DOI:10.1145/1646353.1646363

M. Angela Sasse

Privacy and Security
Not Seeing the Crime for the Cameras?

Why it is difficult—but essential—to monitor the effectiveness of security technologies.

In terms of sales, remote surveillance camera systems—commonly known as closed-circuit television (CCTV)—are a huge success story. Billons of dollars are spent on CCTV schemes by governments in developed countries each year, and sales to commercial companies and home users have been increasing, too. CCTV can be used for many purposes—ranging from monitoring traffic flows on highways, to allowing visitors in zoos to observe newborn animals during their first few days without disturbing them. The vast majority of CCTV purchases are made with the aim of improving safety and security. The London Underground was the first public transport operator to install cameras on station platforms, so train drivers could check doors were clear before closing them. CCTV has come a long way since then: last summer, the technology writer Cory Doctorow noticed that a single London bus now has 16 cameras on it (see Figure 1). The advance from analog to digital technology had a major impact on CCTV: cameras are much smaller and cheaper, video is often transmitted wirelessly, and recordings are stored on hard disks, rather than tapes. Integration with other digital technologies offers further possibilities: image processing makes it possible to recognize automobile license plates automatically and match them against databases to check if a vehicle has been reported as stolen, or is uninsured. Advances in hardware—such as high-definition cameras—and image processing—such as the ability to process face and iris information from images taken at a distance, not detecting unattended objects—will enable a wide range of possible technology solutions (imagine the whole industry salivating).

The burgeoning sales figures and ubiquity of cameras suggest that surely CCTV technology must be effective.

The burgeoning sales figures and ubiquity of cameras suggest that surely CCTV technology must be effective. The U.K. government has invested heavily in CCTV over the past 15 years, making it the country with the highest CCTV camera-to-person ratio on earth (Greater London alone has one camera for every six citizens). A key driver for adoption was that local authorities seeking to combat crime could obtain government funds to purchase CCTV. In the public debate, this policy has been justified mainly with two arguments: "*the public wants it*," and "*surely it's obvious that it works*." As evidence for the latter, policymakers often point to high-profile (and often highly emotionally charged) cases:

- In 1993, CCTV images from a shopping mall camera showed police investigators that the murdered toddler James Bulger had been abducted by two teenagers, who were then apprehended and convicted.
- Images from London Transport

PHOTO COLLAGE BASED ON A PHOTOGRAPH BY TOM PAGE

cameras led to the identification and apprehension of the four men who carried out the failed 7/21 "copycat" bombing attempts in 2005.

The still images from these cases (see Figure 2a/b) have become iconic—visual proof that CCTV works. Those who questioned its value in the public debate, and dared to mention the "p-word"—were largely dismissed as "privacy cranks," out of touch with the needs of policing and the wishes of ordinary citizens. But over the past two years, new doubts have been raised over the benefits:

▸ In summer 2008, a report by London police concluded that CCTV contributed to solving about 3% of street crimes. About £500 million ($700 million) has been spent on publicly funded CCTV in Greater London.

