Universiteit
Leiden
The Netherlands

Privacy-invading technologies : safeguarding privacy, liberty & security in the 21st century

Klitou, D.G.

Citation
Klitou, D. G. (2012, December 14). *Privacy-invading technologies : safeguarding privacy, liberty & security in the 21st century*. Retrieved from https://hdl.handle.net/1887/20288

Version:	Corrected Publisher's Version
License:	Licence agreement concerning inclusion of doctoral thesis in the Institutional Repository of the University of Leiden
Downloaded from:	https://hdl.handle.net/1887/20288

Note: To cite this publication please use the final published version (if applicable).

Cover Page

Universiteit Leiden

The handle http://hdl.handle.net/1887/20288 holds various files of this Leiden University dissertation.

Author: Klitou, Demetrius
Title: Privacy-invading technologies : safeguarding privacy, liberty & security in the 21st century
Date: 2012-12-14

6 PUBLIC SPACE CCTV MICROPHONES and LOUDSPEAKERS: The ears & mouth of 'Big Brother'

6.1 CHAPTER INTRODUCTION

With the exception to where there is an overlap with visual surveillance in public spaces, this chapter specifically addresses the concerns of the public space audio surveillance capabilities of integrated CCTV microphones and the added threat to privacy and liberty posed by the integration of public CCTV loudspeakers.

Section 6.2 introduces the privacy-intrusive evolution of CCTV surveillance technology. Section 6.3 outlines the social and privacy implications of the CCTV microphones and loudspeakers, and how CCTV microphones and loudspeakers are changing the nature and long-established notion of the public space. Section 6.4 reveals the scope of deployment of CCTV microphones and loudspeakers in the UK, whether privately or publicly owned and operated. Section 6.5 outlines the problems, weaknesses and deficiencies of earlier CCTV systems and explains the potential security gains of attaching microphones and loudspeakers to CCTV cameras. Section 6.6 describes the potential alternatives to CCTV microphones and loudspeakers. Section 6.7 gives an overview of the statutory laws and case law of special relevance in the UK. Section 6.8 evaluates and highlights the relevant deficiencies and dilemmas of the UK legal framework in terms of safeguarding privacy and individual liberty with regards to the deployment and use of CCTV microphones and loudspeakers. Section 6.9 proposes relevant policy and legislative recommendations to enhance the UK legal framework. Section 6.10 concludes with a brief summary and some ending remarks.

6.2 THE (PRIVACY-INTRUSIVE) EVOLUTION OF CCTV SURVEILLANCE TECHNOLOGY

CCTV ('Closed-Circuit Television') cameras have been in existence for decades, but during the turn of the 20th Century, particularly in the UK, the number of CCTV cameras deployed has increased dramatically. There are millions of CCTV cameras in the

UK alone.[314] As a result, CCTV cameras continue to play a visually prominent role in the "surveillance society" the UK is rapidly entering.

The ongoing evolution of CCTV technology has evolved from expensive, fixed cameras connected to videocassette recorders (or VCRs) via cables, which recorded and stored restricted amounts of low-resolution video data, to affordable IP (Internet Protocol) addressable, wireless pan/tilt/zoom (PTZ) CCTV cameras, which can be both remotely accessed and controlled, and can record practically unlimited amounts of digital, high-resolution video data, transmitted to computer hard drives for storage and analysis. If a dedicated communications network is not available, the digital video data recorded from these next generation public surveillance cameras can also now be transmitted and easily made available over the Internet or even via mobile phone technologies (Cannataci, 2010).

Other ongoing and/or potential enhancements to public surveillance cameras include the integration of: automatic license plate recognition systems that can track drivers; biometric technology (e.g. advanced face-recognition technology) that can be used to rapidly identify individuals; intelligent software that can recognize in real-time unlawful behavior, activities or events and certain objects;[315] microphones (or audio sensors) that can record audio data; loudspeakers that can enable CCTV control room operators to communicate with people; RFID readers that can track people in possession of RFID tags; software agents that can automatically and purposefully mine the vast

---

[314] "FactCheck: how many CCTV cameras?", Channel 4 News,18 June 2008, available at: http://www.channel4.com/news/articles/society/factcheck+how+many+cctv+cameras/2291167

[315] The Intelligent Video Surveillance (IVS) market is growing rapidly. Honeywell's Active Alert® and Keeneo's tailor-made software are just two examples of systems on the market that can automatically determine and classify different human behaviours and alert CCTV operators. Portsmouth has recently become the first city in the UK to set up a network of 'intelligent' cameras that can alert CCTV operators of 'suspicious' behaviour. see Slack, James. "Minority Report comes to Britain: The CCTV that spots crimes BEFORE they happen" (Daily Mail, 28 November 2008), available at: http://www.dailymail.co.uk/sciencetech/article-1089966/Minority-Report-comes-Britain-The-CCTV-spots-crimes-BEFORE-happen.html; '"Sci-Fi Film' CCTV Predicts Crime" (Sky News, 27 November 2008), available at: http://uk.news.yahoo.com/5/20081127/tuk-sci-fi-film-cctv-predicts-crime-45dbed5.html; An 'intelligent' CCTV camera, nicknamed "the Bug", designed to predict when a person may be about to commit a crime, is also being tested in high streets and shopping centers in the UK. The camera consists of a ring of eight cameras scanning in all directions. Software linked to the camera can determine when anybody is behaving unusually or suspiciously. A ninth camera then zooms in to follow that person. see Iredale, Will and Chris Gourlay. "CCTV camera 'tails' suspects" (Sunday Times, 15 April 2007), available at: http://www.timesonline.co.uk/tol/news/uk/crime/article1655200.ece; There are also a number of ongoing projects funded by the EU to improve the functionality and reliability of IVS. For example, Project SAMURAI and Project ADABTS aim to develop intelligent public surveillance software integrated with CCTV cameras for real-time behaviour profiling. Project Smart-Eyes (SEARISE) is even more advanced. The project's consortium aims to develop an "artificial cognitive visual system" for detecting, tracking and categorizing salient events and behaviours. The plan is to test the system in large crowded public spaces, once completed in 2011.

amounts of visual and audio data generated/stored; millimeter imaging technology that see through clothes (Surette, 2005); networked sensors that can monitor people's eye movements, body heat, etc.; and finally multiple chemical, biological, and radiological sensors (Canantaci, 2010). These enhancements and the integration of other technologies are part of the evolution from first-generation CCTV systems to second-generation systems, in order to address the problems, weaknesses and deficiencies of the earlier systems (Surette, 2005).

The integration of a variety of sensors (audio sensors and chemical, biological, and radiological sensors) with CCTV technology has been categorized in Europe as "Massively Integrated Multiple Sensor Installations" (MIMSI) (Cannataci, 2010). In the US, the term for MIMSI is "Domain Awareness System" (DAS) (*Ibid*.). The New York Police Department (NYPD) defines DAS as "technology deployed in public spaces as part of the counterterrorism program of the NYPD's Counterterrorism Bureau".[316] As Cannataci (2010) shrewdly points out, the NYPD's broad definition of DAS clearly allows for practically any type of technology (device, sensor, etc.) to be integrated.

As part of the increasing enhancement of public surveillance capabilities, highly sensitive omni-directional microphones and (horn) loudspeakers have been integrated into public space CCTV surveillance systems in the UK. This enhancement phase of public space CCTV surveillance systems, which this dissertation principally addresses, is the present move beyond the collection of images to the capability of both recording and communicating audio data with the addition of microphones and loudspeakers respectively.

The increasing integration of additional surveillance technologies with existing CCTV surveillance technology can significantly expand the threat to privacy (Cannataci, 2010). Accordingly, the increase in a surveillance system's capabilities increases the need for additional relevant policies (Surette, 2005, p. 164). The integration of microphones and loudspeakers with CCTV cameras equally requires corresponding policies and regulations to ensure the adequate protection of privacy and liberty.

---

316 NYPD's Public Security Privacy Guidelines, 2 April 2009, p. 2, available at: http://www.nyc.gov/html/nypd/downloads/pdf/crime_prevention/public_security_privacy_guidelines.pdf

6.3 THE EARS AND MOUTH OF 'BIG BROTHER'

Indeed, an era is emerging where practically any individual, and not only governments or large corporations, can engage in activities that intrude upon the privacy of many, as a result of the widespread accessibility and use of advanced technology.[317] In addition, rogue individuals with special computer skills can hack into people's personal computers and mobile phones. Nevertheless, any notion that the infamous 'Big Brother' metaphor is already outdated, as a result of the existence of so-called "small brothers", is still somewhat premature.

In the UK especially, the actions and policies of the British Government have done well to keep 'Big Brother' alive and kicking.[318] In George Orwell's *Nineteen Eighty-Four*, "telecreens" – two-way screens complete with microphones and loudspeakers – surrounded the masses in fictional "Oceania", in order to monitor and control their behaviour both in their homes and in public spaces. With the equivalent of eyes, and now also the equivalent of ears (microphones) and a mouth (loudspeakers), in a matter of speaking, there are valid concerns that CCTV cameras have become much closer to resembling the telescreens of Oceania and have further become an incarnation of 'Big Brother'.

Both CCTV loudspeakers and CCTV microphones could, therefore, reinforce the ability of CCTV cameras to monitor and control public behavior "through the promotion of habituated anticipatory conformity" (Norris and Armstrong, 1999, p. 5). Like in *Nineteen Eighty-Four*, where people assumed that every sound was overheard and movement observed (Orwell, 1949, p. 9), the known presence of CCTV loudspeakers and microphones could lead to not only direct social control, but their perceived presence could wreak indirect control. As Hubert H. Humphrey once observed, "[i]f we can never be sure whether or not we are being watched and listened to, all our actions will be altered and our very character will change".[319] In the words of Foucault, "an inspecting gaze, a gaze which each individual under its weight will end up interiorizing to the

---

317 For example, with a smartphone an ordinary individual can broadcast live videos onto USTREAM and with an iPhone can even control a small flying drone (developed by Parrot) that has a video-streaming camera. Moreover, hundreds of millions of people are walking around with a smartphone video camera and they can easily and immediately upload their videos onto YouTube.

318 The UK Government's plan to install 24-hour CCTV systems in the homes of 20,000 selected families to tackle anti-social behavior is yet another reason why the 'Big Brother' metaphor is still valid. In addition, hundreds of CCTV cameras have already been deployed within housing trusts across the UK. see Little, Alison. "Sin bins for worst families" (Daily Express, 23 July 2009), available at: http://www.express.co.uk/posts/view/115736

319 see Long, Edward V. *The Intruders: The Invasion of Privacy by Government and Industry* (Praeger, 1967), viii.

point that he is his own overseer, each individual thus exercising this surveillance over, and against himself" (Foucault, 1980, p. 155).

Public space CCTV cameras can already bring about the similar panoptic feelings caused by Jeremy Bentham's 'panopticon' design (Bannister et al., 1998). When people have panoptic feelings, they often increasingly adjust their behaviour to comply with what society considers 'normal' or socially acceptable (Schermer, 2007, pp. 217-18). Panoptic feelings may affect greater those who are more aware of the possibility (Schermer, 2007), whether real or potential, that they are being observed, especially if they are reminded of this possibility via CCTV loudspeakers. Attaching both loudspeakers and microphones to CCTV cameras will thus likely only increase the power of CCTV cameras to cause panoptic feelings in the long-term.

6.3.1 The ears (microphones)

Whether over the phone or face-to-face, conversations were beforehand considered private. Today, phone calls can be potentially monitored, and mobile phones (even when turned-off) and computers can be used as an eavesdropping device, while conversations have moved to online instant messaging, which can also be monitored and digitally stored. With the further advancement of listening devices[320] and the continuous evolution of privacy invasion, face-to-face conversations out in public are now potentially the latest target.

The ongoing attachment of microphones to CCTV cameras in the UK, at present, permits the recording of audio data in combination with video data to give a near complete account of activities in the public space(s) concerned. As Steve Harrison, Westminster's Assistant Director of Community Protection asserts, concerning the attachment of microphones to CCTV cameras in Westminster, "[t]his is about trying to instantly capture an image and audio that goes with it to let us know what's going on".[321] The CCTV microphones are reportedly so sensitive that they can provide CCTV control room operators the capability to potentially monitor and record conversations out in public many meters

[320] Revolutionary technology in electronic eavesdropping includes the use of devices that transmit laser beams or very high frequency radio waves, which can enable users to listen in to a conversation hundreds of feet away and practically render windows and/or walls invisible.

