

# BIG BROTHER WATCH

## DEFENDING CIVIL LIBERTIES, PROTECTING PRIVACY

### Home Affairs Select Committee Inquiry into Policing for the future - Big Brother Watch Response

February 2017

#### About Big Brother Watch

1. Big Brother Watch is a civil liberties and privacy campaign group founded in 2009. We have produced unique research exposing the erosion of civil liberties in the UK, looking at the dramatic expansion of surveillance powers, the growth of the database state and the misuse of personal information.
2. Specific to this inquiry we have released reports looking at the police's handling of personal data and the number of times forces request access to communications data. We have also been active in calling for the limited and proportionate use of new technologies such as drones and body worn cameras.

#### Key Points

- **The future of policing will involve new types of crime and new technology.**
- **New technology has to be properly debated and regulated before it is used.**
- **Police forces have to be transparent about what they are doing.**

#### Response

3. The nature of crime is changing. This is shown by the latest Office of National Statistics crime figures; which revealed over two million computer misuse offences occurred in the past year alone.<sup>1</sup> The rise in online and connected technology crime is a new problem not just in the minds of the general public but of the police as well.
4. So with that in mind it is clear that the training and skills of police officers will need to adapt in order to combat new types of crime. It is encouraging to hear the Home Secretary confirm that the College of Policing is now training officers to deal with "*internet crime*" as well as traditional criminal activity. We support this move as we are conscious that there is a profound digital skills gap across the police service as a whole.
5. We cannot avoid the use of technology in policing and nor should we. It is essential that policing moves with the times. Capabilities such as Automatic Number Plate Recognition (ANPR) are longstanding whilst others such as facial recognition technology, body worn cameras and drones are new players and are currently not used everywhere. We acknowledge that there is support for increasing the use of such technology but we raise concern about the pursuit of new capabilities without first considering the legislation, regulation and oversight that must run alongside any deployment.

---

<sup>1</sup> BBC News, *Cybercrime and fraud scale revealed in annual figures*, 19<sup>th</sup> January 2017:  
<http://www.bbc.co.uk/news/uk-38675683>

# BIG BROTHER WATCH

## DEFENDING CIVIL LIBERTIES, PROTECTING PRIVACY

6. From the point of view of the police these technologies offer a number of advantages. But it must be acknowledged that they also have the potential to fundamentally change the relationship between the police and the general public. After all each of these capabilities has the potential to be a tool of surveillance against anyone, regardless of whether they are suspected of criminal activity or not.
7. Whilst it may be assumed that citizens are happy to be monitored in public places for the purpose of their security, we must not be complacent about the risks such technologies can bring. Equally as important is the need to actually inform them of the actions being taken in their name; policing by consent cannot be forgotten just because the tools available are changing.
8. It's vital that every new technology receives proper scrutiny before it is deployed on a permanent basis. A trial alongside real public and parliamentary engagement can help identify any problems, for example with privacy, training or data protection, at an early stage. Any issues can then be addressed more easily than if the project has already been fully embedded in the day to day work of law enforcement.
9. Historically there are numerous examples to show that a lack of scrutiny and effective governance at an early stage has created problems. We refer specifically to ANPR. ANPR collects information about every motorist in the UK regardless of whether they are suspected of being a criminal or not.
10. ANPR was originally used as a tool to tackle the threat of Northern Irish terrorism in the 1980s and 1990s. In the following years, far from being restricted, the system evolved beyond all recognition. It has been widely adopted on all major roads in the UK, capturing the licence plates of every passing car for the purpose of *"tracking MOT, insurance and vehicle theft"*<sup>2</sup>.
11. It is well known that the amount of data captured and retained by the ANPR system is vast. The National ANPR Data Centre (NADC) holds around 30 billion images, with between 30 and 40 million more being captured by cameras every single day<sup>3</sup>. The Surveillance Camera Commissioner (SCC) has repeatedly raised concerns about ANPR defining it as *"one of the largest intelligence gathering tools in the world"*<sup>4</sup> and stating in his 2014-2015 Annual Report that:

---

<sup>2</sup> Surveillance Camera Commissioner, *Annual Report 2015/16*, 16th November 2016, p. 23:  
[https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/569559/57586\\_unnum\\_camera\\_WEB.PDF](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/569559/57586_unnum_camera_WEB.PDF)

<sup>3</sup> Ibid, p. 23

<sup>4</sup> Surveillance Camera Commissioner, *Annual Report 2014/15*, November 2015, p. 13:  
[https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/480176/51745\\_SCC\\_Annual\\_Report\\_2014-15\\_Accessible.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/480176/51745_SCC_Annual_Report_2014-15_Accessible.pdf)

# BIG BROTHER WATCH

## DEFENDING CIVIL LIBERTIES, PROTECTING PRIVACY

*“There is no statutory authority for the creation of the national ANPR database, its creation was never agreed by parliament, and no report on its operation has even been laid before parliament.”<sup>5</sup>*