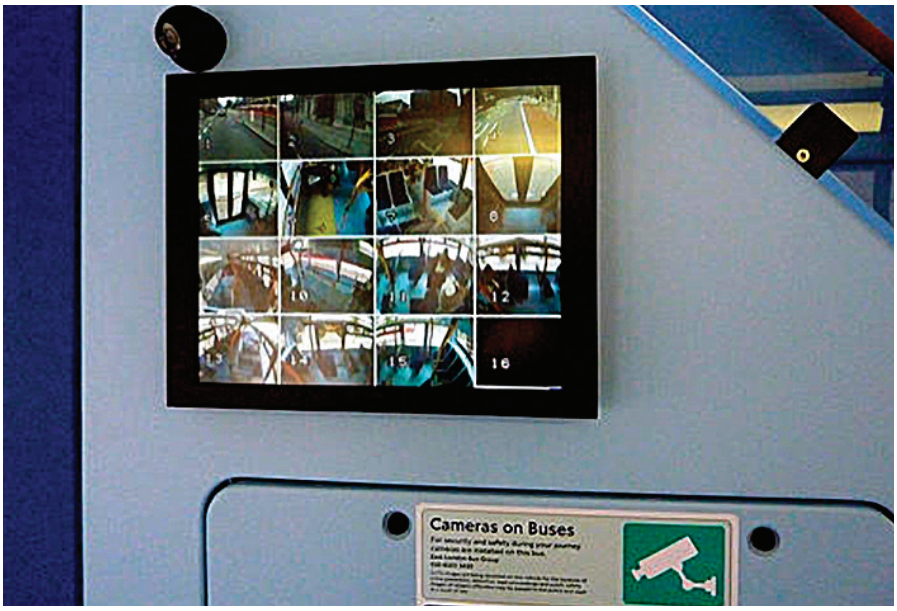
▸ In August 2009, a senior officer in the London police stated that, on an annual basis, about one crime was resolved for every 1,000 cameras in operation. He warned "*police must do more to head off a crisis in public confidence over the use of surveillance cameras.*"

▸ In September 2009, John Bromley-Davenport, a leading criminal lawyer in Manchester, said images from CCTV did not prevent crime or help bring criminals to justice.[3] He prosecuted the killers of a man kicked to death outside a pub. The incident was recorded on CCTV, but police officers did not arrive in time to stop the attack, plus the quality of the recorded footage was too low to be used for identification purposes in court. (The killers were convicted on eyewitness evidence.) The chief executive of a company that helps police analyze CCTV footage estimated "*that about half of the CCTV cameras in the country are next to useless when it comes to safeguarding the public against crime and assisting the police to secure convictions.*" Bromley-Davenport said that large amounts of money spent on technology meant less money was available to have police officers on the street—and that police presence was what mattered for preventing crime.

▸ In October 2009, design college professor Mike Press called for a moratorium on further CCTV deployments in Scotland, because the technology was "*costly and futile* [...] *a lazy approach to crime prevention*" that was dangerous because it created "*a false sense of security, encouraging* [citizens] *to be careless with property and personal safety.*"[6]

Thus, the effectiveness of CCTV is being questioned in the country that has been a leading and enthusiastic adopter. Surely, this must ring alarm bells in the industry supplying such systems? Not really. The industry response is that more advanced technology will fix any problems. High-definition cameras, for instance, would provide better image quality and increase likelihood of identification. The same chief executive who said that half of all current cameras were useless suggests that "*intelligent cameras*" will improve effectiveness and reduce privacy invasion because they "*only alerting a police officer when a potential incident is taking place.*" London police experts also hope that "*future technology will boost conviction rates using CCTV evidence.*"

The proposals for new technology and effectiveness include building a national CCTV database of convicted offenders and unidentified suspects, and use of "*tracking technology developed by*



A single London bus has 16 cameras mounted on it.

the sports advertising industry" to search footage for suspects and incidents. Since that technology is not quite ready, London police publish images of suspects on the Internet and ask the public for help. Recruitment of untrained members of the public to assist in CCTV monitoring is a growing trend:

- In a London housing project, residents have been given access to CCTV cameras, books of photos of individuals who had been warned not to trespass on the estate, and a phone number to call if they spotted any of them.
- In the tourist town of Stratford-on-Avon, residents and business can connect their own CCTV cameras to an Internet portal, and and volunteers who spot and report crimes can win prizes of up to £1,000.[a]
- Approximately $2 million has been spent on Webcams for virtual border surveillance at the Texas-Mexico border, enabling virtual local residents to spot and report illegal immigration.

