CCTV STAKEHOLDER WORKSHOPS

Summary report

December 2014

Prepared by Julie Hunter on behalf of BSI

juliehunter

www.juliehunter.co.uk

bsi.

www.bsigroup.com

1. CONTENTS

2. BACKGROUND

2.1 Increased use of CCTV

Surveillance cameras were first used in the UK in the 1970s and 1980s, with the first local authority installing a CCTV system in 1987. Since then CCTV has become part of our everyday lives. Today surveillance cameras can be seen everywhere - in public spaces such as streets, stations, car parks, housing estates, shopping centres and on public transport. Many private businesses use CCTV in and around their premises and many people use private CCTV systems as part of home security.

It is difficult to estimate how many CCTV cameras there are. But the Gerrard/Thompson study, published in 2011, estimated that there were a total of 1.85 million CCTV cameras in UK public spaces. That equates to 2.805 cameras per 100 population, 33,433 publicly owned cameras and 115,000 cameras on public transport. This does not take account of cameras in private places, which could boost numbers substantially.

There's no doubt that CCTV has had a profound impact on crime detection and prevention. But as the number of cameras has increased and new technology evolved – such as wireless cameras, internet protocol (IP) cameras, facial recognition and body worn cameras – there is growing concern about privacy and security. It is more important than ever that surveillance systems are used proportionately and regulated properly.

2.2 Surveillance Camera Commissioner

The role of the Surveillance Camera Commissioner (the SCC) was created under the Protection of Freedoms Act 2012 to ensure that surveillance camera systems are used to protect and support communities rather than spy on them. The Commissioner is an independent appointee and has no powers of enforcement.

In 2013 the SCC published a voluntary code of practice for CCTV users, which contained 12 guiding principles. Its main aims are:

- to balance the rights of the citizen with the needs of the state;
- to ensure that CCTV systems are used and managed effectively, proportionately and transparently.

Relevant authorities (such as Police Forces and Local Authorities) must pay due regard to the code when installing new systems or when reviewing those they currently use.

2.3 CCTV Framework

The Surveillance Camera Advisory Council (SCAC) was established to support the Commissioner, by considering and offering advice on matters related to the Commissioner's functions. The SCAC approved its business plan in June 2013. One of the aims of the business plan was to develop and publish standards and guidance to meet Principle 8 of the Code of Practice. The Code states:

"Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards."

To fulfil this objective, the SCAC formed a Standards Group whose task is to review existing CCTV standards, training and guidance, identify any gaps and produce a comprehensive national CCTV framework. The framework should promote confidence and support the concept of "surveillance by consent". It should be transparent, easy to understand, user-friendly and affordable. Standards will form an integral part of this framework.

As part of this work, the Standards Group also identified the need to clarify and confirm the terminology used in various CCTV guidance, and to collaborate with key stakeholder organisations that should be involved in the development of the framework.

As a member of the Standards Group, BSI is currently working to produce a comprehensive list of all standards applicable to CCTV – from manufacture to installation and use.

The CCTV workshops that are the subject of this report were designed to help achieve the objectives of the Standards Group:

- to gather information about the existing situation around guidance, standards, training for those involved with CCTV;
- to discover where further work might be needed e.g. to improve information or provide better tools such as new standards;
- to help understand the best ways to clarify and communicate that information.

2.4 CCTV stakeholder workshops

In November 2014, BSI ran three stakeholder workshops (in London, Bristol and Manchester) to seek the views of those currently working in CCTV, learn from their experiences, identify common problems and brainstorm practical solutions.

A total of 101 people attended the three workshops and participated in the discussions. A wide range of stakeholders were represented including:

- Installers
- Manufacturers
- Consumer and public interest groups
- Retailers
- NHS
- Local authorities
- Housing associations
- Universities
- CCTV security consultants
- Police authorities

3. WORKSHOP SUMMARY

3.1 Aims

For BSI and the Surveillance Camera Commissioner, the purpose of the workshops was to:

- actively engage with relevant stakeholders;
- gauge awareness, and usefulness, of existing codes, regulations, standards;
- inform stakeholders about codes of practice/standards/legislation affecting the use of CCTV;
- seek feedback from CCTV users about real problems being experienced and how things are working in practice;
- explore solutions to common problems;
- facilitate CCTV users to share experiences and concerns with one another;
- involve stakeholders in discussions about good/best practice in this area.

The long term aims were to:

- meet the objectives of the SCAC Standards Group **(see. 2.3);**
- simplify approach and make guidance more user friendly;
- identify gaps that could be filled by standards;
- identify other improvements that could be made;
- help raise standards in the CCTV industry.

