National Security Program
Homeland Security Project

A Policy Forum on the Use of Big Data in Homeland Security

Meeting Proceedings

On October 30, 2013, the Bipartisan Policy Center and Intel Corporation hosted a forum to explore the potential for big data innovation to improve homeland security, current and future challenges to overcome, and policy principles that will encourage innovation while safeguarding privacy and security in our increasingly connected society. This event is part of the ongoing Innovation Economy conversation convened by Intel in 2009, focused on the vital role of innovation in sustaining and building upon U.S. competitiveness in the global economy.

Overarching Themes

Security and privacy are not mutually exclusive. Using data in effective ways to create a more secure world shouldn't require a sacrifice of privacy. It does require increased oversight, control, auditing, and accountability programs to ensure that privacy is adequately protected.

The definition of data that is relevant to security can be quite broad. Would-be terrorists engage in many familiar daily-life activities—from paying highway tolls to talking on the phone. It is increasingly difficult to define data that is *not* potentially relevant to terrorist activity.

Featuring remarks from:

Alan Bersin
Assistant Secretary of International Affairs and Chief Diplomatic Officer, Department of Homeland Security

Moderated by:

Carie Lemack
Director, Homeland Security Project, Bipartisan Policy Center

Panel discussion with:

Stewart Baker
Partner, Steptoe & Johnson LLP

Mary Ellen Callahan
Partner, Jenner & Block; Former Chief Privacy Officer, United States Department of Homeland Security

Greg Nojeim
Senior Counsel, Center for Democracy & Technology; Director, Project on Freedom, Security & Technology

Christina Norwich
Forward Deployed Engineer, Palantir

Moderated by:

Ellen Nakashima
National Security Reporter, *The Washington Post*

Welcome remarks by:

David Hoffman
Director of Security Policy and Global Privacy Officer, Intel Corporation

BIPARTISAN POLICY CENTER

The Innovation Economy

Using Data to Track a Terrorist

On May 3, 2010, Faisal Shahzad was pulled off an Emirates airliner waiting to depart for Dubai from Kennedy International Airport. He was arrested for attempting to detonate a bomb in Times Square. Two days prior, he had parked his bomb-laden Nissan Pathfinder near a busy theater on a Saturday night and tried to ignite it. The bomb failed, and Shahzad fled. Authorities uncovered the plot, and his connection to it, and were able to stop him from fleeing to Pakistan. He was tried and sentenced to life imprisonment without the possibility of parole.

Law enforcement authorities worked quickly once the bombs were discovered. The car was traced to the Connecticut Department of Motor Vehicles, and registration records led them to a woman who had recently sold it for cash. There was no paperwork on the sale, but she did recall one important thing: she had exchanged a cell phone call with the buyer. That phone number, still stored in her cell phone records, matched a number in the federal Passenger Name Record database, where Shahzad was noted for his many previous trips abroad. His name was added to the no-fly list, and when the Emirates passenger manifest was reviewed, U.S. Customs and Border Protection officers were able to arrest him before he fled.

Governing data use is a key challenge. Fair Information Practice Principles and the Privacy Act say that entities that collect data must explain publicly how they intend to use the data—and then must use it only for purposes that are compatible with that intention. The potential for secondary use of data after it is collected is a concern for privacy advocates and suggests a need for careful governance of the entire life cycle of data.

Borders are more than lines on a map. Borders represent massive flows of goods and people, and are no longer viewed as the first line of homeland defense, but rather, as the last. The challenge is to push the work of securing the borders outward to the point where flows of goods and people toward the United States originate. Big data is essential in this work, as passenger or freight manifests are cross-checked against databases of known and suspected risks to identify threats as early as possible.

Discussion Summary

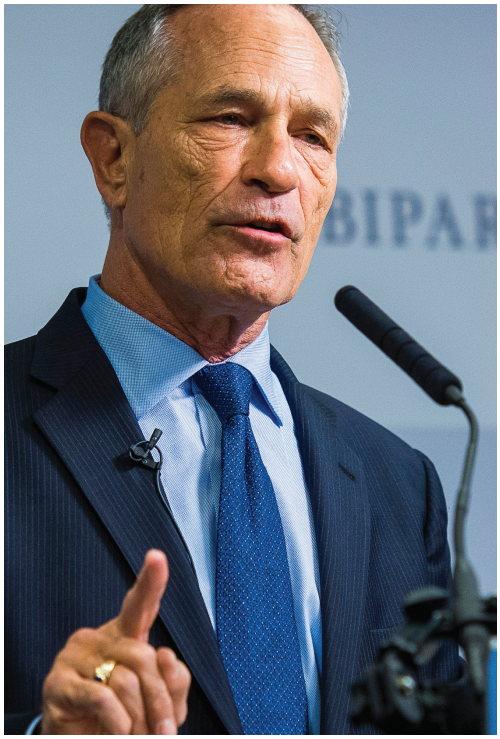
Protecting the homeland is a big and complex job. The United States has 330 official points of entry and exit, including airports, seaports, and land ports. Every day, U.S. Customs and Border Protection clears one million people into the United States. Annually 60 million passengers arrive by air, part of a 2.2 billion-passenger international transit zone. Every day, 60,000 trucks, maritime vessels, and air containers are processed and cleared into the United States. In a typical year, the United States imports $2 trillion in goods and exports $1.9 trillion, all of which enters the global supply chain.

These massive flows of people and goods generate data that can be used to enhance security, enabling analysts to differentiate among the risks presented by a particular person or cargo. Protecting the homeland against dangers posed by individual people or packages is often likened to finding a needle in a haystack. Using big data to differentiate the risk makes the figurative haystack smaller.

