Information Polity 28 (2023) 559–567
DOI 10.3233/IP-239012
IOS Press

Review

Policy Review: The Evolving Governance of Surveillance Cameras in the UK[1]

Pete Fussey[a] and C. William R. Webster[b,*]
[a]*Department of Sociology, University of Essex, UK*
[b]*Stirling Management School, University of Stirling, Stirling, Scotland, UK*

1. Introduction

This policy review explores developments in governance arrangements surrounding the use of surveillance cameras in the UK. It makes specific reference to provisions within the Data Protection and Digital Information (DPDI) Bill[2] (the Bill) introduced into the UK Parliament in spring 2023 and which proposes the abolition of the office of the Biometrics and Surveillance Camera Commissioner (BSCC).[3] The underlying argument, is that the removal of this office, in a period of fast technological change, will result in the loosening of safeguards designed to raise standards and protect citizens, and may ultimately result in the deployment of technologies that are not in the public interest.

The technological backdrop is the widespread use of surveillance cameras, often referred to as CCTV (Closed Circuit Television), in public places in the UK and elsewhere (see for example: Webster, 2009). More recently, advances in computerisation, especially around Artificial Intelligence (AI), have provided new opportunities for innovative applications to be integrated into public space camera systems. The most significant of these is Face Recognition Technology (FRT), where algorithms match faces in crowds to those contained in police databases. FRT is controversial for a number of reasons, including: poor success rates, inbuild racial bias, a presumption of guilt and because there is a lack of public support for such systems (Webster, 2019). To date, FRT applications have been limited in number, primarily because of oversight safeguards embedded in the BSCC's Surveillance Camera Code of Practice[4] which governs how police and local authorities in the UK procure, design, implement and use surveillance cameras.

[1]This article received a correction notice (Erratum) with the reference: 10.3233/IP-239912, available at http://doi.org/10.3233/IP-239912.

[*]Corresponding author: C. William R. Webster, Stirling Management School, University of Stirling, Stirling, Scotland, UK. E-mail: william.webster@stir.ac.uk; www.crisp-surveillance.com/.

[2]UK Data Protection and Digital Information Bill No.2, URL: https://bills.parliament.uk/bills/3430.

[3]Office of the Biometrics and Surveillance Camera Commissioner (BSCC), URL: https://www.gov.uk/government/organisations/biometrics-and-surveillance-camera-commissioner.

[4]Biometrics and Surveillance Camera Commissioner's Surveillance Camera Code of Practice, URL: https://www.gov.uk/government/publications/update-to-surveillance-camera-code.

Whist there is a noticeable evolution of the technology in recent years there is also a significant change about to happen in the regulatory landscape. Buried in the 2023 DPDI Bill is a clause which abolishes the BSCC and its associated functions. Furthermore, there are no clauses in the Bill setting out the transfer of roles or functions to other agencies – instead, the existing legislative requirements relating to surveillance cameras will simply cease to exist. Here the Bill posits that a new 'Information Commission', the proposed UK's new data protection regulatory authority which will replace the Information Commissioner's Office (ICO),[5] will regulate surveillance cameras in the same way as any other digital technology. For some, this is seen as a retrograde step as the BSCC had raised technical standards, encouraged ethical procurement practices, promoted the importance of public confidence in systems and provided national oversight in the way such systems were deployed. Moreover, the view that surveillance cameras are just data processes fails to recognise how they impact on citizen-state relations. The essence of this review is that it assesses the new governance arrangements for surveillance cameras embedded in the 2023 DPDI Bill. It focusses on the perceived benefits of the legislative change and its perceived ramifications. Here, it is evident that there is deep concern amongst stakeholders within the policy community about the future governance of surveillance cameras in the UK.

2. Methodology

The review is based on research commissioned by the BSCC in spring 2023. The authors have acted completely independently in the preparation of the research findings and have not pursued a specific outcome or agenda in relation to specific provisions in the Bill. The research process underpinning the report incorporated: a review of relevant literature, including grey material; a review of relevant provisions in the Bill; an overview of the roles and functions of the office of the BSCC; and, a series of over 20 semi-structured interviews with leading experts, regulators and stakeholders with insight and expertise in the governance and oversight of surveillance and biometrics. They include leading actors responsible for policing, regulation and service provision. Full details of the interviewees are published in the final report. The final report relating to this research is to be published in autumn 2023 on the website of the BSCC.[6] It will identify and analyse in depth the potential and likely ramifications of the provision of the Bill which specifies the abolition of the BSCC

