

Paul Rosenzweig, Esq.
Chair, Data Privacy and Integrity Advisory Committee
214 Massachusetts Ave., NE
Washington, DC 20002

paul.rosenzweig@heritage.org

(202) 608-6190
Fax: (202) 547-0641

October 6, 2005

Via Hand Delivery

Secretary Michael Chertoff
Department of Homeland Security
Washington, DC

Ms. Maureen Cooney
Acting Chief Privacy Officer
Department of Homeland Security
Washington, DC

Re: Report of the Data Privacy and Integrity Advisory Committee No. 2005-01

Dear Secretary Chertoff and Ms. Cooney:

I have the honor to convey to you the enclosed Report of the Data Privacy and Integrity Advisory Committee concerning the Use of Commercial Data to Reduce False Positives in Screening Programs. This first report of the Advisory Committee bears serial report number 2005-01.

In summary, on the issue of false positive errors, the report recommends that commercial data be used for screening programs only when:

- It is necessary to satisfy a defined purpose
- The minimization principle is used
- Data quality issues are analyzed and satisfactorily resolved
- Access to the data is tightly controlled
- The potential harm to the individual from a false positive misidentification is substantial
- Use for secondary purposes is tightly controlled
- Transfer to third parties is carefully managed
- Robust security measures are employed
- The data are retained only for the minimum necessary period of time
- Transparency and oversight are provided
- The restrictions of the Privacy Act are applied, regardless of whether an exemption may apply

Secretary Chertoff

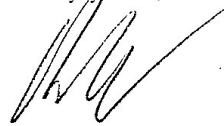
October 6, 2005

Page 2

- Simple and effective redress is provided
- Less invasive alternatives are exhausted

If I can be of any assistance concerning this report, please do not hesitate to contact me.

Sincerely yours,

A handwritten signature in black ink, appearing to read 'Paul Rosenzweig', written in a cursive style.

Paul Rosenzweig
Chair, Data Privacy and Integrity
Advisory Committee

Encl. (as stated)

cc: Members, DHS-DPIAC (via e-mail)

REPORT OF THE DEPARTMENT OF HOMELAND SECURITY
DATA PRIVACY AND INTEGRITY ADVISORY COMMITTEE
Report No. 2005-01

THE USE OF COMMERCIAL DATA TO REDUCE FALSE
POSITIVES IN SCREENING PROGRAMS

Adopted
September 28, 2005

Introduction

This document is an analysis of issues relating to the Department of Homeland Security (DHS)'s consideration of the use of commercial data to reduce the number of false positive identifications in screening programs.¹ DHS has expressed a desire to use personally identifiable information from commercial databases to reduce the number of false positive identifications in screening programs as one justification for the potential use of commercial data. The commercial data could potentially come from large data aggregators or from smaller data sets. The DHS Data Sharing and Usage Subcommittee of the DHS Data Privacy and Integrity Advisory Committee has reviewed the risks created by DHS access to commercial data. In this report, the Subcommittee addresses certain issues it believes must be satisfactorily addressed prior to DHS use of commercial data in terrorist screening programs.

This document does not contain an analysis of all the issues associated with DHS access to commercial data. For example, this paper does not explore the use of commercial data to better target terrorists. The Subcommittee plans, however, to use this paper as a building block for a more detailed analysis of the specific issues associated with such data use.

The report of the Subcommittee has been considered by the full Committee, which has adopted it in the following form.²

¹ This report contains an analysis of broad principles that the Subcommittee believes should apply to all DHS screening programs. The report uses the Secure Flight program as an example only. The Subcommittee notes that the Secure Flight Working Group published a report on September 19, 2005, concluding in part that Congress should prohibit live testing of Secure Flight until DHS provides more information on how the program will collect and use personally identifiable data.

² The Subcommittee recognizes that Congress is independently considering the rules governing DHS's use of commercial data in certain applications. Our recommendations assume the absence of any legislative restrictions and must be read within the context of Congressional enactments that may impact our recommendations.

Background

The goal of reducing the risk of terrorism in the US will continue for the foreseeable future. Security measures, such as screening programs, are a significant part of current terrorism prevention.

