OFFICE OF THE BIOMETRICS
AND SURVEILLANCE
CAMERA COMMISSIONER

The use of overt surveillance camera systems in public places by police forces in England and Wales: An assessment of compliance with section 33(1) of the Protection of Freedoms Act 2012 and the Surveillance Camera Code of Practice

February 2023

Contents

Background

1. Following similar surveys conducted in 2017 and 2019, the Biometrics and Surveillance Camera Commissioner wrote to the chief officers of all 43 geographical police forces in England and Wales, the Ministry of Defence, British Transport Police, the National Crime Agency, and the Civil Nuclear Constabulary in June 2022, asking for details of their use and governance of all overt surveillance camera systems deployed in public places. This included CCTV, ANPR, body-worn video, unmanned aerial vehicles (more commonly referred to as drones), helicopter-borne cameras, and facial recognition technology, as well as any other relevant systems.

2. The response rates for previous surveys had been 100%, so it was disappointing that there were some noticeable absences in returns this time, including some of the larger police forces such as Greater Manchester Police, Merseyside Police, and the National Crime Agency (NCA). Despite accepting returns received more than three months after the closing date, the return rate for the 2022 survey dipped to 91%. The Commissioner is grateful to the forces and organisations which took the time to complete and return the survey, a list of whom is at annexed to this paper.

3. The survey was structured thematically, replicating subject areas covered in surveys conducted by previous Surveillance Camera Commissioners, and asked 119 questions requiring a mix of quantitative and qualitative responses. This paper builds on initial observations on the survey responses published in November 2022[1], and presents the information provided to us by forces, highlights key findings, and makes some high-level observations.

Summary findings and observations

4. For all types of surveillance technology covered by this survey other than helicopter-borne cameras and facial recognition technology, at least one respondent stated that their equipment was manufactured or supplied by a surveillance company outside the UK about which there have been security or ethical concerns.

5. A number of respondents stated that there was a need for further guidance to be issued around the use of existing technology where there are security and/or ethical concerns around its source, although they did not make any suggestions as to who should issue it. This call has become more pertinent since the November 2022 statement by Rt Hon Oliver Dowden MP on Chinese-made surveillance cameras on Government buildings, the policing position on which needs to be clarified.

[1] https://www.gov.uk/government/publications/police-survey-2022-initial-analysis/initial-analysis-of-the-2022-police-survey-returns

6. It is clear that the full capability of some of the technology owned by some respondents is not fully understood, be that at the point of purchase or further down the line when software updates are downloaded. This reinforces the need for thorough due diligence of all aspects of the equipment as an early part of the procurement process.

7. Very little was reported about the use by forces of penetration testing when considering the cyber security of their equipment. Ethical penetration testing is as important as technical testing, and responses gave no evidence of forces using the National Decision Making model in their procurement processes.

8. Not all respondents have completed data protection impact assessments for all the technology under discussion in this survey. This is a concern, particularly given the government's position that much of the work currently undertaken by the Surveillance Camera Commissioner is a data protection issue, and already falls under the remit of the ICO notwithstanding any legislative proposals to abolished the Surveillance Camera Code by the Data Protection and Digital Information Bill.

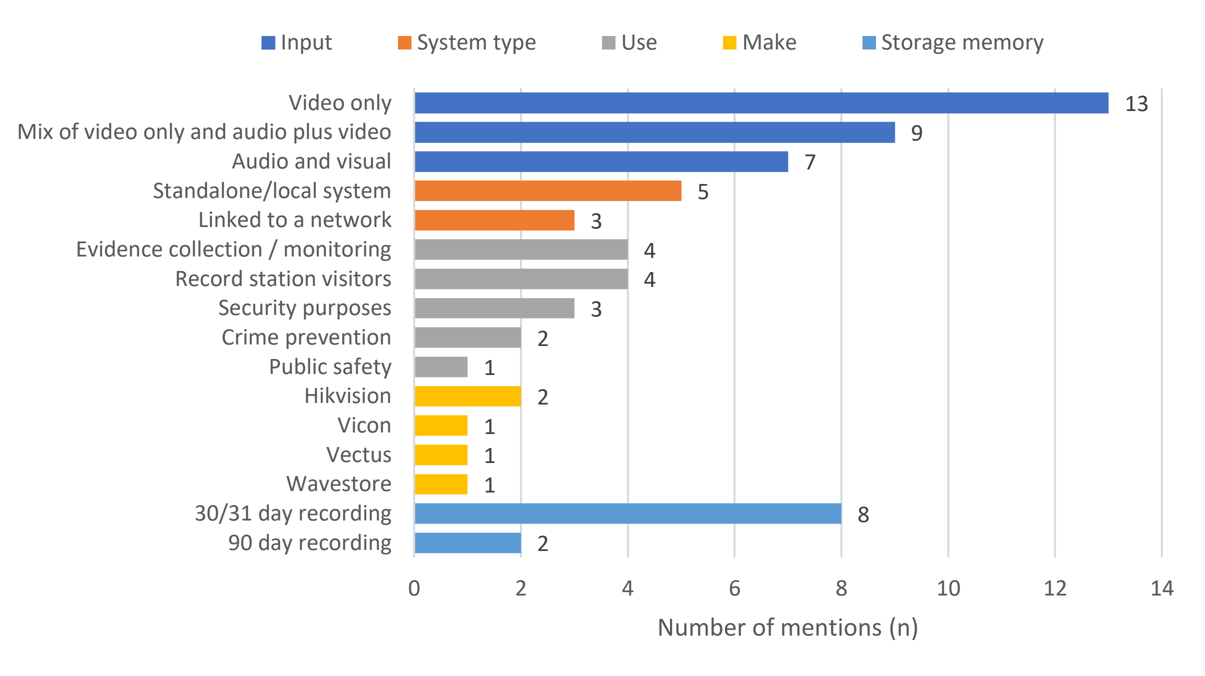
9. There are clearly issues with existing procurement processes, if a strict application of the current rules results in a force acquiring technology from a manufacturer or supplier about which there are legitimate security or ethical concerns. It is hoped that additional guidance will be made available to help mitigate this, but there remain concerns about whether advice was sought when the existing equipment was purchased and, if so, who provided that advice.

10. Closure of the Office of the Biometrics and Surveillance Camera Commissioner in the event that Parliament passes the Data Protection and Digital Information Bill leaves questions around the future of oversight and regulation of public-space surveillance. The responses from this survey underline the fact that the more the police can do with public space surveillance, the more important it will be to show what they are *not* doing, to ensure trust and confidence. This will require trusted partnerships, with trusted partners working in a transparent and accountable way.

