Privacy International Response to Draft national surveillance camera strategy for England and Wales

Surveillance Camera Commissioner
1st Floor, Peel Building, 2 Marsham Street, London, SW1P 4DF
sccconsults@sccomissioner

The Surveillance Camera Commissioner has published and sought views on the draft national surveillance camera strategy for England and Wales. The strategy aims to:

- Provide direction and leadership in the surveillance camera community
- Enable system operators to understand best practice and their legal obligations
- Enable system operators to demonstrate compliance with the principles of the surveillance camera code of practice and other guidance.

Introduction

1. Privacy International was founded in 1990. It is a UK charity working on the right to privacy at an international level. One of its focuses is on tackling the unlawful use of surveillance. It is frequently called upon to give expert evidence to Parliamentary and Governmental committees around the world on privacy issues and has advised, and reported to, among others, the Council of Europe, the European Parliament, the Organisation of Economic Co-operation and Development, and the United Nations.

2. Privacy International's primary aims are to raise awareness about threats to privacy, to monitor and report on surveillance methods and tactics, to work at national and international levels to ensure strong privacy protection, and to seek ways to protect privacy through the use of technology.

3. The Surveillance Camera Commissioner is appointed by the Home Secretary as set out in the Protection of Freedoms Act 2012 (PoFA). It is the Commissioner's role to ensure surveillance camera systems in public places keep people safe and protect and support them.

4. The draft strategy opens with the statement that 'The Government is fully supportive of the use of **overt surveillance cameras in a public place** whenever that use is: **in pursuit of a legitimate aim; necessary to meet a pressing need; proportionate; effective, and; compliant with any relevant legal obligations.'**

5. The premise of the draft strategy and the Commissioner's vision is that the public are assured that surveillance cameras in public places are there to keep them safe and protect and support them.

6. Privacy International are concerned that the framing of the strategy is outdated or at least does not reflect or tackle the reality of the enormous

development in technology, sophistication and use of surveillance cameras to the extent that it can be questioned whether many types of surveillance cameras are indeed 'overt' surveillance and the strategy does not address the risks associated with the insecurities in software and hardware.

7. In respect of the developments in technology and use of surveillance cameras, the Executive Summary of the strategy makes reference to types of surveillance cameras which demonstrate the remit of the SCC has and must move far beyond CCTV. The types of surveillance cameras identified are body worn video, ANPR and unmanned aerial vehicles (aka drones).

8. We would therefore caution against referencing research in the draft strategy, conducted in relation to CCTV only, since this is incomplete:

> *"The available evidence does indicate that the public remains supportive of the use of surveillance cameras. Research in 2014 showed 86% of people support the use of CCTV in public places."*[1]

9. In framing the consultation there is no apparent attempt to tackle whether there is a need to evaluate what constitutes an overt surveillance camera, particularly if it is invisible to the naked eye.

10. In relation to the security risks, we note for example that as the pervasiveness of surveillance cameras has increased, from mobile ANPR to the Internet of Things, we have learned on almost a daily basis of unauthorized access to surveillance cameras and distributed denial-of-service attacks[2]. These attacks

[1] Para 24

[2] On 29 September 2016, Ars Technica reported: 'Last week, security news KrebsOnSecurity went dark for more than 24 hours following what was believed to be a record 620 gigabit-per-second denial of service attack brought on by an ensemble of routers, security cameras, or other so-called Internet of Things devices…
Security experts have been warning for years that Internet-connected devices posed a potential threat. In early 2015, the threat was finally confirmed with evidence showing that

on devices present a serious risk to individuals and their right to privacy, including in public spaces.

11. In these submissions Privacy International will raise concerns that largely relate to the background to the proposed objectives. These are:

    a. the level of understanding relating to the definition of surveillance cameras;
    b. the wider context of camera surveillance, to emphasis the seriousness of the privacy interferences that arise, the increasingly intrusive nature of 'overt' (public) surveillance by cameras; and
    c. highlight some of the technical risks associated with surveillance cameras, from distributed denial-of-service (DDoS) attacks to certain provisions of the Investigatory Powers Act.

12. We hope these are taken into account when reviewing the draft strategy and objectives.

13. Before addressing these we urge that language as to how surveillance cameras make the public feel, as opposed to what they actually do, is removed, i.e.:

DDoSes that disrupted Sony's PlayStation Network and Microsoft's Xbox Live were largely powered by home routers that had been hacked and corralled into a powerful botnet. In June, researchers at security firm Sucuri uncovered a botnet of 25,000 closed-circuit TVs bombarding a brick and mortar jewelry store.'

