

IN FOCUS

IF

ISSUE 04



Reaching for CCTV COMPLIANCE

News from Forum at HSBC – Po4

**THIS
ISSUE:**

Sponsored by



Forthcoming projects | Join CameraWatch
Board appointment | Managing risk | Compliance



CHIEF EXECUTIVE UPDATE



p04 TALKING SHOP
Update from the March Forum
at HSBC Global HQ, London

p06 LEGAL
Tips to make sure you stay
the right side of the law

p08 COMPLIANCE
How your data is being used
and who can see it

CameraWatch gratefully
acknowledges sponsorship from



CameraWatch gratefully
acknowledges business support from



Compliance Solutions
www.cctvcompliance.com

CameraWatch communications
are managed by



CameraWatch Limited
3 Walker Street
Edinburgh
EH3 7JY
Tel: 020 8514 9306
Email: info@camerawatch.org.uk

CEO Gordon Ferrie as CameraWatch celebrates its third birthday...

As CameraWatch moves into its third year of operation, progress has been made to harness all industry CCTV operatives to improve standards and quality in the CCTV industry – but not enough to stop CCTV being brought into disrepute on a daily basis.

There is never a day goes by that you read in the media of the misuse of CCTV systems.

Our initial research showed that up to 90 per cent of CCTV installations fail to comply with the Information Commissioner's UK CCTV Code of Practice and many installations are operated illegally.

Three years on, we are still faced with inefficient and non-compliant CCTV systems.

Although much work has been done, there are still many organisations out there who fail on many fronts towards achieving a fully-compliant CCTV system. That has profound implications for the reputation of the CCTV and camera surveillance industry and all concerned with it. The public are bearing the brunt of this and without doubt it will lead to ineffective prosecutions and infringements of human rights.

Non-compliant Data Protection Act (DPA) CCTV systems will bring the CCTV industry into disrepute if businesses continue to fail to get their surveillance responsibilities right.

Failure might also mean repercussions

The UK - a surveillance society? - most CCTV fails the DPA compliance test



for the specific organisation, damage to their reputation, and lead to a lack of public confidence in surveillance.

Compliance is a complex area not just covering appropriate siting and signage issues, but also various pieces of legislation. In particular, the DPA covers images of people and requires they are held securely if the data is to be used as legal and admissible evidence.

And the Information Commissioner's Office has confirmed that from 1 April 2010, they will be empowered to hand out fines to organisations that are in breach of the DPA.

Until now, the ICO has not been able to issue fines for breaches of the eight data protection principles at the heart of the law. From next April that will change and it will issue fines for knowing or reckless breaches of the DPA's principles.

CCTV is a terrific tool if used correctly and in accordance with the law. Too many organisations don't understand – or simply ignore – their legal obligations.

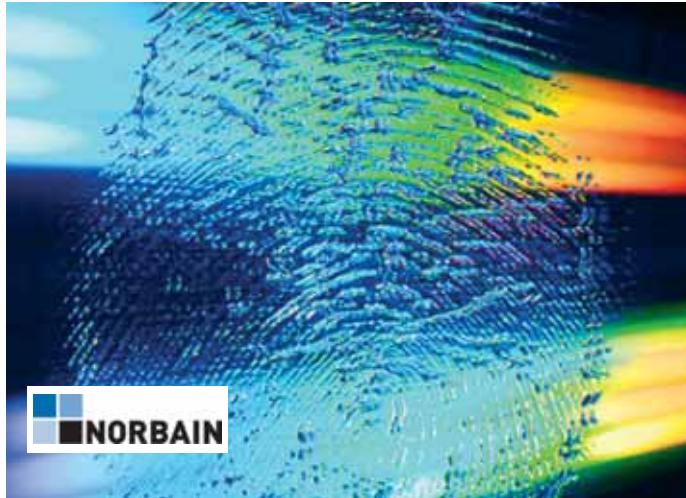
CameraWatch has the key to avoiding difficulty: understand the DPA and you won't go far wrong. Then we can all have confidence in CCTV systems. ■

INDUSTRY SUPPORT VITAL FOR SUCCESS

Norbain have announced their continuing sponsorship of CameraWatch.

