REPORT OF THE DEPARTMENT OF HOMELAND SECURITY DATA PRIVACY AND INTEGRITY ADVISORY COMMITTEE

Report No. 2006-01

Framework for Privacy Analysis of Programs, Technologies, and Applications

Adopted March 7, 2006

Introduction

This document sets forth a recommended framework for analyzing programs, technologies, and applications in light of their effects on privacy and related interests. It is intended as guidance for the Data Privacy and Integrity Advisory Committee (the Committee) to the U.S. Department of Homeland Security (DHS). It may also be useful to the DHS Privacy Office, other DHS components, and other governmental entities that are seeking to reconcile personal data-intensive programs and activities with important social and human values.

Summary

The recommended framework is comprised of five steps. They are summarized on this page and discussed more fully in the Notes on the succeeding pages.

Step 1. Scope

The Committee asks DHS to provide a description of the program, technology, or application. The Committee reviews and comments, as appropriate.

Step 2. Legal Basis

The Committee asks DHS to provide a description of the legal authority and legal limits for program, technology, or application. The Committee reviews and comments, as appropriate.

Step 3. Risk Management: Efficacy

The Committee asks DHS for the results of their risk analysis and estimation of the efficacy of the program, technology, or application. The Committee reviews and comments, as appropriate.

Step 4. Effects on Privacy Interests

The Committee analyzes the privacy interests implicated by the program, technology, or application.

Step 5. Recommendations

The Committee assesses the results of the first four steps and makes recommendations on the program, technology, or application.

Framework

Step 1. Scope

In Step 1, the Committee asks the relevant Department of Homeland Security component to provide a description of the program, technology, or application (hereinafter "program"). The Committee then reviews and comments on the scope, as appropriate.

The description should answer the following questions:

- *What is the program under review?*
- *What is its purpose?*
- *What is its history and origin?*
- *How has it come to be used or considered by the Department?*
- *Where is it used or being considered for use?*

In essence, the scope of the study is described here.

Step 2. Legal Basis

In this step, the Committee asks the relevant DHS component to provide a description of the legal authority for, and legal limits on, the program. The Committee then reviews and comments, if appropriate.

Specifically, the following questions should be answered to the extent reasonably possible:

- *What is the legal authority for the program under consideration? Please consider constitutional, statutory, and other legal authority, including the DHS component's statutory mandate, as appropriate.*
- *What are the pre-existing legal limits on the program under consideration? Please consider statutory protections, constitutional rights such as Due Process, and other legal principles.*

Many programs may implicate the statutory and constitutional rights that underlie privacy and related interests. This step does not require a full inquiry into the meaning of every right, but relevant statutory provisions and constitutional rights as interpreted by the courts should be mentioned and briefly discussed, if appropriate.

Step 3. Risk Management: Efficacy

In Step 3, the Committee asks the relevant Department of Homeland Security component to describe the program's benefits to the homeland security mission in the context of risk management and to show how, and how well, it addresses threats to national security.

The benefits of the program as they relate to the Department's mission can be set forth any number of ways, but the following questions illustrate a general risk management framework:

- *What are you trying to protect?* Every security program or technology is meant to protect some institution, infrastructure, process, person, or group that may be harmed. The asset being protected should be identified with relative particularity along with some assessment of its value if that is not obvious. This is known as "target assessment." A good, specific answer to the question "What are you trying to protect?" might be "My car." Answers that are too general, such as "the American people," are less useful

- *What are you trying to protect it from?* Harm to the asset you are trying to protect can come in various ways. The goal here is to describe vulnerabilities and the relevant ways an asset may be harmed. Threats to a car include theft, accident, vandalism, misuse, grime, scratches, towing, and breakdowns. The listing of threats is called "threat assessment."

- *What is the likelihood of each threat occurring and the consequence if it does?* Each threat has a different likelihood and consequence. As far as risks to a car, grime is inevitable, but it has very low consequences. As another example, the chance of lightning striking a person is very low but the consequences are significant. Comparing and contrasting relevant threats is the heart of risk management, known as "risk assessment." Risk assessment helps target limited resources efficiently by focusing attention on the threats with the greatest combined likelihood and consequence.

- *What kind of action does the program take in response to the threat?* There are four ways of responding to a threat: acceptance, prevention, interdiction, and mitigation. The response that the program represents may be placed in one or more of these categories:

    - *Acceptance* – Acceptance of a threat is a rational alternative that is often chosen when the threat has low probability, low consequence, or both. For example, few people remain indoors during storms to avoid the low probability of being struck by lightning.