False positives are an inevitable consequence of any screening program.³ Screening programs inaccurately identify people as suspected terrorists largely because they rely on loose name-matching algorithms, which must address different cognates. For example, “Tracy” may also appear as “Tracie” or “Tracey.” “Tracy” could be a first or last name; it may also refer to a man or a woman. Often there is limited information on both the watch list and the record DHS is matching (e.g., the list of passengers on a plane). There are further difficulties caused by name changes, aliases, nicknames, and typos. Successful screening programs must identify any individual whose name is approximately equivalent to an entry on the watch list. Currently, individuals who are wrongly flagged are often flagged repeatedly, as DHS is still developing mechanisms to allow individuals to differentiate themselves from the people on the watch list.

False positives can create adverse consequences for misidentified individuals, ranging from missing a flight to being denied a security clearance or job. Therefore, it is important to take steps to minimize such misidentifications. Any mitigation efforts, however, may require DHS to collect, store, access, or process more personally identifiable information, potentially including commercial data. Where DHS finds it necessary to collect, store, access, or process such data, it will need to consider both the potential harm to the individual and the benefits to DHS. This report examines the question of whether information could or should be made more precise, and false positives thereby reduced, by DHS’s access to and use of commercial data.

Commercial Data

A number of private repositories throughout the United States collect, store, analyze, and sell information on individuals. While this information is comprised largely of transactional data, it also contains extensive demographic, psychographic, health and financial information. These databases are expansive, and in some cases consist of hundreds of fields for each individual. Information services companies routinely use information about individuals to identify appropriate recipients of prescreened offers,

³ For purposes of this report, a *false positive* is the misidentification of an individual as a person on a terrorist watch list when he or she is not, in fact, that person. A *false negative*, by contrast, would be the misidentification of someone who is on a watch list as a person who is not on the list.

assess an individual's credit risk, correct duplicate names on marketing lists, run diagnostics on household data, and generate marketing lists. While of demonstrated use in the commercial sphere, there are real questions on the extent of the potential benefits – improved accuracy through fewer false positive errors – to be achieved in a terrorist screening program from the use of commercial data. DHS test data has shown less benefit from the use of commercial data than from the use of alternate mechanisms.⁴ Even if benefits are demonstrated, there are further questions as to whether the benefits gained warrant accepting the attendant potential privacy incursions.

Issues Regarding the Use of Commercial Data to Mitigate False Positives

If DHS uses commercial data for security screening purposes, DHS should consider the following issues:

- 1. The Data** - What information will be accessed? Has care been taken to ensure that the most limited set of data elements necessary is accessed and does each data element accessed directly serve the primary objective of the request? Does the aggregation of the data make the data more sensitive? Are there any less sensitive or potentially less intrusive data elements that could be used to serve the same purpose? To what degree is the information sufficiently accurate that it is likely to reduce the number of false positives? Are there sub-populations of individuals for which the accuracy rate is especially high or low?
- 2. Access** - Who will see the data? Are plans in place to limit information access on a strictly necessary basis? Are there appropriate physical, administrative, and technical controls in place to both secure access and protect the information, while in storage or in transit, from compromise by third parties or non-authorized users within DHS?
- 3. Use, Disclosure and Storage** - Will the data be used to serve only the specific purpose for which DHS acquires or accesses them? With whom, if anyone, will the data be shared? Under what conditions will that sharing take place (e.g., by contract, only with an inspection)? Will anyone use the data for any other purpose? How long will DHS retain the data? Would a shorter retention time still accomplish the stated objective? What security measures will DHS implement to protect the commercial data while in storage and are such measures sufficient to adequately protect the data from unauthorized use, access and disclosure?

³ Response of Justin Oberman, Assistant Administrator, Secure Flight/Registered Traveler, Transportation Security Administration, to questions submitted by the Data Privacy and Integrity Advisory Committee of the United States Department of Homeland Security. http://www.dhs.gov/interweb/assetlibrary/privacy_advcom_06-2005_res_joberman.pdf

4. Transparency and Data Subject Access - Does the general public benefit from knowledge of the categories of commercial data that are shared with DHS for screening programs? What would be the potential privacy consequences from withholding this information? How granular do the details contained in the public disclosure need to be?