3.2 Content

The workshops contained five interactive sessions where attendees were encouraged to share ideas and voice opinions:

Activity 1	Awareness	Group brainstorming session to assess awareness of existing codes, regulations, standards related to CCTV.
Activity 2	Information	Breakout session in small groups to discuss information provision. What information would be useful to new users, what are common sources of information, what are key barriers/difficulties in getting required information?
Activity 3	Operational difficulties	Breakout session in small groups to discuss common problems experienced in the day-to-day use of CCTV.
Activity 4	CCTV as evidence	Breakout session in small groups to discuss problems with using CCTV as evidence and interoperability.
Activity 5	Practical solutions	Group brainstorming exercise to consider practical solutions to the main problems identified during the day.

4. COMMON PROBLEMS IDENTIFIED

4.1 Awareness of existing legislation, codes and standards

The majority of workshop attendees appeared to be very knowledgeable about existing legislation and standards, which are relevant to them in their everyday work. However, we do not believe this to be representative of all CCTV users.

People taking the time to attend such a workshop are likely to be experienced and active members of the CCTV-users community. Delegates felt that general levels of awareness in the industry are low, particularly among smaller organizations. They reported that many CCTV users are not familiar with the relevant rules and regulations and many are working to outdated or obsolete standards.

There appeared to be equal awareness of the SCC and ICO codes, although varied understanding of the details contained in each. Attendees did not understand why there were two codes covering the same topics. They felt that this was confusing and might deter people from using them. All of the main CCTV standards were mentioned in the brainstorming session. Delegates felt that these standards adequately covered the key issues, but that the existence of so many standards created confusion about which were relevant or necessary.

In summary, there was a general consensus of opinion that, although delegates are aware that key CCTV guidance exists, there is a general lack of understanding about the details, how to interpret it, what is relevant and how to apply it.

4.1.1 Other things to consider

Although legislation, standards and codes of practice are important, delegates stressed that there are other things that new CCTV users need to be aware of when setting up a new CCTV system. For example, issues such as budgeting and choosing technology were felt to be essential considerations. It was suggested that these 'things to consider' might form part of a checklist for new users. This is detailed in **section 5.4.2**.

4.1.2 Sources of information

Delegates reported having used the following sources to get information about CCTV:

- Internet – general searches, plus specific organization websites
- Networks – sharing best practice with colleagues, other CCTV users
- Training courses
- The ICO and SCC
- Legal departments within their own companies
- Police
- Local authorities
- Security consultants
- Government bodies – e.g. Home Office, HMRC, CAST
- Professional bodies e.g. BSIA

- Regulators
- Local managers forums
- CCTV User Group
- Compliance officers
- Trade shows
- Certification bodies

Although information from official sources is required, delegates felt information sharing between stakeholders to be equally important. For example, several CCTV users raised the point that they would like more feedback from police - about crime statistics, how CCTV is used, how it has helped reduce crime and cut costs - so that they can justify the use of CCTV systems to budget holders and members of the public.

Some end users said that they had been given incorrect information by installers or consultants, which prompted a discussion about the need for trustworthy, impartial sources of information. Some delegates felt that information sharing should be moderated in some way to ensure accuracy and promote confidence.

4.2 Problems accessing and understanding existing guidance

During the workshop discussions it was evident that CCTV stakeholders found it difficult to access, and make sense of, existing guidance. The common problems raised by delegates were:

4.2.1 Difficulty in accessing guidance

- The sheer volume of guidance available is confusing for stakeholders, making it difficult to know where to go for information and what is relevant.
- The information around CCTV is too fragmented and available from multiple sources, making it easy to miss vital information.
- Too much information is confusing and can act as a barrier, making users less likely to adhere to anything.

4.2.2 Difficulty in understanding guidance

- There are inconsistencies between different sources of information with conflicting advice and guidance.
- Complex standards framework prevents CCTV users from knowing what is or isn't relevant to them.
- Some guidance is inaccurate or out of date and cannot keep up with changing technology.
- There is confusion between different codes of practice, and which applies in which cases.
- Different information and standards apply to equipment etc from abroad and this can make it difficult when importing products and services from other countries.
- There are blurred lines between public and private use, which makes it difficult for users to know which system to use, how to use it and which rules and regulations

apply. There were lots of questions around what defined a public space and how to deal with principles if it was not clear.
- It is difficult to understand what is essential and what is best practice or guidance only.
- There is not enough strategic information to support business cases.

4.2.3 Poor training

- Training courses are difficult to access.
- Most training is not comprehensive, and is not tailored to specific needs.
- Any training that is carried out is often 'one-off' with no continuing developments or updates.
- Many people that operate CCTV systems have a lack of knowledge about relevant rules and regulations.
- There is a lack of a comprehensive training programme that covers the whole length of the process - from deciding to install through to the end use of the images.