12. It is staggering to think that this remains the case over 30 years on from the introduction of the technology. The public has little to no understanding of why the ANPR system is in place or what it is capable of. This could have been avoided had a robust debate about the role of ANPR, followed by clearly drafted legislation, taken place at an early stage.
13. ANPR is not the only example of a technology which has been used without proper scrutiny, transparency, or public engagement. As recent events have shown many forces are well on the way to replicating the poor standard set by ANPR.
14. Leicestershire Police trialled facial recognition software on attendees at Download Festival in 2015. The process of informing people was little more than having your picture taken being a condition of entry to the festival<sup>6</sup>. It failed to state that the images taken would be for policing purposes and that they would be specific facial biometric images rather than your average picture. Furthermore the Force failed to state that every image would be run against a European wide criminal database and there was no immediate information about what the retention policy for the images would be. Indeed when the press got wind of the scheme the force failed to coherently explain their plans, repeatedly changing their story as to why they were deploying this new, little understood and intrusive capability on an unsuspecting and unaware group of people who had paid to attend the festival.
15. The Metropolitan Police attempted to learn from the errors made by Leicestershire Police by taking a far more transparent approach before they conducted a trial of facial recognition cameras at 2016’s Notting Hill Carnival. The Force’s spokesperson for the event gave details on how the system would operate and the news was widely reported. Unfortunately we are not aware of any findings from the trial being published.
16. The poor approach to discussing facial biometrics is longstanding. In 2015 it was revealed that police forces had uploaded 18 million custody suite images to the Police National Database (PND) without consulting either the Home Office or the Biometrics Commissioner. Many of the photos were thought to be of innocent people.
17. This situation occurred because of a lack of leadership on biometrics. The Home Office has repeatedly failed to publish its Biometrics Strategy and there has been no meaningful debate

---

<sup>5</sup> Surveillance Camera Commissioner, *Annual Report 2015/16*, 16th November 2016, p. 23:  
[https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/569559/57586\\_unnum\\_camera\\_WEB.PDF](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/569559/57586_unnum_camera_WEB.PDF)

<sup>6</sup> ITV News, *Download Festival: Police use facial recognition technology on revellers*, 13<sup>th</sup> June 2015:  
<http://www.itv.com/news/2015-06-13/download-festival-police-use-facial-recognition-technology-on-revellers/>

# BIG BROTHER WATCH

## DEFENDING CIVIL LIBERTIES, PROTECTING PRIVACY

about how this new technology should be used by law enforcement. This resulted in a grey area which should not have been exploited.

18. ANPR and facial biometrics are examples of poor communication, scrutiny and governance. But other technologies, such as drones and body worn cameras, are examples of where there has been a slightly more positive approach.
19. Between 2013 and 2015 the number of complaints to the police about drones rose by 2,000%<sup>7</sup>. Clearly the public is concerned about the technology and the police have to lead the way in responsible drone use. To achieve this they have to be clear about why they are using drones and be proactive in engaging members of the public on the issue.
20. The use of drones by police forces across the country is often secretive; which is unhelpful. We understand why trialling technology must have an element of opaqueness to it but too little information creates public mistrust.
21. In a number of cases forces announced they were using drones, but stopped short of giving firm examples of how, why and when. Many relied on broad statements listing a wide range of police activities which officers thought might be enhanced by the use of drones.
22. It is necessary for a properly informed conversation to take place before drones are deployed permanently. For this to happen public engagement needs to be fostered through the publication of good statistics to show how the technology is being used. Without this process the police could find themselves fielding complaints about privacy infringements rather than being able to reassure the public that the technology is keeping them safe.
23. The approach taken to the use of body worn cameras has to our mind been the most positive. The police consulted widely about the technology prior to adopting it.
24. Many police forces worked hard to engage with civil society groups and members of the public to raise awareness before the deployment of body worn cameras. One example is that of the Metropolitan Police which has published detailed information about how the cameras it is deploying will be used, why officers are being equipped with them and what their capabilities are.<sup>8</sup>
25. Unfortunately good engagement can't make up for the confused evidence base which supports the deployment of cameras. Although a number of well publicised reports have been released purporting to show the effectiveness of body worn cameras more work needs to be done to conclusively show where they can be of use.

---

<sup>7</sup> Sky News, *Calls to Police Over Drones up by 2,000%*, 16<sup>th</sup> December 2015: <http://news.sky.com/story/calls-to-police-over-drones-up-by-2000-10335752>

<sup>8</sup> Metropolitan Police Service, *Rollout of body worn cameras*, 17<sup>th</sup> October 2016: <http://news.met.police.uk/news/rollout-of-body-worn-cameras-191380>

# BIG BROTHER WATCH

DEFENDING CIVIL LIBERTIES, PROTECTING PRIVACY

26. In contrast to the good explanations about what the cameras are capable of and why they are being used a report on the Metropolitan Police's trial by the College of Policing and the Mayor's Office for Policing and Crime found that they didn't provide many of the benefits that may be expected. Although there was a decrease in the number of allegations and complaints officers faced whilst wearing body worn cameras this trend was in line with decreases across the force. In addition the report found no impact on the quality or quantity of stop and searches, arrests for violent crime or the way in which officers dealt with victims or suspects.<sup>9</sup>
27. Any new technology should be supported by strong evidence. At present more work needs to be done to justify the number of body worn cameras being purchased by police forces.

---

<sup>9</sup> College of Policing and the Mayor's Office for Policing and Crime, *Police, Camera, Evidence: London's cluster randomised controlled trial of Body Worn Video*, November 2015:  
[http://whatworks.college.police.uk/Research/Documents/Police\\_Camera\\_Evidence.pdf](http://whatworks.college.police.uk/Research/Documents/Police_Camera_Evidence.pdf)