

**FEBRUARY 2020**

**IPVM Interview - Thoughts from the Industry – A BSIA Perspective**

**Question 1 IPVM: What do you think of the perception that video surveillance is becoming a tool of government / corporate oppression, especially thanks to AI technologies?**

This answer can be split into multiple sections.

### **"becoming a tool of government"?**

In previous BSIA research it was determined that only 1 in 70 cameras in the UK are owned by the government for the purpose of public safety, the remainder are privately owned and operated under the scope of the operational requirements of the owners. When the report was published it allayed previous fears that UK was "sleepwalking into a surveillance state" - comments made by the Information Commissioner. The public sentiment towards video surveillance is now that a) it is generally owned and operated by private enterprises and b) when used to prevent or solve crimes this was being done for the greater good of society.

A number of high-profile cases have been solved or helped through the use of evidence extracted from video surveillance systems. This evidence was extracted by the Police using standard methods developed by the BSIA and Home Office to ensure consistency and acceptance into the criminal justice process. In the UK these cases have included preventing mainland IRA activity, finding missing persons, and according to leading police authorities after the 7/7 bombing, the second attack was prevented with substantial help from the video surveillance footage. That footage had to be manually retrieved from 1000's of discrete video surveillance recording systems, and then multiple formats reviewed by police officers and forensic experts in order to create a sequence of events, and to trace the movements of the terror suspects.

### **"corporate oppression"?**

In the UK corporate entities have to operate within the legal framework laid out in company law which requires a consideration towards corporate and social responsibility, they also have to comply with UK Employment Law, GDPR, Protection of Freedoms Act and Equality Act to protect people from exploitation. Corporate entities do need to make a profit eventually to fund the employment of their people and deliver their products to market, but not all corporations are focused on profit alone. There is a growing movement towards a more balanced approach to corporate governance which considers the societal position and not just the returns to shareholders. Many corporates are now taking an approach to employee well-being which serves society. Generally video surveillance in the workplace is

32 Bedford Row, London, WC1R 4HE  
 switchboard 01905 342020 · comms@bsia.co.uk · www.bsia.co.uk



used for process management, safety and security of employees and not to watch employees.

### "the use of AI technologies"?

There is a large public focus on privacy, data and its use across all platforms and publicly accessible places in the UK. There may be some misunderstanding around this subject and it also may not be clearly communicated as to what AI technology is and how it is being used. It is therefore the industry's responsibility to explain its capabilities and provide recommendations as to how it may be best used. The actual use should be governed by ethical, legal and standardised frameworks and if such frameworks are yet to be developed, there has to be a wider consultation which involves engagement with stakeholders and Government. At this stage, the use of facial recognition in South Wales was ruled by a Judge to be legal under GDPR. Generally, if the public are supportive as was the case with general video surveillance, due to the industry explaining how it can be implemented and the Police putting it to good use, it is more likely that the technology will be accepted as a benefit to society.

In the UK, in the event of an incident or criminal investigation, the Police have a legislative framework already available to them which can enable access to the video surveillance recordings from any video system in the UK whether publicly or privately owned with a clearly defined legal justification.

The advent of facial recognition may have challenged the existing legal framework, because the technology makes it easier and faster to automatically find specific individuals in live or recorded images saving Police time, enabling a **faster response** and solving crime more quickly and effectively at a lower public cost.

The private electronic security industry largely self-regulates through standards and codes of practice developed by the BSIA as a trade body, standards bodies and other interested parties. These standards are to ensure the effective and ethical use of video surveillance for the operator's purpose.

#### ***BSIA Statement on Automated Facial Recognition***

*Similar to other security measures or digital tools, Automated Facial Recognition (AFR) can have both positive and negative uses. The BSIA supports this technology when it is used correctly guided by an ethical and unbiased judgement. With that said we believe a standard is necessary to provide guidance on its usage and ensure discriminatory practices are eradicated as we cannot and will not support technology used for these purposes.*

Private operators who form the majority of owners of the video estate have been using facial recognition when combined with access control to improve the security

of educational facilities for many years. Public acceptance of the use of the face as a method of authentication for the payments system is already here.

Any technology can be used in a way which may become detrimental to the individual, for example, a mobile phone may be used to view/monitor a person without their consent. However, there are laws which protect the public and admonish those whom abuse communications technologies. Videos posted on YouTube can be easily downloaded - altered - and re-uploaded to contain deep fake technology. Soon the public may not be able to determine the truth at all when using digital technology.

In the professional video surveillance domain, the potential for the abuse of the technology may exist, **however current standards and legislation do prevent such abuse.**

As progress is made towards the effective harnessing of video surveillance for the greater good of society, influencing standards and challenging the current ethical and legal frameworks is necessary to test their suitability.