On 21 October 2016, KrebsOnSecurity reported that: 'A massive and sustained Internet attack that has caused outages and network congestion today for a large number of Web sites was launched with the help of hacked "Internet of Things" devices such as CCTV video cameras and digital video recorders, new data suggests. Earlier today cyber criminals began training their attack cannons on Dyn, an Internet infrastructure company that provides critical technology services to some of the Internet's top destinations. The attack began creating problems for Internet users reaching an array of sites, including Twitter, Amazon, Tumblr, Reddit, Spotify and Netflix.'

"The Commissioner's strategic vision is:

The public are assured that surveillance cameras in public places are ***there to keep*** ~~***and make***~~ ***them*** ~~***feel***~~ ***safe,*** *and that those cameras are deployed and used responsibly as well as transparently in a manner which is proportionate to their legitimate purpose."*

[strike through = what should be removed]
[emphasis added]

14. If surveillance cameras are justified then this should be real, not illusory. This goes back to the survey being used in paragraph 24: the fact that the public do not know about its efficacy and yet are supportive because of impression and feeling, this is indicative of a failure of public policy, not a fact to be celebrated.

The level of understanding relating to the definition of surveillance cameras: what is included in the definition of surveillance camera

15. The draft SCC Strategy 'objectives' include:

> *2. There is an early warning system to* ***horizon scan technological developments*** *with implications for the scope and capability of surveillance, so that the Commissioner can assess whether regulation is sufficient and advise the Government accordingly.*
>
> *3. Information is freely available to the public and organisations about rights and responsibilities in relation to the operation of surveillance camera systems, so that they can be engaged in meaningful civil engagement/consultation to shape both national development of regulation and local decisions about surveillance of the public.*

16. The Commissioner accepts, as stated in the 'Executive Summary' that *"…technological change is moving at an exponential rate, so the world is changing around us."* The Commissioner states he wants *"to develop a stronger evidence base before 2020 to inform further strategic planning to maintain momentum."*

17. The draft SCC Strategy 'Why we need a strategy' states that:

> *The surveillance camera sector is massive and is an industry that will continue to grow – there was a £2,120m turnover in the UK in 2015 on video and CCTV surveillance. The most recent estimates suggest that there are between 4m – 6m CCTV cameras in the UK. Considering these figures do not include the following types of surveillance camera –* ***automatic number plate recognition, body worn video and unmanned aerial vehicles*** *– that number is likely to be higher when reported in 2013. These figures are indicative of the scale of surveillance, yet give no real indication whether*

surveillance is necessary nor of good compliance with good practice or legislative requirements.'

'…ensure systems are fit for purpose as the 'internet of things' develops and procurement is geared up to meet that challenge.'

[emphasis added]

18. The draft SCC Strategy 'Challenge' states that:

> *"We are on the advent of superfast WiFi and 5G connectivity. Digital data from a wider range of sources can be analysed and compared alongside surveillance camera images and information.* ***Smart cities and internet of things*** *are no longer science fiction but becoming a reality."*

19. Privacy International believes that it is vital that not only the SCC 'horizon scan technological developments' but further, the SCC provide information to the public information as to what constitutes a 'surveillance camera'.

20. It is not sufficient for there be solely information available to the public and organisations about rights and responsibilities in relation to surveillance cameras, the public and organisations need to understand, what is a surveillance camera. They need to understand the nature and type of surveillance cameras, in order to inform the rights and responsibilities and make them effective.

21. If the public are not aware what is meant by an 'overt surveillance camera' then it can be questioned whether the Commissioner's strategy vision, that the public are assured that surveillance cameras in public places are there to keep them safe, can truly be achieved in a meaningful sense.

22. As an initial step Privacy International recommends that the SCC seek to produce a more expansive definition or list of what the SCC includes in the term 'surveillance camera' which includes some information or examples about types of devices and technical specifications. To only briefly refer to CCTV, body worn video, ANPR and unmanned aerial vehicles without further exploration of these surveillance cameras and what others might be in operation is insufficient.