5. Regulation and Redress - What oversight and review exists for the DHS process of seeking access to commercial data? Should the system be subject to the Privacy Act of 1974? What audit procedures exist? Is there a separation of reporting chains and duties between those who operate the system and those who audit it? How is the process reviewed to determine whether too much or inappropriate information is being collected or accessed? What is the complaint mechanism and how is it reviewed? What, if any, rights of access and correction exist for the data subject? Is there a right of appeal or review should the individual remain aggrieved after the completion of the DHS redress process?

6. Alternatives - Are there less invasive and equally effective alternatives?

The list above is not exhaustive; rather, it is meant as a general set of considerations that could apply to a variety of screening programs. This report addresses below each of these issues.

The Data

The Subcommittee presumes that any use of personal data can create privacy risks for individuals (e.g., through unauthorized use, security breaches, etc.). Including poor quality information in a database causes some of these risks. Therefore, any entity intending to use commercial data to reduce false positives should minimize the scope and type of data accessed and its use to the extent necessary to directly satisfy the identified purpose. This minimization principle presupposes that the personal data are of sufficient quality to warrant use for the defined purpose.

Commercial databases usually contain information on names (including middle names), addresses, social security numbers, birth dates, often mothers' maiden names, and age, as well as information on lifestyles, magazine subscriptions, and the like. It is information of this sort that helps establish a suspect's identity and can assist in correcting false positives. In principle, the information in commercial databases can be useful, but only to the extent to which the data are accurate for the defined purpose.

Not all commercial data are necessary for distinct identification purposes. For example, identifying suspected terrorists may require name and birth date matches. Additional information, which can assist in the verification of the

subject's identity, might also be considered. Whatever the necessary variables are, they nonetheless will comprise a small subset of the total information available in any given commercial database.

It is therefore important to identify which particular types of information DHS thinks it must access to reduce false positives. Whether this can be determined beforehand, or can be determined only after considering application to a particular screening program, is unclear. DHS may also find that the ability of the database to rule out false positives increases with the amount of data linked to a specific individual. Some variables, however, can almost certainly be ruled out. An appropriate methodology for DHS to consider would be to start with the smallest number of data elements with the least sensitivity to the individual, then test whether those elements accomplish the stated purpose (*i.e.*, a reduction in false positives). DHS could then slowly add data elements until the purpose is achieved while testing to determine whether such incremental access and use will cause harm to individuals.

Assuming DHS has effectively minimized the amount of commercial data it needs to meet its defined purpose, it should then assess the quality of the data. Any decision to use commercial data should include a quality audit of the data. This audit will help ensure that the data are effective in reducing false positives and will also mitigate risk if the data are subsequently used for a secondary purpose.

Such assessments of accuracy should be based on publicly disclosed metrics. Government access to large commercial databases will have to win public acceptance. Transparency wherever, or to the extent that, national security concerns do not require secrecy, is the best means for such a system of public-private information exchange to gain acceptance. As discussed below, DHS should demonstrate to the public why it believes the system will result in more good than harm.

Access

The Subcommittee explored four questions involving DHS access to commercial data: (i) Who can access the commercial information? (ii) Under what conditions can individuals access the data? (iii) Will such access require the notice or consent of the data subject? (iv) What information can be accessed?

To fully assess issues relating to DHS access to commercial data for screening programs, it is necessary to better understand the context in which such data would be accessed. Misidentification (a false positive) of individuals has created a perceived need for government access to commercial data. An allegedly misidentified individual may flag a misidentification. There are two

ways in which an individual can discover that he or she has been misidentified.⁵ First, an individual may become aware of being on a suspect list as a result of suffering adverse consequences like being refused a license to carry hazardous materials or entry onto a plane. The individual may attempt to determine independently whether his or her name is on a suspect list, to the extent that these lists are made available.⁶ DHS can minimize its access to commercial data by using such information only when an individual claims to have been incorrectly identified by the screening program. This use of commercial data could require storing personally identifiable information in a central database within the government. DHS should also pursue other options, however, like accessing the data in the form held by the commercial holder, which would require less access to the data by government employees.