[321] Derbyshire, David. "Council plans to listen in on street life" (The Telegraph, 4 May 2005), available at: http://www.telegraph.co.uk/news/uknews/1489282/Council-plans-to-listen-in-on-street-life.html

from their location source. This would also raise concerns over the potential for CCTV microphones to possibly record conversations within private homes.[322]

Understandably, individuals often discuss personal thoughts or feelings during their verbal interactions out in public, including political opinions, religious beliefs or other beliefs of a similar nature, which Section 2 of the Data Protection Act 1998 legally recognizes as "sensitive personal data". Although these verbal discussions may occur out in public, they still arguably merit a reasonable expectation of privacy, albeit if kept at a certain volume level,[323] and should not be recorded by public or private bodies. While video surveillance of the general public obviously cannot listen in and record these opinions, feelings or beliefs when expressed verbally, the attachment of microphones to public space CCTV cameras, on the other hand, can provide the audio recording capability necessary to do so.

CCTV microphones could equally jeopardize certain individual liberties and fundamental freedoms, and repress legitimate political dissent, all in the name of security, similar to other technologies capable of mass surveillance (Cockfield, 2003). For instance, CCTV microphones could have the so-called "chilling effect"[324] on the freedom of expression, as people become more cautious of what they express with their friends and family out in public. Governments could even use CCTV microphones to monitor what is being said during a protest or what people generally talk about as means of becoming better aware of public opinion and maintaining political and social control.

On top of that, the audio data collected by CCTV microphones, in conjunction with the video data collected by the cameras, could be used not only to further monitor and control behavior in public spaces, but even also to enforce anti-social behavior rules concerning excessive noise at housing areas under the Anti-social Behaviour Act 2003 and the Crime and Disorder Act 1998. Local governments have already used

---

322 There have already been concerns over the deployment of CCTV cameras positioned in a way that can view inside the windows of private homes.

323 However, perhaps this expectation of privacy could one day be forgotten, as today's Internet generation (or Generation I or Generation Z) have a growing expectation, or even desire, to communicate to an audience what most would traditionally view personal. see Nussbaum, Emily. "Say Everything", Kids the Internet, and the End of Privacy: The Greatest Generation Gap Since Rock and Roll (New York Magazine, 12 February, 2007), available at: http://nymag.com/news/features/27341/

324 A legal term predominantly adopted in US courts, which is used in reference to laws, circumstances or actions that do not explicitly prohibit the exercise of fundamental freedoms, but rather bring about unnecessary repression or an intolerable burden on exercising these freedoms. The term has also been increasingly recognized and referred to by the ECtHR on numerous occasions. see, for example, *Case of Kyprianou v. Cyprus*, Application no. 73797/01, Judgment of 15 December 2005, para. 175: *Steel and Morris v. UK*, Application no. 68416/01, Judgment of 15 February 2005, para. 95; *Case of Wille v. Liechtenstein*, Application no. 28396/95, Judgment of 28 October 1999, para. 50.

CCTV cameras deployed in housing areas to monitor individuals subject to Anti-Social Behaviour Orders (ASBO) or Acceptable Behaviour Contracts (ABCs) and to gather information and evidence in certain locations for an ASBO application.[325] The policy and strategy is thus already potentially in place for using CCTV microphones for the similar purposes.

6.3.2 The mouth (loudspeakers)

Public CCTV loudspeakers primarily concern the component of privacy that endows citizens the right to be left alone. The loudspeakers attached to public CCTV cameras provide their operators the capability not only to observe people in public, but also to scold individuals and shout commands at them. While there are other methods in which CCTV operators can disturb individuals,[326] with the widespread deployment of CCTV loudspeakers, the scope of the ability to do so is unprecedented.

The deployment of CCTV loudspeakers is (or at least was) part of the UK Government's 'Respect Action Plan', a scheme for tackling anti-social behavior or low-level crime.[327] In the words of the Home Office, the use of the "talking cameras", as the Home Office and media refers to them, is to "tackle bad behaviour and promote good".[328] Any individual who engages in an activity considered by the CCTV operator to be "bad behavior" or "anti-social" can potentially be scolded and publicly humiliated or ridiculed into behaving "correctly". CCTV loudspeakers are thus being used as a means of threatening public humiliation, in order to deter anti-social behavior, which may be a form of social control through the conveyance of informal punishments, as opposed to social control through the threat of formal sanctions, such as fines or imprisonment.

While most people may likely not have a problem with CCTV loudspeakers, if their use prevents the vandalizing of property or leads to safer and cleaner streets and

---

325 see "Tackling Anti-Social Behaviour in Mixed Tenure Areas", Office of the Deputy Prime Minister, March 2003, p. 104, available at: http://www.communities.gov.uk/documents/housing/pdf/138706.pdf

326 For example, a CCTV control room operator could bother people he or she sees using public telephone booths. see "Phone Pest picked targets on security video" (The Telegraph, 7 June 1996), available at: www.telegraph.co.uk/htmlContent.jhtml?html=/archive/1996/11/27/ntel27.html

327 see the Respect Action Plan, produced by the Central Office of Information on behalf of the Respect Task Force (based in the Home Office), January 2006.

328 see a promotional image from the Home Office, available at: http://www.respect.gov.uk/uploadedImages/Public_site/Homepage/Main_features/TalkingCCTVbanner428x161.jpg

parks, however, once the public accepts CCTV loudspeakers, their deployment could become further routine. Today, CCTV loudspeakers are largely being used to discourage vandals or fly tippers. But, eventually the widespread, unregulated deployment and use of CCTV loudspeakers could lead to a new echelon of social control.

Rather than using restricted pre-recorded messages, operators have the ability to speak directly to individuals from afar. The CCTV loudspeakers in their present form effectively grant their operators the power to intrude upon the daily lives of ordinary people and disturb the right to be left alone. Without technological or legal limitations as to what can be said, when, where and for which purposes, the potential for CCTV operators to abuse the intrusive capability of loudspeakers is immense. There is essentially nothing to prevent operators from yelling out demeaning statements. Accordingly, the attachment of loudspeakers to CCTV cameras could further threaten personal freedom and personal dignity.

The use of CCTV loudspeakers to tackle anti-social behaviour and/or crime might be just the beginning. As John Willman suggests, an editor of the *Financial Times*, CCTV loudspeakers could be used to greet customers and tell them about new products and special offers, and, with the addition of improved face recognition technology or the development and integration of highly-advanced iris scanners,[329] CCTV loudspeakers could direct these messages to identified customers, much like the personalized talking advertisements in Steven Spielberg's film *Minority Report*.[330] In addition, CCTV loudspeakers could also be used by employers to convey work-related commands to employees and by schools to scold students who break the rules.

Moreover, the 'asymmetrical' design of CCTV loudspeakers, as a result of the inability of the general public to verbally respond to the speaker (i.e. the CCTV loudspeaker operator), in addition to not being able to see him or her, could exacerbate the unequal relationship between the observers (CCTV control room operators) and the observed (general public) (for further discussion, see, e.g., Hubbard et al., 2004, p. 244).

---

329 Iris scanners could rapidly advance, as a result of an innovation, known as Smart-Iris, developed from the ultra high-resolution, ultra-thin, lens-free, Panoptes cameras merged with projection devices. The advancement could remove the problems associated with traditional iris scanners, such as glare, dim lighting and the need for cooperative individuals to stop and stare at the scanners. see Drummond, Katie. "Darpa's Beady-Eyed Camera Spots the 'Non-Cooperative'" (Wired, 27 May 2010), available at: http://www.wired.com/dangerroom/2010/05/darpas-beady-eyed-camera-spots-the-non-cooperative/

330 see John Willman, "Talking cameras are just the start" (Financial Times, 7 April 2007), Ed1, p. 9.

6.4 SCOPE OF DEPLOYMENT IN THE UK

CCTV microphones and loudspeakers, for the most part, are being deployed in the UK alone.

6.4.1 CCTV microphones

Westminster City Council began testing CCTV microphones in 2005 to deal with noise at night,[331] but later reportedly decided not to proceed further.[332] Regardless, apparently more than 300 public CCTV cameras have been fitted with microphones in benefit offices and city centers.[333] For example, the public should be aware that a CCTV microphone is apparently located on Riverside Road near the Wimbledon Stadium, since the media reported that this particular CCTV microphone recorded a suspect's "manic" laughter nearby a crime scene.[334] Nevertheless, the extent to which CCTV microphones have been deployed is not clear. The BBC reported on a controversial proposal to use CCTV microphones on crowds during the 2012 Olympic Games in London,[335] in addition to the estimated 500,000 CCTV cameras the police plan to use.[336]

The increasing deployment of wireless network infrastructure in urban public spaces helps to reduce the costs of setting up and operating CCTV microphones. Moreover, audio data does not require an excessive amount of additional storage space. Therefore, due to the relatively simple installation of CCTV microphones and inexpensiveness and availability of the technology, their widespread deployment is not inconceivable.

---

331 Iain Thomson, "Council listens in to Soho crowds" (Vnunet, 4 May 2005), available at: http://www.vnunet.com/vnunet/news/2127273/council-listens-soho-crowds

332 Iain Thomson, 'Westminster Pulls CCTV Microphones' (Vnunet, 31 January 2008), available at: http://www.vnunet.com/vnunet/news/2208582/westminster-pulls-cctv

333 see statement made by Baroness Walmsley, Daily Hansard for 12 June 2008, Volume No. 702, Part No. 106, Column 736, available at: http://www.publications.parliament.uk/pa/ld200708/ldhansrd/text/80612-0010.htm

334 The man is no longer a suspect in the murder. see Harding, Eleanor. "Mystery chuckler not the killer of Andrew Cunningham from Earlsfield" (Local Guardian, 4 June 2009), available at: http://www.yourlocalguardian.co.uk/news/local/wimbledonnews/4419573.Mystery_laughter_leads_to_dead_end/

335 John Pienaar, 'Olympics audio surveillance row' (BBC News, 26 November, 2006), available at: http://news.bbc.co.uk/1/hi/uk_politics/6186348.stm

336 "CCTV plan to boost 2012 security" (BBC News, 4 March 2008), available at: http://news.bbc.co.uk/2/hi/uk_news/england/london/7278365.stm

The SIgard system, developed by Sound Intelligence,[337] was set up in London, Manchester and Coventry[338] and tested in Glasgow.[339] The CCTV microphones are linked to computers with sound analysis software and are apparently able to determine when sound contains the indicators of aggression (similar to the way the human brain interprets sound) and then alert the CCTV operators.[340] The CCTV microphones that were installed in Westminster were activated if noise levels reached above a certain threshold and made use of the existing Wi-Fi network that links the cameras to Westminster's central CCTV control room.

6.4.2 CCTV loudspeakers

A freedom of information request could reveal precisely how many loudspeakers have been connected to CCTV cameras throughout the UK and, if their use is indeed being tracked, how many times they have been used and precisely for which reasons.[341]

CCTV loudspeakers were first pioneered in Wiltshire in 2003.[342] As part of a special initiative called "Fancy an early night?", CCTV loudspeakers were deployed

---

337 A Netherlands based company, specializing in the development of advanced technology for the detection and analysis of sound. Sound Intelligence, available at: http://www.soundintel.com

338 W. van Reijendam. "English Bobbies can escape the normal life by listening to aggression detection" (Financieel Dagblad, 13 May 2008), available at: http://www.soundintel.com/en/nieuws/algemeen/groningse-camera-hoort-agressie.html

339 see Macdonald, Kenneth. "CCTV cameras 'listen for trouble'" (BBC News, 13 February 2009), available at: http://news.bbc.co.uk/2/hi/uk_news/scotland/7886656.stm

340 Sound Intelligence, available at: http://www.soundintel.com

341 I sent an identical freedom of information request by email on 14 November 2008 to the Home Office. An official reply from the Home Office was received on 26 November 2008 stating that the matters raised in the request are the responsibility of the Communities & Local Government and that the request has been transferred accordingly. After several weeks and not receiving further information, I inquired with the Communities & Local Government and resent my request on 3 March 2009. I was informed within 20 days that my previous request could not be traced, but that I would receive a response to my original request by 2 April 2009. On 27 March 2009, I received the FINAL response (Ref: F0002996) informing me that despite enquiries made of a number of the Business Units, the information I requested could not be provided since the Communities and Local Government does not hold this information. It was suggested that I contact the relevant local authorities or the particular police forces. What I have learned from this process is that either the UK Government does not want to provide this information or worse that indeed the use and deployment of CCTV loudspeakers is not being tracked centrally, if it is even being tracked at all. I can only hope it is being tracked locally.

342 "Talking CCTV pioneered in Wiltshire" (BBC News, 23 May 2003), available at: http://news.bbc.co.uk/2/hi/uk_news/england/wiltshire/2933626.stm

three years later in Middlesbrough Borough. More than a dozen CCTV loudspeakers have been fitted to public space cameras in Middlesbrough. Subsequently, on 4 April 2007, it was announced that loudspeakers would be fitted to numerous CCTV cameras in the following additional 20 areas, boroughs, cities or towns across the UK: Blackpool, Barking and Dagenham, Coventry, Darlington, Derby, Gloucester, Harlow, Ipswich, Mansfield, Northampton, Norwich, Nottingham, Plymouth, Reading, Salford, Sandwell, Southwark, South Tyneside and Wirral.[343] The announcement has been followed through.