4.2.4 Poor communication

- There is lack of communication between different groups/stakeholders e.g. police and CCTV users.
- There is lack of feedback about how CCTV evidence has been used, particularly from criminal cases. There needs to be more two-way communication.
- There are no formally established networks for CCTV users to share knowledge, experiences and best practice.
- It can be difficult to justify the use of CCTV systems, to both the public and to internal budget holders. There needs to be better information about this particularly from a consumer perspective.
- There should be more engagement with the public to inform them of their rights and explain the purpose and intent of any particular CCTV system so that the reasons and "pressing need" for it can be better understood.

4.3 Operational difficulties

Workshop delegates discussed the problems that they had experienced in the day-to-day use of CCTV. They identified common barriers to working and common challenges faced. These were:

4.3.1 Purpose and expectations

A key barrier to operation and use of CCTV is people's misperceptions of what CCTV systems can do. This might be the police not realising how long it takes to download the data, operators not understanding what the system can do or why it is being used.

Delegates reported that it is common for organizations to have unrealistically high expectations of CCTV, tending to think that cameras can solve everything when, in reality, they may not be the best, or only, option. Reliance on CCTV is not always appropriate. For

example, it can be too easy to rely on CCTV to resolve HR issues when the issue should have been dealt with using other channels.

Public expectations are also important. Many workshop attendees felt that public expectations of CCTV are too high. People frequently see 'hi-tech' CCTV systems solving crime in films and on TV, which can lead to them overestimating the capabilities of the system.

Delegates agreed that there are often big differences between what people (e.g. police/public/operators) think CCTV can do and what it can actually do.

4.3.2 Confusion about CCTV guidance

Confusion about codes of practice, standards and legislation can cause operational difficulties. Workshop attendees said that this confusion created problems for CCTV users leaving them unsure about which rules to apply, or whether their system and its operation meet requirements. For example, there is often confusion around whether a system is public or private, meaning that users don't know which guidance should be followed.

Delegates reported that it was difficult to know which guidance was essential and which was only recommendation or best practice. It's not always clear which individuals need licensing (e.g. SIA) or how organizations should support that. It was felt that confusion around guidance could lead to the wrong guidance being applied or, in some cases, deter users from following any guidance at all.

4.3.3 Staff knowledge and training

Workshop attendees identified wages as an ongoing problem. CCTV operators need a certain level of knowledge and skill to operate systems effectively. But operators are often paid low wages, which does not attract staff with the highest levels of experience.

Staff training was also seen as a barrier to effective CCTV operation. Staff require training in their rights and responsibilities regarding data use (legislation, applicable standards and codes of practice) as well as protocols. They also need technical knowledge to understand how to use the existing hardware and software. But not all operators receive adequate training. In some cases this is due to lack of a formal training programme, which identifies competencies and who needs training for what, with regular updates and continual improvement.

Financial resources can also limit training. CCTV technology is constantly evolving and it can be expensive to keep staff up to date with new technology. Conversely, delegates reported that some staff seem reluctant to learn about new technology, preferring to stick with what they know.

Workshop attendees also highlighted a widespread problem of 'siloed' information. Individual members of staff can accumulate huge amounts of CCTV-related knowledge and experience, but this is not always shared between team members or passed on from those leaving the company to new employees.

4.3.4 Choosing technology

There are no standard protocols regarding compatibility of equipment. With the wide range of different technologies available it can be difficult for new users to know which to choose. Lack of protocols means that incompatible systems are often used, which can lead to problems with transferring, retrieving and sharing data for evidence. These issues are discussed in more detail in **section 4.4**. The main problems that CCTV managers might face when choosing/setting up CCTV systems are:

- Do you need CCTV in the first place; is it the best or only option for your needs? It is important to remember the original purpose/justification for installing – what can you use it for?
- What hardware/software offers the best way to meet your needs?
- How much do different systems cost?
- Whose advice can be trusted? Installers/manufacturers may not always give unbiased/objective advice about the best system to use.....
- How can the system be future-proofed? New technology is evolving all the time so it can be difficult to keep up.
- Where to locate cameras to start with? How to assess their effectiveness? Re-locating cameras if necessary.

Workshop attendees warned that there can be an obsession with technology, but CCTV managers need to remember that people and processes are also important.

4.3.5 Storage, security and privacy

Storage, security and privacy are ongoing concerns for CCTV operators and end users. The following concerns and questions were raised:

Equipment	• Where is the equipment being stored? • How secure is it? • Do all personnel who need access have it? • How do you decide/justify who needs access? • Logistically how do you enforce these security procedures?
Data	• Who is allowed in the control room? • Who can see data?
Storage	• Where and how is data stored? Is it safe and secure? • Who has access to stored data? • How much capacity is needed? • Amount of data and storage needed is always expanding – if discs/hard drives are repeatedly overwritten, or more data is compressed onto systems, this can reduce the quality of images.
Transfer	• What rules apply to data transfer? • How do you securely transfer data from one place to another?