Screening programs also might require some level of access to data in order to allow the information to be acted on by security employees, as DHS will call on such employees to make the relevant identification of individuals who are to be screened. DHS may wish to consider whether the purposes of this access can be satisfied through the use of data derived from a comparison of the commercial data to other government-held data, rather than the underlying commercial data itself.

DHS also may need to grant access to information at intermediate stages of the screening process. For example, access to such information at the time of the sale of a plane ticket could help establish (confirm or disprove) the individual's identity, providing clearance earlier and leading to fewer inconveniences to the individual. Other screening programs, such as the provision of hazardous materials licenses, may not require access at intermediate stages. While different screening programs may require access to commercial data at different stages to reduce false positives, DHS should require all such programs to be assessed to determine how such access can be minimized.

Use, Disclosure and Storage

DHS's use of commercial data to reduce false positives requires an assessment of both the benefits and the potential harm to individuals. This analysis of the benefits and harm is dependent, in part, on how narrowly DHS defines the purposes of using the data. One of the potential risks of storing personal information is that the data's purpose may change over time. It is critical that the purpose of acquiring the commercial data be defined up front. Any

⁵ Paul Rosenzweig and Jeff Jonas. "Correcting False Positives: Redress and the Watch List Conundrum," Legal Memorandum No. 17, The Heritage Foundation, Washington, D.C. June 17, 2005.

⁶ It is unlikely that DHS will want to make watch lists public, as such transparency may limit their effectiveness.

modifications to this purpose should be fully disclosed and discussed in accordance with the transparency and regulation comments discussed below.

Use Benefits

The Subcommittee considered two benefits to DHS's use of commercial data to reduce false positives. The first benefit is a reduction of the impact to the misidentified individual. The second is the reduction in the amount of resources DHS expends on incorrect identifications (e.g., the amount of time taken to do a secondary screening and/or the resources associated with addressing complaints from misidentified individuals). DHS has not publicly suggested that the second issue is an important objective of its use of commercial data. This benefit could become more important, however, as DHS develops future screening programs (e.g., a false positive in an immigration screening program could result in incarceration). This type of efficiency benefit may be considered in a subsequent report of the Data Usage and Sharing Subcommittee.

The first benefit of reducing the impact on misidentified individuals has been the subject of considerable public discussion; for example, several individuals have complained of repeated inconveniences due to secondary screenings at airports.⁷ These incidents of airport misidentifications have also resulted in the misidentified individual knowing he or she has been misidentified (i.e., the individual is subject to repeated secondary screenings at airports). The Subcommittee is highly skeptical that these airport misidentifications alone constitute sufficient harm to justify access to a large set of commercial data.⁸

Use Risks

Privacy advocates and members of the general public have expressed concern about government access to commercial data. While the government already has access to large amounts of personally identifiable information (e.g., tax returns, law enforcement files, and government job applications),⁹ there is concern over supplementing such information with detailed transaction data, which creates a clearer picture of an individual's daily life. The specific risks mentioned by those concerned can generally be organized into the following categories.

⁷ The Subcommittee recognizes that it is likely that there are grave consequences from false positives in other DHS screening programs.

⁸ The Subcommittee understands that frequent airport misidentifications could lead to substantial harm to an individual (e.g., missing an important flight or the inability to perform the duties of a travel-dependent job). If there were a significant number of these instances, that might justify access to a large set of commercial data.

⁹ For each of these categories, there are likely restrictions on whether, and how, the relevant government agencies can share such data.

1. Secondary Use - the use of data for any purpose other than that for which they were initially collected. For example, when data collected to prevent terrorist activity are used to identify other non-terrorist criminal acts, some might consider the secondary use of the data inappropriate.

2. Third Party Transfer - when data collected by one government agency are transferred to other third parties that are not the original recipients of the data. These third parties might include other government agencies, contractors, or private commercial data processors that may use the data in ways not envisioned by the original collection agencies.

3. Security Breach - as current events make all too clear, personal information is a valuable commodity. As such, it is an attractive target for theft and misuse. Thus, collections of personal information necessarily risk attack and breaches of information security. Also, use of commercial data for homeland security purposes may create an incentive for terrorists or organized crime to modify the commercial databases. Understanding the safeguards provided for the data both at DHS and at the commercial information provider's data warehouse is critical to protect against the use of such data actually decreasing security.