3. The Regulatory and Governance Landscape in the UK

The existing regulatory landscape in the UK governing the use of surveillance cameras is fragmented and involves multiple agencies and pieces of legislation. Most prominent are the the office of the BSCC and the ICO. The BSCC plays a vital role in the governance of the use of biometric materials and surveillance camera technologies by state and public service agencies. The key roles of the Commissioner are defined in legislation and include statutory and non-statutory activities. Combined these activities provide: important safeguards for users and citizens in a world where fast moving technologies offer the potential for individual and societal harm; guidance for those public agencies wishing to deploy these technologies; and, mechanisms to hold users of these technologies to democratic account. As such, the

[5] Information Commissioner's Office (ICO), URL: https://ico.org.uk.

[6] The Final Report was published on 30th October 2023, URL: https://www.gov.uk/government/publications/changes-to-the-functions-of-the-bscc-independent-report.

Commissioner and the Office, are a significant part of the oversight and stewardship landscape ensuring these technologies are used in the 'public interest'.

The oversight of public space surveillance cameras is realised through statutory functions laid out in Protection of Freedoms Act 2012 (POFA)[7] and realised through the BSCC. The legislative requirements of the Commissioner are principally related to the Government's Surveillance Camera Code of Practice (the Code). POFA places responsibility on the Commissioner to *"(a) encourage compliance with the [Government] surveillance camera code, (b) review the operation of the code, and (c) provide advice about the code (including changes to it or breaches of it)*".[8] The Commissioner also has a duty to report annually to Parliament on progress and activity relating to deployment and use of cameras and adherence to the Code. The Code is expected to cover all aspects of a public space surveillance camera systems, including purpose, procurement, technical specifications and deployment. POFA legislation names those public agencies ('relevant authorities') which are expected to comply with the Code: primary police forces, local authorities and other specified agencies. The Code covers the use of a range of different types of overt cameras, including static and mobile cameras, drones, ANPR and body-worn video cameras. The key purpose behind the legislation is to drive up standards, to ensure 'best practice' and to provide reassurance to the public that the cameras are being used appropriately and within the law.

The Code, as laid before Parliament, is a unique document covering all aspects of a public space surveillance camera system. As a 'code' it is not legally enforceable. However, POFA states that "*relevant authorities must have regard to the surveillance camera code when exercising any functions to which the code relates*". Failure to act in accordance with the Code does not bring criminal or civil liability but may be admissible in relevant legal proceedings. As Section 33(4) of POFA states, *"a court or tribunal may, in particular, take into account a failure by a relevant authority to have regard to the surveillance camera code in determining a question in any such proceedings."* The Code also sets out very clearly, how a designated agency should conceive of a system, how it should be designed, constructed and implemented, including all technical and governance matters. This includes compliance with all relevant legislation and how to approach new technological developments, including AI-driven systems such as FRT. Underpinning the 'purpose' of the Code is the belief that agencies using such systems should comply with legislation and 'best practice'. Adhering to the Code provides these agencies with confidence and certainty regarding how they conduct public surveillance and offers public reassurance over appropriate use.

To deliver the statutory functions set out above a number of activities have been pursued in order to ensure that the Code delivers its purpose and to make sure that those operating camera systems have clear guidance about how they should be used. Whilst many of these activities are not statutory, in that they are not directly specified in POFA, they are crucial in supporting the work of the Commissioner, without these activities the Code could not be realised and oversight not achieved. These activities include the formation of a National Surveillance Camera Strategy,[9] a 'certification scheme', 'self-assessment tool', 'national standards group', 'buyers toolkit', stakeholder forum and various engagement activities (see the BSCC website for full details of these activities). The roles and functions of the BSCC in relation to surveillance cameras combines multiple statutory and non-statutory functions that intertwine and work together with the aims of: fulfilling statutory obligations; raising industry standards; providing guidance;

[7] Protection of Freedoms Act 2012, URL: https://www.legislation.gov.uk/ukpga/2012/9/contents/enacted.

[8] S.34 of POFA https://www.legislation.gov.uk/ukpga/2012/9/enacted/data.pdf.

[9] National Surveillance camera Strategy for England and Wales, URL: https://www.gov.uk/government/publications/national-surveillance-camera-strategy-for-england-and-wales.

and elevating public dialogue around surveillance. In this respect, the Commissioner has become a single point of contact for users, installers and the general public. This model of regulating public space cameras, based on policy and service co-creation, has been recognised as world leading.