Data retention	• How long should you store/retain data for? • There are inconsistencies between law and best practices when it comes to retention of data. • Once the data had been extracted is it still covered by the original retention period or does a new timeline begin? • Is the data backed up or archived? • What are the reasons for retaining the information? • How long do the police require you to retain data?

4.3.6 Budgeting for ongoing costs

Workshop attendees felt that ongoing costs and budget restrictions can be a key barrier to using CCTV systems correctly. Most organizations budget for set-up costs but underestimate how much it will cost to maintain and operate a CCTV system, and ensure that it is fit for purpose. These costs can be difficult to predict or assess, which can put an unforeseen strain on financial resources.

The entire end-to-end budget needs to be taken into consideration from initial installation right through to continual maintenance.

4.3.7 External influences

Delegate raised the point that there are various factors that can potentially affect the day-to-day use of CCTV, which are out of CCTV users' control.

- Political issues – e.g. local government policies that might restrict where cameras are located.
- Environmental issues – e.g. trees growing to obstruct existing cameras or wind moving cameras.
- Transmission issues – e.g. poor internet connections or faulty phone lines.

4.3.8 Review and maintenance

It is important that organizations regularly review their CCTV systems to ensure that they are still fit for purpose. However, workshop attendees reported that in many cases this does not happen. Regular reviews should include:

- Maintenance checks - to ensure that all CCTV equipment is operating correctly. Who is responsible? What should be done? How often should checks be carried out?
- Review of cameras - are existing cameras still useable? Are cameras located in the right places? Are they still useful? Are new cameras required in different locations? Are any existing cameras obstructed by trees, new buildings etc?

4.4 Using CCTV as evidence

One of the main purposes of CCTV is to gain evidence of criminal activity or wrongdoing in case it is needed for prosecution. There were representatives from several police forces at the workshops that were able to tell us about their experiences of accessing and using data from end users. The majority of end users confirmed that they had been asked to provide CCTV as evidence. This might be for:

- Police
- Public subject access requests
- Insurers
- HR departments

But the reality of using CCTV data as evidence seems to be complicated and problematic. Delegates reported several instances where data could not be used as evidence due to lack of knowledge, technological problems or costs. The main problems identified and discussed are detailed in the following **sections 4.4.1 – 4.4.4**.

4.4.1 Lack of knowledge about rules

There appeared to be a high level of confusion around the rules relating to CCTV data access. For example, delegates reported that some CCTV managers and operators use the Data Protection Act as a reason for not providing important evidence. They also felt that knowledge of CCTV operators can cause problems. They reported that many CCTV operators are unaware of the rules and regulations surrounding the use of CCTV, which means that they can be persuaded to hand over data that they should not, or refuse to share data that they should. It was considered essential that operators understand the rules surrounding:

- Subject access requests - What constitutes a request? What is the formal procedure for submitting a request?
- Police requests - When can police legally require you to hand over data? CCTV users had examples of police walking into the control room and physically taking data systems away. What format does it have to be in?

Another issue that can affect the usability of evidential data is lack of knowledge about appropriate signage. If a CCTV user has not displayed appropriate signage it can mean that important evidence captured cannot be used in criminal cases.

4.4.2 Retrieving relevant data

4.4.2.1 Resources required

CCTV users at the workshops reported that trawling though vast amounts of data to locate relevant evidence (which might be only a few seconds on several hours or days' worth of recordings) can take a lot of time and money. Retrieving that data (copying it from the main system) can also take time. End user organizations often don't have these resources, which

appeared to be a key barrier to providing evidence for many. Workshop attendees questioned who should be responsible for doing the work and who should pay for it?

The subject of charges was discussed at length. Retrieving data can be expensive, in terms of staff time, the cost of processing data and getting it into the right format. There is currently a maximum £10 fee for subject access requests, but all agreed that this does not cover the cost of doing the work.

Some delegates from local authorities told us that they charge police/insurers for providing evidential data. Other end users felt that they should only provide raw data to the police and that they should be responsible for sorting through it and retrieving the data that they need. Compatibility issues make this even more difficult.

Workshop attendees felt that timeframes for retrieving data are often unrealistic. Specific and realistic time frames should be given for data retrieval.

4.4.2.2 Compatibility and format

Delegates felt that a key barrier to using CCTV as evidence is the wide range of differing and incompatible systems and formats used. The format used by the CCTV operator may be incompatible with the format required by the police. CCTV operators don't always know what format the police want data in, or how to encrypt it securely so it can be used as evidence. All felt that there should be a standard way of operating.

4.4.2.3 Privacy of third parties

Privacy can be an issue when providing CCTV evidence to the police (or other body). If third parties, for example other staff or members of the public, are captured on CCTV images they may have a legal right to anonymity. To avoid 'inadvertent disclosure' the CCTV operator may need to blank out faces of third parties before passing data onto the police. Workshop attendees reported that the cost of doing this can be very high. One delegate said that, in the past, the organization he worked for had refused to provide evidence to the police as the costs of avoiding inadvertent disclosure were unrealistically high.