CCTV loudspeakers are not only being deployed in city or town centers, but within parks and at hospitals. In Norwich, loudspeakers were fitted to multiple cameras in Waterloo Park and Eaton Park in order to curb littering.[344] In Wolverhampton, New Cross Hospital installed CCTV loudspeakers to scold people for failing to use designated smoking areas.[345]

The deployment is being funded through the Respect Task Force,[346] while the CCTV loudspeakers are being installed by local authorities, in partnership with the local police department and in coordination with the Home Office and local anti-social behaviour coordinators.

According to a statement made by Vernon Coaker, the Minister of State responsible for policing, crime and security at the Home Office, "the [Respect] task force has no current plans to fund further roll-out to other areas".[347] However, this does not mean that CCTV loudspeakers will not be deployed in more and more towns and cities with further funding from other sources. Since then, several additional towns have already followed suit. For example, Bristol subsequently initiated a three-month pilot[348] and

---

343 see "Children remind adults to act responsibly on our streets", Home Office, 4 April 2007, available at: http://www.asb.homeoffice.gov.uk/news/article.aspx?id=10310

344 "Offenders warned by talking CCTV" (BBC News, 13 April 2007), available at: http://news.bbc.co.uk/2/hi/uk_news/england/norfolk/6551501.stm

345 "Talking CCTV' to tackle smokers" (BBC News, 31 July 2008), available at: http://news.bbc.co.uk/1/hi/england/west_midlands/7535927.stm

346 The Respect Task Force is an inter-ministerial steering group, established in 2005, with the direct responsibility over the UK Government's 'Respect' agenda.

347 Daily Hansard for 10 May 2008, Column 427W, available at: http://www.publications.parliament.uk/pa/cm200607/cmhansrd/cm070510/text/70510w0019.htm

348 "City pilots 'talking' CCTV", 10 December 2007, available at: www.bristol.gov.uk/redirect/?oid=PressRelease-id-21982088

Hartlepool also announced their plans to tryout CCTV loudspeakers.[349] Merseyside, a metropolitan county, which includes the City of Liverpool, plans to dismantle thousands of old lampposts and replace them with new high-tech CCTV equipped ones. The new lampposts will reportedly include loudspeakers.[350]

CCTV loudspeakers are also being funded, deployed and operated by private entities. The Leeds-based property developer, Business Homes, have installed what they dub as "a state-of-the-art audio CCTV system" at the business park Halbeath Interchange in Dunfermline and are installing the system on all 25 of the business parks the company is currently developing throughout the UK.[351] McDonald's also deployed at 20 restaurants across the UK a system of CCTV cameras fitted with both microphones and loudspeakers, which are monitored and controlled via a central control room.[352]

The installation of the CCTV loudspeaker systems currently in place in Middlesbrough, West Bromwich and Nottingham, and supplied by Complus Teltronic, utilize the existing fiber optics or communications infrastructure.[353] With the Apex system, however, all information is sent and received via radio waves. Each unit integrated into the CCTV network is composed of a horn loudspeaker, small antenna, radio receiver, transmitter and power supply unit, and has a unique identification number. The CCTV control room can operate the units several kilometres from where the actual CCTV cameras and loudspeakers are located. By entering the unit's identification number and pressing the activation button, the operator can activate the corresponding loudspeaker.[354] Similarly, MEL Secure Systems launched CCTV loudspeaker systems that are ready to install and use digital wireless transmission. The loudspeakers of Bosch Secu-

---

349 "Talking cameras coming soon..." (Hartlepool Mail, 3 October 2008), available at: http://www.hartlepoolmail.co.uk/news/Talking-cameras-coming soon.4556556.jp

350 Coligan, Nick. "CCTV on every corner" (Liverpool Echo, 29 November 2007),

351 "Business Park's Talking CCTV A 'First' for Fife'", Business Homes, 1 September 2007, available at: http://www.businesshomes.com/newsDetails.asp?id=60

352 SourceSecurity.com, available at: http://www.sourcesecurity.com/markets/retail-and-eas/application/co-73-ga.350.html

353 "Talking CCTV Cameras – Middlesbrough", Complus Teltronic, 13 April 2007, available at: http://www.complusteltronic.co.uk/eng/newsdetail.asp?ID=396

354 Apex Radio Systems Ltd., available at: http://www.apexradio.co.uk/talkingcctv.php

rity Systems, on the other hand, apparently have superior sound quality, and have been deployed, for example, in Plymouth city for that reason.[355]

At this rate and level of enthusiasm, there is little reason to believe that CCTV loudspeakers will not eventually be deployed in every major town or city in the UK, and beyond. As a demonstration of what potentially is to come, CCTV loudspeaker technology was displayed at the 2007 Milipol exhibition, the world's largest for internal state security technology.[356] Given the relatively quick and easy installation of CCTV loudspeakers and integration with existing CCTV surveillance systems, the greater widespread deployment of CCTV loudspeakers is also not inconceivable.

6.5 SECURITY GAINS

The public security gains of integrating microphones and loudspeakers to CCTV cameras are centered mostly on their potential to enhance the ability of CCTV control room operators to do their job, which is to assist in the fight against crime and terrorism.

6.5.1 CCTV microphones

CCTV cameras are meant to help ensure public safety, i.e. to prevent crime and help counter-terrorism activities. Indeed, the UK Home Office has spent an overwhelming amount of its crime prevention budget on installing CCTV cameras. However, there is insufficient empirical evidence that CCTV cameras are helpful in preventing or reducing crime, which raises questions on their legitimacy and whether or not the deployment and use of CCTV cameras is proportional and justified. A Home Office report concluded that of the 14 CCTV systems it assessed, "most systems revealed little overall effect on crime levels […]."[357] Even more, CCTV cameras have shown to be more effective for reducing property crimes than violent crimes (Welsh and Farrington, 2003-2004, pp. 513-14) or preventing vehicle crimes in car parks. There is also little reason

---

355 "Bosch delivers CCTV with loudspeakers to Plymouth City", Security World Hotel, 5 May 2007, available at: http://www.securityworldhotel.com/int/news.asp?string1=&string2=&string3=&string4=&YearSearch=2007&category=0&company_id=&NAV=2&id=38223

356 see "Paris - Milipol to Focus on Homeland Security", Intelligence Online, 4 October 2007.

357 Martin Gill, Angela Spriggs et al., "The impact of CCTV: fourteen case studies", Home Office Online Report 15/05, p. 34, available at (last time visited: 23/01/12): http://www.homeoffice.gov.uk/rds/pdfs05/rdsolr1505.pdf

to believe that CCTV cameras significantly aid in criminal investigations. As Detective Chief Inspector Mick Neville asserted in May 2008 at a Conference of the Metropolitan Police's Visual Images Identifications and Detections Office (Viido), although "billions of pounds has been spent on kit" […], "only 3% of crimes were solved by CCTV"[358]. Moreover, an internal Scotland Yard report stated that less than one crime is solved per year for every 1,000 CCTV cameras in London, and there over a million CCTV cameras in London alone (Cannataci, 2010).[359] Therefore, CCTV cameras are not an effective alternative to traditional policing methods and activities and training and deploying more police officers.

Public space CCTV systems especially require human operators to be vigilant and sharp-eyed, in order to effectively observe multiple screens in real-time (or multiple video streams displayed on a single screen simultaneously). Often these images include areas with many persons, objects and activities present. The effectiveness of CCTV cameras is, thus, significantly dependent on the performance of operators, which can also degrade over time due to boredom or fatigue (Smith, 2004; Surette, 2005) or loss of concentration (Cannataci, 2010) and other 'human factors'. There are also a limited number of CCTV control room operators and, at times, the real-time video streams may go unmonitored (Norris and Armstrong, 1999). In addition, CCTV cameras naturally can only observe events, persons or objects within their field of view, which may occasionally be obstructed, for instance, by trucks or trees, or may even be impossible to view.

Although there is equally no empirical evidence proving so, combining microphones with public space CCTV cameras could improve the performance of the CCTV operators and perhaps even reduce the number of CCTV operators needed and/or improve the efficiency of their employment/deployment, which during the current ongoing economic crisis is becoming crucial.[360] CCTV microphones could also significantly enhance the capability of the CCTV cameras to detect crime. As Kim et al. demonstrate, auditory sensors can shorten the time required to locate a specific object, whereby the ability of humans to locate the direction of a sound's source can be mimicked by machines (2007, p. 383).

---

358 "CCTV boom failing to cut crime" (BBC News, 6 May 2008), available at: http://news.bbc.co.uk/2/hi/uk_news/7384843.stm

359 Hickley, Matthew. "CCTV helps solve just ONE crime per 1,000 as officers fail to use film as evidence" (The Daily Mail, 25 August, 2009), available at: http://www.dailymail.co.uk/news/article-1208700/CCTV-helps-solve-just-ONE-crime-1-000-officers-fail-use-film-evidence.html

360 see Camber, Rebecca. "Big brother is NOT watching you: Cash-strapped towns leave CCTV cameras unmonitored" (Daily Mail, 16 December 2008), available at: http://www.dailymail.co.uk/news/article-1095609/Big-brother-NOT-watching-Cash-strapped-towns-leave-CCTV-cameras-unmonitored.html

Sound is omni-directional as opposed to vision, which is directional, and, unlike vision, sound is not negatively affected by poor lighting or entirely obstructed by obstacles. Microphones can provide CCTV systems and operators the ability to detect crime beyond a camera's field of view and can help them to work better in areas with insufficient light. If several microphones are installed at a certain distance from each other, the location of the sound source can automatically be determined, based on the time difference of the arrival from the sound source to the sensors (Kim et al., 2007, p. 384). A pan/tilt/zoom (PTZ) CCTV camera can be pointed in that direction and the operator can simultaneously be both audibly and visibly alerted to contact the police immediately via a wireless network. CCTV microphones can therefore enhance the vigilance and effectiveness of CCTV operators and help them to observe more monitors or video streams, without having to hopelessly attempt to watch each simultaneously at all times. The SIgard system is based on the premise that violent incidents supposedly often start with verbal aggression or shouting, without actually conveying this so-called evidence.[361] While shouting may not justify triggering the CCTV microphones, gunfire, broken glass and explosions certainly do.

CCTV microphones can also potentially provide evidence in a court of law. For instance, the groans of Mark Witherall, while he was being brutally beaten and left to die by thieves, were recorded by a neighbor's security camera, which had audio recording capability, and was used as evidence against the offenders during the criminal trial.[362] In this case, however, microphones attached to public space CCTV cameras were not the source of the evidence, but rather the audio capabilities of security cameras in a private home.

6.5.2 CCTV loudspeakers

CCTV cameras, for the most part, do not prevent or deter crime, but rather simply record the criminal event, since there is a limited number of CCTV control room operators and the operators are not able to do much more beyond contacting the police or sounding an alarm. These deficiencies of CCTV cameras could perhaps be countered by the use of loudspeakers. The argument is that CCTV loudspeakers could potentially be used to combat crime and anti-social behaviour at an early stage by confronting

361 Sound Intelligence, available at: http://www.soundintel.com

362 "Teenagers could be heard on CCTV as they murdered father of three" (Daily Mail, 17 January 2008), available at: http://www.dailymail.co.uk/news/article-508880/Teenagers-heard-CCTV-murdered-father-three.html

those who engage in such acts, issuing warnings and reminding people that they are being monitored. In the words of Graeme Gerrard, the Chair of the CCTV Working Group of the Association of Chief Police Officers (ACPO) and Deputy Chief Constable of Cheshire Police:

> Talking CCTV [CCTV loudspeakers] increases the effectiveness of town centre cameras because it allows the camera operators to intervene and let the offender know their anti-social behaviour has been spotted and is being recorded. In many cases this is enough to stop the offending behaviour which in turn results in safer and tidier streets.[363]

CCTV operators could use the loudspeakers to swiftly intervene and discourage or dissuade unlawful or violent behaviour in real time, or perhaps even before it happens, and to warn someone if danger approaches them. For example, the technology was used as a deterrent at Business Homes' Nottingham site earlier this year against would-be thieves.[364] In addition, CCTV loudspeakers could also be used to reassure someone who requires immediate medical attention that emergency services have been contacted and are on their way.