23. It is noted that the SCC appears amenable to providing a more detailed explanation, stating that '*as the way devices are used changes such as increased use of automatic facial recognition and body worn video'* and thus devices '*become more intrusive'* public support may not remain as it was in 2014 in relation to CCTV. The SCC states that '*Transparency and therefore understanding will become more of a priority as technological advances challenge our views on citizens' right to privacy."*[3]'

24. In relation to 'unmanned aerial vehicles', 'smart cities' and 'internet of things' there is a worrying lack of detail. No context is given aside from referencing these highly intrusive means of surveillance of the public. The SCC must develop their understanding and explain to the public the relevance or prevalence of these issues in respect of including surveillance cameras, in particular as used by law enforcement, local and national government.

25. We note that it may be difficult to provide such a list in relation to personal surveillance cameras used in public, particularly as we see cameras placed in a wide variety of objects, from engagement ring boxes[4] to cycle helmets[5], which could take footage of the public.

[3] Draft national surveillance camera strategy for England and Wales, Para 24
[4] https://www.ringcam.com/
[5] http://www.halfords.com/cycling/cycling-technology/helmet-cameras

26. However, it should not be beyond the powers of the SCC to request details from local and national government and law enforcement, as to what surveillance cameras they purchase, operate and from which they acquire and retain data. If the information does not exist then this is in itself a cause for concern.

27. With this in mind we note the SCC also states as objectives:

> *4. The police pro-actively share relevant information about their own operations of surveillance camera systems and use of data from their own and third party systems, so that the public are reassured about the proportionality and effectiveness of surveillance.*
>
> *5. Local authorities pro-actively share information about the operation of a surveillance camera system in exercising any of its functions and any data sharing arrangements with third parties, so that the public are reassured about the proportionality and effectiveness of surveillance cameras.*

28. As stated above, unlike most traditional CCTV, the public are less likely to be able to see many forms of current and future allegedly 'overt' surveillance cameras, used for example in CCTV, mobile ANPR and drones. Certainly the public are unlikely to be aware that facial recognition technology is being used on images obtained via 'overt' surveillance cameras.

29. Despite issues with potential visibility, the use of CCTV and ANPR is regarded as "*surveillance by consent*" and the police consider that its use "*does not generally result in the obtaining of private information*."[6]

30. The Draft national guidance suggests that, "*The use of overt CCTV cameras by public authorities does not normally require an authorisation under the [Regulation of Investigatory Powers Act 2000]. Members of the public will be aware that such*

systems are in use, and their operation is covered by the Data Protection Act 1998 and the CCTV Code of Practice 2008, issued by the Information Commissioner's Office. Similarly, the overt use of ANPR systems to monitor traffic flows or detect motoring offences does not require an authorisation under the 2000 Act."[7]

31. The use of public or 'overt' surveillance cameras by law enforcement is classed as "*overt*" forms of intelligence-gathering. The recording of information from these forms of technology in large-scale databases is subject to limited legal safeguards, namely the Data Protection Act 1998, a generalised code of practice and Article 8 of the Human Rights Act. Safeguards designed specifically to govern the use of "*overtly*" collected intelligence are often lacking.

32. There is a real risk that we are moving towards or indeed are in a situation where you cannot see the surveillance camera, and you do not know what is included in the definition of a surveillance camera. Yet this surveillance camera is class as 'overt' and it is assumed that the public will be aware that such systems are in use.

33. We therefore suggest that in providing information about what constitutes a surveillance camera, the SCC considers what it means for a surveillance camera to be overt to enable public discussion and debate including over whether certain cameras and types of surveillance cross the boundary to covert surveillance.

34. Finally, there is a lack of clarity, including in areas where the SCC should be able to take action such as local government and law enforcement, as to what happens to the data and images that are collected. For example, what happens to ANPR data? How is it stored? Who is it shared with? What is it used for? Thus whilst the first step is to gain and understanding of types of surveillance cameras, there also must be consideration of what happens to the data.

The wider context of camera surveillance : Increasingly intrusive 'overt' surveillance

35. As technology develops, surveillance cameras that can be used in public places become more affordable and sophisticated. These cameras are less visible or completely invisible to the naked eye, such as unmanned aerial vehicles, or tiny cameras used in some of the plethora of devices which fall under the vague term internet of things. As the ambitions of 'smart' environments and cities grow, we are likely to see the deployment of cameras for purposes beyond public safety, such as computer vision in Amazon Go[8] or use for retail analytics[9]. These new purposes will not be limited to private sector institutions and motivations.

36. We will look in turn at the intrusive nature of newer forms of surveillance cameras.

Public cameras, private life

37. First we note the SCC does not consider in any detail the nature of the data obtained, that it is personal data, and the implications of this.

