current privacy laws, policy and unveils the need for the improvement and evolution of these privacy measures.

1.1 Using Information to Secure the Borders

Recent technology in the U.S. and Europe has enabled governments to secure borders in new ways. In the U.S. and the United Kingdom (U.K.), passports are being developed that will contain biometric identifiers to assure that the passport holder is legitimate. Fingerprint and facial recognition technology taken at the border are compared to the data on the passport. The Secure Flight program in the U.S was designed to replace the troubled CAPPS II program, which had been abandoned due to privacy concerns and scrutiny. It checks information sent to airlines pre-flight against a terrorist screening database.

US-VISIT is an entry/exit program that verifies the integrity of visitors coming to the U.S. using the visitor's biometrics – digital fingerscans – to match that the person at the U.S. port is the same person who received the visa. This type of identity matching helps United States Customs and Border Protection Officers make better admissibility decisions and ensures the overall integrity of the immigrations system. The U.K. is developing a similar program called e-Borders.

Global Challenges with Information Privacy in Securing Borders Worldwide

- Privacy viewed as a fundamental right versus an economic issue
- Tougher international security measures put individual privacy at risk
- Countries with strong privacy protection laws are apprehensive about exchanging information with less protective countries
- Lack of regulatory bodies for data protection (predominantly in the U.S.)
- Privacy rights not extended to visitors entering foreign countries

1.2 Citizen Privacy Considerations

The recent programs developed by the U.S. and the U.K. have been criticized by privacy watchdogs and citizens groups for not being protective enough over sensitive information. Electronic Privacy Information Center (EPIC) is opposed to the e-Borders and e-Passports programs, arguing that they can be used for more than simply tracking potential terrorists. EPIC has criticized Secure Flight for being too similar to the CAPPS II program and improperly flagging names.

1.3 Global Privacy Considerations

One of the main challenges in the current structure of privacy legislation around the world is the lack of compatibility among regulations for different countries. The incompatible laws in the U.S. and the E.U. have impeded travel and business practices in the past. The E.U. originally refused to allow U.S. airlines access to data on European travelers, and American businesses could not access information about European clients. These restrictions have since been lessened with regulation like Safe Harbor that allow data transfer between and U.S and the EU.

2.0 CHALLENGES IN IMPLEMENTING NEW SECURITY MEASURES WITHOUT COMPROMISING PRIVACY

While privacy protections and security measures are each seen as essential components of border management legislation, combining the two is often difficult and if not adequately addressed, may stifle the rapid implementation of new security programs.

Security and privacy are often considered in an either-or context: legislators believe that one cannot exist without the weakening of the other. Compatibility among different countries' privacy regulations has also been a problem. The U.S. suffers from a lack of adequate legislation. The laws in existence are often industry-specific, changing from business to business, instead of remaining relatively constant like those in other countries.

2.1 Challenges Associated with Global Privacy Law

Issues have frequently arisen when Europeans visit the U.S. In the past, weaker privacy protections in the U.S. have led to the withholding of European passenger data by the E.U., which argues that the U.S. laws endanger the privacy of the visitors.

Data collected in the E.U. and the U.S. undergo different processes. The E.U. requires that data be used only for its intended purpose and deleted quickly after use, and citizens must be informed of the purpose of the collection. The U.S. may hold on to most data indefinitely, it may use it for subsequent inquires other than the original purpose, and citizens are not required to know the status and use of their information.

Asia Pacific Economic Cooperation (APEC) drafted a Privacy Framework in October 2004 to serve as a guideline for member states when drafting their own privacy standards. Figure 1 below depicts global security programs and the privacy considerations that have the power to make the programs fail or succeed.

Security Solutions	Privacy Considerations	Example Programs
▪ Checking personally-identifiable information pre-flight	▪ ID theft ▪ Redress measures to deal with ID Theft ▪ Duration of data retention ▪ Accuracy of data ▪ Use of central data banks ▪ Central data bank security	▪ CAPPS II - U.S. ▪ Secure Flight - U.S. ▪ eBorders - U.K. ▪ Passenger Information System - Canada (PAXIS) ▪ Advanced Passenger Information System (APIS) - between U.S. and E.U.
▪ Collection of biometric information from certain travelers ▪ Fingerprint and/or facial analysis compared with data on passport and checked against terrorist watchlists (may include RFID)	▪ Violation of foreign privacy laws ▪ ID theft ▪ Profiling ▪ Central database repository	▪ eBorders - U.K. ▪ US-VISIT - U.S ▪ ePassports – Australia, Slovenia, Netherlands
▪ Implementing mandatory national ID cards that contain biometric information	▪ Discrimination based on demographic data ▪ Inaccuracy of biometric data leading to misidentification ▪ ID theft ▪ Redress measures to deal with ID Theft	▪ Australia ▪ Belgium ▪ China ▪ Estonia ▪ Finland ▪ Italy ▪ The Netherlands ▪ Portugal
▪ Effective exchange of information among member states of the E.U.	▪ Transfer of personal data ▪ Duration of data retention ▪ ID theft ▪ Redress measures to deal with ID Theft and watchlists	▪ Shengen Information System (SIS/SIS II) ▪ Visa Information System (VIS)