According to Middlesbrough Council's security manager, Jack Bonnar, the town had recorded a 65-70% reduction of public order offences, such as disorderly conduct, since the introduction of CCTV loudspeakers.[365] Moreover, Middlesbrough Councilman Barry Coppinger asserts that CCTV loudspeakers have "raised awareness that the town centre is a safe place to visit and also that we are keeping an eye open to make sure it is safe".[366] Other places, such as Ipswich, have also reported a success.[367]

Once again, however, anti-social behaviour, such as littering, dog fouling, public urinating, or loitering, can hardly be considered threats to public safety, which calls

---

363 see "Children remind adults to act responsibly on our streets", Home Office, 4 April 2007, available at: http://www.asb.homeoffice.gov.uk/news/article.aspx?id=10310

364 see "Business Park's Talking CCTV A 'First' for Fife'", Business Homes, 1 September 2007, available at: http://www.businesshomes.com/newsDetails.asp?id=60

365 see "Children remind adults to act responsibly on our streets", Home Office, 4 April 2007, available at: http://www.asb.homeoffice.gov.uk/news/article.aspx?id=10310

366 "Talking' CCTV scolds offenders" (BBC News, 4 April 2007), available at: http://news.bbc.co.uk/2/hi/uk_news/england/6524495.stm

367 "TALKING CCTV cameras are set to stay in Ipswich after a trial proved a success,...", (Evening Star, Ipswich, 20 June 2008).

into question whether or not CCTV loudspeakers should be used to prevent or inhibit these acts and, if so, to what extent. After all, these acts have more than likely occurred millions of times in the UK alone. On the other hand, more serious forms of anti-social behaviour or disorderly conduct, such as vandalism, undoubtedly do pose a more serious threat to public safety and well-being. Nevertheless, the use of CCTV loudspeakers to prevent or deter lower level anti-social behaviour could, in theory, free police to fight real crime by reducing avoidable bureaucracy and paperwork.

Still, the effectiveness of CCTV loudspeakers in improving public safety or reducing anti-social behaviour has yet to be thoroughly evaluated or credibly proven. Moreover, if the commands broadcasted from CCTV loudspeakers are not respected and not enforced then their effectiveness will depreciate overtime until they most likely end up useless. In Salford Council, for instance, over half of the people reprimanded in 2007 for their behaviour via the CCTV loudspeakers ignored the reprimand.[368] On the other hand, in Nottingham, of the 109 people spoken to by CCTV operators using the loudspeakers, 78 did what they were told, and in 16 cases operators called a police officer to the scene and 12 fines were issued as a result.[369]

Nonetheless, the widespread deployment of CCTV loudspeakers could eventually incite rebellious acts in response, if it has not already, which could then result in more anti-social behavior than there was before.

6.6 ALTERNATIVES TO THE CCTV MICROPHONES AND LOUDSPEAKERS DEPLOYED IN THE UK

There are indeed a number of more privacy-friendly alternative devices and/or means, already in existence, with the purpose of helping to prevent and reduce crime and anti-social behaviour.

6.6.1 CCTV microphones

Gunfire and explosive detection systems have been around for more than ten years (Mazerolle et al., 1999). The ShotSpotter™ system, which the local police department

---

368 Haris, Jan. "Most people ignore talking CCTV", CCTV Core, available at: http://www.cctvcore.co.uk/27-09-2007-most-people-ignore-talking-cctv.html

369 "Talking CCTV a success in the city" (Nottingham Evening Post, 5 August 2008).

began operating in Redwood City, California as early as 1995, uses strategically placed sensors or microphones to triangulate the location of gunfire across wide areas within seconds of a weapon being fired (Monmonier, 2004, pp. 116-119). The ShotSpotter™ system has demonstrated accuracy within 25 meters. In addition, ShotSpotter™ can support subsequent forensic analysis, including the type of gun used, the direction of the gunfire, and even information related to the direction and speed of shooters on the move.[370] During the 2004 Olympic Games in Athens, pole-mounted microphones were used to detect explosions and gunfire and quickly pinpoint the location of an incident.[371]

6.6.2 CCTV loudspeakers

Derwent has developed a system, which detects trespassers and then automatically issues a warning over loudspeakers to leave the area. At night, the system's powerful AEGIS White Light LED illuminators, activated by a passive infra-red (PIR) sensor, can flood the area with light.[372] It is not hard to imagine that a sudden burst of bright light will deter trespassers and vandals.

A similar device called FlashCAM-880 developed by Q-Star Technology automatically takes a digital photo and delivers a recorded message, when activated by motion sensors, to deter intruders, vandals, graffiti taggers or illegal dumpers. The digital camera can operate in total darkness and has an operating range of up to 100 feet. FlashCAMs have been deployed in cities throughout the US and have resulted in a number of success stories.[373]

An additional alternative device to CCTV loudspeakers is the Mosquito™, an anti-vandal system developed by Compound Security Systems Ltd., which emits a high frequency sound that is piercing only for teenagers. The Mosquito™ has proven to successfully drive away gangs of youths and in doing so can prevent teenagers from

---

370 ShotSpotter, Inc., available at: http://www.shotspotter.com/products/technology.html

371 'Olympian challenge', Info4 Security, 5 February 2007, available at: http://www.info4security.com/story.asp?storyCode=3093811&sectioncode=16

372 "Derwent's White Light Illuminators Tackle Network Rail Thieves", Derwent, available at: http://www.derwentcctv.com/home/index.php?id=7&nid=75

373 Q-Star Technology, available at: http://www.qstartech.com

engaging in acts of vandalism or loitering in front of businesses. The Mosquito™ has been deployed throughout the UK.[374]

The so-called "Manilow Method", whereby opera, classical or other music unpopular with teenagers is played to drive away youth, has also been used in the UK by shop owners and local councils, reportedly with some success.

Improved street lighting is another alternative to the increased deployment of CCTV cameras. Research has also shown that improved street lighting in a public space setting leads to a greater reduction in overall crime than CCTV cameras (Welsh and Farrington, 2003-2004, p. 513).

The further recruitment and deployment of Police Support Community Officers (PSCOs) or other authorized officers of a local authority or security operatives licensed by the Security Industry Authority, is an additional alternative to the use of CCTV loudspeakers in tackling anti-social behaviour. Whether deploying more human resources on the ground is more effective than using CCTV loudspeakers is debatable, but certainly this method reduces the concerns of 'asymmetric' observation (see Hubbard et al., 2004) and any unnecessary/inappropriate public humiliation.

Other alternatives to CCTV loudspeakers and their approach to 'correcting' anti-social behavior through near public humiliation, are education and after-school social programs, and even video games, such as the interactive gaming technology platform developed by Project rePLAY through EU funding.

6.7 LAWS, CODES AND OTHER LEGAL/POLICY INSTRUMENTS OF SPECIAL RELEVANCE IN THE UK

As widely recognized, CCTV surveillance systems may legitimately be deployed for the sake of preventing and detecting crime, protecting property and individuals, and defending public interests.[375] The police are especially permitted to use CCTV systems for carrying out their duties and functions. Other public entities and private entities may also be permitted to use CCTV cameras, since their use may be considered reasonable to prevent criminal offenses or assist in the lawful arrest of offenders. Consent is not required, since the collection and processing of the data from CCTV surveillance sys-

---

[374] Compound Security Systems, available at: http://www.compoundsecurity.co.uk

[375] see Article 29 Working Party, Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance (WP 89).

tems is deemed necessary to protect the vital interests of society and to prevent threats to public safety/security, when carried out in accordance with the law.

In the opinion of the Article 29 Working Party, Directive 95/46/EC applies to the processing of image and sound data by means of CCTV surveillance systems.[376] The Data Protection Act 1998 (DPA) implements or transposes in its own way Directive 95/46/EC into UK domestic law.

In short form, the eight data protection principles, listed in the DPA,[377] requires that all personal data must be:

- Processed fairly and lawfully;
- Obtained and used only for specified and lawful purposes;
- Adequate and relevant, and not excessive;
- Accurate and, where necessary, up to date;
- Kept no longer than necessary;
- Processed in accordance with the rights of individuals;
- Secure; and
- Transferred only to third-party countries that have adequate data protection laws and practices

Once again, these data protection principles are parallel to the principles of privacy outlined in Chapter 3. The first data protection principle, and the conditions that must be met in accordance with Schedules 2 and 3 of the DPA, are basically parallel to the principle of consent/choice. The second data protection principle is parallel to the purpose specification principle and the use limitation principle. The third data protection principle is parallel to the principles of proportionality and data minimization. The fourth data protection principle is parallel to the access/participation principle and the integrity principle. The fifth data protection principle is parallel to the use limitation principle. The sixth data protection principle is parallel to the principles of notice/awareness and consent/choice. The seventh data protection principle is parallel to the principle of security/integrity.

Part V of the DPA implements the principle of enforcement/redress through the establishment of a Data Protection (Information) Commissioner with the authority to intervene in suspected breaches of the DPA by data controllers and issue enforcement notices requiring rectification. The Data Protection Commissioner may also be granted

---

376 *Ibid.*

377 Data Protection Act 1998, Schedule 1, Part I.

a warrant from a circuit judge to enter and inspect the premises of a data controller. The DPA also provides for prosecutions of persons suspected of violating the provisions of the DPA and, if found guilty, those persons are subject to penalties.

Personal data is defined in Article 2 (a) of Directive 95/46/EC as:

> any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

The definition of personal data in the DPA is different in wording and format from Directive 95/46/EC. Part 1, Section 1(1) of the DPA defines personal data as:

> data which relate to a living individual who can be identified –
> (a) from those data, or
> (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Moreover, in order to determine if data is 'personal', any feasibly possible means to link the data with data relating to an identifiable individual should be taken into account. As Recital 26 of EU Directive 95/46/EC states:

> to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person.

However, as the Article 29 Working Party argues, Recital 26

> means that a mere hypothetical possibility to single out the individual is not enough to consider the person as "identifiable". If, taking into account "*all the means likely reasonably to be used by the controller or any other person*", that possibility does not exist or is negligible, the person should not be

> considered as "identifiable", and the information would not be considered as "personal data".[378]

But, as the Article 29 Working Party further adds, this should particularly "take into account all the factors at stake", including the cost of conducting the identification, the intended purpose and the advantage expected by the controller, and should consider "the state of the art in technology at the time of the processing and the possibilities for development during the period for which the data will be processed".[379]

The UK's Information Commissioner's Office (ICO) is responsible for ensuring that all organizations comply with the obligations of the DPA and has, to a certain extent, the enforcement powers to do so. CCTV operators (i.e. data controllers) must use CCTV systems in accordance with the DPA's data protection principles (where relevant) and the DPA also requires CCTV operators to register with the ICO (Taylor, 2002a). In accordance with Section 51 (3)(b) of the DPA (and Article 27 of Directive 95/46/EC), the ICO also issued the 'CCTV code of practice' to help operators of CCTV surveillance systems to comply with the DPA (where relevant). The CCTV code of practice was updated in July 2000 and again in January 2008.

The UK is a party to the ECHR. The Human Rights Act 1998 (HRA) incorporated the ECHR into UK domestic law, requiring domestic courts to take into consideration the decisions of the ECtHR and requiring all domestic legislation to be interpreted in a way consistent with the ECHR. But, the HRA does not mandate that UK domestic courts must observe ECtHR jurisprudence.[380]

Article 8(1) of the ECHR states:

> Everyone has the right to respect for his private and family life, his home and his correspondence.

It is generally accepted that the right to privacy is not absolute and may be infringed under certain circumstances. Accordingly, Article 8(2) states:

---

[378] Article 29 Working Party, Opinion 4/2007 on the concept of personal data (WP 136), p. 15.

[379] *Ibid*.

[380] For further discussion, see Taylor, Nick. *State Surveillance and the Right to Privacy* (Surveillance & Society 1, 2002a), pp. 66-85.

> There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

With the entry into force of the Treaty of Lisbon in 2009,[381] the Charter of Fundamental Rights of the European Union is equally applicable within UK law and is enforceable within UK domestic courts. Article 7 of the Charter provides for the right to privacy, and Article 8 explicitly stipulates:

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

The Treaty of Lisbon also elevates the right to the protection of personal data in EU law through the adoption of a specific article on the right.[382] Article 16 B (para. 1) of the Treaty on the Functioning of the European Union (TFEU)[383] affirms, "Everyone has the right to the protection of personal data concerning them". Article 16 B (para. 2) grants the EU (i.e. the European Commission, European Parliament and the Council) the power or legal basis to legislate and adopt data protection rules applicable to all sectors, including in the area of freedom, justice and security, and therefore alters the limitations of Article 3 of Directive 95/46/EC.[384]

---

381 Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007 (OJ C 306, 17.12.2007).

382 For further discussion, see Cannataci, Joseph A. *Lex Personalitatis: Personality, Law and Technology in the 21st Century* (Acta Universitatis Lucian Blaga 219, 2008).

383 see Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union (OJ C 83, 30.3.2010)

384 see Com (2007) 87 final, Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive.