Beyond the BSCC a number of other agencies are involved in the governance of surveillance Cameras. This ICO has a key role in governing data processes and has issued guidance for those operating systems.[10] This guidance is generic and applies to commercial operators, public services and residential applications. Here, the focus is compliance with data principles set out in the Data Protection Act 2018.[11] Other agencies worth noting are: the Investigatory Powers Commissioner's Office (IPCO)[12] which independently overseas the use of covert investigation and surveillance powers by public agencies in the UK, including the covert use of public space surveillance cameras; and the Scottish Biometrics Commissioner[13] who has a Scottish geographical remit in relation to biometrics, including digitised faces.

4. Interim Report submitted as Evidence to the House of Commons Public Committee Stage of the Data Protection and Digital Information Bill (11 May 2023)[14]

The following text is a revised version of the Interim Report which was submitted as evidence to the UK Parliament House of Commons Public Committee Stage of the Data Protection and Digital Information Bill. As such, it is recorded in Hansard,[15] the official report of all UK Parliamentary debates. The main changes to the text are to make it more readable for an international audience.

1. Society is witnessing an unprecedented acceleration in the capability and reach of digitally mediated surveillance technologies. These new and advancing technologies hold clear potential to enhance public safety yet also have the capacity for enormous harm. The possibilities for integrated surveillance technology, driven by Artificial Intelligence (AI) and supported by the internet, create genuine public anxieties over civic freedoms. These anxieties exist across almost all jurisdictions. Within this context, consideration of genuine, meaningful and trustworthy governance and oversight is urgent and pressing.

2. In its current form, the Bill will delete several surveillance oversight activities and mechanisms that are set out in legislation and arise from the fulfilment of statutory duties placed on Commissioners. Prominent among these is the tabled abolition of POFA legislative requirements to (a) appoint a Surveillance Camera Commissioner and (b) to publish a Surveillance Camera Code of Practice, which offers governance coverage far beyond data-related issues. The Code is realised through the national Surveillance Camera Strategy, which would also disappear. The value of the Code and Strategy for providing surveillance oversight, raising standards in surveillance practice, delivering guidance for camera users, and offering transparency and public confidence is set out in more detail below. The POFA Act was enacted in 2012 to provide citizens with safeguards in an era where law enforcement agencies were given more intrusive powers to combat terrorism.

3. Other functions of the Biometrics and Surveillance Camera Commissioner are manifold and comprise both judicial and non-judicial elements. Key activities and benefits include, but are not limited to:

[10] ICO guidance on using CCTV systems, URL: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/guidance-on-video-surveillance-including-cctv/.

[11] UK Data Protection Act, URL: https://www.gov.uk/data-protection.

[12] Investigatory Powers Commissioner's Office (IPCO), URL: https://www.ipco.org.uk.

[13] Scottish Biometrics Commissioner, URL: https://www.biometricscommissioner.scot.

[14] BSCC submitted evidence at Reporting Stage of the 2023 Data Protection and Digital Information Bill, URL: https://bills.parliament.uk/publications/51173/documents/3425.

[15] Hansard, URL: https://hansard.parliament.uk.

developing, and encouraging compliance with the Code; raising standards for surveillance camera developers, suppliers and users; public engagement; building legitimacy and consent for surveillance practices; annual reporting to Parliament via the Home Secretary; convening expertise to support these functions; and reviewing all National Security Determinations and other powers by which the police can retain biometric data.

4. Surveillance oversight is historically and currently overburdened and under-resourced. Activities undertaken by the Surveillance Camera Commissioner have extended the Commissioner's role, not in terms of regulatory overreach, but to compensate for this shortfall, thereby raising standards and increasing professionalism across the sector. While not defined in the original legislation (POFA), these activities have arisen *as a result of successive Commissioners fulfilling their statutory duties*. The Bill proposes the erasure of these functions and, by extension, their associated value to society. As one expert interviewee for the report expressed, in relation to a new 'Information Commission' absorbing the BSCC role "*the Bill makes no provision for absorption whatsoever. It just deals with extinction*". For example, the Bill contains no provision for continuing the work of driving up standards for the development, procurement, adoption and use of surveillance cameras, a programme of work widely applauded across police, practitioner and industry communities.

5. The value of these activities is widely recognised and easily evidenced across civil society organisations, industry professionals, Parliament, and law enforcement communities – and is evidenced in the final report for this research. In relation to law enforcement communities, it is important to acknowledge significant evidence of (a) police support for the BSCC role and (b) requests for clarity over appropriate uses of surveillance tools.