“We are extremely grateful to Norbain for their sponsorship,” said Gordon Ferrie, Chief Executive and joint founder of CameraWatch. “Their continued support not only sends out a great message about the importance of data compliance to the industry, but also allows us to continue promoting awareness of camera surveillance to all relevant parties.”

Norbain Chief Executive Alun John said: “We’ve always seen CameraWatch as a very worthwhile initiative, and a focus on best practice is very much in line with Norbain’s own values.



“The importance of legal compliance and data protection continue to become more

pronounced and we’re pleased to be able to do our bit in supporting their work.” ■



For further information, please visit www.camerawatch.org.uk

Scottish Business Crime Centre

CameraWatch is pleased to announce membership of the Scottish Business Crime Centre (SBCC).

SBCC Executive Director Alan Dobie told InFocus of the aims of the organisation:

“The SBCC is committed to working in partnership with local communities, agencies and business partners throughout the country to help create safe, successful, vibrant and thriving city and town centres.

“On the back of the Scottish and UK Government’s funding of a programme of CCTV installations, there is hardly a city or town centre throughout the country which has not readily embraced the adoption of CCTV, or at the very least is planning to do so in the not too distant future.

“Working in the 24-hour economy, there is an ever-increasing acceptance that preventing crime and discouraging criminals is a far more effective tactic than responding to a crime once it has been committed.

“CCTV is one of the mediums that can be used to prevent crime and it can be very successful – particularly when it is part of a

focused and sustained programme incorporating effective crime-fighting strategies in city or town centres and shopping centres.

“We are delighted to welcome CameraWatch as a member of SBCC.”

We’re on the CASE for CCTV



CASE Security are the latest corporate members to join CameraWatch. CEO Dave Newbury (pictured) said: “We are delighted to add

our weight to help raise quality and standards associated with CCTV Data Protection Act compliance. CASE are committed to delivering state-of-the-art security solutions and sees Camerawatch as a flag bearer for the industry on CCTV compliance.”

New Chair at compliance watchdog

Pat Curran has been appointed as the new CameraWatch Chairman. Pat takes over from Gordon Ferrie, who becomes Chief Executive to focus on business development.

Pat’s formidable reputation in the UK security sector derives from co-founding and leading the Bell Security group, from 1986 until it was sold in 2004, to UK and Ireland market-leader status in security systems provision for retail banking groups.

Pat’s current business involvements include the chairmanships of Bell ID, the secure smart card applications provider, and facilities management software specialist FSI.

Welcoming the new non-executive Chairman, Gordon Ferrie said: “It’s with considerable enthusiasm that I welcome Pat to the Board. His established reputation will drive forward CameraWatch’s work in promoting awareness and compliance in CCTV camera surveillance – in both the private and public sector – UK-wide and beyond.”



Pat Curran

CCTV: it's all in the management

Forum talk: Brian Sims, editor of SMT Online

Who could fail to have been moved by the recent story of a young couple who discovered that their daughter's grave had been desecrated – the headstone and other memorabilia removed overnight.

"The Council should put up CCTV" suggested a relative, and many heads in the crowd nodded in agreement.

While incidents like this are appalling to any right-minded individual, I believe the notion that a CCTV camera can be the panacea for all known criminal ills is somewhat misguided.

The local council stated: "We don't feel that CCTV would have been of any value in this particular situation".

How refreshing to find a local government official willing to stand their ground over the use of CCTV, particularly at a time when councils are deploying cameras like confetti in an effort to meet their obligations under the Crime and Disorder Act.

It's said there are now



anything between 4.5 and 6 million CCTV cameras in this country and, if you believe the "conspiracy theorists", they're allegedly recording our every move.

During a recent business trip from my home near London into the capital, I counted no fewer than 68 cameras that may have – allegedly – captured my image. I say "allegedly" because just how many of these cameras are actually working, let alone recording any meaningful data?

