

CCTV: Developing Privacy Best Practices

Privacy Office, Department of Homeland Security
Docket number: DHS-2007-0076.
James A. Lewis, Center for Strategic and International Studies
January 9, 2008

CCTV use can improve security in urban areas, public venues, and around critical infrastructure facilities. The benefits of CCTV use will increase as the technology improves if we do not create a regulatory environment that discourages innovation and use. Privacy guidelines must be flexible enough to accommodate next-generation systems and evolving technologies and should not restrict further technological development.

CCTV is itself an anachronistic term. Old-style CCTV systems – a guard sitting in front of a screen or assembly of screens – will be replaced by automated, digital systems that use computer processing, digital networks and ubiquitous connectivity. In the near future, for example, a computer-controlled sensor will be able to track a vehicle that repeatedly circles a nuclear power plant, identify that vehicle's license number, automatically check that number and alert police or security forces if there is a concern.

CCTV use has grown rapidly because it provides benefits for security. Claims that CCTV does little to improve security should be contrasted with operational experience. When intelligence agencies describe a 'hard target' – e.g. a target where it is difficult to obtain access – the presence of surveillance cameras is one of the factors that makes the target hard. Covert access and the commission of illicit activities are made more difficult and riskier when CCTV surveillance is present. Denigrating the technology as a way to discourage its use should not be confused with a realistic appraisal of its utility.

The experience of other countries' CCTV use suggests that the presence or absence of CCTV is irrelevant to civil liberties. Civil liberties and political freedoms in China are restricted not because CCTV is in use, but because freedoms are generally restricted. In the UK, for example, the widespread use of CCTV has not damaged political freedoms. The effect of CCTV on civil liberties depends entirely on the larger political context. Democracies that have deployed CCTV in large numbers have not seen a chilling political effect.

Safeguards for CCTV should focus on how data that is collected or accessed by government agencies will be used, stored, and shared. Congress and the Courts have not dealt with this issue, although the laws governing search and seizure or wiretaps offer some precedent. There are significant differences however, between CCTV and wiretapping. The central issue is the status of images taken in public spaces. We expect telephone conversations to be private. Actions taken in the public view, where there is no reasonable expectation of privacy, are not private; they are in the public domain. Current laws impose some limits on monitoring. I cannot trespass or intrude ("objectionable intrusion") in collecting data. The data collected cannot be used for commercial or trade purposes (such as an advertisement) without my consent. And if the collector is from the police or another government agency, I cannot be subjected to an "unreasonable search."

The courts have not yet determined what is unreasonable. Is it an unreasonable search, for example, if a camera mounted on a police car can connect wirelessly to police computers running software that can identify a person with an outstanding warrant when that person is walking down the street? That person has no reasonable expectation of privacy, but instead relies on the likelihood that police officers he or she encounters will not know him or her. The use of CCTV can increase the knowledge and situational awareness of the police. Courts have restricted the ability of police to use sensors to look into a house (where there is a reasonable expectation of privacy), but appear open to the monitoring of public spaces.

This suggests that for the monitoring of open spaces or government-owned areas, there should be few constraints on collection and on use by the collecting agency. Retention of data should be for some publically specified and reasonable period. Sharing by the collecting agency with other government agencies is a more complicated issue. At a minimum, however, the shared data should be subject to the same constraints on retention, oversight and notification as apply at the collecting agency.

Changes in CCTV technology are part of a larger transition to a digital environment created by where cheap sensors, abundant processing and storage, and pervasive wireless networks. In this environment, privacy guidelines should focus on how bits are used or stored, not on how they are collected. Privacy guidelines for CCTV should build on public domain and a reasonable expectation of privacy. We should not expand privacy safeguards simply because the collector is a sensor rather than a human. Privacy guidelines address data retention and use. A framework for privacy rules governing CCTV use should consist of the following:

- No limits on collection of visual beyond what is currently required for visual surveillance in public spaces, government-owned spaces, or private spaces where the owner has agreed to allow video surveillance (collection of other kinds of imagery).
- A specified period for retention that is sufficient for law enforcement purposes.
- Clear public notice that CCTV surveillance is taking place.
- Published rules for the dissemination and use of CCTV data by the collector that also apply to third parties with whom such data is shared.
- The right to see photographic evidence if it is used in any legal action.
- Oversight by a body external to the collecting agency and public reporting on use.
- Rules for retention of CCTV data that are consistent with the treatment of similar kinds of government-collected data.
- Rule-making must accommodate the blending of different kinds of sensor data with CCTV data.