6. The Commissioners' functions are not regulatory in the same sense as the Information Commissioner. Whilst the ICO tends to work with a formal regulatory framework the BSCC co-creates standards and rules with stakeholder communities. This difference has several implications. First, the roles are not directly comparable with ICO. Consequently, the impact of BSCC functions arises through different and sometimes less visible or direct means. It also means elements cannot be directly "lifted and shifted" into a different regulatory format and destination.

7. Also crucial is that these activities extend significantly beyond matters of data use. Considering surveillance impacts and harms purely in terms of data protection is widely recognised as a highly restrictive and selective framing. It is also widely acknowledged that rights concerns arising from surveillance are not reducible to issues of privacy alone. One could further argue that adding POFA to the existing data protection landscape constituted recognition of this over a decade ago.

8. Advanced digital surveillance, particularly AI-driven forms, is a global phenomenon. The Bill's reduction of surveillance-related considerations to data protection compares unfavourably to regulatory approaches in other jurisdictions. Many have started from data protection and extended to cover other germane issues. Examples include EU proposals around an AI Commissioner, and the MEP (Members of the European Parliament) vote to support a compromise text for the AI Act[16] that bans public uses of remote biometric identification (including facial recognition) on 11 May 2023.

9. Examples of these wider activities of the BSCC and their impact are:

a. The BSCC's recent success in addressing widespread use of Chinese cameras with known cyber vulnerabilities in sensitive UK sites.[17] The development of these tools is also associated with

[16]European Union Artificial Intelligence Act, URL: https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence.

[17]Report on use of Chinese Surveillance Cameras in the UK conducted by the BSCC and published February 2023, URL: https://www.gov.uk/government/news/uk-policing-shot-through-with-chinese-surveillance-technology.

significant human rights abuses.

b. Automatic Number Plate Recognition (ANPR) surveillance in the UK operates on one of the largest databases in Europe. It has grown from a local to a national network, from focused counterterrorism uses to monitoring urban clean air zones and car park ticketing. Credible estimates suggest a likely 100 million daily ANPR data acquisition points from 2024. ANPR grew with little data protection-related scrutiny. The BSCC role brought proactive engagement that established an independent advisory group to provide standards and governance for this technology, and to convene key stakeholders (including the police) into this activity.[18]
c. The BSCC established current guidance to law enforcement concerning lawful and ethical use of FRT. This guidance transcended data protection issues, addressed standards, transparency, ethics, human decision-making and the authorisation of deployments. It is now incorporated into National Police Chiefs' Council (NPCC) guidance.[19] The NPCC brings UK police leaders together to set law enforcement priorities and direction.

10. The Bill removes reporting obligations to Parliament currently embedded in the Commissioner's statuary obligations. This removes a mechanism for assuring Parliament and the public of appropriate surveillance use, affecting public trust, and legitimacy invested in surveillance practices. We are at a critical moment concerning public trust in institutions, particularly law enforcement, something central to the success of UK policing. As drafted, the Bill reduces public visibility and accountability of related police activities.

11. The independence of oversight is similarly crucial to public trust. Clause 28 of the Bill requires the new 'Information Commissioner' to respond more explicitly to "strategic priorities" designated by the Secretary of State. This may reduce independence of the regulator and risk diluting public trust and confidence in the paramount condition of independent oversight.

12. The Bill seeks to transfer some responsibilities of the BSCC outlined in POFA (fingerprints and DNA) to other entities, allowing others to lapse, and makes no provision to the functions and oversight activities arising from several POFA Commissioner duties. One argument has been that many of the BSCC activities are not defined in POFA and therefore cannot be transferred. However, the Surveillance Camera Code of Practice enables the BSCC to provide and issue guidance across the surveillance landscape. It also requires 'relevant authorities' to comply with its principles. These are two powerful requirements which hold state institutions to account and yet the Code is to be deleted. Several issues arise from this decision to restrict formal transfer of only those biometric responsibilities specified in POFA and deleting anything relating to surveillance camera standards. These are explored below.