As the Editor of Security Management Today and now SMT Online, I've lost count of the number of case studies we've completed wherein retail outlets, for instance, were robbed, burgled or the victims of fraud.

I've also lost count of the number of times when, following an incident, the CCTV system was accessed for the recovery of images of evidential value, only to discover that there weren't any.

Until something is done, we shall continue to harbour surveillance systems that don't function as they should – a status quo that would continually serve to undermine the rationale that underpins CCTV.

Maybe we should spend less time and money on the kit, and focus more on training the operatives.

Brian Sims is the Editor of SMT Online and Group Content Editor of United Business Media's Security Portfolio.

The March CameraWatch gathering attracts

FORUM

Legal compliance of CCTV systems and managing the risks associated with insurance, were top of the agenda at the CameraWatch March Forum at HSBC Global HQ, Canary Wharf, London.

Among those present were Judith Jones from the Information Commissioner's Office and John Williams, Head – Group Physical Risk, HSBC Holdings PLC.

Garry Parkins and Geoff Teale of The National Police Improvements Agency (who are currently delivering the recommendations of the Home office ACPO National CCTV Strategy) opened the

debate on the need for a national CCTV register, with these questions:

1. Would a Voluntary Registration scheme be workable?

2. What information would require to be registered?

3. How would a register be updated?

4. How much data would be publicly available?

5. What type of enforcement powers would a National CCTV Board need?

CameraWatch is already working with ACPOS in Scotland and the Scottish Government to pursue this idea.

Garry Parkins and Geoff Teale were asked to report back to the October Forum with their findings. ■



The CW Forum is a unique occasion that brings together influential and authoritative figures

Progress update and future activity

Outcomes

The CameraWatch (CW) Forum also provided members with an update on recent activity and forthcoming projects, including:

- Compliance and Technical update:**
- Phase 1 Field Study results analysed and published
 - Phase 2 Field Study

lected figures from across the industry for CCTV debate, discussion and dialogue

M FOR IDEAS



An influential range of speakers attracted an audience of industry figures, senior police officers, legal experts and government representatives

now on the CW website

- Building close relationships with ICO and Home Office
- Identifying European Issues
- How to identify and action badly managed systems
- Standardisation of format of the recording and playback of images
- Continual and new ways for promoting the requirements and benefits

of annual audits and regular maintenance

- Ensuring that the reputation of CCTV and the public expectations are not diminished.

Current CameraWatch projects:

- Project 1: Introduction of Lifecycle Guide to CCTV Compliance – in progress
- Project 2: Developing a National CCTV Register: Feasibility Study – Scotland

Positive support received for a pilot in Scotland during meetings with the ICO, ACPOS and the Scottish Government

- Project 3: On-Site Field Studies – ongoing project with four universities in partnership with Association of University Chief Security Officers (AUCSO). Results are currently being analysed
- Project 4: Accreditation Programme – feedback

from various areas of the CCTV industry suggests CameraWatch as an ideal vehicle for the introduction of an independent accreditation scheme for CCTV DPA compliance, including annual audits

- Project 5: Insurers and Compliance – project to highlight the importance of insurance industry in increasing standards in CCTV/DPA compliance.

Managing the risk

Surveillance compliance

If your organisation operates CCTV/VBDS, what can you do to manage the compliance risk? These five general rules may help:

1. Comply from collection to destruction: Personal data generated by video must be handled in accordance with the Data Protection Act (DPA) from the point of capture through to destruction.

Data must be handled 'fairly and lawfully', in line with rights of the individual whose images are taken. Adopt technical and organisational measures to ensure data security.

Fines for reckless data

Adopt a clear incident management procedure and regularly audit your compliance

management will soon be law, so the potential costs of lax security are increasing.

2. Look beyond the DPA: Look at the bigger regulatory picture when compliance planning.

For instance, the Human Rights law applies directly to public authorities' use of images and can extend to private sector businesses.

If you engage someone to operate CCTV on your behalf, ensure that security industry regulations are followed.

