Counterterrorism Technology — the New York City Experience: Privacy and Constitutional Implications

Moderator: Professor Matthew Waxman, Columbia Law School

Panelists: David Raskin, Clifford Chance
Douglass Maynard, New York City Police Department
Andrew Weissmann, NYU School of Law Center for Law and Security and Center on the Administration of Criminal Law
Faiza Patel, NYU School of Law Brennan Center for Liberty and National Security

This panel featured a discussion in the ongoing debate about balancing liberty and security, with a particular focus on the New York City experience. Professor Matthew Waxman began the discussion by noting that debates about privacy and security are often focused on the activities of the federal government, even though for most people the laws and policies of local government set the balance — especially in a place like New York City. With that observation, Professor Waxman invited Douglass Maynard, who at the time of this panel, served as the Deputy Director for Legal Affairs for the New York City Police Department (the "NYPD"), to discuss the new techniques and technologies that the police department is using.

Mr. Maynard first observed that there is a tendency to view the September 11 attacks as an "iconic and historic" event that is "significant but almost distant." In fact, he said, there have been 16 terrorist plots against New York City since then. The ongoing threat is very real, and the threat is evolving, he said. Terrorists are using social media to exhort Westerners to take action. For example, there is an online terrorist magazine called *Inspire* that is very "slick" and that functions as a how-to manual for terrorists. The Tsarnaev brothers, charged with the Boston marathon bomb explosions, learned how to build their bombs from *Inspire*.

What can be done about these threats in New York City? Mr. Maynard said the NYPD does not have the resources of the NSA, and so it relies mostly on its officers to engage in quite traditional surveillance. The NYPD has the advantage of being a diverse police force that

reflects the diversity of the City, and gives the department a deep understanding of institutions and different cultures.

Mr. Maynard then highlighted one non-traditional investigative tool: the Domain Awareness System, which is a computer system that correlates information the NYPD has already gathered. The concept is similar to a detective looking at three case files at the same time, only Domain Awareness does it better and faster. The information processed includes 911 calls, video fees, chemical alert systems and license plate readers.

Professor Waxman then turned to David Raskin, the former head of the terrorism unit in the U.S. Attorney's Office for the Southern District of New York, and asked him to address whether the way data is analyzed and aggregated in systems like Domain Awareness raises concerns distinct from the initial collection of that data.

Mr. Raskin said that since September 11, the government has installed thousands of street cameras that can zoom in and out and can follow people or objects. Information from these cameras is integrated with various other streams of information. Cameras, Mr. Raskin said, have undoubtedly been helpful in investigating terrorism after the fact. Closed circuit cameras identified the Tsarnaev brothers and were critical in identifying the 2005 London subway bombers.

Mr. Raskin noted that the Domain Awareness system is lauded for something different — the ability to use real-time surveillance to detect and prevent attacks. There is a legitimate privacy concern raised with real-time surveillance, especially with a system like Domain Awareness that has "largely no oversight." There is no judicial oversight, and the internal Police Department guidelines give extensive discretion.

Balanced against that concern is the more fundamental question of whether these systems have ever helped prevent a terrorist attack. Domain Awareness did not prevent Najibullah Zazi from bringing explosives into the New York subway system, and it did not detect Faisal Shahzad when he tried to bomb Times Square. That attempt was thwarted when a hot dog vendor alerted the police. The deterrent value is unclear, Mr. Raskin said, especially with terrorists on a suicide mission.

Professor Waxman then turned the discussion to Andrew Weismann, who formerly served as the FBI's General Counsel. Mr. Weissmann discussed a set of internal FBI rules called the Domestic Investigations Operations Guide that attempts to address privacy concerns. By way of background, he explained, FBI investigations are divided into three categories: assessments, preliminary investigations and full investigations. At each stage, the FBI must have a stronger factual basis to suspect wrongdoing and, accordingly, is given access to more investigative tools.

Mr. Weissmann said the greatest concerns regarding privacy and big data arise in the assessment phase. To open an assessment, agents do not need any factual predicate; they need only have an authorized purpose. At the assessment stage, agents do not have the power of grand jury subpoenas, search warrants or wiretapping authority.

Mr. Weissmann offered as an example of an assessment the case of Tamerlan Tsarnaev, one of the Boston marathon bombers prior to the attack. The FBI opened an assessment and thus was permitted to conduct consensual interviews and review various law enforcement databases. Based on that limited investigation, there was no reason to suspect wrongdoing and the assessment was closed. This was necessary because the rules do not allow an open-ended assessment. By the time Mr. Tsarnaev traveled back to Russia and posted extremist material online, the FBI was no longer authorized to investigate him.