    - *Prevention* – Prevention is the alteration of the target or its circumstances to diminish the risk of the bad thing happening. Golfers may come in off the course during a thunderstorm to avoid being struck by lightning. This is a change to the circumstances of the target that helps avoid the threat.

    - *Interdiction* – Interdiction is any confrontation with, or influence exerted on, an attacker to eliminate or limit its movement toward causing harm. In protecting your car, flashing your lights to warn another car about the fact that you are passing is a mild interdiction against the threat that it will veer into your lane. Interdiction stops or slows a person or thing that has a harmful motive or impetus.

    - *Mitigation* – Mitigation is preparation so that, in the event of the bad thing happening, its consequences are reduced. Defibrillators at golf courses are intended to mitigate the consequences when golfers are struck by lightning.

- *Does the response create new risks to the asset or others?* The final step in analyzing the program's efficacy is to be aware of new risks created by the prevention, mitigation, or interdiction of the threats under consideration. Installing heavy iron siding to a car may mitigate the risk to the car from accidents. At the same time, the reinforced car may pose new risks to other cars and pedestrians.

Step 4. Effects on Privacy and Related Interests

This step is the heart of the process. In it, the Committee analyzes the privacy and related interests implicated by the program under study and how they are affected. The overarching question here is: *What are the effects on privacy values and interests?*

Homeland security programs have many costs. The government should rigorously analyze direct and indirect costs to taxpayers and the economy, for example. The focus here is on costs that are less tangible but no less important: costs to privacy and related interests. Some programs may not have such costs and may even benefit these interests.

Many DHS programs will have some costs to privacy and related interests, and this is not fatal. Minimizing these costs, though, is an important part of choosing and shaping the appropriate response.

This analysis begins with the values that underlie and inform the Fair Information Practice Principles, or FIPPs, the well known set of guidelines for organizations on the handling of personal information. The key interests that may be affected by a particular program include the following:

- **Privacy:** *How does the program affect individuals' ability to control how personal information about them is collected, used, or shared?*[1] Important subsets of this value include:

    - **Confidentiality:** *Does the program include rules and practices that protect the confidentiality of personal information once it has been collected?*[2]

    - **Anonymity:** *Does the program erode individuals' ability to control identifying information and to remain anonymous when they want to do so?*[3] *Many transactions and interactions require some kind of identification but anonymity should be available when reasonably possible.*

    - **Seclusion:** *Does the program use or foster surveillance?*[4] Several practices minimize surveillance. The extent of their use may help determine how much a program promotes or restricts surveillance:

        - Collection Limitation and Purpose Specification: Collection limitation requires data collected to be minimized and relevant to an explicit, limited purpose. *Does the program document why specific data elements are needed and appropriately circumscribe the personal data collected to that which is relevant to the need? Does the program document who will be the subject of data collection and why, appropriately circumscribing the population that is subject to surveillance?*

        - Use Limitation: Use limitation prevents the conversion of data collected for one purpose to another use. *Does the program prevent data collected for one purpose from being used for another? Does it use data that was collected for a different purpose?*

        - Retention Limitation: Retention limitation requires the disposal of data once it has been used. *Does the program require the destruction of data as soon as it is no longer needed to serve the purpose for which it was collected?*

- **Fairness:** *Does the program treat individuals fairly at every step?*[5] Several rules and practices promote fairness and due process. The extent of their use may help determine how much a program promotes or denies fair treatment:

    - Data Quality: *Does the program collect data directly from the subject of the information? If the program uses information from other sources, what is done to assure that the sources are reliable?*[6] *How does the program ensure that it uses accurate, timely, and relevant data? Does the program allow individuals access and correction rights? Does it ensure that corrections are propagated throughout the system?*[7]

- NOTICE: *Does the program provide adequate notice to individuals of its data collection, use, disclosure, and redress policies?*

- INDIVIDUAL PARTICIPATION AND ACCOUNTABILITY: *Does the program provide due process through redress mechanisms wherever a person may suffer an adverse action or determination?* [8]

- TRANSPARENCY: *Is the program open to public scrutiny, understanding, and participation? Is information about agreements and contracts with other government agencies, government contractors, and foreign governments available to the public? Are architectures, technologies, data flows, tests, testing criteria, and testing results published?*[9]