The involvement of untrained members of the public in surveillance harbors many potential risks to privacy, public order, and public safety (e.g, vigilantism) that must be identified and considered. But even leaving those concerns aside, early indications from the last project suggest this not a quick fix to make CCTV more effective. The *El Paso Times*[6] reported in January 2009 that the program was not effective because only a dozen incidents had been reported. A spokesperson for the Governor of Texas responded that the problem was not with the technology, but the way its effectiveness was assessed. It may look like a weak argument, but it points to the key problem: How do you assess effectiveness of a security technology such as CCTV? How can you determine whether the results represent value for the money spent on technology, or privacy invasions that occur because of its existence?

The answer is conceptually simple: *effectiveness* of a particular deployment means that it achieves its stated purpose; *efficiency* means the desired results are worth more than the resources required to achieve them. But the execution of a study to measure them is a challenging and costly exercise. One of the few controlled studies to date was carried out in the clothing retail shops in 1999[1]:

- The *purpose* of installing the systems was clearly defined: reduce the stock losses through customer and staff theft.
- The *measures* for stock losses were clearly defined: the number and value of stock losses was monitored, and any reduction of losses calculated as a percentage of sales profits during the same period.
- Stock losses were measured four times—twice during a six-month period *before* and *after* the introduction of CCTV.
- The *efficiency* was calculated in terms of how many years the system would have to operate at the observed level of effectiveness to recover its investment.
- During the one-year period, they monitored for a number of *side effects* such as footfall, overall sales, customer assessment of shops, and so forth.

This illustrates that carrying out a meaningful assessment under controlled conditions requires significant resources and domain expertise, even for a conceptually simple study: the assessment was focused on a single crime, the monitoring environment was constant, and systems for measuring the impact were already in place. The results showed that stock losses were reduced significantly in the first three months of CCTV introduction—but then rose again. After six months, the average loss reduction was a near-insignificant £4—at an average capital expenditure of £12,000 per CCTV system, it would take 58 years to recoup the capital cost. In the end, only shops selling high-value fashion using high-end CCTV systems reduced stock

Still images from two cases that resulted in apprehension of perpetrators.

a Details of the rewards were revealed last December; see http://news.bbc.co.uk/1/hi/technology/8393602.stm

losses to a level that would mean their investment was recouped within two years. The authors concluded that anyone buying an off-the-shelf CCTV system may be wasting their money: only systems designed against a specific threat in a specific operating environment are effective.

A 2005 study of 13 CCTV systems funded by the U.K. government for crime prevention[2] concluded they had little or no impact on crime recorded by the police, or on citizens' perception of crime (based on victimization rates, fear of crime and other information collected via local surveys). A common problem was that those who bought the systems were unclear about the purpose of—and hence the technical and operating requirements for—the systems. Many projects were driven by an "*uncritical view that CCTV was 'a good thing' and that specific objectives were unnecessary*." Systems were bought because funding was available, or because a neighboring town had purchased one. There was no understanding of what CCTV could achieve, what types of problems it was best suited to alleviate, and which configuration and support technologies work best for which requirements. With buyers being unclear about objectives and lacking expertise, the systems were generally chosen by the salesperson—who tended to pick the system that suited the budget. In day-to-day operations, it turned out that many cameras were ineffective because they were badly placed, broken, dirty, or lighting was insufficient—problems that were previously identified in London Underground control rooms.[6] Both Gill and Spriggs[2] and McIntosh[6] also found that operator performance in the control room was hampered by a large number of disparate systems and information sources, and inefficient audio communication channels. Recent research by my own team[5] found these problems continue to affect operator performance, as do ever-increasing camera-to-operator ratios. Recorded video was generally too poor to be used for evidence. These problems suggest CCTV for crime prevention can only be effective as part of an overall set of measures and procedures designed to deal with specific problems. Effective communication and coordination between CCTV control rooms and those on the ground (police, shop and bar staff, private security forces) is key—and of course there must be sufficient staff on the ground to respond. And cameras need clear lines of sight and sufficient lighting. We found current practice is still a long way off: cameras were ineffective because of trees and shrubs growing in front, and autofocus cameras broken because they were pointed at flags and bunting.

