

Inside 1to1 Privacy

Date: 04/09/2009

Issue: April 2009

People: Don Peppers & Martha Rogers, Ph.D.

Surveillance of Public Spaces: A Privacy Issue?

We are perhaps more accustomed than ever before to the surveillance camera on the busy street corner and corporate front entrance. People who pass by them every day don't seem to take a second look anymore. But is there a point at which the ubiquity and potential connectivity of public-space surveillance starts to diminish personal privacy? Companies that occupy a corner in this growing web may find new policy issues at their doorsteps.

Surveillance cameras

Few things symbolize the post-9/11 Western world more than the iconic surveillance camera. From New York to London to Canberra, the electronic eyes have multiplied in the past decade. Consider the facts:

- After British closed-circuit television (CCTV) images in 1993 aided the capture of the murderers of a toddler, and IRA terrorists continued their bombing assaults on London, a willing public backed the installation of what has now become an estimated 1.5 to 4 million cameras, the most in the world.
- Following riots by Muslim youth--the most widespread in Paris since 1968--a 2008 plan will increase the number of police cameras in Paris to 10,000, out of an estimated 340,000 in the country.
- A "London-style" surveillance initiative is scheduled to add thousands of cameras across New York City by 2010.
- A 2008 Department of Homeland Security initiative added 4,500 cameras to the streets of Washington, DC, with "hundreds more" expected to be added in 2009.
- By January 2007, Chicago had installed more than 2,200 surveillance cameras.
- Last month, Winnipeg installed its first CCTV systems, joining other cities in Canada, Denmark, Norway, Germany, and Australia on the surveillance bandwagon.

The growth of surveillance cameras in the West has so far met little resistance from the general public, who perhaps see in the cameras a promise of greater security from terrorists and criminals. Since the vast majority of people aren't perpetrating crime in public, how could the cameras harm them?

A recent documentary on British television, "Every Step You Take," identifies some new and not-so-distant applications of CCTV cameras and their data. Some systems reportedly now "shout out" a verbal warning to people exhibiting anti-social behavior, while others listen for aggressive voices and gun shots.

Some cameras have already been adapted with automatic number-plate recognition technology (ANPR) that reads each passing car's license plate. In the UK, for instance, ANPR technology allows a car's owner to be identified when a car enters a designated "congestion zone" (such as central London) during specified hours. The list of car owners is then compared against payment records to ensure that each congestion charge has been paid when due. Such technology would also allow a camera to feed car-owner data into a database that immediately "pings" the authorities if a license is not current, or the car is not properly insured or certified as roadworthy, or the owner is on a terrorist list, or the car has been involved in a crime.

"Anyone knowing a distinct part of the software code can enter it into Google and consequently gain access to thousands of CCTV feeds from all over the world," claimed the documentary's narrator. "You can watch live broadcasts of cafes in the U.S., churches in Poland, and loads of footage from the UK," he added.

Supplementing the CCTV networks is a growing use of overhead surveillance. Many metropolitan areas in the U.S. and abroad--Washington, DC, New York City, the State of Texas, and India, for example--use aircraft to watch for possible homeland-security concerns and illegal drug operations only visible from above.

But from a privacy perspective, the greatest development has been Google Earth, launched in 2005. Even though Google Earth is not a "real time" system like most surveillance operations, the combination of overhead satellite images and Google's ground-level Street View system, released in 2007, has raised the possibility that anyone with an Internet browser can potentially view anyone else in public.

Vehicle tracking

Smart tags used for frequent travel across toll roads are adding to the growing pool of

data about people's movement through the public space. In the United States, the most ubiquitous smart-tag is the E-ZPass, an interoperable system spanning 13 states in the northeast, where two-thirds of U.S. highway tolls are collected. Other standalone smart-tag systems in southern and western states and Ontario similarly provide state agencies with an ongoing stream of data about a vehicle's time and place.