Accordingly, the EC has adopted a draft proposal for a Directive on the protection of individuals with regard to the processing of personal data for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal offences.[385] The proposal builds on Directive 95/46/EC and the Council Framework Decision 2008/977/JHA (hereinafter: CFD 2008/977/JHA),[386] which addresses the protection of personal data processed by law enforcement authorities in criminal matters and complements Directive 95/46/EC. The United Kingdom also takes part in CFD 2008/977/JHA, in accordance with Article 5 of the Protocol integrating the Schengen acquis into the framework of the European Union.[387]

Purportedly, CCTV surveillance systems are being deployed in the UK to prevent crime (Taylor, 2002a, p. 79). However, while an interference with the right to privacy is permitted, any interference must demonstrate both that it is necessary to fulfill a legitimate aim and is proportionate to fulfilling that aim.[388] Some authors question, for example, whether or not the widespread use of CCTV surveillance systems in public spaces is a proportionate response for preventing crime (see, e.g. Taylor, 2002a, p. 80). In addition, any interference with the right to privacy by public authorities must be "in accordance with the law", and the consequences of the law must be foreseeable.[389]

Certain interpretations of Article 8 of the ECHR finely suggest the notion that even activities or incidents involving identifiable individuals that occur in public and are permanently or systematically recorded may be considered private and may thus engage the right to privacy, albeit balanced with the interests of national or public security. The ECtHR has recognized the possibility of the blurring of the public and private spheres. For instance, in *P.G. and J.H. v. the United Kingdom*, the ECtHR held that there "a zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life"'.[390] The ECtHR also held that:

---

385 see Proposal for a Directive of the European Parliament and of the Council on the protection of Individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM(2012) 10 final, Brussels, 25.1.2012 (Article 1).

386 Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (30.12.2008).

387 *Ibid*., recital 43

388 see Charter of Fundamental Rights of the European Union, Article 52(1).

389 see, e.g., *Kopp v. Switzerland*, Application No. 23224/94, Judgment of 25 March 1998.

390 *P.G. and J.H. v. the United Kingdom*, Application No. 44787/98, Judgment of 25 September 2001, para. 56.

> A person who walks down the street will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means of the same public scene (for example, a security guard viewing through closed-circuit television) is of a similar character. Private-life considerations may arise, however, once any systematic or permanent record comes into existence of such material from the public domain. It is for this reason that files gathered by security services on a particular individual fall within the scope of Article 8, even where the information has not been gathered by any intrusive or covert method.[391]

In *Peck v. the United Kingdom*, the ECtHR judged that the publication or general disclosure for broadcasting purposes of images of identifiable individuals obtained by public space CCTV cameras constitutes an intrusion of the right to privacy enshrined in Article 8 of the ECHR. The ECtHR stated:

> Private life is a broad term not susceptible to exhaustive definition. The court has already held that elements such as gender identification, name, sexual orientation and sexual life are important elements of the personal sphere protected by Art.8. The Article also protects a right to identity and personal development, and the right to establish and develop relationships with other human beings and the outside world and it may include activities of a professional or business nature. There is, therefore, a zone of interaction of a person with others, even in a public context, which may fall within the scope of 'private life' (emphasis added).[392]

Furthermore, in *Niemietz v. Germany*, the ECtHR judged:

> it would be too restrictive to limit the notion to an "inner circle" in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings.[393]

391 *Ibid.*, para. 57.

392 *Peck v. the United Kingdom*, Application No. 44647/98, Judgment of 28 January 2003, para. 57.

393 *Niemietz v. Germany*, Application No. 13710/88, Judgment of 16 December 1992, para. 29.

As Harris et al. argue, "the expanding understanding of private life set out in the *Niemietz* case indicates that a formal public/private distinction about the nature of the location will not always be decisive" (1995, p. 309).[394]

An infringement of privacy can be associated with the infringement of other rights. The ECtHR in *Segerstedt-Wiberg and others v. Sweden* recognized that an unjustified violation of the right to privacy could also be associated with a violation of the rights to freedom of expression and freedom of (peaceful) assembly, enshrined in Articles 10 and 11 of the ECHR respectively. The ECtHR affirmed that

> the storage of personal data related to political opinion, affiliations and activities that is deemed unjustified for the purposes of Article 8 § 2 *ipso facto* constitutes an unjustified interference with the rights protected by Articles 10 and 11.[395]

Therefore, in order to determine the extent to which public surveillance activities may breach Article 8 of the ECHR, one must carefully consider the purposes and basis for the surveillance and the subsequent use and/or disclosure of the audio and video/image data collected.

Finally, it is also important to note here, however, that the DPA and Directive 95/46/EC apply to all data controllers, while the HRA and ECHR only apply to public authorities. Nonetheless, in accordance with Section 3 of the HRA, the DPA must still be legally interpreted in a way consistent with the ECHR.

---

394 For further discussion, see Taylor, Nick. *State Surveillance and the Right to Privacy* (Surveillance & Society 1, 2002a), pp. 66-85.

395 *Segerstedt-Wiberg and others v. Sweden*, Application No. 62332/00, Judgment of 6 June 2006, para. 107.

6.7.1 CCTV microphones

Based on the privacy/data protection principles, the purpose(s) of any CCTV surveillance system should be specified beforehand and the processing of the images (of identifiable persons), or any other (personal) information obtained via CCTV surveillance systems, must be compatible with the lawful and specified purposes. The use of CCTV surveillance systems must only correspond to achieving these specified purposes. The data collected should also not be retained for longer than is necessary to achieve the specified purposes. In addition, based on the privacy/data protection principles, signs must be displayed to clearly inform the public that they are entering an area monitored by CCTV cameras.

Both audio and image data may qualify as personal data.[396] Appropriately, the former Information Commissioner Richard Thomas declared that sound recorded by CCTV cameras would be treated under UK law in the same way as CCTV footage.[397]

Up until January 2008, the CCTV code of practice, however, did cover sound recording capabilities of CCTV cameras. The updated CCTV code of practice issued in January 2008 addresses the concern of CCTV microphones, but does not forbid their use, as somewhat misleadingly reported by *The Telegraph*.[398] Instead, the CCTV code of practice (2008) advises against recording conversations unless in exceptional circumstances and with the presence of signs. The CCTV code of practice (2008) states:

> CCTV must not be used to record conversations between members of the public as this is highly intrusive and unlikely to be justified. You should choose a system without this facility if possible. If your system comes equipped with a sound recording facility then you should turn this off or disable it in some other way. There are limited circumstances in which audio recording may be justified, subject to sufficient safeguards. These could include: Audio based alert systems (such as those triggered by changes in noise patterns such as sudden shouting). Conversations must not be recorded, and operators should not listen in.[399]

---

396 see Directive 95/46/EC, Recital 14.

397 "Word on the street ... they're listening" (Sunday Times, 26 November 2006), available at: http://www.timesonline.co.uk/tol/news/uk/article650166.ece

398 Hennessy, Patrick. "CCTV camera microphones to be axed" (Telegraph, 28 January 2008), available at: http://www.telegraph.co.uk/news/uknews/1576686/CCTV-camera-microphones-to-be-axed.html#continue

399 CCTV code of practice 2008, p. 10.

Any automated decision, using intelligent software, pertaining to the audio data recorded from the CCTV microphones, would fall under Article 7 of the CFD 2008/977/JHA and would thus be subject to its safeguards.

6.7.2 CCTV loudspeakers

While the CCTV code of practice addresses the use of CCTV loudspeakers, it is difficult to determine the relevant binding statutory laws and case law that pertain to CCTV loudspeakers. The CCTV code of practice exclusively addresses CCTV loudspeakers with the following statement:

> The use of audio to broadcast messages to those under surveillance should be restricted to messages directly related to the purpose for which the system was established.[400]

CCTV loudspeakers are being used to curtail anti-social behaviour, which is rather broadly defined by the Crime and Disorder Act 1998 as acting

> in a manner that caused or was likely to cause harassment, alarm or distress to one or more persons not of the same household as himself.[401]

Anti-social behaviour may include the following acts, just to name a few: vandalism, graffiti, indecent exposure, inappropriate sexual conduct in public, soliciting, illegal parking, fly tipping,[402] public drunken behaviour, and urinating or defecating in public.

---

400 *Ibid.*, p. 11.

401 Section 1, para. 1 (a).

402 Fly tipping is a form of littering that involves dumping large objects or large quantities of material.

6.8 DEFICIENCIES AND DILEMMAS OF THE UK LEGAL FRAMEWORK

Based on the principles of privacy and the criteria of adequacy, as outlined in Chapter 3, an assessment of the UK legal framework reveals significant legal dilemmas and deficiencies, with regards to the deployment and use of public space CCTV microphones and loudspeakers.

6.8.1 CCTV microphones

The DPA certainly incorporates the data protection principles and fully transposes Directive 95/46/EC into UK law. Although the data protection legislation was not originally foreseen to cover CCTV surveillance, Directive 95/46/EC indeed covers both audio and video surveillance, as recognized by the Article 29 Working Party,[403] and in accordance with Recital 14 of Directive 95/46/EC. Still, the DPA or Directive 95/46/EC does not provide a comprehensive legal framework for regulating CCTV surveillance systems, in particular concerning the latest enhancements to public CCTV surveillance capabilities. Besides, as the EC has acknowledged, "[t]he combination of sound and image data with automatic recognition imposes particular care when applying the principles of the Directive".[404] Moreover, the DPA, for the most part, regulates the processing, retention and dissemination of personal data, which may or may not include the audio/video data collected through public space CCTV surveillance systems, but does not actually regulate the deployment of public space CCTV systems nor does it regulate their general use when no audio/video data is stored. This could mean that, even if the DPA regulates the subsequent use of the audio data collected and stored via CCTV microphones, the DPA may not necessarily regulate the use of CCTV microphones to simply listen in to conversations occurring out in public.

All the same, Directive 95/46/EC does not apply to the processing of personal data concerning public security, defence, state security or the activities of the State in areas of criminal law. In particular, Article 3 of Directive 95/46/EC excludes "activities of the State in areas of criminal law" and "operations concerning public security". Moreover, the audio data collected through CCTV microphones is exempt from the first data protection principle of the DPA, since the UK Government is arguably deploying and using

---

403 see Article 29 Working Party, Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance (WP 89).

404 Com (2007) 87 final, Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive, p. 7.

public CCTV microphones to prevent or detect crime.[405] This exemption is equally in line with Article 13 of Directive 95/46/EC.

Again, Article 16 B (para. 2) of the TFEU creates a legal basis for the EU to legislate and adopt instruments applicable to all sectors, including in the area of freedom, justice and security, and therefore also alters the limitations of Article 3 of Directive 95/46/EC.[406] But, in accordance with Article 6a of Protocol No 21 of the Treaty of Lisbon, the UK is not bound by the rules laid down on the basis of Article 16 when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three of the Lisbon Treaty, which deal with criminal matters. In addition, while the Charter of Fundamental Rights of the European Union, including Articles 7 and 8, also applies to the UK (as an EU Member State), in accordance with Article 51, the Charter is not applicable to activities, which are considered a domestic matter outside the scope of EU law.

While CFD 2008/977/JHA aims to protect individuals with regards to processing of their personal data for law enforcement purposes, the scope of the Framework Decision has a limited scope of application, since it only applies to the cross-border data processing of law enforcement agencies and not national/domestic activities.[407] Furthermore, as Cannataci (2010) notably points out, CFD 2008/977/JHA does not provide any concrete details on how to uphold the rights of data subjects affected by 'smart surveillance' or MIMSI surveillance systems.

The fact that Article 3 of Directive 95/46/EC excludes "activities of the State in areas of criminal law" and "operations concerning public security" and the fact that the scope of CFD 2008/977/JHA is limited to cross-border data processing compelled

---

405 Data Protection Act 1998, s. 29 (1) (a).

406 For further information, see Com (2007) 87 final, Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive. (Hence, the reason for the emergence of the Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM(2012) 10 final, Brussels, 25.1.2012.

407 see Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (30.12.2008), recital 3. For further discussion, see Cannataci (2010).

the EC to propose a new Directive on the protection of individuals with regard to the processing of personal data for law enforcement purposes.[408]

With regards to the general use of CCTV microphones, the legal framework additionally does not fulfill the ***principles of use limitation*** and ***purpose specification***. To begin with, the judgment adopted by the Court of Appeal in *Durant v. Financial Services Authority*[409] narrowed the meaning of 'personal data' in the UK. For data to be "personal" the concerned individual needs to be the "focus" and the data needs to be intended to provide specific intelligence of a "biographical" nature about a particular person.[410] As Rempell (2006) notably argues, this narrowed definition of personal data, which was accomplished by narrowing the meaning of the words "relate to" within the definition, is flawed (2006, p. 823) and is against the proper intentions of the drafters of Directive 95/46/EC for a broader definition (2006, pp. 825-26). As Rempell concludes in his analysis of the judgment, the problem is not necessarily with the content of the DPA, but rather the Court of Appeal's decision, which seriously deviates from Directive 95/46/EC (2006, p. 840). In direct response to the judgment, the ICO was forced to issue corresponding guidance on the definition of what amounts to personal data.[411]

The consequences of *Durant v. Financial Services Authority* went beyond data held by the Federal Services Authority (FSA) and, as widely recognized, directly affected the data captured via public space CCTV cameras (Rempell, 2006). With regards to the images generated by public space CCTV cameras, the narrowing of the definition of personal data essentially meant that if only a general scene is recorded with no focus on any particular individual's activities, these images are not covered by the DPA, as they are no longer regarded as personal data (Rempell, 2006). Therefore, in actuality the DPA does not apply to a large part of the data captured by public CCTV cameras.