38. In the landmark decision Peck v United Kingdom (2003) 36 EHRR 41; [2003] EMLR 287 the ECHR accepted that certain incidents which take place in public can still fall within someone's private life and for which they can have a reasonable expectation of privacy.

[8] https://www.google.co.uk/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8#q=amazon%20go%2C%20just%20walk%20out%2C%20computer%20vision

[9] http://www.techradar.com/news/world-of-tech/future-tech/in-store-analytics-tracking-real-world-customers-just-like-online-shoppers-1286293

39. In this case the applicant, who was suffering from depression, complained about the disclosure in the media of footage from a close-circuit television (CCTV) camera mounted in the street showing him walking alone with a kitchen knife in his hand. He was also filmed in a public street, moments after he had attempted to commit suicide by slashing his wrists with a kitchen knife.

40. Some months later, the Council issued two photographs taken from the CCTV footage for publication in an article about the preventative benefits of CCTV. The applicant's face was not specifically masked. Extracts from the CCTV footage were also shown on regional television in which the applicant's face had been masked at the Council's request. The Applicant sought judicial review of the Council's decision to release the CCTV footage. His application was rejected and confirmed by the Court of Appeal. He applied to the ECHR.

41. The Court found that the disclosure of the footage by the municipal council had not been accompanied by sufficient safeguards and constituted disproportionate and unjustified interference with the applicant's private life, in breach of Article 8 (right to respect for private life) of the Convention. Furthermore, at the relevant time, the applicant had not had an effective remedy for breach of confidence, in violation of Article 13 (right to an effective remedy) read in conjunction with Article 8 of the Convention.

42. The Office of Surveillance Commissioners[10] Procedures and Guidance document states[11] that:

[10] The Office of Surveillance Commissioners (OSC) oversees the conduct of covert surveillance and covert human intelligence sources by public authorities in accordance with the Police Act 1997 and the Regulation of Investigatory Powers Act 2000 (RIPA). OSC is a tribunal non-departmental public body, sponsored by the Home Office.

[11] OSC's 2016 Procedures & Guidance document https://osc.independent.gov.uk/wp-content/uploads/2016/07/OSC-Procedures-Guidance-July-2016.pdf

> *"217. The 'private life' of a car driver is not interfered with when the registration number of his vehicle is recorded by ANPR while he is travelling on a public road, because the registration plate is a publicly displayed object. It is not adequate to say that recording and storing data capable of identifying the occupants of the car does not require authorisation because they are in a public place: they are, but they are ignorant of the capacity of the camera and the extent to which the data may be retained and used. Some ANPR cameras are now capable of producing clear images of the occupants of a car, as well as the vehicle make and registration number…It is therefore possible to interfere with a person's private life. If the occupant is in a private vehicle such use of ANPR may in consequence constitute intrusive surveillance if data that is recorded for potential later use is capable of identifying him."*

43. Information captured on CCTV and on surveillance cameras can be personal data, including sensitive personal data, and should be subject to protection. The vast data mining capabilities of public and private sector organisations today makes even the smallest types of data capable of unlocking vast amounts of intelligence about the lives of individuals, public and private (if there is such a thing).

CCTV and Security

44. The role of the SCC will no doubt have changed dramatically from the initial inception where it addressed, predominantly, concerns related to CCTV i.e. video surveillance rather than looking at the current plethora of surveillance cameras. However, even in terms of CCTV the changes are rapid. There are new sophisticated cameras which produce highly detailed facial images; greater zoom capacity; the use of facial recognition technology and ANPR.

45. Little discussed are the security issues related to both older CCTV models, where for example software is not updated, and relating to new surveillance

cameras, such as those which operate wirelessly or where default factory settings and passwords are not updated.

46. As reported by Kaspersky blog[12], local government and law enforcement are becoming increasingly more reliant on networked surveillance cameras in order to monitor densely populated urban areas. CCTV cameras in the UK can be networked wirelessly into the Internet, so they can be remotely monitored by law enforcement. However, many of these wireless connections are not secure and thus unauthorised third parties not only have the capacity to passively monitor security camera feeds, but can also inject code into their networks, providing fake footage or knocking system offline entirely.