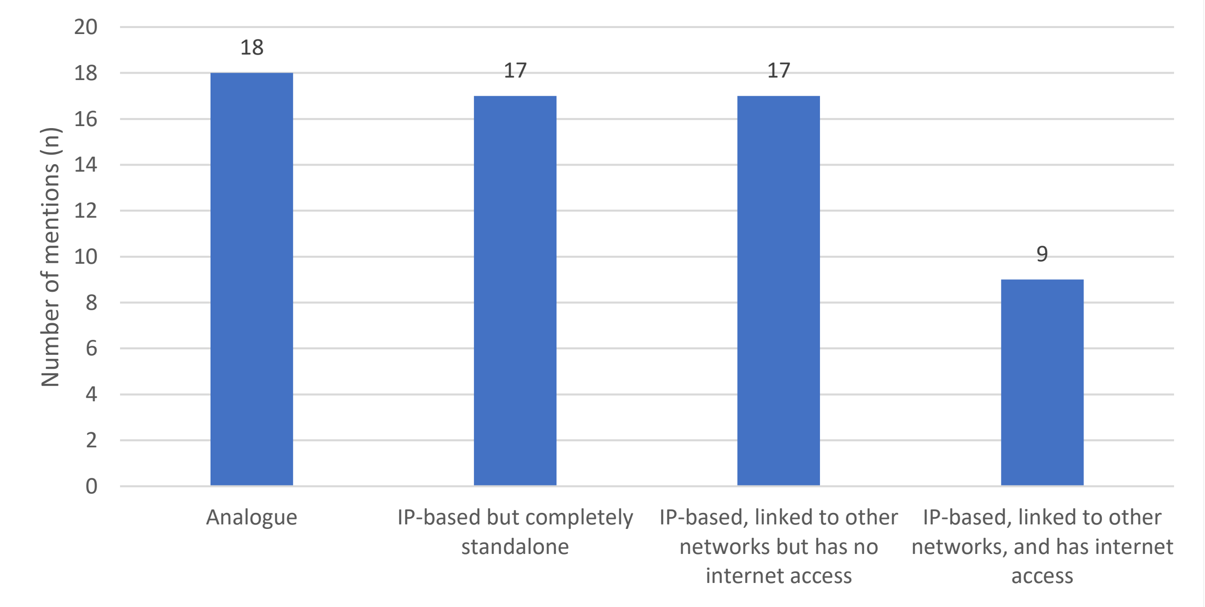
Survey responses

Surveillance camera systems – internal CCTV

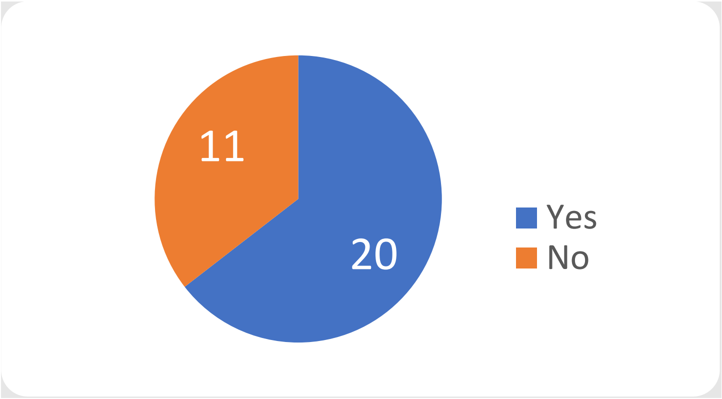
Q: If your force operates internal public space CCTV, please provide a description of the system and its capabilities, including the number of cameras and whether the system uses visual only or audio-visual capability



Q: What network topology does your organisation use for the video surveillance system?



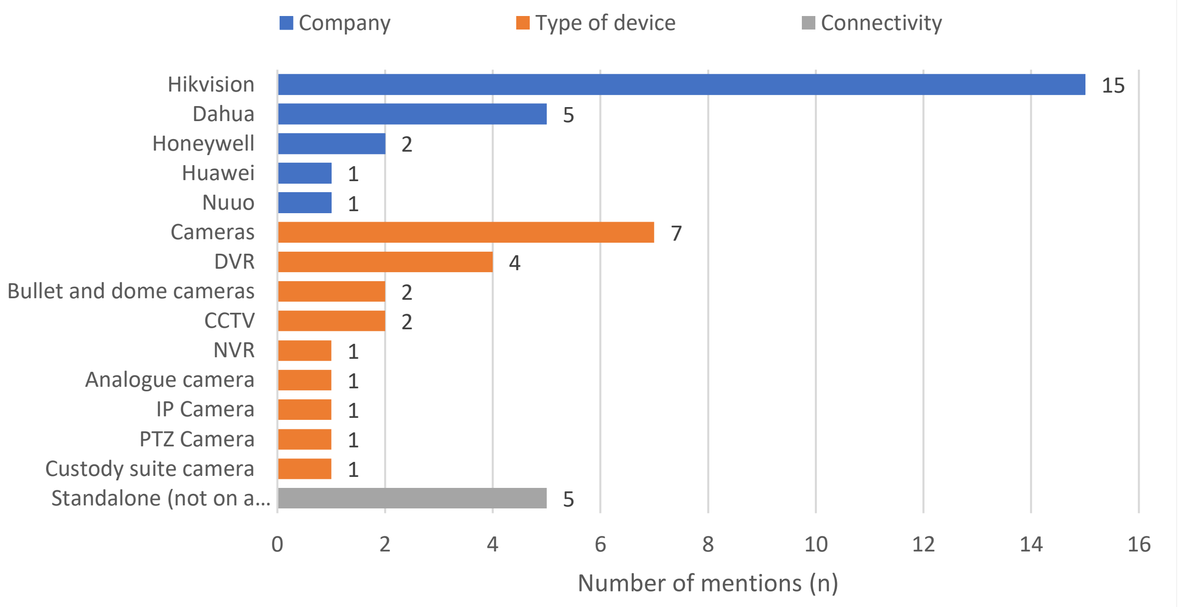
Q: Is this CCTV system verifiably compliant with Section 33(1) of PoFA and the principles of the Surveillance Camera Code of Practice?



11. Reasons given for systems being non-compliant included that the review of CCTV systems was still ongoing (3 responses), or that there were areas for improvement (3 responses). 2 respondents simply said that their CCTV systems were not DPIA-compliant, whilst another 2 stated that they may also be following other policies. To rectify non-compliance, the most commonly cited future solution (4 respondents) was to implement a strategy that delivered compliance, whilst others stated that the intention was to undertake work to better understand their level of non-compliance.

12. It is concerning that, when posed the question, only 19 respondents stated that their force or organisation had completed a Data Protection Impact Assessment (DPIA). Those that did variously used an internal/corporate template or the Biometrics and Surveillance Camera Commissioner's template. We continue to encourage organisations to publish the DPIAs on their external website.

Q: Does your system have any cameras or equipment manufactured or supplied by surveillance companies outside the UK about which there have been any security or ethical concerns?