In general, big data is used for security purposes in four basic ways:

- To screen individuals against known watch lists;
- To identify high-risk subjects;
- To generate investigative leads; and
- To electronically gather intelligence.

The Department of Homeland Security (DHS) currently focuses primarily on the first two categories of big data use—using federated computer searches to scan large amounts of data and algorithms that highlight matches with specific criteria. These processes and systems are overseen by the DHS Office of Privacy to ensure that appropriate protocols are in use governing the data, its collection, its analysis, and its dissemination.



From left to right: Alan Bersin, Assistant Secretary of International Affairs and Chief Diplomatic Officer, Department of Homeland Security; Ellen Nakashima, National Security Reporter, The Washington Post*; Greg Nojeim, Senior Counsel, Center for Democracy & Technology, Director, Project on Freedom, Security & Technology; Christina Norwich, Forward Deployed Engineer, Palantir; Stewart Baker, Partner, Steptoe & Johnson LLP; Mary Ellen Callahan, Partner, Jenner & Block, Former Chief Privacy Officer, United States Department of Homeland Security*

Balancing Security and Trust

Concerns about privacy have been heightened in recent months by revelations that the National Security Administration collected the bulk telephone records and e-mails of millions of Americans. Section 215 of the Patriot Act, originally authorized by Congress in the weeks following the September 11 attacks, gives the federal government the right to collect "tangible things" such as telephone or business records, or items such as books, records, papers, and documents, if the FBI asserts that the items may be related to investigations into international terrorist activities.

Privacy advocates worry about "who is watching the watchers," and call for more transparency from the government about its collection and use of data. Security experts seek ways to offer transparency without compromising effectiveness. The answer to this tension may be found through technology. Rule-based internal access controls can be built into data systems to monitor access and use and prevent the misuse of proprietary information.

The National Counterterrorism Center (NCTC), established in 2004, is the primary organization in the U.S. government for integrating and analyzing all intelligence pertaining to counterterrorism. The NCTC collects data related to travel, immigration benefits, and suspicious financial transactions—types of data found to be most likely to contain significant amounts of terrorism information. These categories of data are subject to specific standards and protocols.

> "The bulk phone records program is a good example of the shift of surveillance to collecting the haystack and then, based on reasonable articulable suspicion, trying to find the needle."
>
> *—Ellen Nakashima, The Washington Post*

On all sides of the privacy-security debate, there is support for strong controls on data access and use, clear protocols for and transparency about its collection, and robust auditing procedures to oversee its use.

Top row, left to right: David Hoffman, Director of Security Policy and Global Privacy Officer, Intel Corporation; Alan Bersin, Assistant Secretary of International Affairs and Chief Diplomatic Officer, Department of Homeland Security; Carie Lemack, Director, BPC Homeland Security Project; Ellen Nakashima, National Security Reporter, The Washington Post

Bottom row, left to right: Greg Nojeim, Senior Counsel, Center for Democracy & Technology, Director, Project on Freedom, Security & Technology; Christina Norwich, Forward Deployed Engineer, Palantir; Stewart Baker, Partner, Steptoe & Johnson LLP; Mary Ellen Callahan, Partner, Jenner & Block, Former Chief Privacy Officer, United States Department of Homeland Security

Conclusion

In the post-9/11 era, Americans want and expect authorities to detect and stop terrorist attacks before they happen. Big data is instrumental in achieving this goal. At the same time, Americans also want and expect that their personal information, when collected, will be safeguarded and their privacy protected. These goals are not mutually exclusive, but they do require the review, development, and continual monitoring of appropriate standards, practices, and policies.

"There is nothing inconsistent between the use of big data [in homeland security] … and the protection of personal data."

—Alan Bersin, Department of Homeland Security

About the Innovation Economy Series

The Bipartisan Policy Center hosted two forums in collaboration with Intel to explore the potential for big data innovation to advance efforts in the areas of homeland security and health care. Discussions focused on the promise of big data, current and future challenges to overcome, and policy issues that must be addressed to encourage innovation while safeguarding privacy and security in our increasingly connected society.

This event is part of a broader 2013 "Innovation Economy: Information Revolution" series of roundtable and public forums convened in parallel by the Aspen Institute and the Bipartisan Policy Center, in collaboration with Intel. The Innovation Economy conversation was convened by Intel in 2009 to focus on the vital role of innovation in sustaining and building upon U.S. competitiveness in the global economy.

About the BPC Homeland Security Project

The BPC Homeland Security Project's core mission is to be an active, bipartisan voice on homeland and national security issues. With terrorist threats and tactics still lethal, and becoming more complex, the project works to foster public discourse, evaluate reform, provide expert analysis, and develop proactive policy solutions on how to best address emerging security challenges. Carie Lemack serves as the director of the Homeland Security Project.

Disclaimer

This event was hosted by the BPC Homeland Security Project. The findings and recommendations expressed herein do not necessarily represent the views or opinions of the Bipartisan Policy Center, its founders, or its board of directors.

Founded in 2007 by former Senate Majority Leaders Howard Baker, Tom Daschle, Bob Dole and George Mitchell, the Bipartisan Policy Center (BPC) is a non-profit organization that drives principled solutions through rigorous analysis, reasoned negotiation and respectful dialogue. With projects in multiple issue areas, BPC combines politically balanced policymaking with strong, proactive advocacy and outreach.

BIPARTISAN POLICY CENTER

1225 Eye Street NW, Suite 1000
Washington, DC 20005
(202) 204-2400

WWW.BIPARTISANPOLICY.ORG