The Subcommittee recognizes the significance of these privacy and security risks and makes the following recommendations:

1. Secondary Use - to minimize risk from the use of commercial data, DHS should make clear to the public how it will ensure that such data are not used for any purpose other than that for which they were initially intended.
2. Third Party Transfer - DHS should make clear what types of third parties (e.g., contractors, data processors) will have access to the data and whether those third parties will have the right to transfer the data to other affiliated or non-affiliated entities.
3. Security Breach - the only certain method for securing personally identifiable data is not to collect or store them in the first place. If the data are necessary, however, DHS should provide public assurances that robust mechanisms and procedures are in place to adequately protect against a) an authorized person using or disclosing the data inappropriately, and b) an unauthorized person obtaining or modifying the data. One example of a necessary security mechanism is the deployment of secure and unalterable logs to record the use of and access to the data. It is critical that such logs be appropriately reviewed. Another example is the need to apply strong access controls.

An additional element that is critical to the security of the data is to have a sound data retention policy and enforcement process. DHS should never retain commercial information longer than is necessary to fulfill its intended purpose. Where appropriate, DHS should automate such data retention policies (e.g., by using metadata tags that include the date on which the data should be deleted) to provide for an effective compliance process.

Authorization Limitations as a Means of Mitigating Risk

Commercial data might be useful in reducing false positives. In the face of an adverse consequence, authorities could check information drawn from commercial databases to see whether the individual is in fact the suspect on the terrorist watch list. The information would confirm or refute the supposition, or fail to do either.

If the primary benefit from such use of commercial data is allowing an individual to avoid an obvious inconvenience (for example, undergoing secondary screening while traveling), however, then DHS should consider less intrusive options, such as requiring the permission of the individual prior to accessing the person's data or having the individual provide supplemental information to obtain a credential of trustworthiness.¹⁰ An individual may refuse (for a variety of reasons) the government the right to access the information. This person may be willing to suffer related adverse consequences, depending on what those might be.

There may be instances where repeated inconveniences rise to the level of substantial harm to an individual. For example, a person who is repeatedly stopped for secondary screening may have difficulty performing the duties of employment that requires extensive travel. In these instances, DHS should look for alternatives similar to those mentioned in this report to allow the impacted individual to avoid repeated misidentifications. It will be critical in these circumstances for DHS to implement an efficient, simple and easily understandable system for taking advantage of such alternatives.

How DHS should apply these principles will vary, depending upon the program in question. For example, in the Secure Flight program, where the misidentified people suffer the inconvenience of secondary screening and are aware of their identification, the principle of prior authorization as a limitation seems particularly apt and substantially moots the need for commercial data.

It is likely these conditions (of relatively minor inconvenience and awareness of identification) may not hold true for other existing and future DHS screening

¹⁰ More discussion on possible alternatives is provided below; these are just examples. DHS will also need to assess any possible alternative to make certain it does not allow potential terrorists to manipulate the system.

programs. For example, DHS may screen people to allow them to work for contractors at sensitive infrastructure locations (e.g., power plants, bridges, airports). A false positive in such a screening program may cause considerable harm to an individual. Further, the individual may never be told why he or she was not granted the position. In these instances, DHS will need to perform a new assessment of the benefits and potential harm, and identify new methods of controlling the use of the commercial data. Also, such considerable harm may implicate due process issues.

The Subcommittee believes that, in instances where the amount of harm suffered by the individual is not grave, the use of commercial data to reduce false positives is not warranted. If the benefits to be derived are not great, then incurring the risks associated with access to commercial data is unwise. If the harm is serious, but is obvious to and avoidable by the individual (e.g., being denied a passport and being told the reason for the denial), then the individual could have an opportunity to opt into other measures to reduce the risk of false positives. While assessing these competing values is a question best left for elected representatives, the Subcommittee is of the view that the strongest case for the use of commercial data arises when an individual will suffer substantial harm and may not know they have suffered such harm.

If, after an assessment of the benefits and potential harm, DHS concludes it does need to access to commercial data, then it will need to show that it has taken appropriate measures to secure the data and will only retain the data for the minimum amount of time necessary to accomplish the defined purpose.