---

408 see Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM(2012) 10 final, Brussels, 25.1.2012.

409 *Michael John Durant v. Financial Services Authority* [2003] EWCA (Civ) 1746. Durant made a request under Part II, Section 7 of the Data Protection Act 1998 to obtain 'personal data' about him which was held by the Financial Services Authority (FSA). The FSA refused to provide all the data requested by Durant, arguing that not all of it constituted personal data, and emphasized that the definition of the words "relate to" in the DPA's definition of personal data meant "have reference to, concern" instead of "have some connection with, connected to" (para. 25). The Court of Appeal agreed with the FSA.

410 *Ibid.*, para. 28.

411 "*The Durant case and its impact on the interpretation of the Data Protection Act 1998'", Information Commissioner's Office, 2 February 2004.*

Equally, likely for the same reason, the ICO determined that Google Street View does not breach the DPA.[412]

Following pressure from the EC[413] and the threat that the EC could begin infringement procedures against the UK for the unacceptable or objectionable implementation of Directive 95/46/EC, and the adoption by the Article 29 Working Party of a much broader interpretation of personal data,[414] the ICO issued once again revised guidance, titled "Data Protection Technical Guidance – determining what is personal", which stretched, to a certain extent, the narrow definition of personal data in the UK. But, the judgment of the Court of Appeal in *Durant v. Financial Services Authority* is legally superior to the guidance of the ICO. Nevertheless, as a result of the Charter of Fundamental Rights of the European Union and the entry into force of the Treaty of Lisbon, both the European Commission and UK citizens could potentially further challenge the UK's implementation of the DPA (i.e. Directive 95/46/EC).

Overall, the situation represents an example of the non-uniform implementation and interpretation of the provisions of Directive 95/46/EC by EU Member States (Rempell, 2006), and the UK's common practice of moving beyond the limits of the "margin of maneuver" as permitted by Recital 9 of Directive 95/46/EC.[415]

Applying the same rationale of *Durant v. Financial Services Authority* to audio recorded by CCTV microphones, general sound recorded in public is not considered personal data and therefore is not covered by the DPA, since it is not focused on any particular individual. With additional technology, however, the background noise can be filtered out using inverse phasing, which cancels out unwanted noise, to discern private conversations concerning particular individuals. Therefore, general sound recorded in public at the point of collection might not be considered personal data, but may later be converted, with little effort, into personally identifiable information and, in accordance with Recital 26 of Directive 95/46/EC, constitute personal data.

---

412 Information Commissioner's Office, Press Release, "Common sense on Street View must prevail, says the ICO", available at: http://www.ico.gov.uk/upload/documents/pressreleases/2009/google_streetview_220409_v2.pdf

413 see "European Commission suggests UK's Data Protection Act is deficient" (OUT-LAW News, 15 July 2004), available at: www.out-law.com/page-4717

414 see Article 29 Working Party, Opinion 4/2007 on the concept of personal data (WP 136).

415 Hence, the reason why the EC has proposed to replace Directive 95/46/EC with a Regulation, in order to eliminate the existing fragmentation and to ensure the uniform and effective implementation of the data protection rules within every EU Member State. For further discussion, see COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, Safeguarding Privacy in a Connected World, A European Data Protection Framework for the 21st Century, COM(2012) 9 final, Brussels, 25.1.2012.

However, even if general sound recorded in public and stored on databases could be considered personal data, or construed as such, and thus protected by the DPA, the act of recording sound out in public is not prohibited. In essence, only what is done with that stored audio data afterwards is regulated.

Nevertheless, audio data collected from public CCTV microphones is wrongfully being equated with video data collected from public CCTV cameras. Audio data, even recorded in public, can be considerably more 'sensitive', since it may record private conversations and thus the political opinions and religious beliefs of individuals – information which video data normally cannot discover, unless the messages/words are both written down, for example on a sign or t-shirt, and are discernible via the CCTV cameras.

With further sophistication, CCTV microphones can also potentially lead to the greater identification and tracking of individuals in public. Software can identify an individual by comparing their voice with voice-prints[416] stored in a database. According to the Police IT Organization (PITO), voice is an additional mode of identification that is already being considered for inclusion into IDENT1,[417] the UK central national database for storing biometric information.[418] The legal framework does not necessarily prevent the use of CCTV microphones for this purpose.

Furthermore, the CCTV code of practice (2008) addresses CCTV microphones, but it is not binding law in itself and does not offer any actionable rights for citizens. Nevertheless, the CCTV code of practice (2008) only briefly deals with the issues surrounding CCTV microphones, lacks specificity and leaves open several legal loopholes. Although the CCTV code of practice (2008) states, "CCTV must not be used to record conversations between members of the public as this is highly intrusive and unlikely to be justified",[419] it is unclear what is the actual legal basis of this declaration. Nor is it clear whether this includes conversations occurring in public places, particularly if people are aware that microphones are being overtly fitted to public space CCTV cameras.

Supporters in favor of public CCTV microphones could argue that if a person does not want to be heard or recorded, he/she can choose not to speak when out in public or at least not about 'sensitive' topics, such as religion or politics. Moreover, it can be further argued that the presence of any CCTV surveillance system is merely comparable to

---

416 A voice-print is data representing patterns in a digital recording of an individual's voice.

417 PART 1: Identification Roadmap 2005 – 2020, Biometrics Technology Roadmap for Person Identification within the Police Service, Police IT Organization, p. 4.

418 However, the Identity Documents Act 2010 recently repealed the Identity Cards Act 2006, which permitted the recording of any type of biometric information for the National Identity Register (NIR).

419 CCTV code of practice 2008, p. 10.

the presence of an individual observer, such as a security guard. As the ECtHR in *P.G. and J.H. v. the United Kingdom* judged:

> A person who walks down the street will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means of the same public scene (for example, a security guard viewing through closed-circuit television) is of a similar character.[420]

Therefore, since CCTV cameras installed in public places are already legitimately considered as the eyes of security guards or law enforcement officers/agents, microphones could legitimately be considered as their ears.

While covertly recording private conversations is regulated and is often considered eavesdropping, like video surveillance, it is only prohibited, without due authorization, in areas where privacy can reasonably be expected. Although Moreham (2006) is indeed correct in arguing that a person would have a reasonable expectation that another person, for instance, is not recording their conversations with a shotgun microphone, however, any expectation of privacy of conversations out in public straightaway vanishes with the positioning of signs or notices warning that public space CCTV cameras fitted with microphones are present. Accordingly, the notices would cause the audio recording to be conducted overtly, as opposed to covertly. Continuing to speak out in public, while knowing or having been given notice that microphones are present, could be legally considered as implicit consent to be recorded. Audio recording is not considered eavesdropping when consent is given and/or the persons concerned have been informed.

Moreover, the Regulation of Investigatory Powers Act 2000 (RIPA) does not cover the overt, general use of public CCTV microphones, in accordance with paragraph 1.4 of the Covert Surveillance Code of Practice, unless specifically used for targeted/directed surveillance for specific investigations. The covert use of CCTV microphones in public spaces for targeted/directed surveillance by police or local authorities is also still lawful, albeit subject to certain safeguards of RIPA. Furthermore, as Donohue (2006) asserts, there is no legitimate expectation of privacy of illegitimate activities in public places, pointing out that the ECtHR previously judged that there is no legal authority in the UK for the judicial regulation of police placing a microphone on the outside of a building (Donohue, 2006).[421]

---

[420] *P.G. and J.H. v. the United Kingdom*, Application no. 44787/98, Judgment of 25 September 2001, para. 57.

[421] see *Khan v. United Kingdom*, Application no. 35394/97, Judgment of 12 May 2000.

Although under the latest CCTV code of practice (2008), CCTV surveillance systems are supposed to not be used for recording private conversations, the law arguably permits the random or general recording of the public at large, as long as it is done so in a public place and especially if the public is informed that CCTV microphones are present. The general observation or surveillance of public places is lawful, while conversations knowingly exposed in public are not protected. As Taylor points out, although the influence of Article 8 of the ECHR "has not yet been fully realised in the area of [overt] public space surveillance" (2002a, p. 73), "to find that CCTV surveillance in public spaces is a breach of privacy per se would be to broaden Article 8 in a way that, it appears, the European Court [ECtHR] is not prepared to do" (2002a, p. 76). Furthermore, as Victoria Williams argues, while Article 8 of the ECHR and ECtHR jurisprudence may recognize a legal basis for privacy in public spaces, the conventional notions of privacy do not translate well in public settings.[422]

The legal framework is equally ***ambiguous and vague***. For instance, the language of the CCTV code of practice (2008) is particularly problematic. It permits "limited circumstances in which audio recording may be justified, subject to sufficient safeguards", such as "audio based alert systems triggered by changes in noise patterns such as sudden shouting".[423] However, it does not explain what are these "limited circumstances" and "sufficient safeguards".

CCTV microphones can be triggered on the basis of decibel level or sound intensity and the speed at which words are spoken. With artificial intelligence (AI) technology,[424] the microphones can also be triggered by certain key words, such as expletive words considered aggressive.

Nevertheless, "sudden shouting" should not be enough to warrant the activation of the recording of CCTV microphones. This would permit the recording of a brief argument or heated debate between two or more people, which cannot justifiably be considered necessary for preventing or detecting crime. Moreover, the CCTV code of practice uses the words "*such as* sudden shouting" (emphasis added), which indicates that other criteria or circumstances are permitted to trigger CCTV microphones to begin recording.

---

422 see, for further discussion, the Memorandum by Victoria Williams for the House of Lords Constitution Committee inquiry into the impact of surveillance and data collection upon the privacy of citizens, available at: http://www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/8051402.htm
Victoria Williams is the author of the *Surveillance and Intelligence Law Handbook* (Oxford University Press, 2006).

423 CCTV code of practice 2008, p. 10.

424 Artificial-intelligence is defined as "the art of creating machines that perform functions that require intelligence when performed by people". Kurzweil, Ray. *The age of intelligent machines* (MIT Press, 1990), p. 14.

The triggering of CCTV microphones to begin recording once a certain sound intensity[425] is reached is both unwarranted and impractical. A normal spoken conversation, for example at 60 decibels (dB) or more, can have about the same sound intensity level as ordinary street noise. Traffic, therefore, could trigger recording and in doing so also record normal spoken conversations occurring nearby (see Table 1).[426] Nevertheless, who is to determine with certainty at what intensity in decibels is an exchange between two or more people really an argument or a normal conversation.[427] Such determination could easily vary from culture to culture. Using sound intensity as the basis of triggering CCTV microphones to begin recording will also permit the blanket recording of conversations at noisy locations, such as nightlife areas. While triggering the microphones based on sound intensity is impractical, justifying the recording of conversations out in public because someone uses expletive words or speaks quickly is simply absurd and is against common sense and reason.

Type of Sound	Sound intensity level (dB)
Normal spoken conversation	60
Ordinary street noise	70
Shouting	80
A pneumatic drill in use nearby	110

Table 1: Sound intensity of different types of sounds[428]

[425] Sound intensity is the amount of sound energy per unit area. The basic units are either watts/m^2 or watts/cm^2. Sound intensity level is measured in decibels (dB). Decibels measure the ratio of a given sound intensity I to the threshold of hearing. The threshold of hearing is assigned a sound level of 0 decibels, which corresponds to an intensity of 10-12 watts/m^2. A sound that is 10 times more intense (10-11 watts/m^2) is assigned a sound level of 10 dB, and so on. see "sound intensity", Encyclopedia Britannica 2009, Encyclopedia Britannica Online, 11 Nov. 2009, available at: http://www.britannica.com/EBchecked/topic/555343/sound-intensity; "sound", Encyclopedia Britannica 2009, Encyclopedia Britannica Online, 11 Nov. 2009, available at: http://www.britannica.com/EBchecked/topic/555255/sound

[426] Note that the distance between the source and the microphones plays a role.

[427] Using a Velleman DVM 805 sound level meter, I measured the 'normal' conversation of two colleagues in a quiet office setting for two minutes. The meter was placed at around two meters from the source. While no one was arguing or shouting, the sound levels still reached up to 70 dBA on several occasions. Note: dBA is the meter's use of an "A" filter, which is used to match more precisely what the human ear actually hears by "A-weighting" the decibel measurements.

