Discoverability

MARKLE

Task Force on National Security in the Information Age

MEETING THE THREAT OF TERRORISM:

Improve Information Sharing, Create a Trusted System, Facilitate Access to Critical Data

Discoverability is the first step in an effective system for information sharing, offering users the ability to "discover" data that exists elsewhere. Data is tagged at the point of collection with standardized information (e.g., who, what, where, when) and submitted to a central index. Just as a card catalogue in a library serves as a central index, directing users to relevant books—but doesn't provide the book itself—these "data indices" point users to data holders and documents, depending on the search criteria used.

Knowing where relevant information can be found or who has the information is the essential first step towards information sharing.

Discoverability means users can "discover" selected values (e.g., who, what, where, when), but cannot gain access to the underlying information until the user requesting access is authorized and authenticated. In many ways, knowing where relevant information can be found or who has the information is the essential first step towards information sharing as this makes collaboration and analysis possible. A system of discoverability also avoids the bulk transfers of data required in large centralized databases, improving security and minimizing privacy risks.

Commercially available, off-the-shelf technology can make government information discoverable and accessible to authorized users, virtually eliminating wholesale information transfers. In addition, emerging anonymization technology that allows for the removal of personally identifiable information (PII) even in the card catalog or indexes greatly reduces the risk of unintended disclosure of this information.

The traditional information sharing model falls short by requiring either the sender to know what information to send to whom ("push"), or the end user to know whom to ask for information ("pull"). Whether push or pull, there are too many doors on which to knock. The chances of the right data holder and the right end user locating each other and sharing the right information are slim at best.

Results

Discoverability will:

- Create a secure foundation for effective information access and improved decision-making that increases national security by providing government officials the ability to locate relevant information.

- Enhance privacy and security protections by ensuring that users can locate what they need, but only what they need, eliminating the need for bulk transfers of data, and implementing tamper-resistant logs to enable a clean, central, and standard audit facility. Enforcement of the authorized use standard regulates information sharing based on how information will be used rather than where it was collected.

- Improve cooperation. As related data points are connected, so too are related analysts and agencies who might be unaware of their connection or shared goals.

- Strengthen cyber security. Commons audit logs facilitate automated compliance and behavior audits that can identify attempts to move beyond authorized access and/or misuse.

Action

Government-Wide Policy Guidance, Accountability, and Implementation

The Obama administration and Congress should establish policy to achieve the following:

- Require all agencies with a national security mission—not just agencies in the Intelligence Community but also others, such as the Federal Emergency Management Agency—to make their data discoverable by tagging data at the point of collection, contributing key categories of data (such as names, addresses, passport numbers) to data indices, and implementing widely available technologies to search data indices.

- Require audits to ensure accountability, which allows for better enforcement of the authorized use standard, enhanced information security, and greater privacy protections by enhancing the government's ability to detect misuse of information networks and attempts to compromise the data on such networks or the networks themselves.

- Privacy concerns must be paramount. Improved discoverability must be accompanied by a trusted system that simultaneously empowers and constrains government officials, making clear what is permitted and what is not. Information sharing succeeds only with government-wide policies and oversight providing robust protections for privacy and civil liberties. ■

About the Markle Task Force

The Markle Task Force on National Security in the Information Age has been a diverse and bipartisan group of former policy makers from the past six presidential administrations, senior information technology executives, and privacy advocates from both the public and private sectors. The Markle Task Force has recommended ways of improving national security decisions by transforming business processes and how information is shared. Its recommendations informed the 9/11 Commission Report and were subsequently included in two federal laws.

Learn more about the Markle Task Force at www.markle.org/national-security.

MARKLE
Advancing National Security in a Connected World