4.4.3 Transferring data

4.4.3.1 Lack of knowledge about systems

Transferring data from one system to another is vital if CCTV footage is to be used as evidence. But delegates reported that many CCTV operators don't know how best to use the hardware/software to extract information or transfer data.

4.4.3.2 Incompatibility of systems

Incompatible hardware/software used by different departments or organizations means that it is not always simple to transfer data from the CCTV user (e.g. local authority) to the organization requiring evidence (e.g. the police). Some organizations are still using video systems. Others have to burn data onto DVDs, which then have to be transferred physically. Others use computerised, digital files that can be transferred remotely. To facilitate the

portability of data and enable the transfer of large volumes, the correct software and hardware needs to be used with adequate storage at both ends.

4.4.3.3 Privacy and security

There are increased privacy and security risks when data is transferred from one place to another. Data may pass through several different systems or organizations before it reaches its final destination. It is vital that an audit trail is recorded so that everyone involved knows which path the data followed and which staff and organizations had access to it on the way.

Delegates stressed that evidential integrity needs to be maintained, so that the police can be sure that data has not been changed or modified in any way from the original. When data is transferred to the police it must be sufficiently encrypted so it can't be modified and is therefore useable in prosecution. This can cause problems as not all operators know how to do this.

4.4.4 Using data

The use of data, once retrieved and transferred, depends on playback. However, footage can only be played back on compatible systems. Image quality is also critical. If this is not good enough the police may not be able to rely on the image as evidence in a court of law. Inferior recording equipment, the use of wireless transmission systems and the reuse of storage tapes or discs, can all affect image playback quality.

However, CCTV users are not responsible for all the problems. Several CCTV system managers reported that, even when they had supplied good quality footage, they had experienced problems getting the police to use it as evidence.

5. POTENTIAL SOLUTIONS

Throughout the day, workshop attendees suggested possible solutions to the problems being discussed and practical steps that might help to achieve common goals. It was widely understood that these were 'ideal solutions' and that, realistically, it might not be feasible to implement all of these changes. This section gives an overview of the delegates' key recommendations.

5.1 Review and harmonize existing guidance

5.1.1 Simplify guidance

In summary, workshop attendees identified an urgent need to review the existing guidance and information to:

- simplify guidance;
- make it clearer which guidance is applicable to different people at different times;
- remove inconsistencies;
- delete repetitions and overlaps between various codes and standards

Delegates agreed that the sheer volume of CCTV guidance from different sources is a barrier to effective working. They felt that it was necessary to review the existing guidance and that this could only be done by stepping back and looking at the big picture. It was suggested that existing guidance needed to be harmonized to delete repetitions, overlaps and inconsistencies. For example, many felt that it was unnecessary to have two codes of practice (ICO and SCC).

The general consensus of opinion was that this information review should be the logical first step in any practical plan of action. Delegates agreed that there seemed little point relocating information and advice to a central hub, or carrying out work to increase awareness or take-up of existing guidance, before the guidance itself was simplified and accessible to all.

5.1.2 Format of guidance

Delegates expressed a preference for information to be available online, but felt that it was also useful to have printed leaflets that they could share with colleagues and keep as a handy reference guide. It was suggested that existing information should be consolidated; with no need to re-write content completely. Before new information is published the pathways that people use to gather information must be explored. This will ensure that the right information is being distributed to the places where it will be most effective and useful.

5.2 Offer guidance tailored to specific needs

All workshop attendees agreed that they would find it useful to have guidance that was tailored to their specific needs. People felt that, where possible, information should be clearly sector specific so that it is relevant and useful to those that need it. No one has time to wade through lots of irrelevant information and this can just add to confusion.

Delegates also said that it would be useful to have more impartial advice, and recommendations about what was relevant and important, rather than just being given facts. For example:

- How to tell if CCTV is really needed or the best option?
- What types of systems are required to achieve different aims?
- Being given a summary of the key points of various codes and guidance and how to apply them, rather than just being directed to a copy of the full text.
- What to consider at different stages of the process.
- What is essential and what is only recommended.

They said efforts should be made to promote the right information to the right people at the right time.

5.3 Raise awareness

5.3.1 CCTV users

The workshops clearly identified the need to raise awareness of existing guidance. Delegates believe that all of the essential information about CCTV is already contained in existing legislation, codes of practice and standards (e.g. BS 7958), but the main problems are that people do not know that it exists, or don't understand it.