The effectiveness of CCTV is being questioned in the country that has been a leading and enthusiastic adopter.

Current research shows that CCTV for crime prevention is largely ineffective. It is "lazy" to assume that installing technology solves the problem. It takes domain knowledge and attention to detail to make security technology work effectively—to date, this has been ignored, with expensive consequences.

References

1. Beck, A., and Willis, A. Context-specific measures of CCTV effectiveness in the retail sector. *Crime Prevention Studies 10* (1999), 251–269; http://www.popcenter.org/library/crimeprevention/volume_10/10-BeckWillis.pdf
2. Gill, M. and Spriggs, A. Assessing the impact of CCTV. Home Office Research Study 292. UK Home Office Research, Development and Statistics Directorate, February 2005; http://www.homeoffice.gov.uk/rds/pdfs05/hors292.pdf
3. Hope, C. 'Worthless' CCTV camera footage is not good enough to fight crime. *The Daily Telegraph*, (Aug. 26, 2009); http://www.telegraph.co.uk/news/newstopics/politics/6088086/Worthless-CCTV-camera-footage-is-not-good-enough-to-fight-crime-leading-QC-warns.html
4. Keval, H.U. and Sasse, M.A. "Not the usual suspects": A study of factors reducing the effectiveness of CCTV. To appear in *The Security Journal 23*, 2 (Apr. 2010); http://www.palgrave-journals.com/sj/journal/vaop/ncurrent/abs/sj20082a.html
5. Luff, P., Heath, C., and Jirotka, M. (2000): Surveying the scene: technologies for everyday awareness and monitoring in control rooms. *Interacting with Computers 13*, (2000), 193–228.
6. McIntosh, L. Soaring CCTV cameras 'are costly, futile and politically motivated'. *The Times* (Oct. 13, 2009); http://www.timesonline.co.uk/tol/news/uk/scotland/article6871833.ece?token=null&offset=12&page=2

M. Angela Sasse (a.sasse@cs.ucl.ac.uk) is Head of Information Security Research in the Department of Computer Science at University College London.

Calendar of Events

February 15–17
International Symposium on BioComputing 2010,
Calicut, India,
Contact: Dan Tulpan,
Phone: 506-861-0958,
Email: dan.tulpan@nrc-cnrc.gc.ca

February 19–21
Symposium on Interactive 3D Graphics and Games,
Bethesda, MD,
Sponsored: SIGGRAPH,
Contact: Chris Wyman,
Phone: 319-353-2549,
Email: cwyman@cs.uiowa.edu

February 22–23
Workshop on Mobile Opportunistic Networking,
Pisa, Italy,
Sponsored: SIGMOBILE,
Contact: Sergio Polazzo,
Phone: 390957382370,
Email: polazzo@iit.unict.it

February 22–23
Multimedia Systems Conference
Phoenix, Arizona,
Sponsored: SIGMM,
Contact: Wu-Chi Feng,
Phone: 503-725-2408,
Email: wuchi@cs.pdx.edu

February 25–27
India Software Engineering Conference,
Mysore, India,
Contact: Srinivas Padmanabhuni,
Email: s_padmana@yahoo.com

February 26–27
International Conference and Workshop on Emerging Trends in Technology,
Mumbai, India,
Contact: Poorva Girish Waingankar,
Email: poorva.waingankar@thekureducation.org

March 2–5
International Conference on Human Robot Interaction,
Nara, Japan,
Sponsored: SIGCHI, SIGART,
Contact: Pamela J. Hinds,
Phone: 650-723-3843,
Email: phinds@stanford.edu

March 2–5
IEEE Pacific Visualization 2010,
Taipei, Taiwan,
Contact: Shen Han-Wei,
Email: hwshen@cse.ohio-state.edu