Figure 1. Security and Privacy. *Security initiatives should consider privacy in the earliest stages of planning to design and implement a successful program.*

3.0 CRITICAL SUCCESS FACTORS FOR DEVELOPING SECURITY SOLUTIONS THAT ACCOMMODATE PRIVACY

Learning from past failures like CAPPS II and implementing current privacy guidelines builds a strong and effective culture of privacy in new security initiatives allowing for the successful design, development and implementation of security programs.

3.1 Failure of CAPPS II

When security solutions incorporate privacy protections inadequately, it can often lead to the dissolution of the program in its entirety. A good example of such a program is the Computer Assisted Passenger Prescreening System (CAPPS II). CAPPS II was a U.S. government project designed to monitor airline passengers and screen them against terrorist watchlists. It checked customer data against commercial and government databases and coded each passenger according to risk. Those coded at high risk would be banned from flying.

CAPPS II never materialized because of controversy that arose after plans were announced. Concern over costs, civil liberties, and race relations fueled pressure from groups and helped to prevent the program from being implemented. Implementing critical success factors as seen in Figure 2 is the first step to program success.

Critical Success Factors

- Design the solution with privacy in mind, just as many programs do this with security today
- Start with a proof of concept and build on the solution over time
- Identify a program resource as the single point of contact for privacy information
- Conduct a Privacy Impact Assessment (PIA) early, before major decisions on external data sources are made
- Implement regular PIA updates and keep agency leadership informed on program decisions
- Involve a Chief Privacy Officer and a Chief Information Officer during development and privacy review prior to program inception
- Limit the amount of external data that is stored by the Government
- Collaborate with Departmental privacy policy personnel from program inception
- Identify and proactively communicate with key stakeholders who have privacy concerns
- Require contractors who are supporting the program to demonstrate their understanding of privacy requirements and their experience with privacy

Figure 2. Critical Success Factors. *Proven tactics for privacy planning in new programs helps avert program failure.*

3.2 Legislative Components of a Strong and Effective Culture of Privacy

Some legislation currently offers degrees of privacy protection. However, there was a significant change in mindset after the September 11th attacks and privacy protections were reduced in hopes of increasing security. The Privacy Act of 1974 requires that companies register systems containing potentially sensitive information with the government. Consumers must have access to their information, and limits are placed on data sharing between agencies. However, the Privacy Act applies only to U.S. citizens, which can make foreign companies and residents hesitant to engage in business or travel in the U.S. Also, the exceptions to the Privacy Act weaken its scope. Material collected for "law enforcement purposes" is exempt from the Privacy Act, and the broad definition of "system of records" leaves seemingly applicable systems out of the Act's reach.

Figure 3 on the next page describes the current privacy laws pertinent to government programs, shows their weaknesses, and suggested ramifications.

Description	Strengths and Weaknesses	Recommendation
Freedom of Information Act (FOIA)		
▪ Right for anyone to request access to federal agency records and information	Contingent on exemptions some of which include: ▪ Classified information ▪ Privileged information ▪ Inter- or intra-agency memos ▪ Law enforcement records ▪ Financial Institution regulatory records	▪ Require government to provide timely response to FOIA request ▪ Re-evaluate the exemptions for specific FOIA requests
Privacy Act of 1974		
▪ Limits the collection of personal information ▪ Prohibits use of secret government records ▪ Safeguards for security and accuracy of government files	▪ Applies only to U.S citizens and lawfully admitted permanent alien residents Access and redress measures are not adequately enforced by one central regulatory body	▪ Update and extend to visitors whose information is collected for security purposes ▪ Establish a viable oversight body to regulate and enforce these privacy regulations
e-Government Act		
▪ Vast Framework of standards that require using Internet-based information technology to enhance citizen access to Government and information services using Privacy Impact Assessments (PIA's) and posting website privacy policies	Contingent on exemptions: ▪ For national security systems ▪ Previously assessed systems under evaluation similar to PIA ▪ Internal Government-run websites that do not collect identifiable information about the public ▪ System collecting non-identifiable information	▪ Create more transparency in Government data collection ▪ Define purpose of data collection ▪ Allow access in order to modify incorrect information
Data Quality Act		
▪ Guidelines for ensuring and maximizing the quality, objectivity, utility and integrity of information ▪ Regulated by the Office of Management and Budget (OMB)	▪ Regulation body has a large quantity of institutions to oversee	▪ Improve the efficiency of regulation and enforcement of the Data Quality Guidelines
Federal Information Security Management Act (FISMA)		
▪ Framework for ensuring the effectiveness of information security controls ▪ Guidelines for monitoring federal programs ▪ Specifies responsibilities of various entity heads, CIOs and other ▪ Specifies requirements for incident response capability and awareness training ▪ Specifies annual reports to Congress Headed by a director who oversees adherence to federal security laws	▪ Provides a universal means of reporting information to congress ▪ Agencies may be unprepared to supply information about the effectiveness of newly implemented programs ▪ Complicated and time-consuming process for company CIOs and CSOs ▪ Report card-style system of grading agencies of FISMA compliance ▪ High cost of conducting surveys of systems	▪ Improve the efficiency of overseeing the compliance for the federal information security
The USA PATRIOT ACT (The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001)		
▪ Detailed laws permitting law enforcement officials to have greater Access to previously private information about civilians if it is necessary to prevent terrorism (e.g. library and bookstore records	▪ Increased powers for law enforcement officials when conducting anti-terrorism investigations Strong protections for national security, but many have concerns over breaches of individual privacy	▪ Provision of the Act should be reexamined on a more regular basis (currently every 10 years)