It was suggested that awareness could be raised by:

- advertising in trade magazines or at trade shows/exhibitions;
- using positive case studies to showcase organizations that have successfully implemented codes of practice or standards;
- co-ordinating visits to sites to share experiences of best practice – promote 'old school' face-to-face meetings;
- organizing local forums and networking events to give background to codes of practice and standards and to share knowledge and procedures with other working in the same field;
- developing partnerships with local national membership organizations e.g. BRC;
- making the most of companies' marketing tools to make the public aware of changes in practice;
- cascading information internally to make sure that it reaches everyone that needs it within an organization;
- increasing use of social media.

5.3.2 Raise public awareness

The delegates also identified a need for the general public to be better informed about CCTV. For example, what's being done, who's being watched, where and why? This could help to tackle some of the unrealistic expectations that consumers currently have of CCTV systems and dispel some myths about privacy and security.

It was felt that local authorities and other public bodies should publish more information about their use of CCTV. Some of the organizations represented at the workshop already

had a dedicated area on their website to do this. Others didn't. It was felt that CCTV users should be more transparent about their systems. It was agreed that there was no need to give specific details of cameras locations but, at a minimum, organizations should publish information about:

- the legislation/codes they follow;
- the number of cameras they have in operation and what geographical area they cover;
- what the CCTV is there for and what it can/can't do;
- who members of the public should contact if they have any problems or enquiries.

5.4 A central hub for guidance and information

It was widely agreed that information and advice should be drawn together in one place **(see Fig 1).** It was felt that an online tool would be the best way of doing this. The central hub or 'one stop shop' should:

- provide one simple access point for all CCTV users seeking information and advice so that people know where to go and can find everything in one place;
- offer a checklist, tailored to different users, so that users can see what is relevant to them;
- explain what is essential and what should be considered;
- clearly communicate key information to all relevant parties;
- be run by an independent, trusted, impartial source to avoid bias and promote trust in the information being given e.g. the SCC;
- be free and accessible to all;
- signpost to further information/tools/standards/useful contacts;
- be set up with involvement from key stakeholder organizations.

5.4.1 Needs assessment

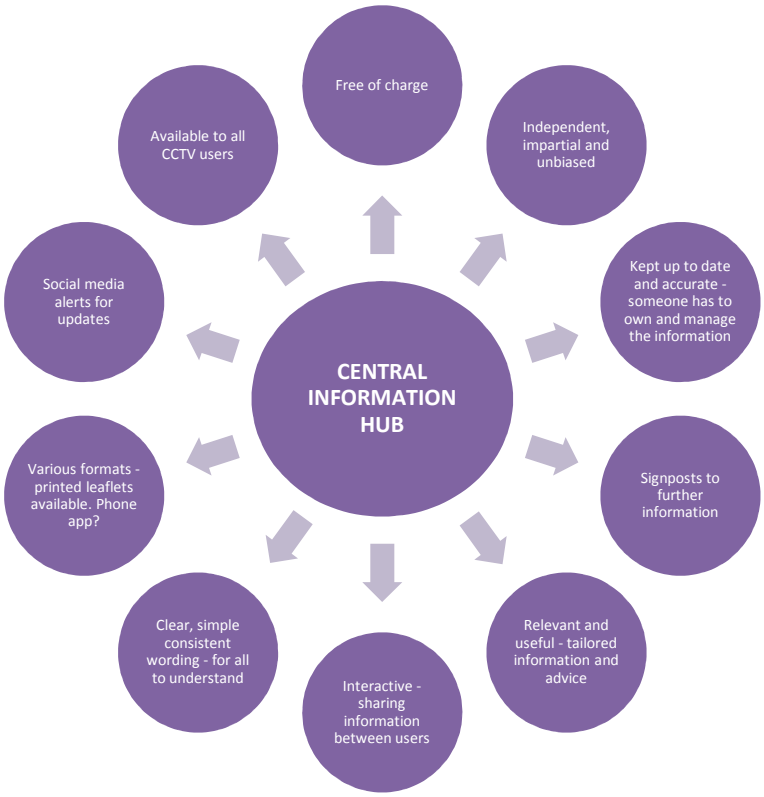
It should be recognised that different stakeholders will require different types of information. Key stakeholders being:

- Installers
- Public/consumers
- End users
- Enforcers/police

Delegates felt that guidance given by the 'central hub' should be sector specific, tailored to the needs of the user. For people that enter the website looking for information there should be some kind of interactive flow chart, with links to further information and resources where required.

This initial 'needs assessment' or 'triage' should determine who the user is, the organization they represent, their proposed use of CCTV (public or private space) and their operational needs to ensure that relevant information and guidance is given. Too much information can be confusing so people should only be given the information they need.

Fig.1: Central information hub



5.4.2 Checklist

Delegates suggested that once an initial assessment has taken place users could be presented with a checklist of relevant information with signposts to further information and advice.

