COUNCIL on FOREIGN RELATIONS

NYPD's Powers of Threat Perception

Author: Matthew C. Waxman, Adjunct Senior Fellow for Law and Foreign Policy
August 9, 2012

The New York Police Department (NYPD) unveiled a new "**Domain Awareness System**" on Wednesday that combines and analyzes many streams of information to track possible criminals and terrorists. According to Mayor Michael Bloomberg, "This new system capitalizes on new powerful policing software that allows police officers and other personnel to more quickly access relevant information gathered from existing cameras, 911 calls, previous crime reports, and other existing tools and technology." The program illustrates the growing power of data analytics technology to support counterterrorism and law enforcement, and it raises questions about the appropriate limits and oversight of those processes.

Concerns Over Surveillance

The fiercest debates about domestic counterterrorism since the 9/11 al-Qaeda attacks have generally focused on the methods by which government collects information. At the federal level, for example, the controversy surrounding the NSA's warrantless surveillance programs in 2005 was intense. In New York City, the NYPD's reported programs to gather information on **ethnic and religious communities (AP)** have spurred demands from some quarters for tighter restrictions and oversight. Recently, public and congressional attention has shifted to emergent technologies such as unmanned drone aircraft and the pervasiveness of location-tracking signals in mobile electronic devices and, again, the authority of government to collect information on individuals.

The NYPD's Domain Awareness System shows the significant intelligence value of analytic technologies for integrating various government information caches. In announcing the program, which is governed by guidelines and safeguards developed several years ago, the mayor's office emphasized the important collaborative role that police officers and private sector software developers played in designing the system. But surprisingly, given recent controversies, its written press release did not explicitly address potential privacy and oversight concerns.

Expectations of Privacy

Although novel surveillance technologies always prompt new questions about civil liberties, setting and enforcing appropriate limits on government *collection* of data--at least conceptually--present a very familiar challenge: with regard to searching an individual's home or listening to an individual's phone calls, the government must usually have sufficient suspicion of wrong-doing and obtain a warrant from a court. As a legal matter, the standard is generally whether an individual has a "reasonable expectation of privacy."

New means of communication, monitoring, or information storage--take, for example, license plate readers, which are one data source for the NYPD program--raise fresh questions about collection methods that some might feel clash with those reasonable expectations, but we can reason by analogy to draw and enforce new lines. This is by no means to say that this is an easy exercise. It is not, and those new lines will often be highly contested. In a case last year (***U.S. v. Jones***) about the constitutionality of warrantless GPS tracking of a suspect's car, some members of the Supreme Court noted that, "Dramatic technological change may lead to periods in which popular expectations [of privacy] are in flux and may ultimately produce significant changes in popular attitudes."

Integration and analysis of collected data streams, however, is a government power that does not fit neatly into existing conceptual frameworks for safeguarding liberty. To what extent, if any, does synthesizing data streams pose additional or aggravate privacy concerns above and beyond those associated with collecting the data in the first place? Data analytics may increase government demand for more data. Or, more optimistically, they may obviate the need for more invasive investigative or surveillance methods. And what limits should be placed on the use to which this analysis is put, and who should oversee it? Like any intelligence tool, checks are important not only to guard against abuses but to ensure continual improvement.

A Federal, State, and Local Debate

To some, the NYPD's new system--or at least its name--might seem reminiscent of the federal government's aborted **"Total Information Awareness" (TIA) program**, a program the Defense Department launched soon after the 9/11 attacks. That much more expansive and ambitious program was shut down in the face of public and congressional backlash, though similar programs were continued within federal intelligence agencies and remain important counterterrorism tools.

The fact, however, that the NYPD's Domain Awareness System is a city program (a uniquely large city, to be sure) shows that resolution of appropriate limits and oversight will play out at multiple levels of government: federal, state, and local. Besides federal data-mining programs, most states, and many major cities, for example, now have intelligence fusion centers for combining and analyzing threat information and coordinating across many jurisdictions. Herein lies additional legal and policy complexity, but also opportunity to work through it.

Given that it is highly unlikely that comprehensive federal legislation in this area will be enacted anytime soon, we will not have uniform rules to govern these growing capabilities. That is a good thing, because different locales face such different threats. Moreover, experimentation and adaptation, along with the public debate that accompanies them, can help cultivate and extend best-practices as these powerful analytic technologies continue to advance and spread.

Matthew C. Waxman is also Professor of Law at Columbia Law School and a member of the Hoover Institution Task Force on National Security and Law.