

After Boston: The Pros and Cons of Surveillance Cameras

April 2013

Source: CNN

Available at: <https://www.cnn.com/2013/04/26/tech/innovation/security-cameras-boston-bombings/index.html>

STORY HIGHLIGHTS

- New technology makes it easier to identify suspects in surveillance photos and video
- The Boston bombing suspects were identified on security-camera footage
- Cities such as New York and London now have thousands of cameras on the streets
- Facial-recognition software can detect age, gender and even moods

Even after the identification of the Boston bombing suspects through grainy security-camera images, officials say that blanketing a city in surveillance cameras can create as many problems as it solves.

A network of cameras on city streets and other public spaces increases the chances of capturing a criminal on video but can generate an overwhelming amount of evidence to sift through. The cameras make some people feel more secure, knowing that bad guys are being watched. But privacy advocates and other citizens are uneasy with the idea that Big Brother is monitoring their every public move.

Meanwhile, facial-recognition software and other technologies are making security-camera images more valuable to law enforcement. Now, software can automatically mine surveillance footage for information, such as a specific person's face, and create a giant searchable database.

After last week's bombings at the Boston Marathon, authorities had to sift through a mountain of footage from government surveillance cameras, private security cameras and imagery shot by bystanders on smartphones. It took the FBI only three days to release blurry shots of the two suspects, taken by a department store's cameras.

Compare their quick turnaround with the 2005 London bombings, when it took thousands of investigators weeks to parse the city's CCTV (closed-circuit television) footage after the attacks. The cameras, software and algorithms have come a long way in eight years.

Cities under surveillance

In major cities, in the age of terrorism, someone is almost always watching.

The cameras used in London are part of the city's extensive and sophisticated "Ring of Steel" surveillance system that combines nearly a half million cameras, roadblocks and license plate readers to monitor the heart of the city. Set up in 1998, the system is one of the most advanced in the world and allows authorities to track anyone going into or out of central London.

Many residents question the effectiveness of London's system, however. In 2008, only one crime was solved for every 1,000 cameras, according to the city's police. CCTV cameras across Britain also cost authorities nearly \$800 million over the past four years, according to civil liberties group [Big Brother Watch](#).

Modeled after London's system, New York's [Lower Manhattan Security Initiative](#) monitors 4,000 security cameras and license plate readers south of Canal Street. The project uses feeds from both private and public security cameras, which are all monitored 24 hours a day by the NYPD.

Using face and object-detection technology, the police can track cars and people moving through 1.7 square miles in lower Manhattan and even detect unattended packages. The \$150 million initiative also includes a number of radiation detectors and automatic roadblocks that can be used to stop traffic in an emergency.

Boston's camera network is smaller than those in London and New York, though that is likely to change soon. In 2007, Boston law enforcement had an estimated 55 CCTV cameras set up around the city. Since then, the city has expanded its surveillance system, though authorities there are not commenting on the exact scope of the current camera setup.

Boston's example has shown the power of these systems to help solve crimes, causing many to call for even more cameras. But it's still not clear whether they are effective at preventing crimes. According to the [Surveillance Studies Centre](#) at Queen's University in Ontario, urban surveillance systems have not been proven to have any effect on deterring criminals.

Facial recognition

As the volume and quality of cameras and sensors are ramped up, cities are turning to more advanced face- and object-recognition software to make sense of the data.

"We describe what's in the video, and we store that in a database," said Al Shipp, CEO of San Francisco-based 3VR, one of several companies that makes this type of facial-recognition technology.

The company's first investor was In-Q-Tel, the CIA's venture-capital arm, which finds and funds promising security-related technology. Now, 3VR works with federal and local law enforcement agencies, as well as private companies and banks.

Its software can identify objects by shape, size and color. It can read license plates and recognize cars. When it comes to people, it can detect their gender, approximate age, mood and other demographic information. Using multiple cameras, it can track their patterns and some behaviors. It automatically zooms in on any person's face and identifies them based on things like the distance between their eyes or the shape of their nose.

All that information is stored in a database. Big clues that would take a traditional investigator untold hours of watching video to uncover can be found with a 15-second search query.

For example, they could do a search for anyone who entered a 7-Eleven store between 8 and 11 p.m. on a specific night, pull up the times that certain cars have entered and left a parking lot, or ask for images of every person who has entered a certain building over the past year.

"It instantaneously gives you a picture of everybody who has walked in the door in the past based on the geometries of their face," Shipp said.

Privacy concerns

Civil-liberties activists are concerned about how this technology could be abused. With cameras in far-flung cities all connecting to the same database, a person's movements can be tracked across states or continents. For example, it could be used to single out a person attending multiple political protests.

"We like to think we have some privacy in our lives, that we can go places that we don't necessarily want the government to know about," said Jennifer Lynch, an attorney at the Electronic Frontier Foundation, an Internet civil-liberties group. "What concerns me is if all of those cameras get linked together at some point, and if we apply facial recognition on the back end, we'll be able to track people wherever they go."

For now, many of the biometrics databases in the United States are still separated. Some are scattered across various federal and local government agencies, and connecting them will take time and big budgets. The FBI is in the process of building out its own facial-recognition database and is working with state DMVs to access their photos.

It's less likely the government will be able to tap into private databases anytime soon, but it's still a cause for concern down the line, privacy advocates say. Facebook has the largest facial-recognition database in the world, a potentially rich vein of data for any government agency.

Another worry is the misidentification of suspects. Shipp acknowledges that these systems can make mistakes but says the computers aren't there to take over for humans but to assist investigators by weeding out useless information.

"The cameras themselves are not a panacea. They're not going to solve the problem. It's one of the steps," he said.

But at least one prominent tech blogger thinks the benefits of surveillance cameras outweigh our fears about privacy.

"The idea of submitting to constant monitoring feels wrong, nearly un-American, to most of us. Cameras in the sky are the ultimate manifestation of Big Brother -- way for

the government to watch you all the time, everywhere," Farhad Manjoo wrote last week in Slate.

But Manjoo thinks we need to be thinking about ways to make cameras work for us, not reasons to abolish them.

"When you weigh cameras against other security measures, they emerge as the least costly and most effective choice. In the aftermath of 9/11, we've turned most public spaces into fortresses -- now, it's impossible for you to get into tall buildings, airports, many museums, concerts, and even public celebrations without being subjected to pat-downs and metal detectors. When combined with competent law enforcement, surveillance cameras are more effective, less intrusive, less psychologically draining, and much more pleasant than these alternatives."