Another way the FBI rules address privacy is by restricting how data can be used after it is collected. This type of privacy protection generally falls outside the Fourth Amendment, which is focused on the initial collection. For every new investigative program, the FBI has several privacy lawyers focused on the question of how to limit the use of the data collected.

Professor Waxman then turned the discussion to Faiza Patel. Ms. Patel said she wanted to "take the lens out a little bit." Discussions of privacy and security tend to focus on terrorism, but, in fact, the tools for monitoring are used in all types of routine criminal cases. They are used in the context of public safety and in dealing with demonstrations like Occupy Wall Street.

It also is important to keep in mind, Ms. Patel said, that data aggregation and collection are almost always "about people who haven't done anything wrong and people who aren't even suspected of doing anything wrong." License plate readers, video cameras and location tracking gather data on everyone, not just criminals. Governments now have the capability to use a device called a Stingray, which basically mimics a cell phone tower, to read location data without having to go to the phone companies or get a court order.

Other areas of indiscriminate data collection include facial recognition technology, credit card data and public motor vehicle and school records. The "common thread" is "indiscriminate collection involving primarily non-criminal activity."

Ms. Patel said that these data gathering tools are touted as deterring crime, but that this claim is far from clear. She referred to a study of 13 police districts in London that installed video cameras. There was a statistically significant crime drop in only one district and an increase in crime in six.

The data gathering tools also are touted for being able to predict terrorist attacks, but Ms. Patel said that this claim is doubtful. The use of big data to predict consumer spending habits is based on millions of purchasing decisions, but terrorist attacks are very few, and each is distinctive. There is no evidence of big data predicting or preventing one.

Ms. Patel said that these threats to liberty pose a unique challenge because of the lack of democratic controls. Whereas a law enforcement policy like stop-and-frisk is highly visible in a community and can be the subject of a vigorous political response, it is harder for the public to respond to tactics when citizens are not informed about what the government is doing.

Professor Waxman invited Mr. Maynard to respond.

Mr. Maynard first noted that the Domain Awareness System was not intended to be a "magic machine" to identify terrorists and that it should not be judged by that standard. He added that the deterrent effect of systems like Domain Awareness cannot be overstated: "The attack that doesn't happen is one you never know about." He offered two examples to suggest the value of deterrence. First, a suspect named Iyman Faris was scouting the Brooklyn Bridge for a potential attack, but reported to his co-conspirators that it was "too hot," *i.e.*, that there was too much surveillance. Second, the terrorist magazine *Inspire* praised the Tsarnaev brothers for having chosen Boston because it was "relatively out of the enemy's attention," unlike New York. For all the privacy concerns about video cameras, Mr. Maynard stated that the public and politicians actually want *more* cameras.

Mr. Maynard then said the NYPD policy protects privacy through various internal policies, including policies about data destruction. Videos, for example, are destroyed automatically after 30 days, and license plate information after five years. There is limited access within the department to surveillance data, and there is a complete audit trail of who accessed what data and when.

Mr. Maynard disagreed with Ms. Patel's suggestion that there was limited democratic accountability because, from his perspective, the NYPD's policies are subject to extensive political and media attention.

Professor Waxman then asked: Are these new technologies "game changing," and, if so, how does law and policy address that?

Ms. Patel agreed that "we're at a game changing moment" because it is so easy and cheap to aggregate data about people. The law is beginning to catch up. Ms. Patel referred to the Supreme Court's decision in *United States v. Jones*, 132 S. Ct. 945 (2012), which recognized that the Fourth Amendment can be triggered with ongoing location tracking. She also mentioned the Eleventh Circuit's decision from the prior week in *United States v. Davis*, 754 F.3d 1205 (11th Cir. 2014), which held that a warrant was necessary for cell phone location information.

Mr. Weissmann also agreed with the "game changer" characterization, but highlighted that advancing technology was being used by criminals and terrorists too. He added that the focus of discussion tends to be on technology enabling the government to collect too much, but what is often missing is the countervailing concern of technology preventing the government from collecting anything. Terrorists and criminals can use technology to communicate in ways the government cannot monitor — *i.e.*, "going dark." That is why it is imperative, he said, for there to be the capability to intercept communications, irrespective of the legal standard used to determine when it is permissible to do so. Mr. Weissmann said that the fix for the problem of "going dark" needs to come from Congress, but he doubted that Congress was likely to act.