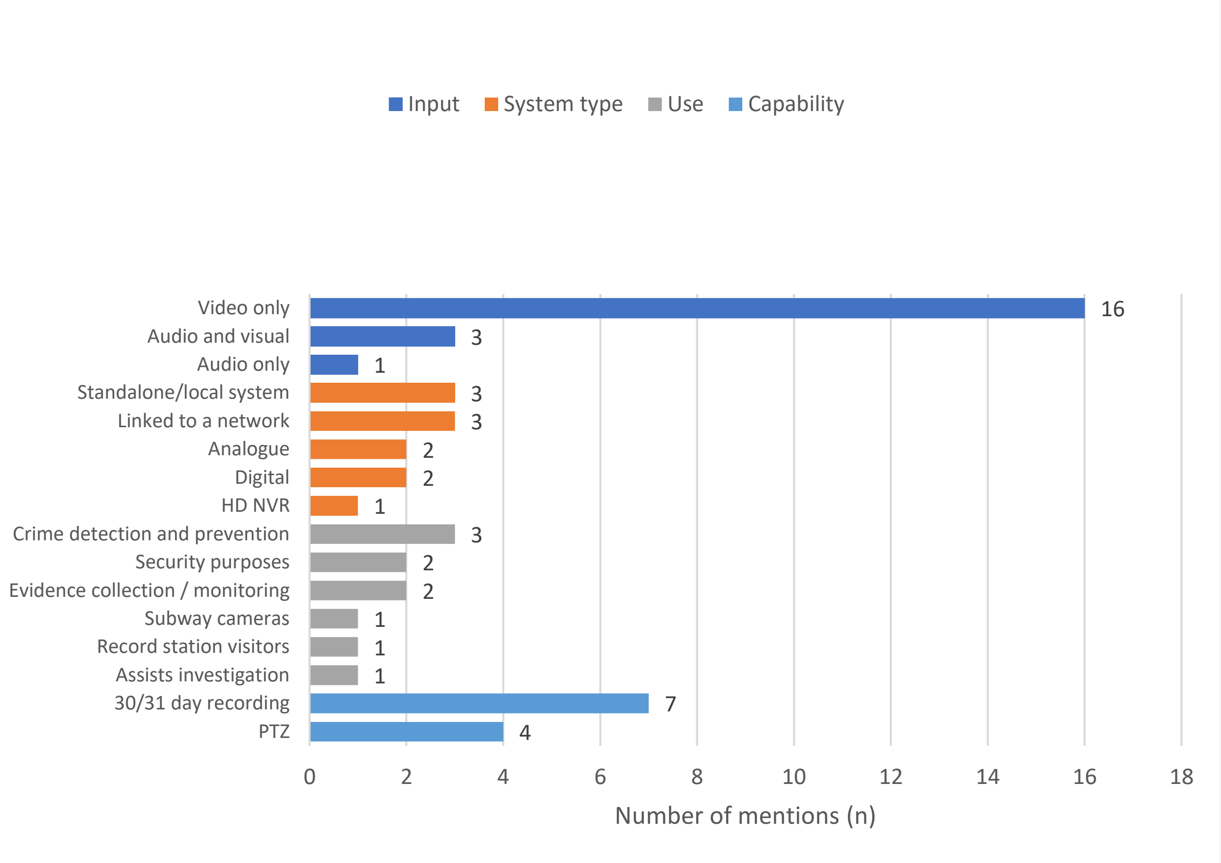


13. It is of interest that 5 respondents highlighted that their non-UK CCTV technology is standalone, and not connected to a network, which may be an attempt to demonstrate a reduced risk in their use. But this poses a question about how such technology is maintained, what system testing is undertaken, and whether and how they carry out software updates. If no refresh is done, then that raises its own risk. However, if forces do download system updates, there is a question as to whether the capability contained within that update is fully understood. We do not know how rigorous the testing of the update is in each case. This is of concern beyond CCTV and is pertinent to many of the areas of technology included in this survey. Some respondents suggested that clearer government guidance on CCTV procurement and suppliers would be helpful. In light of the Rt Hon Oliver Dowden's Written Ministerial Statement in November 2022 on Chinese-made surveillance cameras on Government buildings[2], this would seem very sensible, and whether that sits with the National Police Chiefs' Council, the College of Policing, the Information Commissioner's Office and/or others is a discussion that urgently needs to take place.

[2] https://questions-statements.parliament.uk/written-statements/detail/2022-11-24/hcws386

Surveillance camera systems – external CCTV

Q: If your force operates external public space CCTV, please provide a description of the system and its capabilities, including the number of cameras and whether the system uses visual only or audio-visual capability



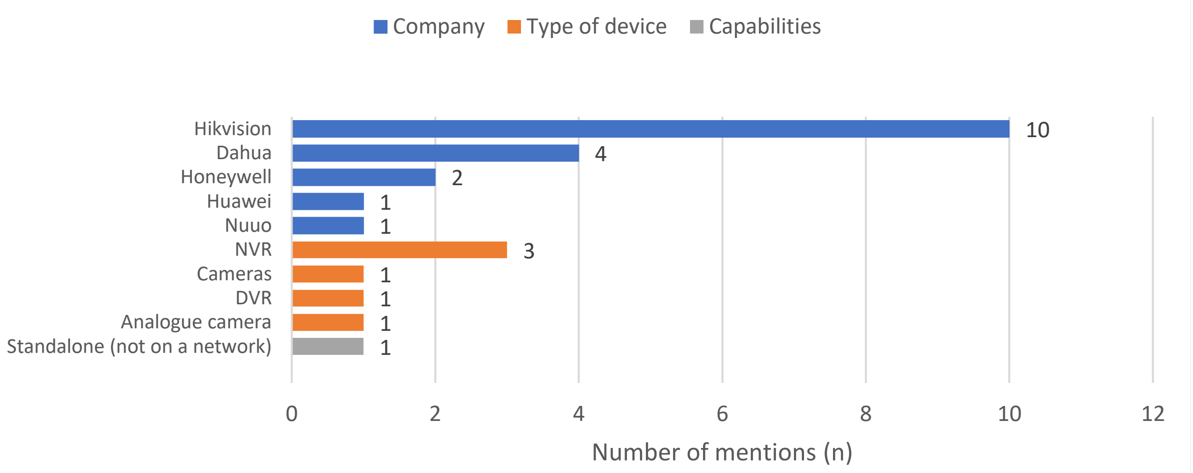
14. 29 respondents stated they operate external public space CCTV, and 28 went on to describe the network topology as variously being IP-based but completely standalone (17 respondents), IP-based and linked to other networks but with no internet access (14), analogue (7) and IP-based linked to other networks with internet access (2).

15. 19 respondents stated that their external public space CCTV was compliant, compared with 7 who stated it was not. Of those 19 compliant respondents, 15 had completed the BSCC self-assessment tool, and 4 had not. 17 respondents stated that a DPIA was in place for the system.

16. There were several reasons given for non-compliance. Single mention rationales include that it was highlighted by a recent review (perhaps implying they have not yet had time to rectify), low risk of non-compliance, no internal procedure for designing the CCTV system, an ongoing review, the system being compliant but with improvement needed, and legacy police sites which are not maintained/compliant. Similar to reported intentions for non-compliant

public space CCTV, future aims to ensure compliance include conducting a review to understand the level of non-compliance (2 respondents) or that a strategy is currently being delivered to ensure compliance (2 respondents).

Q: Does your system have any cameras or equipment manufactured or supplied by surveillance companies outside the UK about which there have been any security or ethical concerns?

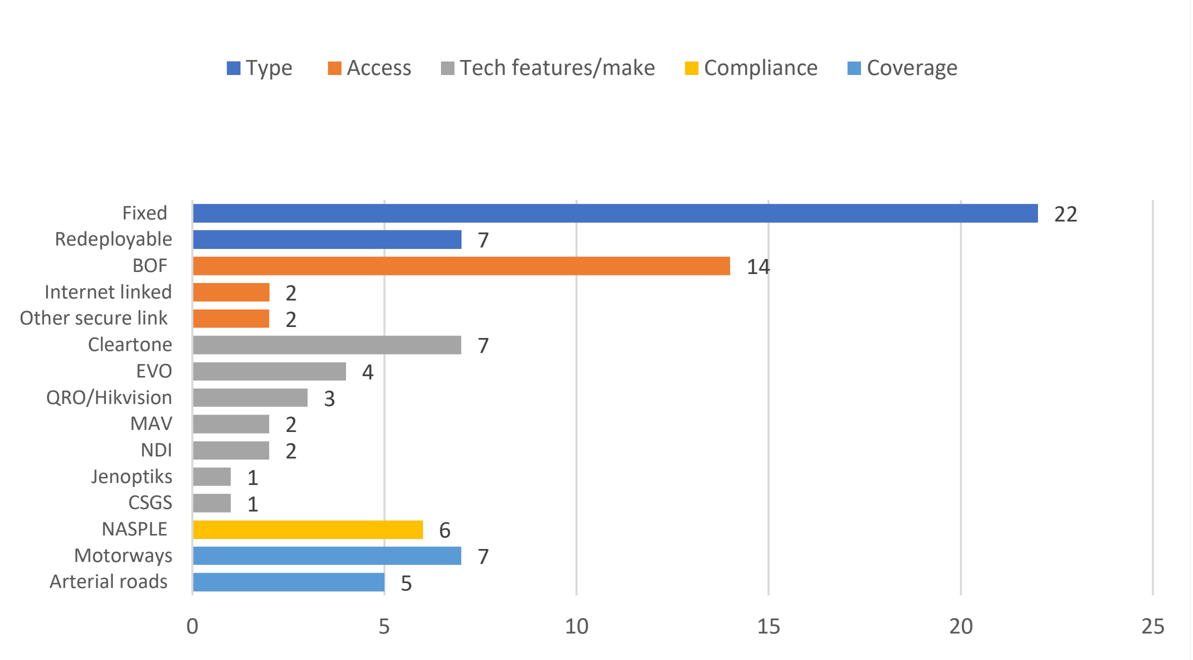


17. As noted above in relation to internal CCTV, two respondents stated that further, clearer guidance on procurement policies would be helpful, although they did not go on to suggest who that guidance might come from.

