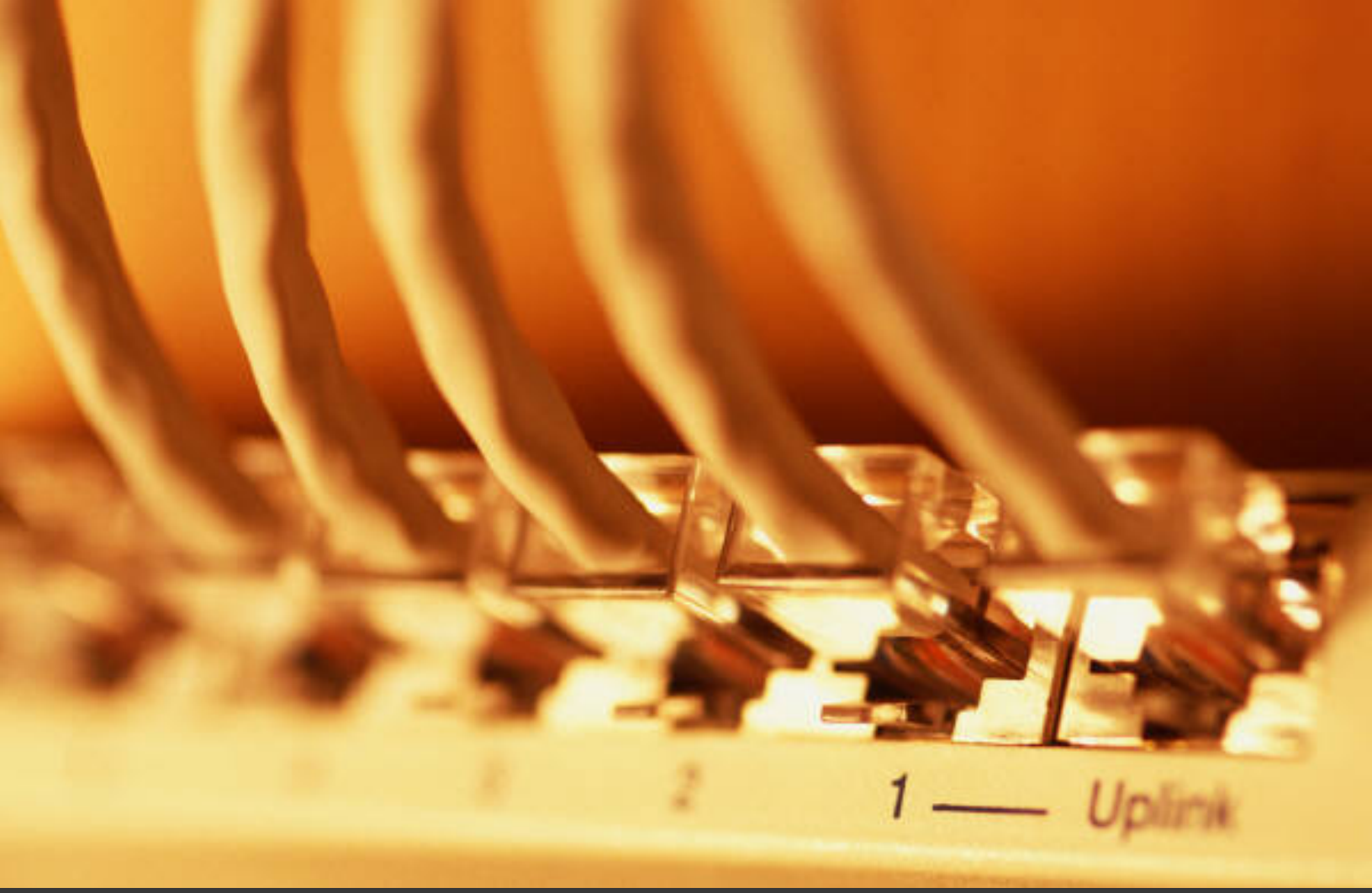

MATRIX Report

DHS Privacy Office Report to the Public Concerning the Multistate Anti-Terrorism Information Exchange (MATRIX) Pilot Project

December 2006

Homeland Security

Report to the Public Concerning the Multistate Anti-Terrorism Information Exchange (MATRIX) Pilot Project