Facial recognition

47. There has been a rapid increase in the availability and accuracy of facial recognition technology in recent years. Furthermore, this technology has been integrated into online and mobile services for the identification, authentication/verification or categorization of individual.[13]

48. Facial recognition technology has been trialled by UK police forces. A trial was conducted by Leicestershire Police at a music festival in 2015.[14] In August 2016, the Metropolitan Police Service used automated facial recognition technology to monitor and identify people at the Notting Hill Carnival.[15] This

[12] https://blog.kaspersky.com/urban-surveillance-not-secure/8901/
[13] Article 29 Data Protection Working Party 00727/12/EN WP 192 Opinion 02/2012 on facial recognition in online and mobile services, adopted on 22 March 2012

[14] *Daily Telegraph,* 17th July 2014: http://www.telegraph.co.uk/technology/news/10973185/Police-trial-facial-recognition-software-that-can-ID-suspects-in-seconds.html

[15] *Police Oracle*, 27th August 2016: https://www.policeoracle.com/news/police_it_and_technology/2016/Aug/26/met-trialling-facial-recognition-technology-at-notting-hill-carnival_92773.html/specialist;

technology, which is classed by police forces as "*overt surveillance*", works by scanning the faces of those passing by overt cameras and then comparing the images against a database of images populated by the police force in question. At the Notting Hill Carnival, the database was populated with images of individuals who were forbidden from attending Carnival, as well as individuals who the police believed may attend Carnival to commit offences.

49. The combination of image databases and facial recognition technology could be used to track people's movements by combining widespread CCTV and access to a huge searchable database of facial images. Such technology has attracted concern from the UK Commissioner for the Retention and Use of Biometric Material, Alastair R MacGregor QC[16] and from the Science and Technology Committee of the UK Parliament;[17]

50. There is "*no specific legislation covering*" the use of facial recognition technology (with associated image databases) according to the Information Commissioner's Office. The Biometrics Commissioner has questioned how "*appropriate*" it was for the police to put "*a searchable database of custody photographs*" into "*operational use*" in the absence of any "*proper and effective regulatory regime […] beyond that provided for in the Data Protection Act 1998*";[18]

51. The SCC has raised the issue of facial recognition technology, however, neither the Biometrics Commissioner nor the SCC has responsibility for any form of statutory oversight of this technology. The SCC states:

Metropolitan Police Service, 30th August 2016: http://news.met.police.uk/news/statement-from-police-commander-for-notting-hill-carnival-2016-182480

[16] Commissioner for the Retention and Use of Biometric Material, "*Annual Report 2015*", at section 7.

[17] House of Commons Science and Technology Committee: "*Current and future uses of biometric data and technologies*", Sixth Report of Session 2014-15, at §§53-59 and §§94-100.

[18] House of Commons Science and Technology Committee: "*Current and future uses of biometric data and technologies*", Sixth Report of Session 2014-15, at §97.

a. *"We are seeing continual technological advancements that mean how surveillance cameras are used in the present and future is changing significantly – as is the data they capture. For example in 2016 the Metropolitan Police used automatic facial recognition at the Notting Hill Carnival using a database of individuals who were forbidden from attending the Carnival as well as individuals wanted by police who it was believed may attend the Carnival, as well as individuals wanted by police who it was believed may attend the Carnival to committee offences. Technology companies are fast improving facial recognition software and other analytical capabilities such as sensors that can detect explosives."*

52. As noted by the Article 29 Working Party, the body of privacy regulators across the European Union, 'Facial recognition is considered within the scope of biometrics as, in many cases, it contains sufficient detail to allow an individual to be uniquely identified'. In Opinion 03/2012 the Article 29 Working Party commented that:

> *"[biometrics] allow for automated tracking, tracing or profiling of persons and as such their potential impact on the privacy and the right to data protection of individuals is high."*

53. The Article 29 Working Party[19] goes on to state:

> 'Furthermore as digital images of individuals and templates relate to the "biological properties, behavioural aspects, physiological characteristics, living traits or repeatable actions where those features and/or actions are both unique to that individual and measurable" they should be considered as biometric data.'

[19] Article 29 Data Protection Working Party 00727/12/EN WP 192 Opinion 02/2012 on facial recognition in online and mobile services, adopted on 22 March 2012

> 'Digital images of individuals may in some specific cases be considered as a special category of personal data. Specifically, where digital images of individuals or templates are further processed to derive special categories of data, they would certainly be considered within this category. For example, if they are going to be used to obtain ethnic origin, religion or health information can be derived.'

54. The SCC states as one of its objectives:

> 4. The police pro-actively share relevant information about their own operations of surveillance camera systems and use of data from their own and third party systems, so that the public are reassured about the proportionality and effectiveness of surveillance.