The industry is supportive of the challenge and is lobbying the relevant authorities to improve existing or create new frameworks for the safe use of AI with video surveillance data.

### Question 2 IPVM: Are you concerned about the long-term reputation of the industry?

**The BSIA is recognised as ‘the voice of the professional security industry’** and as such takes great interest in the reputation of the industry which is why it relentlessly lobbies government and relevant stakeholders whom may wish to use video surveillance images for a new purpose beyond the original operational requirements specification e.g. for the purpose of security of a facility. BSIA are at the heart of all relevant standards bodies, seeking the views of the stakeholders and influencing where it can influence.

### Question 3 IPVM: Does BSIA have a response to the criticism that the video surveillance industry itself is doing little on the human rights/privacy front and is "primarily driven by profit" as one activist told us?

We believe the industry would not thrive if it existed only for the purpose of profit. Profit is a hygiene factor which enables the greater good. BSIA members are commercial organisations and all businesses have to make a profit at some point in their lifecycle. However, the security industry has pioneered self-regulation through its investment into the safe use of technology, creating inspirational value over a number of years.

The Association offers the opportunity for members to collectively come together to improve the industry. BSIA has been at the forefront of creating standards and codes of practice since the advent of video surveillance technology. Examples include: privacy masking guide, chip and PIN guide, BS 8418, IEC 62676, Cyber Secure It, Cyber Security Guide, as stakeholder in the Surveillance Camera Commissioner's Buyers Toolkit (privacy impact assessment), and submission of evidence to the select committee examining the relationship between the citizen and the state during the readings of the Protection of Freedom's Act.

#### **Question 4 IPVM: Does BSIA have an ethics committee / Code of Conduct that addresses such issues for example?**

Whilst the BSIA does not have a Code of Ethics for its Video Surveillance Section it does require members to sign a Code of Conduct and supplemental rulebook before joining the Association, as well as adhering to ISO 90001. Regarding video surveillance, human rights and privacy this is something that is widely debated within the industry and at our various meetings which results in the BSIA taking a leading role in lobbying government and the further industry to create standards surrounding the topics. The BSIA provides guidance for industry to use and where appropriate votes to support and facilitate implementation through its members.

As per the BSIA statement earlier:

*“Similar to other security measures or digital tools, Automated Facial Recognition (AFR) can have both positive and negative uses. The BSIA supports this technology when it is used correctly guided by an ethical and unbiased judgement. With that said we believe a standard is necessary to provide guidance on its usage and ensure discriminatory practices are eradicated as we cannot and will not support technology used for these purposes.*

The private electronic security industry largely self-regulates through standards and codes of practice developed by the BSIA, certification bodies and other interested parties. These standards are to ensure the effective and ethical use of video surveillance for the operator's purpose.

#### **Question 5 IPVM: Briefly, some activists are calling for a total moratorium on CCTV facial recognition, do you think this is overreach or a necessary measure?**

We are aware of the Private Members Bill which started in the House of Lords prior to the UK elections. This calls for a moratorium on the use of all facial recognition technology in public places until the ethical and legal frameworks have been examined. It is unknown whether this bill will continue.

32 Bedford Row, London, WC1R 4HE  
 switchboard 01905 342020 · comms@bsia.co.uk · www.bsia.co.uk



ISO 9001:2015  
 Certificate No. FS 14657

BSIA is against the misuse of any technology and where it has a negative impact on the individual and are calling for the creation of relevant ethical and legal frameworks for the safe use of facial recognition in public places. This should also be underpinned by a standard which may define the scope of use, the legal framework under which it has to be operated, privacy impact and ethical considerations. In the meantime, BSIA supports the best use of technology within current frameworks that improve the security and safety of the world we live in with greater explanation and transparency.

ENDS

**Press contact: Katherine Ingram** PR & Communications Officer  
Mobile: 07764 968196 [k.ingram@bsia.co.uk](mailto:k.ingram@bsia.co.uk)

#### Editors Notes

The British Security Industry Association, as the voice of the professional security industry, represents multiple sectors of private security in the UK. Its members provide over 70% of the UK's security products, services and they adhere to strict quality standards. For more information visit <http://www.bsia.co.uk>

#### **BSIA Statement on Automated Facial Recognition**

*Similar to other security measures or digital tools, Automated Facial Recognition (AFR) can have both positive and negative uses. The BSIA supports this technology when it is used correctly guided by an ethical and unbiased judgement. With that said we believe a standard is necessary to provide guidance on its usage and ensure discriminatory practices are eradicated as we cannot and will not support technology used for these purposes.*

32 Bedford Row, London, WC1R 4HE  
switchboard 01905 342020 · [comms@bsia.co.uk](mailto:comms@bsia.co.uk) · [www.bsia.co.uk](http://www.bsia.co.uk)



ISO 9001:2015  
Certificate No. FS 14657