[428] Sources: The Royal National Institute of Deaf People / Encyclopaedia Britannica Online 2009.

Moreover, the law does not place specific limits on the key words the AI software is permitted to be triggered by, which could freely enable the UK Government to use CCTV microphones to monitor conversations out in public, similar to the way conversations over the phone may be monitored.

In sum, there is a lack of harmonized implementation of the Data Protection Directive (Directive 95/46/EC) and consensus on what legally constitutes personal data. The UK legal framework is *ambiguous* and *inconsistent* with regards to both the images and sound captured or recorded via public space CCTV surveillance systems. There is essentially no clear understanding as to the extent to which privacy exists out in public, if it even does exist at all. Moreover, the UK legal framework is not clear on what are the limited circumstances the use of CCTV microphones by law enforcement agencies are justified and the CCTV code of practice (2008) only leaves open more significant legal questions.

6.8.2 CCTV loudspeakers

While the illegitimate and disproportional use of CCTV loudspeakers should be considered an interference with the right to be left alone, it is nonetheless difficult to determine what laws are actually violated. The principles of data protection, for the most part, are not meant in actuality to apply to CCTV loudspeakers, since the loudspeakers themselves do not collect, store or process data. Furthermore, it also difficult to apply Article 8 of the ECHR to CCTV loudspeakers owned and operated by public authorities.

However, the second data protection principle, which is parallel to the *purpose specification principle*, the fifth data protection principle, which is parallel to the *use limitation principle*, and the *principle of proportionality* are still applicable.

The CCTV code of practice (2008) does not at all sufficiently address CCTV loudspeakers, nor fulfill the ***use limitation or purpose specification principles*** and satisfy the required legal characteristics of ***foreseeability*** and ***clarity***. Although the CCTV code of practice (2008) restricts the use of CCTV loudspeakers "to messages directly related to the purpose for which the system was established",[429] it does not define under what circumstances are those purposes legitimate or proportionate, nor the scope of a CCTV control room operator's discretion to use the CCTV loudspeakers, what should and should not be communicated or how and why those messages should be communicated.

[429] CCTV code of practice 2008, p. 7.

There is (or at least was) mounting concern that CCTV surveillance technology is being used for trivial reasons, such as to prevent littering under the "Keep Britain Tidy" campaign, and for other trivial offences, such as public drunkenness, etc. The focus on trivial offences results in more individuals being arrested for such low-level categories of offenses rather than serious crimes (Surette, 2005, p. 155). There is equally growing concern that local governments are excessively taking advantage of the broad powers of the RIPA to carry out surveillance for reasons other than to prevent or detect crime or ensure national/public security. RIPA is rather being used to carry out surveillance for reasons far less important, such as catching people putting out their rubbish too early, failing to clean up their dog's waste or dropping litter, and to investigate noise pollution. According to a freedom of information request made by the *Daily Mail*, more than half of town halls in the last three years have used the powers of RIPA to spy on families suspected of putting their rubbish out on the wrong day. In addition to covertly following the suspected targets, the surveillance tactics have also included putting secret cameras in tin cans and on lampposts.[430] RIPA permits the conduct of surveillance by a variety of public authorities, including town halls and not just the police and intelligence agencies, for reasons of preventing or detecting crime or ensuring national security and to 'protect public health' and the 'economic well-being'.[431] The latter two reasons serve as the potential basis for conducting surveillance for environmental concerns. The problem is, however, that the ambiguous wording of RIPA can justify surveillance operations for a variety of reasons.[432] Surely, there is little concern that the legislation can be used to prevent and punish, for instance, commercial fly tipping. But, abusing the powers of RIPA for trivial reasons is a serious concern. The wider use of CCTV loudspeakers could potentially be further bolstered by the common practice of using CCTV cameras and applying RIPA for trivial reasons.

---

430 Borland, Sophie and James Slack. "March of the dustbin Stasi: Half of councils use anti-terror laws to watch people putting rubbish out on the wrong day" (Daily Mail, 1 November 2008), available at: http://www.dailymail.co.uk/news/article-1082225/March-dustbin-Stasi-Half-councils-use-anti-terror-laws-watch-people-putting-rubbish-wrong-day.html

431 Regulation of Investigatory Powers Act 2000, Part II, Section 28 (3).

432 As a result, proposals to amend RIPA, in order to restrict the ability of local authorities to use CCTV surveillance systems for trivial purposes and to provide for judicial approval in relation to certain authorisations and notices under RIPA, were introduced to Parliament on 11 February 2011 in a bill, titled the "Protection of Freedoms Bill 2010-11".

6.9 RECOMMENDATIONS ON ENHANCING THE UK LEGAL FRAMEWORK

Although, as Taylor (2002, 2002a) argues, UK domestic courts might be in a position to develop the concept of privacy in public spaces, can we really wait for the courts to slowly do so? Public surveillance CCTV systems and enhancements to the technology integrated to these systems demand specific laws from the UK Parliament immediately.

The European Commission for Democracy through Law (Venice Commission) of the Council of Europe published an opinion on video surveillance in public places by public authorities, concluding that

> specific regulations should be enacted at both international and national level in order to cover the specific issue of video surveillance by public authorities of public areas as a limitation of the right to privacy.[433]

Similarly, the Constitution Committee of the UK House of Lords recommended that the UK Government should adopt a statutory regime for the use of CCTV by *both* the public and private sectors, including codes of practice that are legally binding and overseen by the Office of Surveillance Commissioners (OSC) together with the ICO.[434]

Nevertheless, the UK legal framework does not necessarily require a complete overhaul and the DPA presents a basis for public space CCTV operators to work from (see Taylor, 2002a, p. 82-83). While that may be the case, specific rules/regulations are still required to bring clarity to the purpose and scope of CCTV microphones and CCTV loudspeakers. Indeed, as Taylor points out, "[t]here are situations when the state has to intervene in the lives of its citizens, such as to prevent crime, but such intervention must be based on, and restricted by, principled legislation" (*Ibid*., p. 83). A framework or basis by which to distinguish the legitimate and proportional or illegitimate and disproportional use of CCTV microphones and CCTV loudspeakers is required. For the moment, however, regulations on the use and deployment of CCTV microphones and CCTV loudspeakers may not require EU action or intervention, since the deployment of these CCTV enhancements are occurring exclusively in the UK, with the exception of CCTV microphones being tested and deployed in the Netherlands. But,

---

433 Draft Opinion on Video Surveillance and the Protection of Human Rights, adopted by the Venice Commission at its 70th Plenary Session, Venice, Italy, 16-17 March 2007, para. 81, available at: http://www.venice.coe.int/docs/2007/CDL-AD(2007)014-e.asp

434 Constitution Committee - Second Report, Surveillance: Citizens and the State (Session 2008-09), Chapter 4, para. 219, available at: http://www.parliament.the-stationery-office.com/pa/ld200809/ldselect/ldconst/18/1802.htm

the European Commission and Article 29 Working Party should remain vigilant on any expanded deployment of CCTV microphones and CCTV loudspeakers within Europe.

It is important to point out, on the other hand, that the means to protecting privacy are not just legal-orientated or policy-orientated. Regulating the design and development of CCTV microphones and CCTV loudspeakers can inherently minimize their intrusive capability from the start. Moreover, since there seems to be no clear understanding of the extent to which privacy exists in public, if it even does, or clear way of determining so, there is even more reason to focus on the design, development and deployment of CCTV microphones and CCTV loudspeakers, as opposed to solely on their use. Accordingly, many of the obligations should fall upon the manufacturers of CCTV microphones and loudspeakers, rather than merely on their operators.

In addition, since the effects of both CCTV microphones and CCTV loudspeakers go beyond privacy, their use could pose a serious threat, if left unchecked, to personal freedom and autonomy, freedom of speech and our sense of dignity. The law and technological solutions should therefore also possess the demonstrable ability to preserve both privacy and liberty overall.

6.9.1 CCTV microphones

Indeed, the integration of microphones to CCTV cameras can offer security gains and thus should not be completely outlawed. However, before they are widely deployed, specific regulations must be put into place.

Since it is unclear how and under what circumstances it is lawful or legitimate for law enforcement agencies to use CCTV microphones or whether or not Article 8 of the ECHR (and the DPA) are applicable to the audio data collected, regulations on public space CCTV microphones should explicitly focus on their design, development and deployment for public use, rather than solely on their use, by placing significant limits on the technology itself.

Unlike the SIgard system, or other public CCTV audio surveillance systems, public CCTV microphones, based on the ***principle of proportionality***, must not be capable of recording conversations nor programmed to be triggered by shouting or verbal aggression (or how something is said), since this is not sufficiently justified for the purposes of ensuring public security. Moreover, the temptation for abuse or the propensity towards 'function creep' or 'surveillance creep' is just too great, as we have already seen

with the use of CCTV visual surveillance capabilities for voyeurism (Surette, 2005) or 'cheap thrills' in the UK.[435]

The framework or basis by which to distinguish between the legitimate and proportional or illegitimate and disproportional use of CCTV microphones for security purposes should be based on the common understandings of which sounds or noises actually constitute a public danger or security threat and justify their detection and the audio recording of the incident. Therefore, the activation of the recording capabilities of CCTV microphones should be limited to those particular sounds only, thereby guaranteeing the legitimate and proportional use of CCTV microphones. In order to remove all areas of ambiguity, the law should explicitly restrict the activation of the public CCTV microphones to the following set of sounds: gunfire; explosions; breaking glass; car alarms; car crashes; burglar alarms; and screams that contain the specific words "help" or "fire". If and where necessary, the microphones could also detect or recognize these words shouted in other languages. Based on the framework, other sounds and shouted out words might also merit the activation of CCTV microphones. While this list of sounds may not be exhaustive, the delineation of which sounds may activate the CCTV microphones to begin recording must be precise. However, the adding of any additional sounds is up for debate, and security experts, law enforcement agencies and the public at large should be consulted beforehand.

The detection of these diverse, yet very distinct sounds and the two specific words "help" and "fire", shouted at no less than 65 decibels or more, can be achieved with the use of AI software or the incorporation of software agents with reactive abilities.[436] Researchers from the University of Portsmouth are already working to develop AI software that can recognize sounds and words.[437] The incorporation of AI or software agents, however, may also require separate legislation (Schermer, 2007). Moreover, the

---

435 see "Peeping tom CCTV workers jailed" (BBC News, 13 January 2006), available at: http://news.bbc.co.uk/1/hi/england/merseyside/4609746.stm

436 A software agent is any software that exhibits any character commonly associated with agency, such as reactive, proactive, goal orientated, deliberative, communicative and adaptive. Software agents with reactive abilities or characteristics "employ any type and number of sensors to sense its environment. The software can react to sensory input using its actuators" (Schermer, 2007, p. 22).

437 Thurston, Richard. "CCTV cameras that listen as well as watch" (SC Magazine, 25 June 2008), available at: http://www.scmagazineuk.com/CCTV-cameras-that-listen-as-well-as watch/article/111675/

decisions of a software agent may classify as an "automated individual decision" and, therefore, should set off the safeguards of CFD 2008/977/JHA.[438]

When gunfire, etc. is detected, the microphones can immediately begin to record, calculate the location of the sound source, direct the cameras in that direction and alert the CCTV control room operators, who in turn can alert a police dispatcher to send the closest police officer(s) or unit. Based on the ***purpose specification*** **principle**, however, the audio recording must cease within a definite short period of time after each new event or incident is detected. In addition, based on the ***use limitation principle***, the audio data must only be accessed and used for evidential purposes and, where possible or necessary, any unrelated background sound should be edited out, which could also be helpful for the related criminal investigation and prosecution. Shouting "help" or "fire", in order to intentionally trigger the CCTV cameras without justification, should accordingly be prohibited.

Thus, in line with the ***principle of notice/awareness***, the placement of additional or different notice signs from the ones already available may not necessarily be required, since the CCTV microphones will not record any personal data.

A CCTV system that can only detect the above specific sounds and shouted words, as mandated by law, is the way forward to both enhance public security and guarantee that privacy safeguards are in place and unwavering. Moreover, such a system may require fewer cameras to cover larger areas and thus less recorded visual data of the public space (Kim et al., 2007, p. 389).

6.9.2 CCTV loudspeakers

Even if CCTV loudspeakers do prove to be effective for public safety reasons, they still require the proper checks and balances.

Once again, it is difficult to clearly determine the relevant laws that pertain to CCTV loudspeakers and what laws CCTV loudspeakers violate. Regulations on CCTV loudspeakers should therefore equally focus on their development, manufacture and deployment rather than solely address their use.

---

438 Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (30.12.2008), Article 7.
Article 9 of the EC's proposal for a Directive on the protection of individuals with regard to the processing of personal data for law enforcement purposes (COM(2012) 10 final, Brussels, 25.1.2012) prohibits measures based solely on the automated processing of personal data, if not authorised by law and subject to appropriate safeguards (in line with Article 7 of CFD 2008/977/JHA).