And even drivers not on toll roads may be leaving a data trail. Users of devices connected with the U.S. Air Force-managed Global Positioning System (GPS) can optionally allow their data to be sent back to the device maker for improvements on route information.

Pedestrian tracking

The futuristic scenes in the 2002 movie *Minority Report*--where billboards detected Tom Cruise's character passing by and then delivered customized messages to him--are now one step closer to reality. Paris-based Quividi in 2006 launched an "automated audience measurement solution" in hundreds of retail stores in Europe and Asia, and more recently in America. Its camera-enabled digital billboards detect the demographics of passersby and then deliver messages tailored to those demographics. Israel-based TruMedia offers a similar technology being tested in more than 30 U.S. locations.

Drivers who don't use smart tags or GPS devices and people who don't walk in front of digital billboards, but carry a GPS-enabled mobile phone, nonetheless are sending position information to their telephone company. Two new mobile phone applications--Loopt for the Apple iPhone and Google's Latitude--enable people to share their location information voluntarily, through phone-based browsers.

Privacy risks?

The growing amount and connectivity of data about people's actions and movements outside their homes has raised concerns among privacy advocates including the Electronic Privacy Information Center (EPIC), Privacy International, and the American Civil Liberties Union (ACLU). They say this type of data collection is inherently prone to abuse--expanding data uses beyond the original purposes of collection, sharing data with third parties beyond reasonable expectations, and heightening vulnerability to security breaches. A criminal's knowledge of a person's location could, for example, heighten that person's vulnerability to property theft, physical harm, and child abduction.

Motivated by these risks, the privacy commissioners of Canada, British Columbia, and

Alberta in March 2008 released Guidelines for Overt Video Surveillance in the Private Sector, and have continued to apply these guidelines to public-sector deployment of surveillance cameras. Among their guidelines: determining whether a less privacy-invasive alternative to video surveillance would meet the stated need, limiting data use and retention to what is stated in a privacy policy, and training camera operators on the privacy policy.

So far, however, privacy professionals mostly have been unable to counter the argument that a person should have no expectation of privacy in a public space. What, after all, does a person have to hide about his walking along the street, through a park, or through a shopping center? If this information can be secured, what is the harm to human dignity?

Longstanding battles over two legal precedents--concealment and vagrancy statutes--in the U.S. and other countries based on England's common-law system show how the common good of public safety has often triumphed over what has been viewed as the lesser privacy good of individual identification in public. In the U.S., masked rioting farmers and Ku Klux Klan members, viewed as domestic terrorists, led at least seven states starting in 1845 to prohibit mask wearing in public.

Occasionally the enforcement of these laws makes headlines, such as when police arrested a New York man wearing a Grinch mask and a Florida man dressed as Batman. Police argue that the wearing of a mask in public amounts to concealment of malicious intent.

Vagrancy laws have also provided precedents for requiring people to identify themselves as they pass through public spaces. According to the Encyclopedia Britannica, England first established the concept that a vagrant was a person who had deserted his wife and children, was able to work but preferred to drift idly from place to place, or who was unable to give an account of himself. In the United States, Supreme Court decisions have narrowed the application of vagrancy laws but have also reconfirmed their constitutionality. In *Terry v Ohio* (1968), for example, the Court held that the need for law enforcement to dispel suspicion of criminal activity justified the minimal intrusion upon the individual to identify himself. In *Hiibel v Sixth Judicial District Court of Nevada* (2004), the Court concluded that requiring suspects to identify themselves did not violate the Fourth or Fifth Amendments.

What should corporate privacy officers do when faced with these ever new and evolving policy questions presented by the age of ubiquitous identification? Former U.S. Department of Homeland Security Chief Privacy Officer Hugo Teufel may have given the

best advice: "If you stick to the fair information principles," he told a St. Paul audience in January, "you'll always come out with the right answer." When it comes to surveillance, this means, at a minimum, clearly disclosing surveillance activities, limiting data uses to defined purposes, and securing the images. Surveillance programs that don't incorporate these principles run the risk of losing public support for their continuance.