Privacy vs. Security: Electronic Surveillance in the Nation’s Capital

John D. Woodward, Jr., Esq.

CT-194

March 2002

Testimony before the Subcommittee on the District of Columbia of the Committee on Government Reform, United States House of Representatives, on March 22, 2002
This testimony is based on a variety of sources, including research conducted at RAND. The author thanks Professor Julie R. O’Sullivan of Georgetown University Law Center, Shirley Woodward, Esq. and Paul Steinberg for their comments. However, the opinions and conclusions expressed are solely those of the author and should not be interpreted as representing those of RAND or any of the agencies or others sponsoring its research.
Introduction

Chairwoman Morella, Ranking Member Norton, and Members of the Subcommittee on the District of Columbia, I am honored to participate in these timely hearings to discuss electronic surveillance. This forum provides an excellent opportunity for policymakers to examine government’s use of such technologies as well as to gain greater understanding of the privacy and security concerns related to such use.

The many subject-matter experts and public officials appearing before the Subcommittee are better qualified than I to discuss the specific facts and the detailed history of electronic video surveillance in the District of Columbia. Therefore, I will focus my testimony on reasons for and concerns about the use of such technology, the legal status quo with respect to such use, options for Congress to consider, and issues related to future use of electronic surveillance and other technologies.

Reasons for and Concerns about Community Use of Electronic Surveillance

Over a million video surveillance cameras are used in the United States, with many government organizations deploying forms of electronic surveillance (e.g., closed circuit television (“CCTV”), open circuit television (“OCTV”), video cameras, etc.) to monitor public places.1 The United Kingdom has an estimated one million CCTV cameras in operation.2 Various reasons have been cited for this extensive public sector use of this technology. These reasons include:

1. Preventing crime from occurring,
2. Detecting crime as it occurs,
3. Reducing citizens’ fear of crime,
4. Aiding criminal investigations after a crime has occurred by what is known as post event analysis,
5. Making better use of public safety resources, and,
6. Countering terrorism.

Despite these reasons for using the technology, critics claim the use of surveillance cameras is not in keeping with “the values of an open society.”3 Some argue that their use leads to “video voyeurism” on the part of the police and forces “social conformity” on people. Others believe that the cameras’ use may lead to racial discrimination.4 For many, the government’s use of surveillance cameras suggests that “Big Brother” is always out there secretly watching a citizen’s every move. The Orwellian concerns are largely two-fold: the fear of tracking and the problem of clandestine capture of personal data.

Tracking refers to the ability to monitor an individual’s actions in real time or over a period of time. In its most extreme incarnation, tracking could become a kind of “super surveillance” that lets the tracker to both “follow” a person today as well as search databases to learn where he was months ago.5 The possibility that the government could compile such massive databases, and that such databases could be used by law enforcement, raises the specter of “Big Brother” tracking its citizens’ every move.
The clandestine capture of a person’s face increases these fears because surveillance cameras can surreptitiously track individuals without their knowledge or permission. Moreover, the information from tracking can be combined with other personal data, acquired by other means, such as credit card or other consumer purchasing records, to provide even more insight into an individual’s private life.

**Legal Status Quo of Community Use of Surveillance Cameras**

Let’s establish the legal status quo by asking: Does the use of this technology violate legally protected privacy rights? Legal rights to privacy may generally be found in three sources:

1. Federal and state constitutions (if the entity invading an individual’s rights is a government actor),
2. The common law of torts (if the entity invading an individual’s rights is a private actor), and,
3. Statutory law (at the federal and state level).

Although the word “privacy” does not appear in the U.S. Constitution, the concern with protecting citizens against government intrusions into their private sphere is reflected in many of its provisions. For example, the First Amendment protects freedom of expression and association, as well as the free exercise of religion, the Third Amendment prohibits the quartering of soldiers in one’s home, the Fourth Amendment protects against unreasonable searches and seizures, the Fifth Amendment protects against self-incrimination, and the Due Process Clauses of the Fifth and Fourteenth Amendment protects certain fundamental “personal decisions relating to marriage, procreation, contraception, family relationship, child rearing, and education.”

Therefore, the constitutional “right to privacy” reflects concerns not only for one’s physical privacy—the idea that government agents cannot barge into one’s home—but also for less tangible interests—the idea that citizens should be able to control certain information about themselves and to make certain decisions free of government compulsion. And the Supreme Court has cautioned that it is “not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files.”

A community’s use of surveillance cameras could potentially implicate both types of privacy interests. For example, if the compilation of information in these databases had a significant chilling effect on First Amendment rights, such as discouraging citizens from attending political rallies, if it impinged on fundamental rights of decisional privacy, or if the information were insufficiently safeguarded against unauthorized disclosure, then the maintenance of such databases could potentially run afoul of the law.