13. Biometric technology is expanding and diversifying at an unprecedented rate. Specifying only those biometric techniques mentioned in legislation of over a decade ago challenges notions that the Bill is "future proofed". By designating fingerprints and DNA to the Investigatory Powers Commissioner (IPCO) also risks a de facto segregation in the oversight of different biometrics techniques, where the governance of all other forms rests elsewhere. It removes any statutory duties from the interface of biometrics and surveillance, the policy basis on which UK Ministers recently combined the 'biometric' and 'surveillance

[18]Correspondence between the BSCC and the UK Secretary of State for Transport, published 11 October 2023, URL: https://www.gov.uk/government/publications/letter-to-the-secretary-of-state-for-transport/letter-to-the-secretary-of-state-for-transport-risks-to-the-anpr-system-accessible-version.

[19]See for example, NPCC Face Recognition Technology Board, URL: https://www.npcc.police.uk/SysSiteAssets/media/downloads/publications/disclosure-logs/national-crime-coordination-committee/2023/155-2023-npcc-frt-board-minutes-2023.04.20_v1-draft-with-redaction-21062023.docx.pdf.

camera' functions. Moreover, one could argue that given the potential for collateral intrusion, remote biometric surveillance resonates more closely with IPCO's remit than fingerprints and DNA.

14. The original proposal consulted on was for all biometric and overt surveillance functions to be absorbed by the ICO. The Bill reflects the view of many that biometric casework sits more naturally with IPCO. Expert interviewees for the report highlighted how most gaps left by this Bill could also be addressed if responsibility for the Surveillance Camera Code of Practice (only recently approved by Parliament) also moved under IPCO. This would harmonise all functions for oversight of traditional and remote biometrics in policing under one established and internationally regarded judicial oversight body. Such a move could also add genuine 'future proofing' by anticipating the increasing potential for blurring boundaries between overt and covert surveillance brought by new advances in technology.

15. Academic research has demonstrated significant public concern over one such form of remote biometric monitoring, FRT (Fussey & Murray, 2019). Other experts and public bodies have called for more detailed rules for uses of this technology in public. A stark contrast exists in the working of the Bill between mention of relatively uncontroversial decades old biometric techniques and the cutting-edge technologies currently animating public debate. Reference to "remote biometric identification" could be one entry point to addressing this issue.

16. This issue is made more pressing given the Policing Minister expressed his desire to embed facial recognition technology in policing and is considering what more the Government can do to support the police on this.[20] Such embedding is extremely likely to include exploring integration of this technology with police body worn video. At the 2023 Conservative Party Conference, the Policing Minister also expressed a desire for passport data to be used in conjunction with face recognition, which would be a purpose beyond which the data was originally collected.[21]

17. Excluding IPCO, expert interviewees questioned the suitability of alternative venues for surveillance and biometric oversight. This issue invokes several considerations. One concerns thematic coverage and the spectrum of potential surveillance harms that transcend data-related matters. Additionally, two organisations have been highlighted as possible venues for absorbing public surveillance oversight functions: a modified Information Commissioner's Office and, separately the Equality and Human Rights Commission (EHRC).[22] Taking these in turn, POFA oversight is mostly limited to the activities of public bodies. Existing data protection regulation covers both public and private entities. Housing oversight in the later may provide wider scope and address complexities of regulating public-private surveillance activities. However, research has demonstrated the limited role data protection controllers have played in providing enforcement against breaches in relation to video surveillance in a significant number of countries including the UK. In addition, without further specific legislation the EHRC are arguably not currently constituted to legitimately address many of the functions and activities outlined above and the totality of surveillance oversight needs.

18. It is widely accepted that current oversight of complex surveillance practices is considered patchy and requires simplification. Simplifying oversight has been consistently stated as a key aim for the Bill. However, such simplification entails at least three further considerations:

a. Calls for simplified oversight correctly include a requirement for companion policies for implementation and compliance. These translate abstract principles into clear guidance and standards

[20] Reported in an interview for this research by the BSCC.

[21] As reported in the media, URL: https://www.computerweekly.com/news/366554287/Policing-minister-wants-to-use-UK-passport-data-in-facial-recognition.