Figure 3. U.S. Privacy Laws. *Recognizing the current weaknesses in privacy legislation identifies the necessary improvements to build a strong and effective culture of privacy for future solutions.*

4.0 ACHIEVING PRIVACY PROTECTIONS WITHIN SECURE BORDERS

With the evolution and improvement of current privacy legislation and a broader understanding of how the use of technology impacts citizen privacy the U.S. Government can achieve the design, development and implementation of new security programs to secure our borders successfully.

By increasing the scope of some current legislation, lawmakers can create a new way of incorporating privacy provisions effectively in security solutions. Figure 4 below summarizes the immediate, short-term and long-term goals for achieving privacy protections within secure borders.

Immediate steps include the development of measures to protect privacy as part of security solutions from the beginning. Technology such as RFID is implemented before privacy protections are instituted. Once privacy protections are put in place, PIAs should be performed to keep privacy protections updated.

CPOs should be required in companies that handle sensitive information. Right now, they are only required in some government agencies and companies.

As a short-term goal, legislators can review existing laws to standardize them and create more active privacy policies. Currently, legislation often applies to specific industries and changes frequently. This makes it difficult to follow privacy procedures. A standardized policy would simplify privacy protection and encourage more companies to follow the guidelines.

Several improvements can be made in the oversight of current privacy legislation as a long-term goal. For example, FISMA and the Data Quality Act are overseen primarily by the OMB. Both require annual reports to be submitted by agencies to OMB to monitor compliance, who then submits annual reports to Congress. FISMA requires agencies to undergo independent evaluations by the inspectors general of each agency, who then submit their own reports to OMB. A single, clear, and comprehensive guide to privacy policy could greatly help agencies follow the requirements and improve information privacy.

Awareness of privacy and automatic incorporation of privacy protection into security developments is essential as a long-term goal. Creating successful security programs that consider citizen protection and citizen privacy protection requires a new approach and new techniques. Effective border security solutions include privacy professional involvement from that start that facilitate privacy protection implementation and promote policy improvements for the future.

Immediate Steps	Short-term Goals	Long-term Goals
▪ Include privacy protections when developing technology to improve security ▪ Encourage and sometimes mandate CPO, CIO, and CSO positions to be established in programs that handle sensitive information ▪ Perform privacy impact assessments (PIAs) before new processes and systems are designed	▪ Review and standardize existing privacy laws ▪ Create privacy policies that change easily depending on current events and new situations ▪ Implement cross-functional teams to protect privacy at all levels of companies and all phases of projects	▪ Establish oversight body to regulate and enforce privacy regulations (currently, OMB, IG, GAO)

Figure 4. Achieving Results. *Privacy planning in each stage of a project design and implementation is critical to public acceptance and long-term program viability.*

Arc Aspicio is a global management consulting company. Committed to architecting visionary and tactical solutions, Arc Aspicio collaborates with our clients every day to solve immediate and long-term challenges by thinking about problems differently. Specifically, we have a passion for solving homeland security, border management and law enforcement challenges around the world. With deep government, business process, and organizational change expertise, Arc Aspicio can mobilize the right people, skills and solutions to help clients achieve transformational change.

Arc Aspicio LLC
3318 Lorcom Lane
Arlington, VA 22207
1.703.465.2060
info@arcaspicio.com

www.arcaspicio.com