Privacy Office
U.S. Department of Homeland Security
Washington, DC

December 2006

TABLE OF CONTENTS

MATRIX Report
DHS Privacy Office
December 2006

I. Introduction

The Department of Homeland Security (DHS) Privacy Office was established pursuant to Section 222 of the Homeland Security Act of 2002, and is headed by the Chief Privacy Officer, who is responsible for privacy policy within the Department. Among the responsibilities of the Privacy Office is the obligation to report on complaints and inquiries regarding possible privacy violations. In response to a request by the American Civil Liberties Union, the Privacy Office has conducted a review of the Multistate Anti-Terrorism Information Exchange (MATRIX) pilot project and the role of DHS in that program. Although the MATRIX program has now been discontinued, the Privacy Office's review illuminates several lessons to be learned from the program which are applicable to any program involving the collection and use of personally identifiable information.

The MATRIX pilot project was a "proof of concept" initiated in response to the need for information sharing within the state law enforcement community after the September 11, 2001, terrorist attack. It was born out of a series of meetings of state law enforcement officials who wanted to improve data sharing for domestic security and law enforcement purposes. In May 2002, the Coalition of State Law Enforcement Agencies (the Coalition) decided to pursue a data integration project using criminal and public databases. The proposed project was called the Multistate Coalition Project to Exchange Intelligence and Other Information, and included: California, Florida, Georgia, Kentucky, Louisiana, Michigan, New York, Ohio, Oregon, Pennsylvania, South Carolina, Texas, and Utah. The Coalition project adopted the Multistate Anti-Terrorism Information Exchange (MATRIX) name in October 2002 and sought Federal funding.

The MATRIX pilot project was a collaborative information sharing effort involving public, private, and non-profit entities. The project was funded first through a $4 million grant by the Department of Justice's Bureau of Justice Assistance in December 2002, and then, in July 2003, through an $8 million Cooperative Agreement with the DHS Office for Domestic Preparedness, located within the Office of State and Local Government Coordination and Preparedness (ODP/SLGCP). Though the project received Federal funds, it was a state-controlled information program. DHS and the Department of Justice selected the non-profit Institute for Intergovernmental Research (IIR) to administer the project. IIR then selected Seisint, Inc. (Seisint), an information and technology company, acquired in September 2004 by LexisNexis, to provide search capability and access to certain state and public databases.

In response to a number of national security efforts involving information gathering undertaken after 9/11, some members of the public became increasingly concerned about how government programs were using personal information and whether these programs were engaging in "mission creep" or in unrestricted "data mining." This heightened sensitivity to privacy in the post 9/11 period generated concern about the MATRIX project from the beginning.

As discussed below, the MATRIX pilot project was not a data mining project, but rather an information sharing program among the states to increase the speed, accuracy, and efficiency of law enforcement investigations. The project was a state-controlled information program and only accessed state-owned or publicly available records that were otherwise already available to law enforcement without a subpoena or court order. Confusion regarding the MATRIX project arose, however, in part because of misinformation disseminated in the early stages of organizing the project, as well as the project's failure to consider privacy from the inception of development.

II. DHS Involvement with the MATRIX Pilot Project

In July 2003, ODP/SLGCP entered into a Cooperative Agreement with IIR to serve as the administrator for the project. The goal of the Cooperative Agreement was to enhance state and local capabilities to share and exchange terrorist threat information. Under the terms of the Cooperative Agreement, the funding was designated to assist with pilot testing a system for data analysis and integration of terrorist threat and other intelligence information. In addition, the Cooperative Agreement designated funding to establish user accounts for MATRIX participants, and to create a secure web site for each participating state to facilitate information sharing.

Although the Cooperative Agreement described the project's application to terrorism, IIR reported that only 2.6% of the cases investigated over the course of the MATRIX pilot project were related to terrorism. In fact, the MATRIX project was predominantly used to investigate fraud, robbery, and other crimes, including assault, homicide, and narcotics cases, underscoring the value of the program as a tool for traditional law enforcement.