Nevertheless, law enforcement’s proposed use of the technology in Washington, D.C. does not appear to run afoul of the protections afforded by the U.S. Constitution. Some civil libertarians may argue that a community’s use of mass, dragnet video surveillance is improper, and that law enforcement should have individualized, reasonable suspicion that criminal activity is afoot before it can “search” a subject’s face.
to see if the person is a criminal or terrorist. However, this argument is premised on what would be a dramatic expansion of current law. The Supreme Court has explained that government action constitutes a search requiring conformity with the Fourth Amendment when it invades a person’s reasonable expectation of privacy. But the Court has also found that a person does not have a reasonable expectation of privacy with regard to physical characteristics that are constantly exposed to the public, such as one’s facial features, voice, and handwriting.9

Similarly, the Court has determined that “[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.” The Court reasoned “[w]hen [an individual] traveled over the public streets he voluntarily conveyed to anyone who wanted to look the fact that he was traveling over particular roads in a particular direction, and the fact of his final destination when he exited from public roads onto private property.”10

So although the Fourth Amendment requires that a search conducted by government actors be “reasonable,” which generally means that there must be some degree of suspicion that the person to be searched is engaged in wrongdoing, the government’s taking video of a person’s face that the person shows in a public place does not constitute a search.11 And with respect to concerns about information privacy, if law enforcement officials limited their actions to simply comparing images of people in public places with databases of terrorists and known criminals, then information privacy concerns would be unlikely to arise.

**Options for Congress**

Congress is free to provide greater privacy protections than those found in the Constitution. Ample precedent exists for Congress to do so, particularly in the privacy realm. To cite one well-known example, in *United States v. Miller*, a case involving a bootlegger’s private financial records, which were given to U.S. Treasury agents by his bank, the bootlegger tried to have this evidence excluded unsuccessfully.12 The Supreme Court found that Miller had no expectation of privacy in the bank records, reasoning, “The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. . ..” The records could not, therefore, be considered confidential communications, because Miller had voluntarily conveyed them to the bank in the “ordinary course of business.” Following the *Miller* decision, Congress, in 1976, passed the Right to Financial Privacy Act (12 U.S.C. 3401 *et seq.*) to establish procedural requirements that financial institutions must follow when disclosing information to the government. Thus, the refusal of the Supreme Court to find a Constitutionally-mandated privacy right does not as a practical matter end the debate. In sum, Congress is free to act by passing legislation to create new individual privacy rights.

Having established that Congress can act in this arena, we next need to ask: What options can Congress pursue with respect to government use of surveillance cameras?
It seems Congress has three broad policy choices:

1. Prohibit its use,
2. Regulate its use, and,
3. Take no immediate action, pending further study.

1. Prohibit Its Use: Congress could decide that the use of surveillance cameras is so dangerous to citizens and society that the law should prohibit such use. In other words, the law could treat surveillance cameras as a form of “technological heroin” to be outlawed. In the process, Congress could help to establish an all-encompassing individual right to “public privacy,” that is, regardless of whether the individual is in a private place (e.g., the home) or in a public setting (e.g., the street), the government cannot watch or record the event with surveillance cameras.

The counterargument to this approach is that surveillance cameras are not a form of “technological heroin” because, unlike heroin, their use benefits the individual and the community. Specifically, the community must maintain public safety. To fulfill this essential duty, law enforcement must monitor public places. This age-old concept is the rationale for the “police officer on the beat.” To extend the analogy, a surveillance camera can be viewed as a form of mechanical police officer that watches or records events occurring in public places in which the person has no reasonable expectation of privacy.13

2. Regulate Its Use: Congress could decide to regulate the use of surveillance cameras in many ways.14 Most notably, Congress could place statutory restrictions on use in the form of time, place or manner restrictions.15 For example, Congress could restrict the District of Columbia’s use of surveillance cameras to the duration of a planned protest (time), to monitor only those sensitive locations susceptible to attack (place), and to prohibit continuous video recording (manner).

Or as an alternative, Congress could require prior judicial (or executive) branch approval for the technology’s use. A rough parallel can be drawn to the legal requirement for law enforcement to obtain a warrant prior to intercepting certain communications. Congress could extend a similar requirement to law enforcement’s use of video surveillance. On this note, the House of Delegates of the Commonwealth of Virginia recently took this approach by passing House Bill 454, requiring that state and local law enforcement agencies obtain an order from a circuit court prior to using facial recognition technology.16 The legislation has been sent to the Virginia State Senate.