55. Privacy International is deeply concerned by the lack of progress on securing any form of independent oversight of the use of facial recognition technology, particularly as used by law enforcement, and urges the SCC to push for greater safeguards, regulation, and transparency.

Internet of things

56. The Internet of Things (IoT) as they relate to the presence of surveillance cameras in common, everyday devices in public places raise significant privacy and security challenges. These devices are designed to record, process, store and transfer data. They interact with other devices or systems using networking capabilities.

57. IoT devices are likely to exist in public places including in airports, smart cities, retail, commercial buildings. They may be vulnerable to attack, and an unauthorized user may be able to remotely activate a camera on a device,

install malware to access the video feed or use it for a distributed denial-of-service attack.

58. These are issues not properly considered in the SCC's strategy.

59. The Article 29 Data Protection Working Party[20] noted:

> 'Many questions arise around the vulnerability of these devices, often deployed outside a traditional IT structure and lacking sufficient security built into them. Data losses, infection by malware, but also unauthorised access to personal data, intrusive use of wearable devices or unlawful surveillance…'
>
> '…devices operating in the IoT are also difficult to secure, both for technical and business reasons. As their components usually use wireless communications infrastructure and are characterized by limited resources in terms of energy and computing power, devices are vulnerable to physical attacks, eavesdropping or proxy attacks…The IoT entails a complex supply chain with multiple stakeholders assuming different degrees of responsibility. A security breach might have origins from any of them, especially when considering Machine to Machine environment based on exchange of data among devices.'
>
> '…devices that are designed to be accessed directly via the Internet are not always configured by the user. They may thus provide an easy access path to intruders if they keep running with default settings…Additionally, the absence of automatic updates results in frequent unpatched vulnerabilities that can easily be discovered through specialized search engines.

[20] Article 29 Data Protection Working Party, Opinion 8/2014 on the Recent Developments on the Internet of Things, adopted on 16 September 2014

60. The Broadband Internet Technical Advisory Group[21] report 'Internet of Things, Security and Privacy Recommendations' states:

> 'IoT can refer to much more than simply consumer-oriented devices.'
>
> 'Several recent reports have shown that some devices do not abide by rudimentary security and privacy best practices. In some cases, devices have been compromised and allowed unauthorized users to perform surveillance and monitoring, gain access or control, induce device or system failures and disturb or harass authorized users or device owners.'
>
> 'Potential issues contributing to the lack of security and privacy best practices include: lack of IoT supply chain experience with security and privacy, lack of incentives to develop and deploy updates after the initial sale, difficulty of secure over-the-network software updates, devices with constrained or limited hardware resources, devices with constrained or limited user-interfaces, and devices with malware inserted during the manufacturing process.'

61. BITAG has made observations regarding security vulnerabilities, insecure communications, lack of mutual authentication and authorisation, lack of network isolation, data leaks, susceptibility to malware infection and other abuse, potential for service disruption, potential that device security and privacy problems will persist. The group emphasizes the importance of strong cryptography and security.

[21] BITAG is a non-profit, multi-stakeholder organization focused on bringing together engineers and technologists in a Technical Working Group (TWG) to develop consensus on broadband network management practices and other related technical issues that can affect users' Internet experience, including the impact to and from applications, content and devices that utilize the Internet.

62. Not only are there issues the Commissioner should consider about the security vulnerabilities of devices, there are, on the flip side valid concerns about legislation which undermines strong security measures. This results in a confusing message from government about their commitment to the importance of strong encryption to protect the private lives of individuals.

63. Aspects of the Investigatory Powers Act ("IPA") undermine device security which will have implications for IoT devices including those with cameras. The SCC has not commented on the impact of the IPA and we encourage the SCC to consider the implications of this Act for the security of surveillance cameras in public places, given, for example, it allows for the imposition of technical measures to negate or limit the operation of safety features. This can be found in particular (but not only) in the provisions of the legislation relating to *technical capability notices*[22]. The powers are developed in the Code of Practice[23] where we see the ability to compel companies to provide advanced copies of new and updated software.

---

[22] The relevant parts of the IPA in this respect include Technical Capability Notices:
253(2) A "technical capability notice" is a notice -
(a) imposing on the relevant operator **any** applicable obligations specified in the notice and
(b) requiring the person to take all the steps specified in the notice for the purpose of complying with those obligations

255(4) In the case of a technical capability notice that would impose any obligations relating to the **removal by a person of electronic protection** applied by or on behalf of that person to any communications or data, in complying with subsection (3). the Secretary of State must in particular take into account the technical feasibility and the likely cost of complying with those regulations.
255 (9) A person to whom a relevant notice is given **must comply** with the notice
255(10) The duty imposed by subsection (9) is enforceable…by civil proceedings by the Secretary of State.