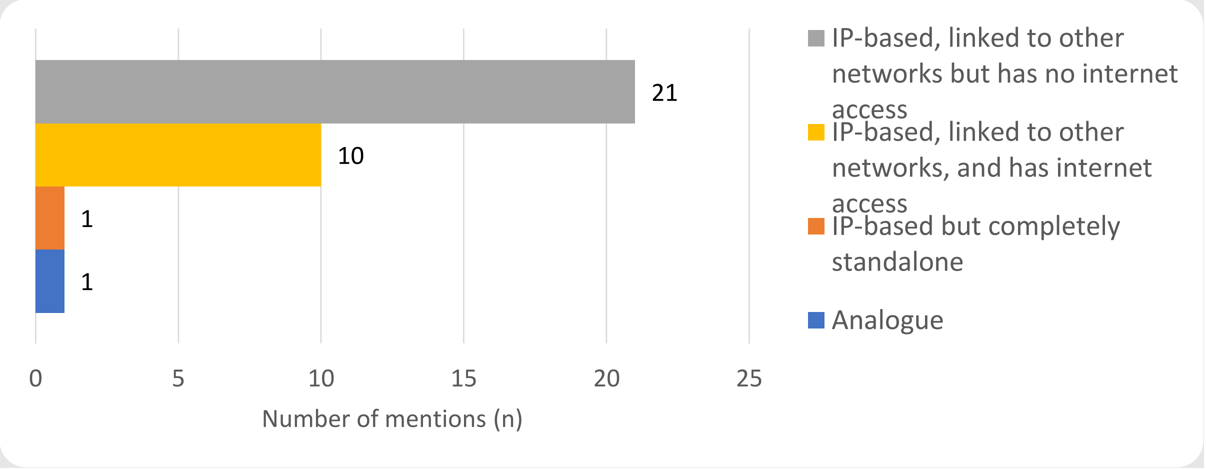
Automatic Number Plate Recognition (ANPR) – fixed site

18. All but one respondent confirmed that they use ANPR. 22 stated that they used fixed ANPR, and 7 said their ANPR could be redeployed. 19 organisations stated that their ANPR system was being operated as part of a collaborative approach with other organisations, 16 were not.

Q: If your forces use ANPR, provide a description of the system and its capabilities, including camera numbers of known.

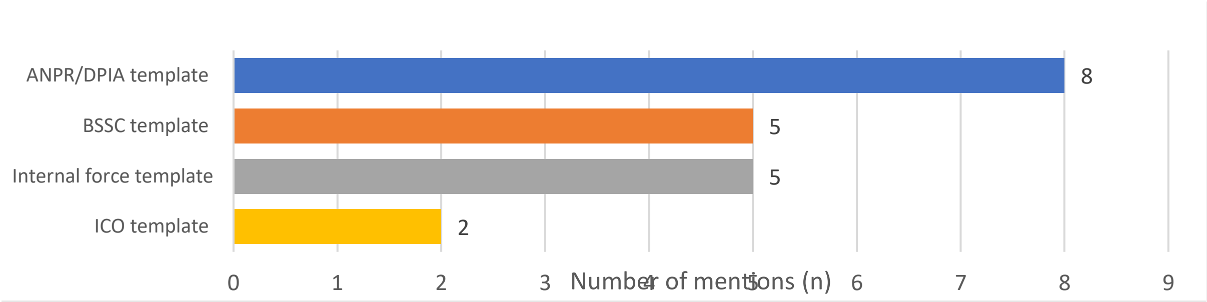


Q: What network topology does your organisation use for ANPR?

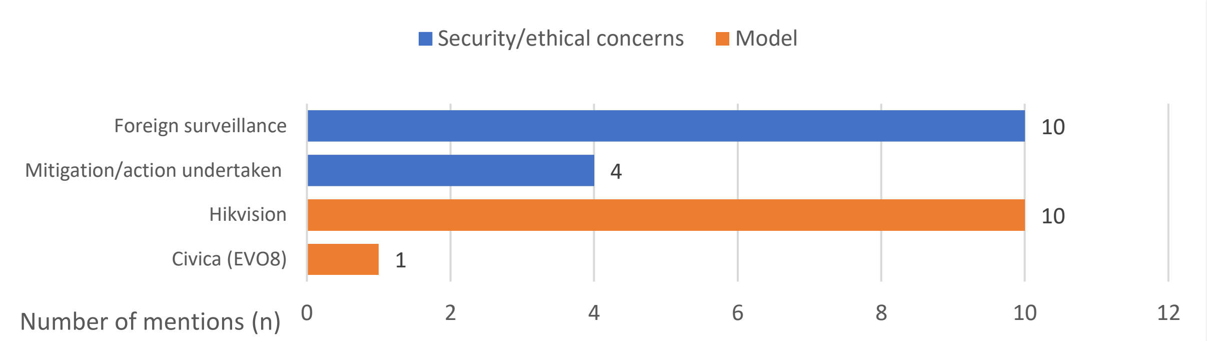


19. All forces stated that their ANPR was compliant with section 33(1) PoFA and the principles of the surveillance camera code, 31 of whom said the BSCC Self-Assessment Tool had either been completed, or was in the process of being completed. 2 other forces stated that compliance was achieved through internal policies and procedures. Where systems were not compliant, it was stated that reviews were ongoing, that they were compliant but there were areas for improvement, or that a review needs to take place to understand the level of non-compliance.

Q: Has a Data Protection Impact Assessment or Human Rights Impact Assessment been completed for the system?



Q: Does your system have any cameras or equipment manufactured or supplied by surveillance companies outside the UK about which there have been any security or ethical concerns?



20. 11 forces state they have security or ethical concerns about the ANPR equipment they are using. Ten mention having QRO/Hikvision ANPR equipment and one mentions having Civica equipment. The average number of cameras used by each force, of which the force has security/ethical concerns, is 39. This ranges from a low of 2, to a high of 165.

ANPR – dashboard mounted

21. 32 forces operated dashboard-mounted ANPR, some of which were as part of collaboration with other forces. The systems were variously reported as being internet-linked, part of a back office facility, or encrypted. Most commonly cited makes of this type of ANPR are Cleartone (7), NASCAR (2), QRO/Hikvision (2), Puma (1) and Jenoptiks (1). This type of ANPR technology was all either IP-based technology which linked to other networks, and which either did not have internet access (19) or did (9).

22. 28 of the 32 forces reporting that they operate dashboard mounted ANPR said that the Self-Assessment Tool has been completed for the system, with 5 reporting that SAT had been published on their website. Other means of compliance were reported as being via NASPLE[3] (3 respondents), Regulation 109 (4 respondents) and Regulation 106 (1 respondent).

[3] NASPLE is the National ANPR Standards for policing and law enforcement

23. Only 23 of the respondents stated that a DPIA had been completed for their dashboard-mounted ANPR, 5 of whom said they used the BSCC template, and 5 of whom used an internal template. What that means in terms of data protection or human rights compliance for the remaining forces who did not claim to have completed a DPIA is not clear from the responses received. Who this might sit with in the future, for instance the ICO or the College of Policing, is for others to decide, but is highlighted as a point for consideration.