Existing guidance	• Are you aware of the relevant legislation? • What are the relevant codes? E.g. ICO and SCC • What are the relevant standards?
Scheme objectives	• What do you want to achieve? • Is CCTV the right/only answer? • Reasons for installing - Can you justify use? Is there a pressing need? • What are the operational requirements? • How the information will be used? Who will it be shared with and how? • End user requirements
External factors	• Political demands • Public consultation - Privacy Impact assessment, PACE – public ethics/ opinion • Collation of evidence – other stakeholders • Citizen requirements

	• Police data sharing protocol
Set up	• Registration with the correct/relevant authorities e.g. ICO? • Staff - Who will be operating the system? Do they have the right experience, knowledge, training? Who's controlling the data? Are they properly qualified/trained to do so? Training – what kind of training is needed? How much is needed? Who needs to complete it? • In house or contracted? • Data storage – do you plan to retain images? How long for? How much storage do you need? Where will data be stored? Real time? • Protecting data – how will you ensure safety/security of data. How to comply with data protection • Choosing the right equipment - What hardware/software do I need? Is it fit for purpose? Type of technology to be used – e.g. facial recognition, voice recording etc. Consideration of future tech • Location of cameras - Position and control of cameras • Installation – who will install the system? How to select specifiers/installers? How much will this cost? • Members of the public – Do I need signage/public notices. If so where should I put them? • Budget – set up costs for equipment, hardware, software, consultancy, staff training etc
Operation	• What plans are in place for continual review • Ongoing costs – how much will the system cost to run? E.g. staff costs, regular training, running equipment, upgrading hardware/software. • Ongoing maintenance – who will carry this out? What will they be looking at and how often? • Contingency plans – what if things go wrong? Back up? • How to measure effectiveness? • Staffing levels required to install, operate and maintain the system • Who can access data? Who has the right to request data? What can or can't be provided? What are the rules surrounding this?

5.5 Better communication between stakeholders

Stakeholders agreed that better communication between relevant stakeholders could improve effectiveness. Communication needs to be improved all the way through the chain e.g. between installers and end users, between end users and police. It was felt that communication between local government and police particularly needed to be improved.

The CCTV workshops proved that colleagues are a valuable source of information and advice. After some debate, it was proposed that communication between stakeholders could be improved by the development of a secure online forum to facilitate information sharing. Stakeholders would be able to create local community or specific interest groups, post

questions and share information, experiences and best practice with other CCTV users. The user forum could incorporate a document library, where users could upload their own documents and compare against others as a way of information sharing. This could be a valuable source of information and advice for both new and existing CCTV users.

It was suggested that a CCTV user forum could be facilitated through the Central Hub website **(see 5.4)**. The site should require registration to monitor membership and maintain security.

The following solutions were also suggested:

- A public awareness campaign to tackle misperceptions about CCTV. Local authorities could publish information about how they use CCTV in their area.
- The creation of police liaison officers to tell CCTV users what they require in terms of evidential data, so that systems can be set up appropriately in the first place.
- That written information should be provided with equipment from the manufacturer, especially to private CCTV users e.g. home owners.

5.6 Comprehensive training scheme

Workshop attendees agreed that training is essential for anyone working with CCTV e.g. operators, managers, police and lawyers. Delegates felt that, although various training schemes exist, there is a lack of a cohesive and holistic approach.

It was suggested that there should be one national training scheme, with requisite recognition attached, which would ensure a consistent, accurate and comprehensive approach. Such a scheme should be accessible to all users to whom it is relevant, or likely to become relevant. Training should be timely (given at the right time, when useful, before needed) by a qualified trainer. To be most effective it should also be tailored to the specific needs of the user.

Each organization using CCTV should have a structured training programme that details what skills and knowledge are needed for specific roles and ensure that each individual receives the training that he/she needs to effectively fulfil their role.

Delegates also felt that each organization should appoint a single person to be responsible for identifying training needs, ensuring that they are met and keeping training records up-to-date. Training should be an ongoing process that is continually reviewed and updated. Not just something that is done for new staff members. Technology and rules change and CCTV users need to be kept up to date.

5.7 Organizational policies

Delegates believed that any organization working with CCTV should devise its own internal policy, devised by management and filtered down to all staff, which should:

- identify a single person responsible for CCTV policy, training, contacts and communications;
- assign clear responsibilities to all staff members working on the system;

- appoint named CCTV liaison officers to deal with external organizations e.g. police enquiries and subject access requests;
- develop a process to ensure that key information is communicated between staff members so that vital knowledge and expertise is not lost, for example, when a member of staff leaves;
- create processes to help staff deal with common problems and difficult situations;
- plan regular reviews to ensure that their surveillance systems are fit for purpose.

However, delegates warned that expectations need to be realistic. For example, small retailers may not have sufficient resources and capabilities to develop policies and implement procedures.