Transparency and Data Subject Access

DHS (or any government agency seeking to use commercial data) must give careful consideration to public oversight and the process for providing transparency.

The public policy imperative of a transparent government is a cornerstone of our democracy, but it is not an absolute. How much information to disclose and by what mechanism are important issues for DHS's consideration.

Questions to be considered should include: Does the general public benefit from knowledge about which classes of commercial data are used by DHS for traveler screening programs? What would be the potential privacy consequences from withholding this information? How granular do the details contained in the public disclosure need to be?

Decisions about how much to disclose to the general public must also take into account whether disclosure of information about commercial data used for homeland security purposes would enable manipulation of the system. Would terrorists or criminals be able to use the provided information in a way that

assists them in their efforts to evade detection and perpetrate an act of terrorism?

One approach to providing transparency involves the development of a calibrated disclosure system.¹¹ Decisions about whether to disclose and how much detail to provide could be calibrated to the nature of the adverse action. As described above, in the future DHS may operate screening programs that have substantial consequences to misidentified individuals. Examples of such consequences could be the denial of certain privileges (*e.g.*, a hazmat license), or even detention or incarceration. The Subcommittee believes the more significant the adverse consequences may be, the greater the need for transparency. One mechanism for assuring transparency may be for DHS to have an objective third party provide a full assessment of the system.

The members of the Subcommittee see merit in seeking new methods for transparency and access and believe many equally valid approaches may exist and are worth considering. Which approach DHS ultimately chooses is not as important as the DHS commitment to address issues of transparency—both to the general public and to individuals as a means of redress—before acting to acquire and use commercial data.

Regulation and Redress

As described above in the *Use Risks* section, there is potential for DHS's use of commercial data to result in harm to misidentified individuals. In these instances, the individual should be protected against such harm.

If the government collects, maintains, and uses the data—or if they are co-mingled with government data and stored on government hardware—the data may not be subject to the exceptions in the Privacy Act of 1974.

The Privacy Act requires disclosure to individuals of the information gathered, governs how and under what circumstances the government may disclose information to others, provides principles regarding the gathering and use of information, and specifies liability for misuse. The Privacy Act also restricts the transfer of data for purposes other than those for which they were originally collected.

There are many ways DHS can obtain the benefits of commercial data without being subject to the Privacy Act. Use of contractors, for example, may be deemed to avoid application of Privacy Act rules. The Subcommittee believes, however, that DHS should subject itself to the provisions of the Privacy Act for its uses of commercial data as a means of ensuring greater transparency for its

¹¹ Rosenzweig and Jonas, *supra*.

activities and more significant avenues of redress.¹² Further, there should be adverse consequences should DHS programs not comply with these restrictions.

The Subcommittee also recommends that DHS adopt easy-to-use mechanisms by which individuals may submit questions or complaints. These mechanisms should be clearly communicated to affected individuals (e.g., through signage at airports and prominent placement on DHS websites) and be made easily accessible to misidentified individuals. DHS also should provide a mechanism for individuals to understand their rights and receive reports on the status of their questions or complaints.

Alternatives

The Subcommittee has identified three less invasive options for DHS's use of commercial data to drive down the rate of false positives. These are only examples of possible alternatives. The Subcommittee recommends that each DHS department considering access to commercial data to decrease false positives conduct a thorough assessment of potential alternatives.

One alternative is for DHS to ensure that all public record data are optimally utilized across agencies and screening programs. The removal of any unnecessary legacy data blockages, with appropriate data security and data integrity safeguards, may contribute to a reduction in false positives. Interagency/departmental data sharing for security purposes should be optimized, regardless of what direction a particular agency or department ultimately takes. If, however, this type of optimization results in a substantial reduction in false positives, DHS should weigh whether the use of commercial data is necessary at all. Of course, any potential inter-governmental data sharing for DHS screening programs should be subject to the same considerations outlined above, including the minimization principle and appropriate oversight, access, and redress mechanisms.