[23] The Code of Practice[23] states:

8.4 An obligation placed on a communications service provider to remove encryption only relates to electronic protections that the company has itself applied to the intercepted communications (and secondary data), or where those protections have been placed on behalf of that communications service provider, and not to encryption applied by any other party. The purpose of this obligation is to ensure that the content of communications can be provided to the intercepting agencies in intelligible form. References to protections applied on behalf of the communications service provider include circumstances where the communications service provider has contracted a third party to apply electronic protections

Unmanned aerial vehicles

64. Privacy International encourage the SCC to consider whether unmanned aerial vehicles (UAV), otherwise known as drones, are covert or overt surveillance.

65. As stated by the Article 29 Working Party[24]:

> 'Indeed, several privacy risks may arise in relation to the processing of data (such as images, sound and geolocation relating to an identified or identifiable natural person) carried out by the equipment on-board a drone. Such risks can range from a lack of transparency of the types of processing due to the difficulty of being able to view drones from the ground to, in any event, a difficulty to know which data processing equipment are on-board, for what purposes personal data are being collected and by whom. Furthermore the dexterity of drones and the possibility to interconnect multiple drones further facilitates their ability to achieve unique vantage points, for example avoid obstacles

---

to a telecommunications service offered by that communications service provider to its customers.

8.20 Any person to whom a technical capability notice is given, or any person employed or engaged for the purposes of that person's business, is **under a duty not to disclose the existence or contents of that notice to any person**.

8.52 In certain circumstances it may be more economical for **products to be developed centrally,** rather than communications service providers or public authorities creating multiple different systems to achieve the same end. Where multiple different systems exist, it can lead to increased complexity, delays and higher costs when updating systems (for example, security updates).

8.53 Section 226 of the Act provides a **power for the Secretary of State to develop compliance systems**. This power could be used, for example, to develop consistent systems for use by communications service providers to intercept communications and secondary data. Such systems could operate in respect of multiple powers under the Act.

[24] Article 29 Data Protection Working Party, Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones, Adopted 16 June 2015

or not being constrained by barriers, walls or fences, so to easily enable the collection of a wide variety of information even without the need for a direct line of sight, for long periods of time and across large area without intermission (with a high risk of bulk data gathering and possible unlawful multipurpose uses). '

'Even higher risks for the rights and freedoms of individuals arise when the processing of personal data by means of drones is carried out for law enforcement purposes.'

'…the processing of personal data by drones has a peculiar nature due to the unique vantage point that magnifies the effectiveness of any on-board sensors and implies a reduced transparency and increased privacy intrusion compared to a similar fixed sensor in spite of their perceived similarities – consider, for example, video surveillance by drone versus the use of a fixed CCTV camera.'

The analysis goes on to consider equipment that could have an impact on privacy and data protection including:

Smart cameras with fixed or variable focal length, capable to store and transmit lives images, with on-board or ground-based facial recognition capabilities, allowing drones to identify and track specific individuals, objects or situations, identify patterns of movement, to read license plates on vehicles, whilst guaranteeing a 360° view, enabled to detect the thermal energy emitted by a target, allowing the flight and the recording of images in poor visibility conditions (due to fog, smoke or debris) or during night hours;

'…the relevant point from a privacy and data protection standpoint, is not the use of drone per-se but the data processing equipment on-board the drone and the subsequent processing of personal data that

may take place. Indeed, it is the processing of images (including images of individuals, houses, vehicles, driving license plates, etc) sound, geolocation data or any other electromagnetic signals related to an identified or identifiable natural person carried out by the data processing equipment on-board a drone that may have an impact on privacy and data protection and therefore trigger the application of data protection legislation.'

'…it is likely in a number of cases, that the data subjects would not be aware of the drone or any processing of their personal data which is being carried out given that these devices can be difficult to view from the ground. In any event, even if individuals are aware that a drone is in the area it is difficult to know which data processing equipment are on-board, for what purposes they are being collected and by whom. This will result in an increased feeling of being under surveillance and a subsequent possible decrease in the legitimate exercise of civil liberties and rights, best known as 'chilling effect'.