Although DHS was a key grantor of funds for the MATRIX pilot project, DHS funds were not used to support DHS access to the project's databases. Instead, according to IIR, the Florida Department of Law Enforcement (FDLE) independently funded several hundred user licenses, including licenses for 17 DHS U.S. Immigration and Customs Enforcement and U.S. Coast Guard investigators based in Florida. The DHS components were participants, along with state and local entities, in one or more Regional Domestic Security Taskforces, and FDLE provided the licenses pursuant to these partnership programs. IIR reported that these 17 licensees combined queried MATRIX data a total of 11 times as part of their law enforcement duties.

III. Privacy Concerns Posed by the MATRIX Pilot Project

The Privacy Office believes that the MATRIX pilot project lost public support because it failed to consider and adopt comprehensive privacy protections from the beginning. The project lacked a privacy policy that clearly articulated the project's purpose, how it would use personal information, the types of information contained, and the security and auditing protections governing the project. Such a policy framework is necessary to promote transparency to the public and establish the boundaries of an information program to reduce the possibility of mission creep and the risk that information could be

used for unauthorized purposes. Although the pilot project was launched in July 2003, a Privacy Policy was not approved by the MATRIX Board of Directors, which oversaw the project, until November 2003. Issuing such a policy at the time the project was launched could have prevented some of the privacy backlash that the project received.

Second, the MATRIX project lacked adequate audit controls. It was not until May 2004, that the Board established an audit requirement, and it was limited to requiring that participating states conduct self-audits. IIR told the Privacy Office that, to its knowledge, during the project only three of the states conducted a self-audit. As always, independent, third party audits are preferable, although the resources needed to conduct such audits are not insignificant. Moreover, over the course of the project, neither the DOJ nor DHS conducted an independent, formal audit; instead, they relied on IIR progress reports, some site visits, attendance at the MATRIX Board meetings, and one-on-one consultations to monitor IIR and the agreements.

IV. Privacy Practices During MATRIX Pilot Project

Although the above review underscores the MATRIX project's shortcomings with regard to privacy, over the course of the pilot project, the MATRIX Board of Directors, which was composed of state law enforcement agency representatives, took a series of steps to mitigate the privacy concerns that were raised in the public media. First, as noted above, the Board adopted a Privacy Policy in November 2003 and published it on its website. As a state-controlled project, the Privacy Policy assigned compliance with the policy to each participating state. Second, in April 2004, the MATRIX Board decided to alter the structure of the project from a centralized, single-database system housed on the premises of Seisint, to a decentralized or "distributed" model that would allow each state to keep its own data. Third, at subsequent meetings, the Board supported the continued use of its website, www.matrix-at.org, to increase the transparency of the MATRIX project. Fourth, the Board directed FDLE to draft audit procedures and a standard audit form to establish a minimum standard among the states, advising states that they could implement a stricter set of audit procedures if they so chose. In addition, in February 2005, the Board invited noted privacy experts to review the project and provide guidance on enhancing the privacy components of the project. The experts provided the following recommendations to the Board:

1. Require a user to provide a case identifier or case number prior to running a query to facilitate auditing and ensure the data is being used appropriately.

2. Help to avoid mission creep by ensuring the data sets are locked in as they currently exist and develop a process for the Board to add or delete data sets with justification.

3. Define public records to mean information available to the public by accessing data from courts, Department of State, the internet, and other sources, as distinguished from commercially available data sets.

4. Ensure the system is only used for law enforcement purposes and develop a vetting process for changing or adding to the purpose to include members of the privacy community.

In addition to these recommendations, the experts shared a number of other observations with the Privacy Office during interviews for this review. They believed the MATRIX project was misunderstood because of a lack of transparency, and that the project would have benefited from having a comprehensive privacy policy from the outset. They also stated that the project was over-sold as a pattern analysis tool for anti-terrorism purposes, but was a valuable tool to improve traditional law enforcement investigations by making searches more efficient and identifying linkages that would otherwise be difficult to reproduce manually. Moreover, they noted that the Board had made strides in addressing privacy issues over the course of the project and believed that MATRIX could have been well received if privacy had been addressed more thoroughly before it was launched. Finally, they suggested that in the future, such programs think carefully about their name selection, since too many projects have used names that were inflammatory and did not accurately describe their purpose.

The MATRIX Board responded to a number of the experts' recommendations, including mandating that investigators using the system input a case name prior to running a query to facilitate audits and project oversight and directing IIR to draft a charter for the MATRIX project to increase transparency. With regard to auditing, the Board also agreed to include an audit report during each Board meeting. These audit reports would include the audit findings from the respective states and actions taken as a result of those findings. These recommendations were not fully implemented, however, due to the termination of the project.