A second approach employs limited access to and use of commercial data in screening programs. In sharp contrast to the *carte blanche* approach, which involves unfettered government access to commercial data on millions of Americans, a more measured approach would permit access to data only on subjects who have experienced adverse consequences as a result of an alleged false positive. In an effort to provide redress for an adverse reaction caused directly by an alleged false positive, the relevant government agency would secure permission from the data subject to access commercial data about him or her. Under this scenario, the benefits of additional information are enjoyed without raising additional privacy concerns. By the same token, those

¹² This recommendation presumes that application of the Privacy Act would not create additional security issues. If DHS has information to support a contrary conclusion, the Subcommittee recommends a public discussion of whether the Privacy Act should apply.

individuals who elect to withhold their information would be subject to additional security measures, such as secondary screenings or even missed flights, but would preserve their privacy at their comfort level.

Third, DHS (or its departments, such as TSA) could provide individuals an opportunity to provide additional identifiers about themselves at the time of their first false positive experience. There is preliminary evidence suggesting that such an information exchange substantially reduces the incidence of being misidentified.¹³ After providing such information, the government could issue the individual a credential of trustworthiness. Individuals who would prefer not to provide additional information could instead opt to accept the risk of future false positives.

Conclusion

At the core of the commercial data question is the issue of privacy-sensitive alternatives. Recently, DHS Assistant Administrator Justin Oberman shared his view of how commercial data is being used by DHS in domestic airline passenger prescreening test programs:

“[W]e are conducting a test which is ongoing. In fact, we’ve just recently extended it to look at the potential application of commercial data in domestic passenger prescreening. The two major objectives of this commercial data test are as follows: Number one is to see if we can use this data to enhance and build passenger information, received from carriers, to more effectively match against the list. So what we mean is that, for example, there are today instances in which an innocent individual will have the same first, middle, last name, and date of birth as someone on the watch list. It happens more than you probably think. One of the things we’re looking at is can we, with the addition of more information on a passenger, be able to more effectively determine whether or not that person is on the list, even if we have the full name and date of birth coming in. So that’s one piece, and we refer to that as enhanced watch list matching. The second thing we’re looking at is the idea or ability to verify passenger’s (sic) identities. The U.S. Government has a very comprehensive list of known or suspected terrorist threats. But, of course, it’s highly likely that there are other threats there that may or may not, in fact, be on the list.”¹⁴

Thus, at least one senior staff member at DHS would like to access and use commercial data not only to reduce false positives, but also to reduce false negatives (i.e., to help identify terrorists). The envisioned dual use of broad

¹³ See response of Justin Oberman:
http://www.dhs.gov/interweb/assetlibrary/privacy_advcom_06-2005_res_joberman.pdf.

¹⁴ Oral testimony of Justin Oberman before the United States Department of Homeland Security’s Data Privacy and Integrity Advisory Committee, Cambridge, MA June 15, 2005.

categories of commercial data to reduce false negative misidentifications raises serious issues and, as noted above, will be addressed further in a subsequent Subcommittee report. On the issue of false positive errors, the Subcommittee recommends commercial data be used only when:

- It is necessary to satisfy a defined purpose
- The minimization principle is used
- Data quality issues are analyzed and satisfactorily resolved
- Access to the data is tightly controlled
- The potential harm to the individual from a false positive misidentification is substantial
- Use for secondary purposes is tightly controlled
- Transfer to third parties is carefully managed
- Robust security measures are employed
- The data are retained only for the minimum necessary period of time
- Transparency and oversight are provided
- The restrictions of the Privacy Act are applied, regardless of whether an exemption may apply
- Simple and effective redress is provided
- Less invasive alternatives are exhausted

The members of the Subcommittee believe effective screening programs, as part of a broader homeland security platform, are fundamental and necessary. The Subcommittee also realizes all new programs experience glitches during their early stages of development and implementation. For example, unacceptably high levels of false positive errors seem to be the most significant early complication associated with traveler screening programs now widely deployed throughout the United States. The Subcommittee concludes that it is of primary importance for DHS to continue to foster a relationship of trust with the individuals whose personal information it collects, stores and processes. As DHS explores how to reduce false positives, the Subcommittee hopes DHS will strongly consider adopting the recommendations made in this report and designing in such recommendations early in the development of new programs.