3. Take No Immediate Action, Pending Further Study: The third option is for Congress to take no immediate action in the nature of prohibition or regulation, but rather to continue studying and assessing the issue, and remain poised and prepared to act if deemed necessary or advisable. Based on what it has learned at this hearing and at similar public forums, Congress can begin to formulate more complete answers to questions about the use of the technology.
As a start, these questions include:

1. Does electronic surveillance prevent crime? Or does it merely shift crime to other locations?
2. How effectively does electronic surveillance detect crime?
3. How do citizens perceive the technology’s use? Do citizens favor the use of the technology?
4. How much of an aid is electronic surveillance in criminal investigations?
5. Does electronic surveillance enable public safety resources to be deployed more efficiently and effectively?
6. Does electronic surveillance counter terrorism?

Moreover, Congress can be particularly attentive to any solid evidence of actual harm caused by the technology. For example, when use of the technology leads to misidentifications resulting in the arrest and conviction of innocent individuals. Granted, it is very hard to measure or to develop the “metrics” needed for these answers. More and better public policy research on the use of the technology, its security and privacy implications, as well as the effects of regulation is needed.

As it develops answers to these and related questions, Congress has a plethora of policy choices to consider. As with any technology, public understanding of the operation and uses of electronic surveillance may mitigate many of the fears about Big Brother. To that end, the government should be encouraged to use the technology openly, rather than clandestinely. To the extent possible, prominent notice should be given that the technology is being used. Moreover, the government entity using video surveillance should provide as much information as possible to the public about the technology’s purposes and capabilities. This transparency should help prevent misuse or abuse. This effort at transparency could even include broadcasting the actual operations of the electronic surveillance on a public access television channel.17

One controversial issue that may arise concerns what the government does with the data it collects. Thus a first question to consider is whether the surveillance camera systems should be limited to actively monitoring or if they should have a recording capability as well. A recording capability can be helpful for post-event analysis. For example, it’s good that we have videotape of Mohamed Atta at the screening area of the Portland, Maine airport at 5:45 a.m. on September 11, 2001. It’s bad that the Washington Metro CCTV system did not have a recording capability on June 10, 2001, when an assailant fatally shot Metropolitan Transit Officer Marlon Morales at the U Street station.

If surveillance data are recorded, however, then a retention policy should be considered. After a certain time period, the data should be erased. Similarly, the data should be securely kept. And an auditing process should be established to ensure accountability and to prevent the misuse of the data.

Finally, some form of active oversight, either government-only or a cooperative effort between government officials and private citizens, such as citizen oversight
committees, would be useful not only to quell fears about the technology’s use but also to ensure that it will not be abused.

**Future Use of the Technologies**

These hearings are extremely timely, and this topic will continue to occupy the attention of policymakers because of continuing technological developments. Both the public and private sectors are making growing use of electronic surveillance technologies as well as other emerging technologies that can gather information about us.\(^{18}\) We are also seeing increasing interlinkages among these various information-gathering technologies. The chart below shows these interlinkages.\(^{19}\) The center of the chart depicts average citizens, all of whom have different types of personal information associated with them (e.g., biographical, consumer, biometric, medical, financial, and behavioral). Surrounding this information are various technologies that can obtain this personal information (e.g., overhead imaging, genomics, biometrics, thermal imaging, computer monitoring, data mining, micro sensors, global positioning systems, geographical information systems, surveillance cameras (CCTV), and bio-nano-materials technology). When these technologies are interlinked, the ability to collect information, and the amount of information collected increases significantly, thereby significantly increasing the potential privacy invasions.

![Emerging Technologies Diagram](image)

A well-publicized example of such interlinkages of the technologies occurred at Super Bowl XXXV at Raymond James Stadium in Tampa, Florida on January 25, 2001 when authorities used facial recognition technology and surveillance cameras to capture spectators’ biometric information, combined with a little data mining, to determine biographical information (e.g., is this person a wanted criminal?). The chart below shows these interlinkages.
And this use of interlinked surveillance technology is not limited to law enforcement. We have now not only entered the world of webcam, Kindercam, nannycam, and grannycam, but we have also entered the realm of countless other means of information-gathering technologies. These developments do not mean that Big Brother is alive and well. Rather, these same technologies can be used to protect citizens’ rights. For example, with respect to video cameras:

- In 1991, a bystander videoed the arrest of Rodney King; this video allowed many Americans to “see for themselves” what otherwise would not have been seen.
- Currently, many police departments have installed video cameras on squad cars to video certain traffic stops and similar events to show that officers satisfy legal requirements.
- In the near future, a citizen, wearing a mini-camera on her jacket lapel, may be able to effortlessly video her encounters with law enforcement or anyone else and wirelessly transmit the information to where she desires.