24. 4 forces had security or ethical concerns about whether manufacturers of their dashboard mounted ANPR systems were supplied by companies outside the UK. QRO/Hikvision and Jenoptiks were each cited once as suppliers of concern by respondents. Of the forces that did provide further detail, the majority stated that all equipment had been procured in line with force procurement policies and to existing Government procurement advice, of which ethical considerations are an integral factor. This feels at odds with the fact that concerns do still exist, despite following established procurement rules, and points to the need to ensure thorough due diligence as an early part of the procurement process.

Other ANPR systems

25. 13 forces stated they operate other ANPR systems, which included mobile camera enforcement or portable ANPR systems. All of these other systems were image only cameras; none were audio enabled. In terms of manufacturer, QRO/Hikvision is most commonly reported (6 respondents), then Hota Laser (1 mention). Only 2 forces raised possible ethical concerns relating to their ‘other’ ANPR system, citing the companies of concern as Truvelo and Hikvision.

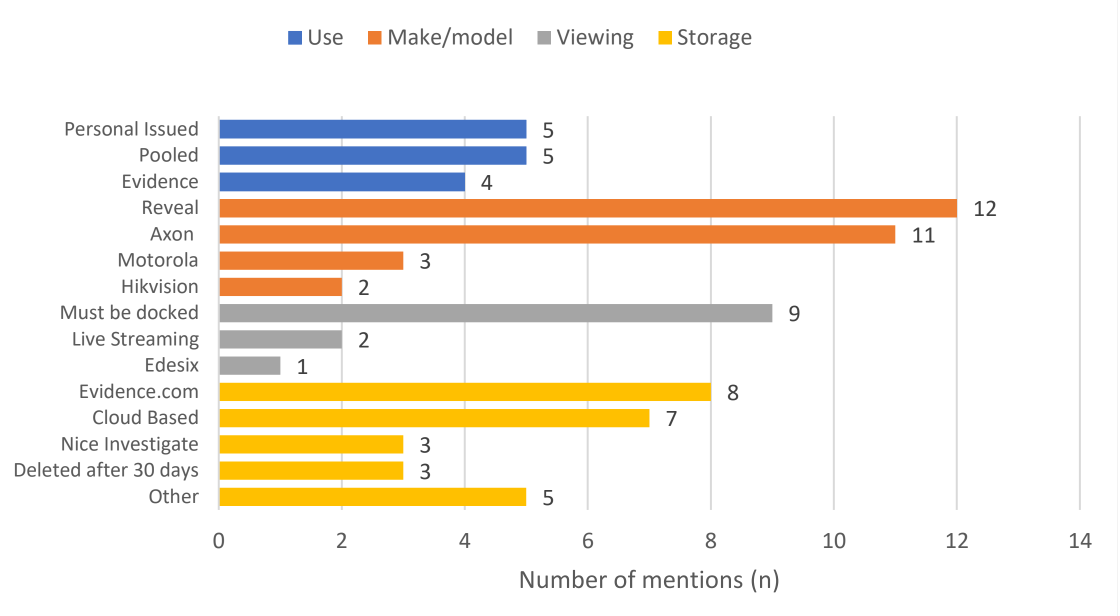
26. 10 forces stated that they had completed the Commissioner’s Self-Assessment Tool (SAT) and were compliant, and two reported that they have completed subsequent reviews of the SAT. 2 forces also confirmed that the completed SAT had been published on their website. 3 forces believed they may be non-compliant according to the SAT, with two of those stating that they were compliant with NASPLE and the National Authority, and the third endeavouring to complete it in the future for baselining purposes.

27. 14 force areas have completed DPIAs for their other ANPR systems, and 3 have gone on to complete subsequent reviews. Some reported using an internal template, whilst another stated the BSCC template had been utilised.

Body worn video

28. All but one of the forces stated that they routinely use body worn video (BWV) with both audio and image capability, with just over half (19) incorporating other technology as well.

Q: If your force utilises body worn video, please describe the system and its capabilities



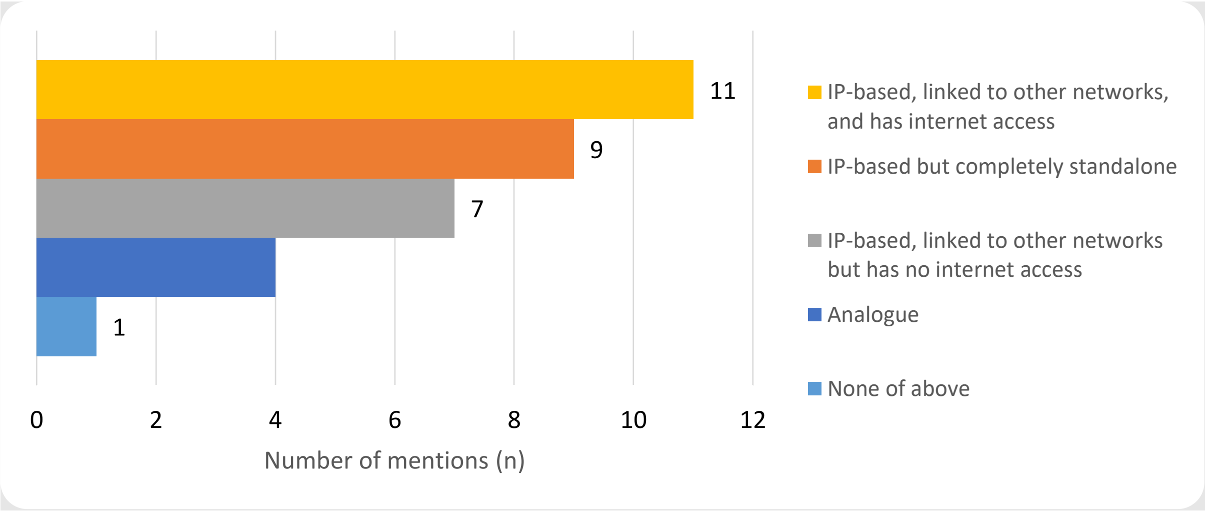
29. 33 of the respondents stated that their BWV system is compliant with PoFA Section 33(1), with 23 having completed the Self-Assessment Tool. Where it was stated that the system was not compliant, 3 respondents stated this was because they are DPIA compliant. All 33 forces stated they are DPIA compliant, with respondents stating use of various different template to achieve this (16 utilised an internal template, whilst 5 stated an ‘other’ template was used). It is worth considering whether a standardised approach to DPIA compliance through a single template would be beneficial.

30. In terms of ethical and security issues surrounding BWV technology, only four respondents commented on the specific manufacturers they used, one of which was Motorola, and the other Reveal.

Unmanned Aerial Vehicle-borne Cameras (UAV – drones)

31. 31 respondents said they used UAV-borne cameras, typically stating that they were able to record video (15 respondents), with a small number also being capable of recording audio (2). 26 drones have thermal imaging capability or night vision, and 14 have an optical zoom facility. DJI is the most commonly-cited manufacturer (17 respondents), with other drones deployed including Sky Mantis and Airvon. When specifically asked if they had any UAVs manufactured or supplied by surveillance companies outside the UK about which there have been any security or ethical concerns, at least 23 forces mention having such concerns about their use of DJI drones, however 11 mitigate this by stating there are no government restrictions in place prohibiting the use of these drones.

Q: What network topology does your organisation use for the UAV surveillance system?