Public authorities and their contractors should assess the potential impact of local government rules and freedom of information law.



Kenneth Mullen,
CameraWatch Legal Director

3. Follow relevant guidance: The Information Commissioner's Office (ICO) Code of Practice. A separate ICO Employment Code also covers video surveillance of staff.

Observing technical recommendations such as ACPO/ACPOS codes may be important, for example, when it comes to insurance. Complying with industry standards like BSI 7958:2005 (CCTV Management) may help you rely on CCTV images as evidence in the courts.

4. Review external compliance: Maintain registration as a 'data controller' with the ICO. Where third parties operate systems on your behalf, the law demands that you implement a written 'data processor' contract. Establish clear procedures for handling external requests to access CCTV data.

5. Maintain internal controls: Make sure that CCTV is properly administered internally. Employees, need to be trained and understand data protection issues. Adopt a clear incident management procedure and regularly audit your CCTV compliance.

Kenneth Mullen, is the Legal Director of CameraWatch and a partner with leading law firm Shepherd and Wedderburn, where he specialises in media and technology law.

CCTV IN P

Licensed premises must be careful with the customer data they hold



Earlier this year, there was considerable media attention when the

Metropolitan Police tried to force the prospective landlord of the Drapers Arms in Islington to install CCTV in the premises as a condition of obtaining a drinks licence.

Although a CCTV condition is included amongst the "Model Pool of Conditions" (published to guide licence applicants in the preparation of the operating schedules required as part of the application), these conditions are for guidance only and there is no absolute requirement that CCTV be installed.

Indeed, it is the stated policy of Islington Council that individual licence applications should be considered in the light of representations made to the Licensing Committee and decisions made on a case-by-case basis.

Notwithstanding that, Islington police

recommended that before any licence is granted, applicants should be required to install CCTV and to agree to make available the recorded images to police upon request. Such a system would have to be capable of enabling the frontal identification of every person entering the premises, recordings would have to be kept for a minimum of 31 days and they had to be made available to an authorised officer or a police officer within 24 hours of any request – subject, of course, to the Data Protection Act 1998 (DPA).

Imposing such a blanket requirement irrespective of concerns about particular premises was felt by the Information Commissioner (ICO) to raise significant questions about data protection compliance and, subsequently, the police withdrew their objection and the licence was granted.

Compare that to the situation in Scotland. Although the general principles and processes surrounding an application

Imposing such a blanket requirement irrespective of concerns about particular premises was felt by the ICO to raise significant questions

PUBS & CLUBS



are broadly similar, there are distinct differences in law. The Licensing (Scotland) Act 2005 provides for regulations prescribing conditions to attach to licences. These associated regulations now provide a statutory basis for CCTV installation in licensed premises, in summary, requiring certain premises – those open after 1:00am and with a capacity of over 250 people – to install a system “to the satisfaction of the appropriate chief constable”. It also requires that the system must be kept in good working order.

That difference in law explains why the ICO intervened in the Islington case, but would find it much more difficult to do so in Scotland, at least where the premises have extended hours. Though in both cases the police would have had significant powers in relation to the operation

of the CCTV equipment, in Scotland it is now a legal requirement for those licensees affected by the legislation to install a system to the chief constable’s satisfaction.

As a consequence, the ICO would find it far more difficult to take regulatory action relating to the requirement to install itself, whereas in Islington action was taken because the non-statutory blanket requirement which the police tried to impose was deemed to raise questions about unfair and unlawful processing and the holding excessive and irrelevant data.

This, of course, does not mean that the ICO’s hands are totally tied in Scotland. Whatever is deemed to satisfy the relevant chief constable must also comply with the DPA. For example, the chief constable himself cannot require the data controller to disclose images obtained using

the equipment to the police; it is for the data controller to determine whether the disclosure is justified under s29 of the Act. Should the chief constable require images be retained for, say, six months, it may be deemed in breach of Principle 5 of the DPA as it is likely that any request for a images relating to an incident would be submitted soon after the event. A requirement to collect audio recordings with the images would be deemed to be excessive.