In conclusion, the Subcommittee on the District of Columbia is holding a hearing on an important topic of public concern that presents complicated privacy and security issues, and possibly balancing of the two. Moreover, the technology moves quickly and the law and policy concerns often struggle to keep apace. However, this situation is not new in the American experience. We should be mindful of technologies that may invade our privacy, and it is wise to monitor their development to forestall potential abuses. We should, however, also ensure that perceived or potential threats to our privacy do not blind us to the positive uses of electronic surveillance. And rather than acting hastily, it might be better to first try to develop thorough answers to questions about the use of surveillance cameras, their impact on public safety, and the policy and social concerns
they raise. Thank you for inviting me to share my thoughts with you. I am happy to answer any questions you may have.

Biographical Information

John D. Woodward, Jr., an attorney, is a senior policy analyst at RAND where he works on national security, intelligence, and technology policy issues. He is particularly interested in biometrics and surveillance technologies. He has testified about biometrics before Congress, the congressionally created Commission on Online Child Protection, and the California State Assembly.

Prior to joining RAND full-time in 2000, Mr. Woodward served as an Operations Officer for the Central Intelligence Agency for twelve years. His overseas assignments included tours in East Asia and East Africa.

Mr. Woodward received his Juris Doctor degree magna cum laude from Georgetown University Law Center in Washington, D.C. He was a Thouron Scholar at the London School of Economics, University of London, where he received his M.S. in Economics. He received his B.S. in Economics from the Wharton School of the University of Pennsylvania. He served as a law clerk to the Hon. Roderick R. McKelvie, a U.S. District Court Judge in Wilmington, Delaware.

---

1 Closed circuit television (“CCTV”) refers to a system in which the circuit is closed and all the elements are directly connected. Open circuit television (“OCTV”) transmits video images over wireless networks to portable devices. Cameras are used for both systems.


4 According to Barry Steinhardt, Associate Director of the American Civil Liberties Union, “People of color in the U.K. have been singled out to be followed by the cameras.” quoted in Stephen Cass and Michael J. Riezenman, “Improving Security, Preserving Privacy,” IEEE Spectrum Online, Jan. 4, 2002. In his New York Times Magazine article, Jeffrey Rosen states “In Hull [United Kingdom] and elsewhere, rather than eliminating prejudicial surveillance and racial profiling, CCTV surveillance has tended to amplify it.”


States are free to provide greater privacy protections in their own state constitutions than those afforded in the U.S. Constitution. When evaluating the use of a specific system, therefore, its legality must be analyzed under state constitutional provisions as well.


See also U.S. Department of Justice, *Criminal Resource Manual* 32 (Oct. 1997) (“Video surveillance, which is the use of closed-circuit television (CCTV) to conduct a visual surveillance of a person or a place, is not covered by Title III. Rather, its use is governed by the Fourth Amendment and, therefore, when a reasonable expectation of privacy exists, a search warrant should be sought.”)


The United Kingdom, for example, regulates the public and private sector use of CCTV systems with a CCTV Code of Practice issued under the Data Protection Act 1998. See, e.g., Office of Information Commissioner available at http://www.dataprotection.gov.uk/.

In October 2001, the Privacy Commissioner of Canada, George Radwanski, released a letter of finding following his investigation of video surveillance activities by the Royal Canadian Mounted Police (RCMP) in Kelowna, British Columbia. In his letter of finding, Commissioner Radwanski suggested several such limitations be placed on the RCMP’s use of video surveillance, based on his interpretation of Canada’s Privacy Act. His suggestions include limiting the use of video surveillance, without continuous recording, to “particularly sensitive locations that are so susceptible to some form of terrorist or other attack as to require intensive security measures,” a “particular place [where] there might be such an exceptional threat to public safety, combined with other circumstances that made conventional policing unfeasible,” and “special circumstances where, to investigate a particular crime, it might be appropriate for police to temporarily establish a video camera in a given location and record images of everyone who frequents that location.” See Office of the Privacy Commissioner of Canada, *News Release: Privacy Commissioner Releases Finding on Video Surveillance by RCMP in Kelowna*, Oct. 4, 2001 available at http://www.privcom.gc.ca/media/nr-c/02_05_b_011004_e.pdf. On March 15, 2002, Commissioner Radwanski sent a letter to Lawrence MacAulay, Solicitor General of Canada, regarding the RCMP’s continued use of video surveillance in Kelowna. See Office of the Privacy Commissioner of Canada, *News Release*, Mar. 15, 2002 available at http://www.privcom.gc.ca/media/nr-c/02_05_b_020315_e.pdf


This chart grew out of discussions at a “Privacy and Emerging Technologies” Conference hosted by RAND in July 2001. My former RAND colleague, Kristina Larson, contributed immensely in the development of this chart.