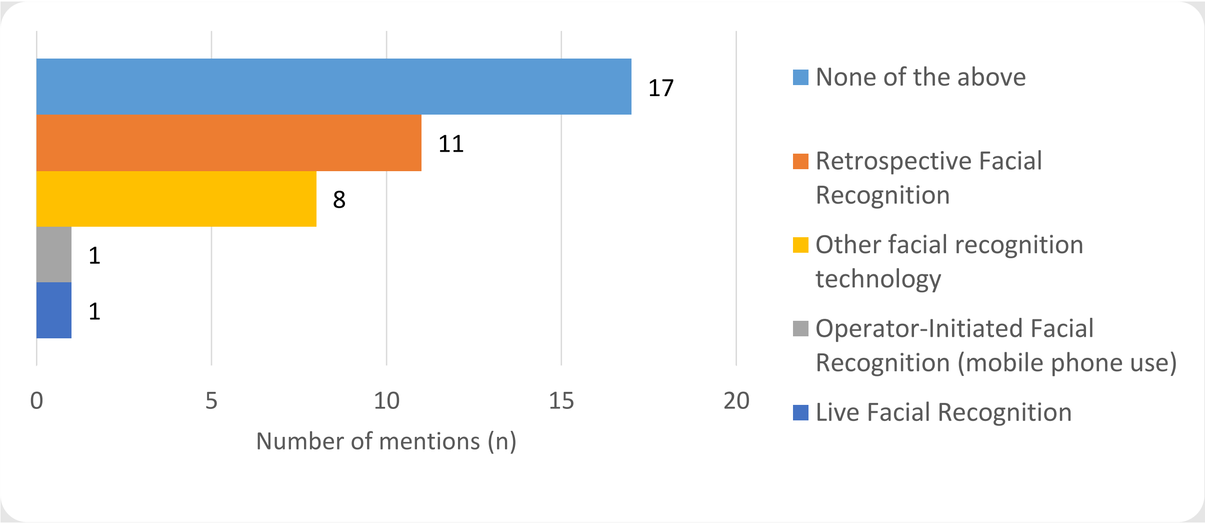
32. 28 respondents said that their UAV system is PoFA compliant, and 18 that it is SAT compliant. For those not stating compliance, this was typically because they were working towards being SAT compliant, or that they are compliant in other areas, such as DPIA. DPIAs had been completed by 25 respondents, again using a variety of different templates.

Helicopter-borne Cameras

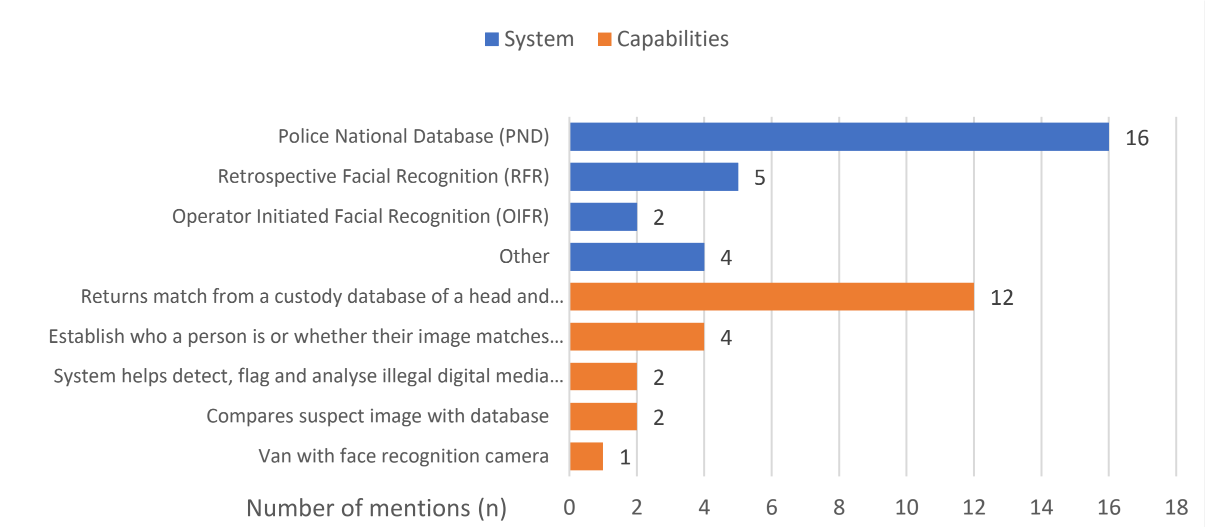
33. West Yorkshire leads the all-force collaboration with the National Police Air Service (NPAS), which provides a service to all 43 police forces in England and Wales, plus British Transport Police. The fleet consists of 19 helicopters and 4 fixed-wing aircraft, all of which are fitted with a camera and recording system, and is both DPIA and SAT compliant. Cameras are operated by NPAS staff at the direction of the requesting police force for each tasking.

Facial Recognition Technology (FRT)

Q: Is your organisation operating facial recognition technology?

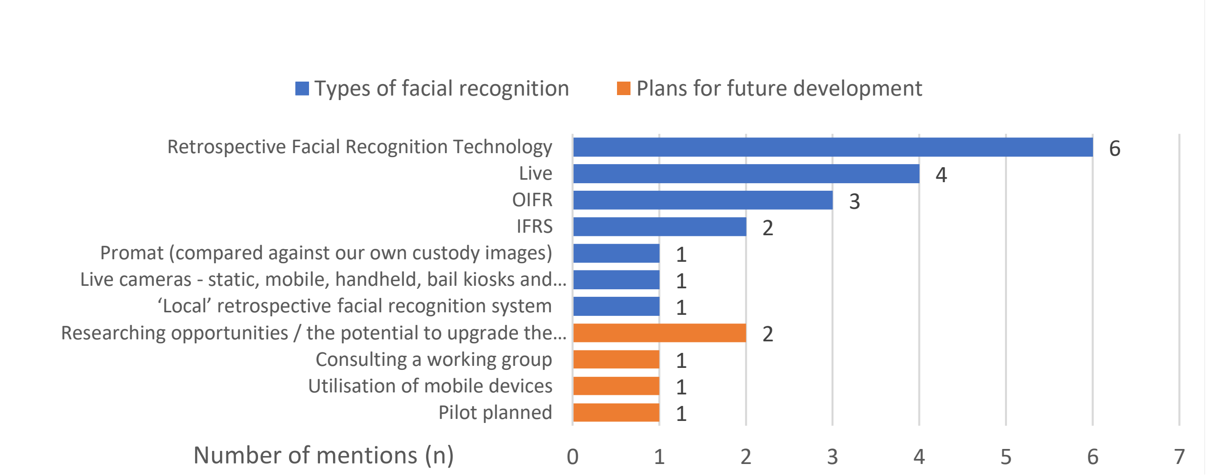


34. Just under half of respondents are not operating facial recognition technology (FRT). Of those that are, the most commonly used is the Police National Database (16 respondents), followed by retrospective facial recognition (5 respondents) and operator-initiated facial recognition (2 respondents).



35. Compliance with PoFA was confirmed by just 7 forces for their FRT, and 2 stated they had completed the SAT for theirs, one of whom had published it on their external website, whilst the other had not. As mentioned elsewhere in this paper, it is recommended these assessments are made publicly available in the interests of transparency and accountability. For those who had not completed the SAT, this was variously because it was not considered relevant to their FRT, or that the technology is nationally recognised, for example where it is a Home Office system (e.g. PND). Separately, only 11 forces using FRT state they have completed a DPIA for this capability. No ethical or security concerns were reported for the FRT currently in use.