V. The End of the MATRIX Pilot Project

Although the Cooperative Agreement with DHS remained in effect until December 31, 2005, access to Seisint's search application was terminated on April 15, 2005, effectively ending the MATRIX pilot project. As of April 2005, only four states out of the original 13 Coalition states remained: Connecticut, Florida, Ohio, and Pennsylvania. Florida and Ohio signed new, individual agreements with LexisNexis allowing each state to continue to use Seisint's search application to analyze its own data. There was no longer, however, any networking among states using the Seisint search application.

VI. Conclusion

The review conducted by the Privacy Office sought to clarify the scope of the MATRIX pilot project and its operations. As described above, the project was a state-controlled information program and only accessed state-owned or publicly available records that were otherwise already available to law enforcement without a subpoena or court order. These records did not include financial or medical information. Moreover, the law enforcement investigators who were licensed to use the program only accessed it to

support specific investigations, directly tied to an active criminal investigation, or to prevent a criminal act based on investigative information. The project's search technology did not have the ability to monitor, track, or conduct surveillance. It was not a "data mining" program designed to search for patterns of suspicious behavior of unsuspected individuals to predict criminal, including terrorist, activity or to produce profiles of terrorists. It was used solely for the purpose of pursuing investigative leads, which in turn, had to be followed up by traditional investigative analysis and confirmation by a law enforcement officer. Fundamentally, the project allowed for greater efficiency and effectiveness in conducting traditional law enforcement investigations.

The Privacy Office believes, however, that the MATRIX pilot project was undermined, and ultimately halted, in large part because it did not have a comprehensive privacy policy from the outset to provide transparency about the project's purpose and practices and protect against mission creep or abuse. The recommendations of the Privacy Office rest on the basic premise that information programs such as the MATRIX pilot project can protect privacy, while increasing homeland security. Building privacy into the architecture of an information program can help ensure that the program achieves its objectives while safeguarding individual privacy. The Privacy Office offers the following recommendations as lessons learned from its review of the MATRIX project. These recommendations build on the objectives of the Privacy Act of 1974 and the underlying fair information principles to foster public trust in information programs.

VII. Summary of Recommendations

1. Developers of information programs should build privacy into the architecture of the program during the earliest stages of program development.

2. Government funded information programs should obtain leadership support for privacy from the very top of the agency and invite participation of all of the offices affected or involved, including the CIO, legal, public affairs, and privacy offices, in order to build effective privacy policies and practices into such programs.

3. Since transparency is the most fundamental of all the fair information principles, agencies, pursuant to the Privacy Act of 1974, programs must give the public notice, with limited exceptions, of the existence of an information program and inform them of (a) the purpose of the information collection; (b) what information is collected; (c) how it will be used; (d) to whom it will be disclosed; and (e) what rights, if any, individuals have to access or correct the information. To promote transparency, the Privacy Office recommends that agencies extend the Privacy Impact Assessment (PIA) requirement of the E-Government Act of 2002 to any Federal contract, grant, or cooperative agreement creating or supporting an information system. In addition, agencies should consider publicizing information

programs on their website and through press releases so that the public is fully aware of new programs and the scope of their practices.

4. To further promote transparency, the Privacy Office recommends that any government contract, grant, or cooperative agreement creating or supporting an information program include a provision requiring compliance with any SORN or PIA addressing the program.

5. A number of technologies exist to help prevent "mission creep" and enforce compliance with a program's privacy policies. The Privacy Office recommends that information programs consider employing privacy-enhancing technology tools, including:

    a. rules-based systems, in which information programs embed business rules using computer code into the program, to ensure that the program implements all of its access and use policies;

    b. anonymization tools that enable programs to use data without exposing the identifying information except on a need-to-know basis (e.g. in data matching and linking analysis programs); and

    c. real-time, immutable audits that identify when data are accessed, by whom, and when data are changed to help prevent abuses before they occur.

The Privacy Office recognizes that the Government's use of personal information and, in particular private sector databases, is a pressing privacy issue for DHS and the public. The Office hopes that this report helps government agencies better understand how to protect the privacy of individuals while achieving critical national security objectives.