All systems should comply with the CCTV Code of Practice published by the ICO. By following its provisions, CCTV operators should remain within the law. ■

Ken Macdonald,
Assistant Commissioner
(Scotland), Information
Commissioner’s Office.

JOIN CAMERA WATCH NOW

“CameraWatch members include stakeholders from right across the UK CCTV spectrum”

Camera Watch™
Surveillance Compliance

- CCTV manufacturers, distributors and installation companies
- Data services
- Law enforcement
- Law
- Private and public sectors
- Security industry.

For further details, contact CameraWatch Helpline:

020 8514 9306

Email:

info@camerawatch.org.uk

Web:

www.camerawatch.org.uk

For all press and media enquiries, please contact:

Robin McEwen

Tel: 0141 560 3028

Email: robin@connectcommunications.co.uk

CameraWatch operates in accordance with the Data Protection Act (1998).

DIARY

Tuesday, 27 October 2009

Full forum meeting

RBS Global HQ,

Gogarburn, Edinburgh

Contact kimnorris@partnersecurity.co.uk

for more information.

LAST WORD



CCTV over the internet – commonly known as IP (Internet Protocol) sounds great. If you have adequate permissions, you can access the CCTV system from anywhere in the country (or indeed the world, even when you are on holiday).

One example was a children's nursery who bought a CCTV system that did just that – and part of the advantage was that parents could log in to the website and watch their kids whenever they wanted, playing in the nursery.

What wasn't taken into account was that no-one had looked at the legal obligations on managing a CCTV system, and specifically the fact that images of all the children taken by the CCTV system were the personal information (or personal data) of those children and should not be shared with people who had no good reason to see the images.

ALL the parents could watch ALL the other children under the gaze of the CCTV system. Not only did this breach the Data Protection Act (DPA) it was allowing unauthorised persons to see these images. In addition, was it possible for people with no connection at all to the children or the school to gain access and view the activities?

If in any doubt over how your data is to be used, seek expert advice from compliance experts.

CameraWatch's Paul Mackie muses on access to data and CCTV image quality...

Another area of contention is when buying or upgrading a CCTV system. How much importance do you put on the actual recording device?

And how many people who specify the requirements look at the format of the end result? In other words, will your records actually be in the correct format when played by the police or courts?

If it does, then great. If it doesn't, it means that the CCTV "evidence" may not be able to be presented. Again, if in any doubt, seek advice from experts.

Finally, remember the main CameraWatch message, endorsed by the ICO CCTV Code of Practice – conduct an annual audit or assessment of your CCTV system! ■



Paul Mackie is Camerawatch Compliance Director (Compliance@camerawatch.org.uk) and Managing Director of Compliance Solutions (paul.mackie@cctvcompliance.com)

Surveillance: an insurance perspective

Barrie Lloyd, of QBE Insurance European Operations, considers some issues of insurance for CCTV systems users

Insurance

IT can be a condition of insurers accepting a risk that there is CCTV installed in a premises.

Clearly, situations can arise such as breakdown or maintenance, where a system is temporarily out of action. In such cases, it is important that insurers are informed.

They may simply accept the situation or they may ask for temporary additional security measures, but if you have notified insurers, you have clarity about this and no arguments about cover if there is an incident during this time.

If CCTV is not stipulated, it may nevertheless have been material to the insurer's decision on pricing. In such a case, it is wise to notify insurers of longer gaps in CCTV coverage.

At present, it is unusual for insurers to get into the question of whether a CCTV system is or isn't compliant. While an insurer may well "approve" an installation from the point of view of catching criminals, it is unlikely to approve it from a compliance point of view.

This is based upon the fundamental principle that an insurance company cannot be expected to take over responsibility for the corporate governance of its clients. There must be a general expectation that our clients will behave in a responsible and correct manner.

This does not mean that insurers will totally ignore compliance questions. It just means that they do not see it as their function to sign off systems from a compliance point of view.