- ACCOUNTABILITY: *Is the program manager accountable for compliance with privacy laws and principles? Does the program contain appropriate control measures, such as privacy audits and review by the DHS Privacy Office or the Inspector General?*[10]

- **Liberty:** *Does the program limit individual freedom in some dimension? For example, does it condition freedom of movement or action on the diminution of some privacy interest? Is interaction with the program mandatory or effectively mandatory?*[11]

- **Data Security:** *How is personal information secured against threats to privacy and integrity?*[12] *Does the program use reasonable and appropriate safeguards (including administrative, technical, and physical measures) to protect against unauthorized access, use, disclosure, modification, and destruction of data?*

Step 5. Recommendations

In the final step, the Committee assesses the results of the first four steps and makes recommendations as to the program. The recommendations section should include any commentary, suggestions, or material that the Committee deems appropriate, but particular questions that should be answered include:

- *Are there changes that could be made in the program that would reduce its privacy costs?*

- *Should the program proceed?* Do the benefits of the program described in Step 3 justify the costs to privacy interests described in Step 4? Would the changes described above affect this analysis?

Notes

[1] **Privacy**: In PRIVACY AND FREEDOM (1967), Alan Westin formulated the classic early definition of privacy: "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."

[2] **Confidentiality**: A pledge of confidentiality is a promise not to further share information that has already been shared. In commercial environments, this protects privacy because it allows sharing consistent with what a consumer likely wants, and no further. When governments mandate the collection of information, confidentiality rules approximate privacy as well as possible.

[3] **Anonymity** is the condition of having one's name or identity unknown or concealed. It serves valuable social purposes and empowers individuals as against institutions by limiting surveillance, but it is also used by wrongdoers to hide their actions or avoid accountability.

[4] **Seclusion and Surveillance**: Seclusion is the quality of being secluded from the presence or view of others, an important dimension of privacy that is eroded by surveillance. Active surveillance is directed observation of some person or entity using means such as bugs or human operatives. Passive surveillance is the indirect monitoring of a person or entity through observation of actions, transactions, or communications. Surveillance is not inherently wrong or harmful, but awareness or even suspicion of surveillance in some contexts can inhibit individuals' senses of freedom, privacy, and self-determination.

[5] **Fairness**: People very much want to be treated fairly. The constitutional requirement of due process mandates essential fairness in government decision-making.

[6] **Source Limitation**: Information whose source and provenance is known and capable of independent verification is more accurate, more useful, and fairer to use than information from unknown or undisclosed sources. Data should be collected from the subject individual when the information may result in adverse determinations about the individual's rights, benefits, or privileges.

[7] **Accuracy**: Accurate information is essential to accurate decision-making. Rights to access and correct personal information promote accuracy and concomitant fairness. Giving individuals access to personal information — within a reasonable time, in a reasonable manner, and for a minimal fee, if any — promotes fairness. The ability to challenge accuracy and correct inaccurate information does so as well.

[8] **Individual Participation and Accountability**: When an adverse determination has been made about an individual's rights, benefits, or privileges, timely redress — the opportunity to contest that determination with an impartial arbiter — is an essential element of the fairness of that process.

[9] **Transparency**: Transparency and participation promote the perception of fairness to go along with the reality of it. People should be able to find out about what personal information is collected about them, how it is used, and whom to contact with questions or concerns. People who understand how a program, technology, or application works, why it works, their role in it, and their rights are more inclined to perceive it as fair.

[10] **Accountability**: People expect organizations that maintain personal information about them to be accountable for complying with laws, regulations, and fair information practice principles in managing that information.

[11] **Liberty**: The liberties enjoyed by Americans include simple freedoms to move about, speak freely, transact business, and structure their lives and lifestyles as they choose. Programs, technologies, or applications that diminish freedom of action, movement, conscience, or choice undermine liberty. Conditioning the exercise of certain freedoms on degradation of interests like privacy also undermines liberty.

[12] **Security**: People expect organizations that collect personal information about them to protect it from unauthorized access, use, disclosure, modification, or destruction. The steps that an organization must take to protect its assets, processes, and functions include securing servers and computers inside locked and patrolled buildings; checking the background of employees, if appropriate, and training them to use procedures that protect data; and ensuring that software systems are up-to-date and that new vulnerabilities are patched quickly. An institution that lacks security cannot be certain of its ability to protect privacy and related interests. (Failure to provide sufficient data security creates new risks to others, as discussed at the end of Step 3.)