Q: Is your force intending to use facial recognition technology in the future? If so, please provide type of facial recognition technology and plans for future deployments



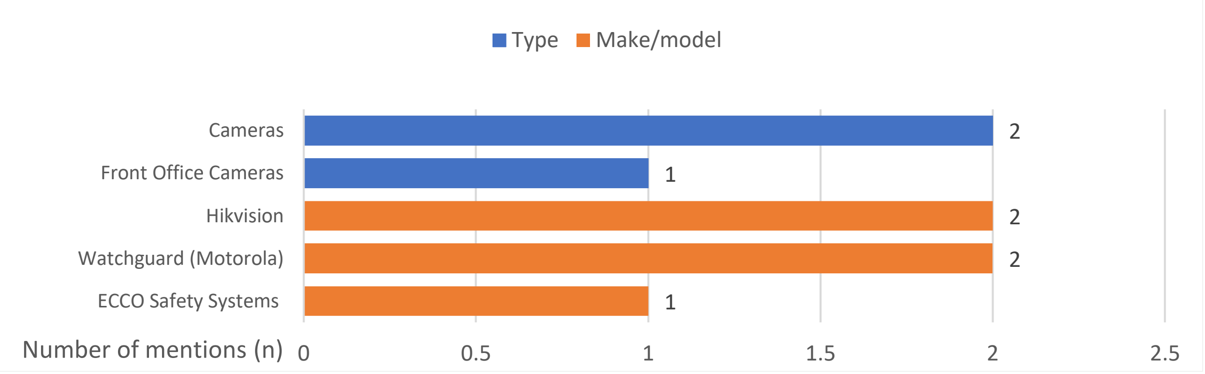
36. All 28 respondents indicated they were aware of the *Facing the Camera* guidance and reported that engaging the public in the use of FRT is important. One force singled out the need to gain public trust to ensure successful roll out of FRT, whilst another suggested using 'softer' terminology when discussing FRT with the public.

Other surveillance camera systems

37. In addition to the public surveillance systems already set out, 24 respondents stated that they operate other surveillance camera systems relevant to this survey. Of the 10 forces who gave a count for the number of other surveillance systems they have, the average across them comes to 73 per force. Examples of other systems reported include dashcams (featured in 5 responses) and dog mounted cameras (2), while other single mentions are given to bike mounted cameras, mounted section GoPros, and in-car video solutions.

38. 19 of the 24 respondents said these additional systems are PoFA compliant, and 16 said they were DPIA compliant. Of those acknowledging their non-compliance, reasons given included awaiting further information, that they are DPIA compliant which takes into account SAT principles, that their system was standalone and unused, or that they have only just discovered they are non-compliant and are taking action in the future to rectify the position. One force stated they intended to complete a DPIA and SAT when appropriate, but provided no further detail on the circumstances in which they thought that might be.

Q: Does your system have any cameras or equipment manufactured or supplied by surveillance companies outside the UK about which there have been any security or ethical concerns?

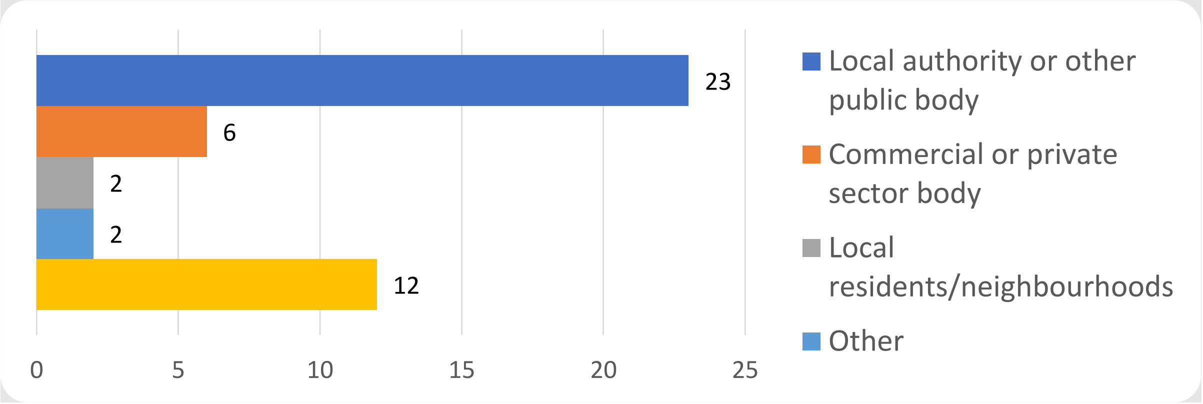


39. As has been seen throughout the responses so far, technology is installed and continues to be deployed where the provenance of the technology raises security or ethical concerns. For FRT, 3 respondents reported concerns about their equipment, and described them simply as cameras, or front office cameras manufactured by Hikvision (2), WatchGuard (2) and ECCO Safety Systems (1).

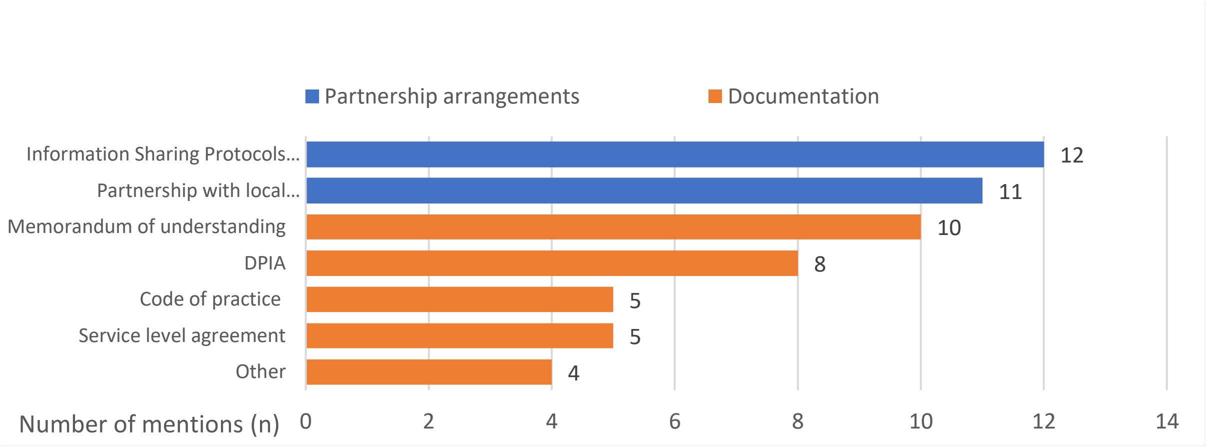
40. One force reported using a number of evidence gathering cameras, which it has indicated are not compliant with the Surveillance Camera Code of Practice. Furthermore, there is an issue of compatibility which precludes the ability to weed the data gathered, and therefore does not comply with MoPI. We are informed that the Information Management team are aware and seeking a solution, although no timeframes were provided for that work, but this does highlight the need to fully understand the capabilities, or lack thereof, of technology as part of the procurement process.

Partnerships and Third-Party Owned Systems

Q: Does your organisation have a partnership or other arrangement with any of the following in the operation of any surveillance camera system for a policing purpose?



