Framework for Privacy Analysis of Programs, Technologies, and Applications

This document is a recommended framework for analyzing programs, technologies, and applications in light of their effects on privacy and related interests. It was written for the use of the U.S. Department of Homeland Security's Data Privacy and Integrity Advisory Committee but it may also be useful elsewhere within the Department and for other governmental entities that are working to reconcile personal data-intensive programs and activities with important social and human values.

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

Step 2. Legal Basis
Committee asks DHS to provide legal authority and legal limits for program, technology, or application. Committee reviews and comments, if appropriate.

Step 3. Risk Management: Efficacy
Committee asks DHS to provide results of their risk analysis and estimation of the efficacy of the program, technology, or application. Committee reviews and comments.

Step 4. Effects on Privacy Interests
Committee analyzes privacy interests implicated by the program, technology, or application.

Step 5. Conclusion: Recommendation
Committee assesses results of first four steps and makes recommendations on the program, technology, or application.

Framework Notes

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, if appropriate.

The description should answer the following questions:

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

Depending on the circumstances, it might also be important to exclude programs, technologies, or applications that are not within the ambit of the current study. In essence, the scope of the study is described here.

Step 2. Legal Basis
In this step, the Committee asks the relevant Department of Homeland Security component to provide the legal authority for and legal limits on the program, technology or application. The Committee then reviews and comments, if appropriate.

Specifically, the following questions should be answered to the extent they can be:

- *What is the legal authority for the item under consideration? Please consider constitutional, statutory, and other legal authority.*
- *What are the legal limits on the item under consideration? Please consider constitutional, statutory, and other legal authority.*

Many programs, technologies, or applications may implicate the constitutional rights that underlie privacy and related interests. This step does not require a full inquiry into the meaning of every right, but relevant constitutional provisions and 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 in the context of risk management and to show how, and how well, it addresses threats.

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 impacted by a threat. 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?" would be "My car." Less useful answers are too general, such as "the American people."

- *What are you trying to protect it from?* Harm can come to the asset you are trying to protect various ways. The job here is to describe 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. Accidents are rare and have consequences that range from simple embarrassment to fatality and massive property destruction. Comparing and contrasting among 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?* Acceptance of a threat is a rational alternative that is often chosen when it has low probability, low consequence, or both. When it merits one, there are three ways of responding to a threat: prevention, mitigation, and interdiction. The response that the program represents may be placed in one or more of these categories:

    - *Prevention* – Prevention is the alteration of the target or its circumstances to diminish the risk of the bad thing happening. Driving defensively and soberly is a way of preventing accidents, for example, as is taking alternate forms of transportation. These are changes to the circumstances of the target that help avoid the threat.

    - *Mitigation* – Mitigation is preparation so that, in the event of the bad thing happening, its consequences are reduced. Carrying automobile insurance is a way of reducing the consequences to you when your car is involved in an accident.

    - *Interdiction* – Interdiction is any confrontation with, or influence exerted on, an attacker to eliminate or limit its movement toward causing harm. 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.

- *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. The creation of new risk to others is called "risk transfer."

Step 4. Effects on Privacy Interests

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

Homeland security programs have many costs. Costs denominated in dollars are relatively easy to track. The focus here is on costs that are less tangible but no less important: costs to privacy and related interests.

Nearly every program 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 molding the appropriate response. The key privacy interests that may be affected by a particular program include:

- **Privacy:** *Does the program erode individuals' ability to control how personal information is collected, used, or shared?*[i] Important subsets of this value include:
  - **Confidentiality:** *Does the program include rules and practices that maximize the confidentiality of personal information?*[ii]
  - **Anonymity:** *Does the program erode individuals' ability to control identifying information and to remain anonymous when they want?*[iii]
  - **Freedom from Surveillance:** *Does the program unduly use or foster surveillance?*[iv] Several rules and practices minimize surveillance. The extent of their use may help determine how much a program promotes or restricts surveillance:
    - Collection limitations require data collected to be highly relevant to a limited purpose. *Does the program carefully circumscribe the personal data it uses or collects to that which is highly relevant?*
    - Use limitations prevent the conversion of data collected for one purpose to another use. *Does the program prevent data collected*

for one purpose from being used in another? Does it use data that was collected for a different purpose?

- Retention limitations require 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?*

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

  - *Does the program collect data from the subject of the information and from known, verifiable sources?*[vi]

  - *Does the program ensure that it uses accurate and timely data and allow individuals access and correction rights? Does it ensure that corrections are propagated throughout the system?*[vii]

  - *Does the program provide redress mechanisms wherever a person may suffer an adverse determination?*[viii]

  - *Is the program open to public scrutiny, understanding, and participation?*[ix]

- **Liberty:** *Does the program limit individual freedom in some dimension or condition freedom of movement or action on the diminution of some privacy interest?*[x]

- **Data Security:** *Is the program secure against threats to the privacy and integrity of personal data?*[xi]

Step 5. Conclusion: Recommendation

In the final step, the Committee assesses the results of first four steps and makes recommendations as to the program. The conclusion 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?*

- *Is the program worth it?* Does the efficacy of the program as described in Step 3 justify the costs to privacy interests described in Step 4? Would the changes described above affect this analysis?

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

[ii] **Confidentiality**: A pledge of confidentiality is a promise not to share further 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.

[iii] **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.

[iv] **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.

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

[vi] **Source Limitation**: Source limitations require data to be collected from the subject individual when the information may result in adverse determinations about the individual's rights, benefits, and privileges. 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.

[vii] **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 information does so as well.

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

[ix] **Transparency and Individual Participation**: 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 collected, the uses of it, 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.

[x] **Liberty**: The liberties enjoyed in a republic like the United States are many. These include Americans' simple freedoms to move about, speak freely, transact business, and structure their lives and lifestyles as they choose. Programs, technologies, or applications that lessen freedom of action, movement, conscience, or choice undermine liberty. Conditioning the exercise of certain freedoms on degradation of interests like privacy also undermines liberty.

[xi] **Security**: People expect organizations that collect personal information about them to protect it from unauthorized access, use, disclosure, 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; ensuring that software systems are up-to-date and that new exploits 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.)