Based on the understanding of privacy as the right to be left alone, CCTV loudspeakers should not be capable of being used for disturbing or scolding individuals. The possibility of operators to abuse CCTV loudspeakers by harassing people from afar must be minimized.

Indeed, as Taylor points out, the CCTV operator "phone pest" occurrence,[439] whereby an operator used public pay phones to pester people he could see via CCTV cameras, could not have been prevented by laws that only regulate the collection, use and storage of CCTV images (2002, p. 107). However, regulations concerning the design and development of public space CCTV loudspeakers, in combination with specific rules on their use and specified penalties for misuse, could significantly minimize the chances of this occurring with CCTV loudspeakers.

The use of specific pre-recorded messages and the removal of the ability of CCTV operators to speak directly to the public can automatically limit what operators can communicate via CCTV loudspeakers. The different pre-recorded messages could be activated by entering a designated three-digit number that corresponds with each message onto computer keypads. For example, 146 for "CCTV cameras are monitoring you, please discontinue the graffiti" or 112 for "stay where you are, the police are on their way". CCTV loudspeakers should only be capable of delivering these pre-recorded messages at a certain volume and should not use the voice of children to leverage their so-called "pester power" nor the voice of celebrities to leverage their influence, but rather a generic male or female voice.

Some might argue that the use of pre-recorded messages will make it difficult to deliver more specific or detailed messages, since they are fixed. However, surely one of the hundred or so different pre-recorded messages that can be stored will be capable of getting the appropriate point across to the concerned individual(s). Others might also argue that discovering the correct three-digit number to enter in order to deliver the appropriate pre-recorded message will take longer or prove more difficult than speaking directly. But, an electronic list of the available pre-recorded messages can be easily displayed on a monitor. Moreover, trained and experienced operators will begin to memorize a number of different three-digit numbers and their corresponding pre-recorded messages, which might in fact enable operators to communicate with targeted individuals quicker, easier and more effective than having to do so by spoken words. Pre-recorded messages, rather than speaking directly to perpetrators, might also enhance compliance and reduce the provoking of rebellious acts in response.

---

[439] see "Phone Pest picked targets on security video" (The Telegraph, 7 June 1996), available at: www.telegraph.co.uk/htmlContent.jhtml?html=/archive/1996/11/27/ntel27.html

Even pre-recorded messages can be illegitimately, inappropriately and/or disproportionately used, resulting in the unnecessary cause of harm to a person's dignity or individual liberties and the unnecessary disturbance of the public peace. The framework by which to distinguish if the use of CCTV loudspeakers is legitimate and proportional should be based on whether or not their use serves the purpose of preventing, deterring or discontinuing an anti-social act that threatens public security and/or well-being.

The pre-recorded messages used to prevent, deter or discontinue an anti-social act must be used in accordance with the Anti-Social Behaviour Act 2003 and not for trivial reasons that do not threaten public security and/or well-being. For instance, littering, such as dropping a chewing gum wrapper or putting out a cigarette on the sidewalk, does not justify the use of CCTV loudspeakers. Only more serious forms of littering and hazards to the environment, such as fly tipping, justify the use of CCTV loudspeakers. More to the point, the law should also further clarify that the powers of RIPA should not be used for trivial reasons.[440] Besides, the use of CCTV loudspeakers for trivial reasons would likely lead to rebellious acts and depreciating levels of compliance.

Still, the automatic limitation on what can be communicated using CCTV loudspeakers via pre-recorded messages already provides the means to better preserve the legitimate use of CCTV loudspeakers and prevent harm to a person's dignity and personal autonomy.

In the end, it is the public CCTV operators who have to make the decision whether or not to use the loudspeakers. Keeping track of the number of times the CCTV loudspeakers are used will help to ensure they are being used legitimately and proportionally, and not for 'cheap thrills' or on grounds of discrimination. Since the pre-recorded messages are activated by entering numbers into computer keypads, tracking the use of CCTV loudspeakers can be done automatically. This will also permit an accurate and easier evaluation on their impact in each specific area.

Taylor argues that "[i]f Article 8 [of the ECHR] were to apply to public visual surveillance systems it would at least ensure a debate about whether or not CCTV surveillance could be justified in an individual situation, or whether other methods of crime prevention might be equally, or more, successful with less intrusion" (2002a, p. 81). Taylor goes on to write that "[i]f Article 8 were engaged the issue of proportionality would require that the least obtrusive means necessary should be undertaken, thus

---

[440] Proposals to amend RIPA, in order to restrict the ability of local authorities to use CCTV surveillance systems for trivial purposes and to provide for judicial approval in relation to certain authorisations and notices under RIPA, were introduced to Parliament on 11 February 2011 in a bill, titled the "Protection of Freedoms Bill 2010-11". The bill also calls for the appointment of a Surveillance Camera Commissioner and introduces a code of practice for surveillance camera systems. As of October 2011, the bill has only just entered into the report stage in the House of Commons.

not barring surveillance, but ensuring it is appropriate and justifiable" (*Ibid*., p. 81-82). Accordingly, this would call for the deployment of CCTV loudspeakers to be restricted to certain areas of public space, which have credibly been identified as 'hotspots' or high-risk areas of anti-social behaviour and where an evaluation has determined that the CCTV loudspeakers would be the appropriate and effective solution to the problem. This will better ensure that CCTV loudspeakers are proportionally deployed and that their deployment and use is based on legitimate aims, in accordance with the law and the ***principle of purpose specification*** and ***principle of proportionality***. In addition, before a decision is taken by local authorities to deploy CCTV loudspeakers anywhere, there should be an open dialogue with the surrounding neighborhood or the public directly affected.

The well thought-out deployment of CCTV loudspeakers will also help ensure the noise generated by the loudspeakers does not unnecessarily disturb those nearby. CCTV loudspeakers should equally be banned from being deployed nearby medical facilities so as to not disturb patients. Perhaps, the use of CCTV loudspeakers should also be prohibited during certain times of the day, unless in exceptional circumstances that merit their use, such as to prevent serious crimes, rather than low-level anti-social behaviour.

With "single wire digital transmission" technology, for example, thousands of CCTV loudspeakers could potentially be operated individually or in groups from a single location hundreds of kilometers from where they are located. However, in order to check the concentration of power, the law should prohibit the centralization of the ability to operate that many CCTV loudspeakers from a single control room.

With more advanced technology, such as HyperSonic Sound (HSS),[441] it may also be possible to deliver the pre-recorded messages in a way only audible to the targeted individual. The basis of excluding CCTV loudspeakers from certain public areas in order to ensure the sound does not unnecessarily disturb others may, as a result, no longer be compelling. Still, the use of HSS in CCTV loudspeakers should be banned in order to ensure 'mental privacy', which also requires separate legislation in itself.

CCTV loudspeakers can be used as a form of verbal warning or reprimand for juveniles or means to convey informal punishments. Therefore, if CCTV loudspeakers are to be the "voice of authority",[442] then only publicly authorized public authorities should

---

441 HyperSonic Sound technology, developed by American Technology Corporation, provides the ability to direct sound to a specific area or target, similar to light, using ultrasonic sound energy. American Technology Corporation, available at: http://www.atcsd.com/site/content/view/34/47/

442 "Talking CCTV brings voice of authority to streets", Home Office, 4 April 2007, available at: http://www.homeoffice.gov.uk/about-us/news/talking-cctv

be allowed to use them. Furthermore, the integration of loudspeakers must be restricted to publicly owned and managed surveillance CCTV systems.

The law needs to specify the consequences of ignoring verbal warnings communicated via CCTV loudspeakers for anti-social behaviour. After the first verbal warning, if the perpetrator does not comply, then a second verbal warning should follow. If the perpetrator still does not comply, then a police officer should be dispatched, when necessary, to resolve the issue or penalize that person, in accordance with the law.[443] Under certain circumstances, fines and/or ASBOs could be issued after failing to comply with the second warning. If the person runs from the scene, the perpetrator could potentially be identified, with the enhancement of CCTV image quality, addition of face recognition technology[444] and linkage to the NIR. The verbal warning or reprimand can then be registered in the record of the person concerned.

Failure to comply with verbal warnings from CCTV loudspeakers to refrain from anti-social behaviour does not immediately merit the use of non-lethal force deterrence technology, also known as less-than-lethal force or compliance weapons. However, the integration of non-lethal deterrence technology to public space CCTV cameras, such as the scheme developed by ICx Imaging Systems, which consists of a high-powered strobe light to temporarily disorientate perpetrators,[445] or LRADs could be legitimate if used to bring to an end violent or dangerous acts alone and subject to specific rules.[446] The use of less-than-lethal force simply for crowd control should be considered illegitimate.

Still, CCTV control room operators should receive additional special training, in coordination with the Home Office, in order to be allowed to operate the loudspeakers. Training should ensure that the operators are better equipped to base their decision on using CCTV loudspeakers in a standardized and objective manner and in accordance with the relevant privacy principles and framework of proportionality and necessity, as far as humanly possible, and with a sound knowledge and understanding of the special circumstances in their area.

---

443 Crime and Disorder Act 1998; Anti-Social Behaviour Act 2003.

444 "Better CCTV needed for ID" (BBC News, 11 May 2006), available at: http://news.bbc.co.uk/2/hi/uk_news/politics/4761519.stm

445 ICx Technologies, Inc., http://www.icxt.com/products/icx-surveillance/thermal-imaging/illuminator/

446 LRADs are already being deployed in the US by police for crowd control purposes and this recent development has rightfully caused an outrage. see "Sheriff's Department Responds To Sonic Device Outrage" (10news.com, 15 September 2009), available at: http://www.10news.com/news/20931535/detail.html
LRADs were most recently deployed and used by police for protests during G20 Pittsburgh Summit.

CCTV loudspeakers can also be used alongside 'intelligent' CCTV cameras. With the use of software agents, the pre-recorded messages could instead be activated exclusive of human involvement. Software agents with the ability to deliberate extensively before reacting (Schermer, 2007, p. 22) could determine when an anti-social act is being committed and then broadcast the relevant pre-recorded message or even automatically alert the police. Software agents could also solve the difficultly of monitoring all the CCTV cameras and provide a better assurance that the loudspeakers are used objectively and flawlessly.

However, once again, software agents potentially require separate legislation (Schermer, 2007) and the technology is likely not yet sophisticated enough. Moreover, the decisions of a software agent may classify as an "automated individual decision" and, therefore, should set off the safeguards of Council Framework Decision 2008/977/JHA.[447]

In a "symmetrical surveillance" scheme for CCTV systems (Goold, 2006), the data on the use and deployment of CCTV loudspeakers, including the messages used, where, when and by whom, would be easily and readily available to the public on the Internet. This could further deter the abuse of the intrusive power of CCTV loudspeakers by operators, address the concern over "who watches the watchers" (Cockfield, 2003), and reduce the problem of the "unobservable observer" (Goold, 2006) or, more precisely, in the case of CCTV loudspeakers, the 'unobservable speaker'.

The control room supervisor should also be responsible for monitoring the use of CCTV loudspeakers by the operators. If any operator uses the loudspeakers in an unwarranted manner, such as for 'cheap thrills' or in a racial discriminatory manner,[448] he or she may be subject to disciplinary action, including, but not limited to, dismissal. Based on the ***principle of enforcement***, an oversight/supervisory committee should be established to oversee the proportional and warranted deployment and use of the CCTV loudspeakers on a nationwide scale, ensuring individual liberty, public peace and the right to be left alone out in public is better preserved.

---

447 Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (30.12.2008), article 7.

448 As Norris and Armstrong point out, evidence increasingly shows that CCTV operators are already using the surveillance capabilities of CCTV cameras in a racial discriminatory manner (1999, pp. 110-111).

6.10 CONCLUDING REMARKS

The deployment and use of CCTV microphones and loudspeakers, in conjunction with other technologies, could potentially enhance the ability of CCTV cameras to prevent and fight crime and serious anti-social behaviour. Therefore, CCTV microphones and loudspeakers ought not to be completely banned.

However, without an unambiguous understanding of the scope of privacy in public and/or the necessary regulations on the development, deployment and use of CCTV microphones and loudspeakers, there is no assurance that our legitimate rights and freedoms will not be unreasonably and disproportionally intruded upon. Until these regulations are in place and put into effect, there are alternative privacy-friendly devices and means of preventing and fighting crime and anti-social behaviour already in existence.

Indeed, being out in public entails a much lesser degree of privacy, and those who engage in unlawful, wicked or serious anti-social behaviour, whether thieves, murderers, vandals or terrorists, substantially lose their right to be left alone. However, the legitimate governmental interest in curtailing crime and anti-social behaviour should not mean that our conversations out in public may simply be recorded or citizens may be publicly humiliated into behaving 'correctly'.