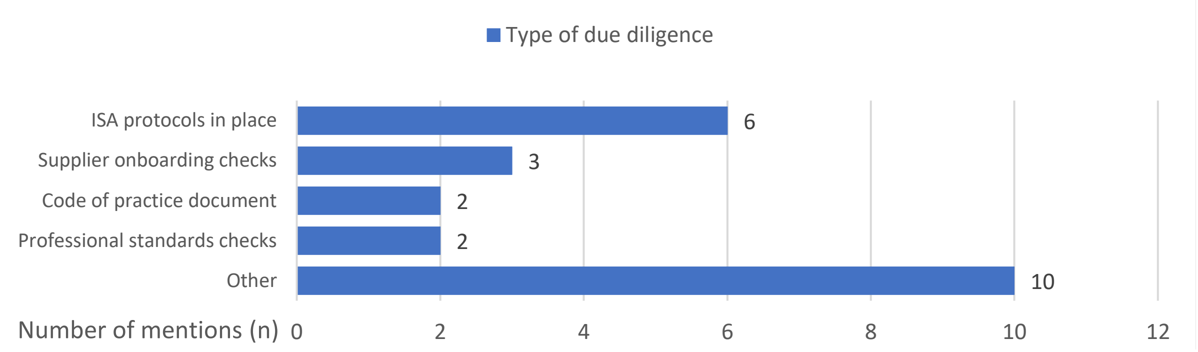
Q: Please provide a brief explanation of any partnership arrangements in place, including details of any documentation in place



41. One would expect to see information sharing agreements in place between all organisations who share data. Responses reported information sharing protocols and data sharing agreements being in place across 12 forces, while 11 respondents stated they have a partnership with local councils and local authorities. Memoranda of Understanding (10 respondents) or DPIA (8 respondents) are the most frequently cited as the types of documentation in place, while other types that get just a single mention include Terms of

Reference, Standard Operating Procedures, and a Live Use Partnership document.

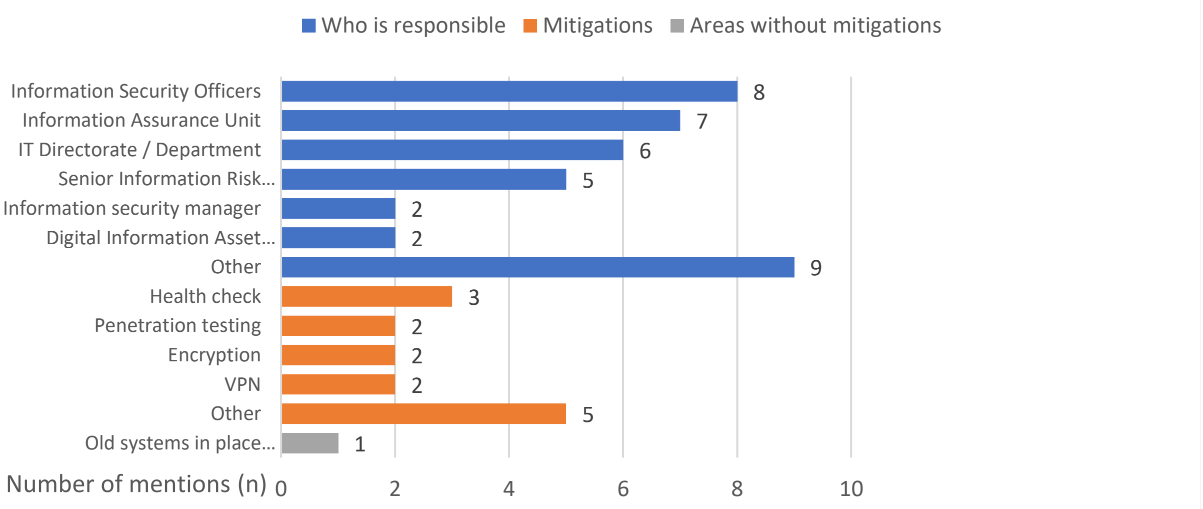
Q: What due diligence have you undertaken to assure yourselves that the companies with whom you are in a surveillance partnership are in no way connected to activities that involve any element of modern slavery, forced labour or otherwise unethical conditions?



42. Single mentions of due diligence undertaken include partners subject to Public Service Network requirements, DfT due diligence, Ethical Procurement Strand Action Plan, Welsh Governments Code of Practice for tackling Modern Slavery and Human Rights Abuses, the collaborative-commercial-and-procurement-strategy, open source checks, SLA, government agency policies, national framework agreement and commercial regulation. It is interesting to see that there is such a variety of approaches taken by respondents to such an important issue, and it begs the question whether the same results are achieved each time, or if a standard method needs to be developed and overseen. And if so, who would provide it.

Accountability and Governance

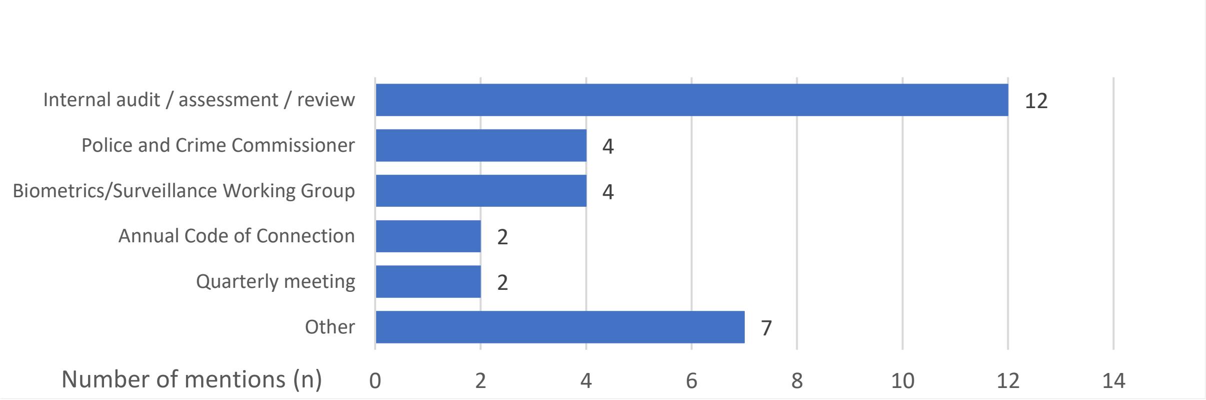
Q: Do you as an organisation consider the cyber security of your equipment?



43. It is reported that cyber security typically falls to an organisation's information security officer, information assurance unit, IT department or senior information risk owner, and that organisations have a variety of techniques to mitigate that risk. Aside from the more commonly-cited examples, other techniques mentioned include information/cyber security assurance, firewalls, intrusion prevention systems, and intrusion detection systems. Only 2 respondents stated that their equipment was subjected to penetration testing when assessing the cyber security of their equipment, while other respondents relied on encryption, VPNs or 'health checks'. This lack of proactive testing makes it hard to see how forces derive their assurances around data security.

44. When considering their supply chain requirements, 10 respondents state the main considerations are social and ethical, and 9 cite purchasing supply chain considerations. There is demonstrably a conflict involving existing procurement restrictions around cost, which means that security and ethical considerations appear to be less important.

Q: How is your force held to account for its performance in relation to biometrics and surveillance camera systems generally?



45. Only two forces have obtained full Third-Party Certification against the Surveillance Camera Code of Practice. The 30 respondents stating that have not cited a need to improve or review systems before obtaining certification (9), not being aware the scheme existed (8), not deeming it necessary (7), and simply not having progressed it (2) as reasons. Other reasons cited include certification being expired, the process being too complicated, and resource issues precluding application.

Annex - Forces and organisations providing returns

- Avon & Somerset
- Bedfordshire
- Cambridgeshire
- Cheshire
- Cleveland
- Cumbria
- Derbyshire
- Devon & Cornwall
- Dorset
- Durham
- Dyfed Powys
- Essex
- Hampshire
- Hertfordshire
- Humberside
- Kent
- Lancashire
- Leicestershire
- Lincolnshire
- Norfolk
- Northamptonshire
- Northumbria
- North Yorkshire
- North Wales
- Nottinghamshire
- Metropolitan Police Service
- South Wales
- Staffordshire
- Suffolk
- Surrey
- Sussex
- Warwickshire
- West Mercia
- West Midlands
- West Yorkshire
- Wiltshire
- British Transport Police
- Civil Nuclear Constabulary
- Ministry of Defence