[22] Equality and Human Rights Commission, URL: https://www.equalityhumanrights.com/en.

for users of biometric and other surveillance technologies while offering mechanisms for auditing compliance. This relationship between law and policy was central to the *Bridges* Court of Appeal judgement[23] on facial recognition technology in light of which the Home Secretary amended the Surveillance Camera Code of Practice. The Bill contains no mention of guidance or compliance mechanisms aside from those pertaining to data management. The absence of requirements for guidance and to ensure compliance generates vulnerabilities for users of these technologies and for the rights of individuals subjected to them, and is particularly important given the significant uncertainties brought by emerging technologies.

b. Simplification is an important ambition but should not come at the expense of meaningful oversight. For example, as one expert interviewee remarked, "*why is it that simplification is more important than raising standards?*"

c. What may appear as simplification in organisational terms does not naturally translate into a simplification in a practical sense. As stated above regarding different biometric techniques, this ambition for simplification may actually complicate the oversight landscape. Removing a Commissioner who proactively interfaces with developers and users of surveillance technologies may generate future difficulties. For example, it may take longer for aspiring technology users to access knowledge. In addition to impacting public resources, pressing ahead with surveillance deployments before such advice is received may generate greater exposure to litigation for public bodies. Alternatively, the absence of such information may lead users to highly conservative interpretations of the law which may dissuade legitimate uses of surveillance technology for public safety.

5. Concluding comments

The above text sets out a summary of the ramifications of abolishing the BSCC as proposed by the DPDI Bill. Contemporary digital technologies are evolving rapidly at the moment, especially in the realm of AI. This manifests itself in relation to surveillance cameras and biometrics in the development of applications like FRT, gate analysis and emotional sensing surveillance. These technological developments are happening in the UK at the same time as a substantial reworking of the regulatory landscape overseeing governance and oversight. In particular, the abolition of the BSCC, as proposed by the DPDI Bill, removes all direct regulation of these technologies, and explicitly assumes the new generalist 'Information Commission' (replacing the ICO) will provide satisfactory regulation of these technologies. This position fails to recognise that the provision of surveillance cameras and the use of DNA goes beyond mere data processes, and that there is significant regulator activity around procurement, standardisation, certification and training for example, not to mention governing the citizen-state relationship. With these shortcomings in mind, it becomes important to consider the ramifications of the Bill, and the likely outcomes to regulatory practice and technological development. On the one hand, it can be argued that the removal of technological barriers will allow for innovation and encourage public agencies to deploy contested technologies like FRT, whilst on the other, there is a view that significant citizen protections have been removed and the potential for personal and societal harm has increased. It is the view of the authors that the provisions of the Bill relating to citizen safeguards and the provision of surveillance cameras are a retrograde step and will create a vacuum in the governance of public space surveillance camera systems. As a final comment, it is important to note that the provisions of the Bill are likely to change as it

[23] As reported by the BBC in 2020, URL: https://www.bbc.co.uk/news/uk-wales-53734716.

passes through the legislative process in 2023–4 and that it is possible that amendments to the Bill retain elements of the functionality of the BSCC. Whatever happens, it is clear that the governance landscape for surveillance cameras will change in the furure.

Acknowledgments

This contribution is based on research commissioned by the office of the Biometrics and Surveillance Commissioner in spring 2023. The research was conducted independently by the authors and published as an interim report in May 2023, with a full report to be published in autumn 2023. The text presented here derives from the interim report and is published in Hansard (UK Parliament) as part of the Data Protection and Digital Information Bill. It was published as evidence at the House of Commons Committee reporting stage by the Biometrics and Surveillance Camera Commissioner.[24] The final full report will be published on the website of the Biometrics and Surveillance Camera Commissioner.[25]

References

Fussey, P., & Murray, D. (2019). *Independent report on the London Metropolitan Police Service's trial of live face recognition technology*. Human Rights Centre, July 2019, URL: https://repository.essex.ac.uk/24946/1/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report-2.pdf.

Fussey, P., & Webster, C.W.R. (2023). *Independent report on changes to the functions of the Biometrics and Surveillance Camera Commissioner arising from the Data Protection and Digital Innovation Bill* (No.2) 2023. CRISP, Office of the Biometrics and Surveillance Camera Commissioner. 6th October 2023, URL: https://www.gov.uk/government/publications/changes-to-the-functions-of-the-bscc-independent-report.

Webster, C.W.R. (2009). CCTV policy in the UK: Reconsidering the evidence base. *Surveillance and Society*, *6*(1), 10-22.

Webster, C.W.R. (2019). Surveillance cameras will soon be unrecognisable – time for an urgent public conversation. The Conversation, Published: 18 June 2019, URL: https://theconversation.com/surveillance-cameras-will-soon-be-unrecognisable-time-for-an-urgent-public-conversation-118931.

[24] BSCC submitted evidence at Reporting Stage of the 2023 Data Protection and Digital Information Bill, URL: https://bills.parliament.uk/publications/51173/documents/3425.

[25] BSCC website: https://www.gov.uk/government/organisations/biometrics-and-surveillance-camera-commissioner.