5.8 Increase take-up of existing guidance

5.8.1 Encouraging take-up

Workshop attendees agreed that raised awareness and better information are key to encouraging take up. But people also need to understand the benefits of adopting CCTV guidance in real terms – the use of positive case studies and successes could demonstrate this.

A couple of delegates suggested that local authorities and other public bodies could encourage take-up of standards by stipulating that all contractors must comply with key guidance. This should be something that they felt should be written into each organizational policies **(see 5.7)**, rather than something that could be expected by law.

5.8.2 Enforcement

Stakeholders felt that compliance with key codes and standards should be enforced to encourage a wider take-up. It was felt that this would greatly benefit the industry as a whole. Several delegates expressed a desire for the SCC to be given more powers of enforcement so that it was a watchdog 'with teeth'.

Many of the workshop attendees represented organizations that do comply with relevant codes and standards. They felt it was unfair that organizations that fail to comply do not face penalties of any kind. It was felt that there should be consequences of non compliance - both internally within an organization and externally with regulation. It was suggested that individual organizations should impose consequences on staff for non-compliance – this could be incorporated into organizational policies **(see 5.7).**

It was also felt that those setting the codes or standards should be able to enforce compliance. The majority of stakeholders said that organizations should be subject to an independent audit to assess compliance. Others felt that a self-assessment process would be better, as organizations would not have to pay an external auditor to demonstrate their compliance.

5.8.3 Symbol of compliance

Workshop attendees felt that it was unfair that consumers have no way to differentiate between an organization that is following good practice and one that isn't.

They felt that more recognition should be given to those organizations that are compliant with a standard (e.g. BS 7958) to show that they are operating in a way that promotes best practice. Some delegates complained that standards numbers can be difficult to understand, remember or relate to. Stakeholders agreed that a visual symbol or mark, to demonstrate compliance with key legislation, standards and guidance, would be easier for consumers to identify with and understand.

However, it was felt that the industry should avoid creating another 'stamp' completely as too many could confuse both consumers and businesses.

It was suggested that the Kitemark could be used more widely by those complying with CCTV standards. It was also proposed that the SCC could develop its own quality mark – a visual symbol of compliance - that could be awarded to every organization that demonstrated compliance with the relevant guidance recommended by the SCC's online central hub tool.

Organizations should be able to 'earn' the mark through their actions, without paying for it. If organizations are able to get the mark simply by paying this erodes trust that organizations are getting it by merit.

5.9 Need for research

Workshop attendees said that it would be useful to have more research to help them decide if CCTV was needed; if it was worth the time and expense; if it would actually help prevent crime. The following research might be useful:

- CCTV user experiences – the realities of implementing current guidance (in terms of staff time taken, the financial costs) and the benefits that each organization has seen e.g. successful case studies,
- Crime statistics – which areas are most at risk from crime? What sorts of crime? Could CCTV possibly act as a deterrent in these areas?
- Police experiences - how the police use CCTV data. Has CCTV helped in the reduction of crime? Have there been more successful prosecutions?
- Public perception of CCTV – what information do they want from organizations using CCTV?

6. CONCLUSION

6.1 Meeting objectives

Overall, the CCTV stakeholder workshops were successful in meeting the objectives of BSI and the SCC. The following outcomes were achieved:

- active engagement with a wide range of CCTV stakeholders;
- assessment of awareness, and usefulness, of existing codes, regulations, standards;
- stakeholders informed about existing codes of practice/standards/legislation affecting the use of CCTV;
- feedback received from CCTV users about real problems being experienced and how things are working in practice;
- solutions to common problems explored and possible improvements identified;
- stakeholder discussion about good/best practice in this area.

This report summarises the key problems experienced by various CCTV users **(section 4)** and makes recommendations for potential solutions **(section 5).**

6.2 Summary of key recommendations

As a result of the workshop, nine key recommendations were identified.

1. To review, harmonize and simplify existing guidance **(see 5.1)**
2. To develop guidance tailored to specific user needs **(see 5.2)**
3. To raise awareness of CCTV guidance, use and capabilities **(see 5.3)**
4. To create an online central information hub **(see 5.4)**
5. To improve communication between stakeholders and develop an online CCTV user forum for information sharing **(see 5.5)**
6. To create one comprehensive national training scheme, accessible to all **(see 5.6)**
7. To require all organizations using CCTV to have an internal CCTV policy **(see 5.7)**
8. To increase take-up of existing guidance, via compliance and enforcement **(see 5.8)**
9. To commission research to provide statistical evidence **(see 5.9)**

6.3 The future

The recommendations from this report provide valuable stakeholder insight that will help to shape the future of the CCTV landscape in the UK. The findings will be shared with the Surveillance Camera Advisory Committee and will hopefully assist the Standards Group in delivering a National CCTV Framework that is clear, effective and transparent, and meets the needs of those working in the industry.