66. The SCC's strategy briefly mentions unmanned aerial vehicles. Privacy International considers, given the large number of issues that this particular form of surveillance camera raises, that it requires detailed consideration, including whether this can be considered open / overt surveillance or is in fact covert in nature.

Data agglomeration

67. Each of the cited forms of technology can be used to monitor and record individuals' activities in public. They represent a significant intrusion into individual privacy. For example, images recorded on body-worn cameras at protest encampments can reveal not only, "*any interactions with individual officers, but potentially images of protesters cooking meals, talking to each other, and other activities that are a routine part of daily life.* The use of CCTV and ANPR

can then monitor and record individual movements (including vehicle movements) around the country.

68. We encourage the SCC to assess the privacy implication of the agglomeration of surveillance camera data.

69. In the recent judgment of the United States Supreme Court in *United States v Jones*, 132 S Ct 945 (2012), a case considering monitoring of largely public movements by GPS technology. As Justice Sotomayor explained in her concurring opinion, at 956:

> "*Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring – by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track – may 'alter the relationship between citizen and government in a way that is inimical to democratic society.'*"

70. We note the case of John Oldroyd Catt [Catt v United Kingdom (Application No.43514/15) and the existence of the 'Extremism Database'. There is little information on the data contained in this database and the sources of information. However, it is known that it contains a wealth of highly personal information about individuals including and there is the distinct possibility it could include data from a variety of surveillance cameras including ANPR, CCTV and unmanned aerial vehicles.

71. Privacy International encourages the SCC assesses the potential privacy intrusion resulting from the agglomeration of different surveillance camera data.

Anonymisation of personal data

72. The SCC states:

> "Whilst these technical advances present us with many exciting opportunities we must be mindful of how they will impact individuals' right to privacy. Equally technology is being developed that means the data captured can be anonymized in such a way that it further protects an individual's privacy – software that turns people into avatars on monitors so all that is viewed on the screen is a computer generate image rather than images of people."

73. In the context of the proliferation of devices, generating vast amounts of data and the ever-increasing processing capabilities of new technologies, data is increasingly at risk of re-identification. The Working Party 29 noted that "even data relating to individuals that is intended to be processed only after the implementation of pseudonymisation, or even of anonymisation techniques may have to be considered as personal data."25 The European Data Protection Supervisor, in his Opinion 7/2015 argues that it "will be ever easier to infer a person's identity by combining allegedly 'anonymous' data with publicly available information such as on social media".26

25 Opinion 8/2014 on the on Recent Developments on the Internet of Things, available here: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

26 Opinion 7/2015, Meeting the Challenges of Big Data, available here: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-11-19_Big_Data_EN.pdf

74. The above considerations point to the need of a significant shift in the way data perceived as "anonymous data" is considered and treated.

75. It is key that the SSC takes into account this reality and addresses the limits of anonymisation.

Machine learning

76. In recent years there has been a surge in technological developments in the fields of machine learning and automated visual analysis as they relate to the CCTV solution. It has been reported that that there is a 'surge in demand' globally for 'automated video analysis technologies' and 'Increasing number of CCTV solutions are made available with some degree of automated analytic capabilities by suppliers from large-scale system integrators to small and medium enterprise (SME) software developers including IBM, Bosch…'[27].

77. What this leads to is to the increase in "predictive policing" based on CCTV automated analysis[28]:

> *'Next time you see a surveillance camera following you down an alleyway, don't be too sure that there's a human watching.*
>
> *Surveillance camera companies are increasingly relying on artificial intelligence (AI) to automatically identify and detect problematic criminal behaviour as it happens… "We are recognizing a precursor pattern that may*

[27] https://www.eecs.qmul.ac.uk/~sgg/papers/GongEtAl_SecuritySurveillance2011.pdf

[28] http://uk.businessinsider.com/security-cameras-use-artificial-intelligence-to-detect-crime-2015-8?r=US&IR=T

be associated with a crime that happens" Wesley Cobb, chief science officer at [AIsight] told Bloomberg." '

78. We know about these developments, but there is little information about any use or reliance on such mechanisms by law enforcement and intelligence agencies - let alone developed any public policies or guidelines on their use. The Commissioner should thus step in and fill this void.

Conclusion

79. The mere fact that data is obtained through so-called 'overt' surveillance cameras, does not mean that the resulting interference with an individual's private life is minor. New forms of technology permit local and national government and law enforcement agencies to record and monitor large amounts of increasingly intimate information.