Police Drones and the Possible Human Rights Issues:

A Case Study from England and Wales

Angela Paul

PhD Candidate in Law, Northumbria University, UK

BILETA Annual Conference 2023

Abstract

This paper stems from my PhD project centred on the use of Unmanned Aerial Vehicles (UAVs), or drones. Here, the main emphasis is placed on the human rights implications related to the use of the technology for law enforcement purposes. Generally, the unique capabilities of drones are highly useful in police operations such as missing people searches, collecting evidence from dangerous situations, and disaster relief efforts. However, the usage of drones for surveillance purposes, in particular, can bring in issues related to privacy and unnecessary biases. This paper, therefore, will explore these issues by presenting some key findings from my research, involving police forces in England and Wales. There is currently no national policy and guidelines specifically for the deployment of drones by the police, and therefore Freedom of Information (FOI) requests were distributed to the concerned police forces, with a view to explore their norms and practices in relation to the use of drones. More specifically, whether their procedures address the possible human rights implications. Lessons from this case study are also expected to provide important insights into the use of related AI technologies in the policing realm.

The existing legislation mainly focuses on physical safety concerns associated with drones, aviation rules, and the drones used by criminals. However, the seamless embedding of drones into the civilian sphere by the police will raise concerns of a lack of transparency with the public. Therefore, the current work stresses the importance of direct research with law enforcement, as policing research should act as a collaboration between law enforcement and academia. Thus, the paper takes an approach which not only acknowledges the advantages of drones as an efficient technology, but also asserts how addressing the human rights threats can in fact improve the effectiveness of its use in law enforcement.

Introduction

A historical concept which is prevalent in the discussion of omnipresent, secretive surveillance in law enforcement would be the Panopticon. The Panopticon, as coined by Jeremy Bentham in the 19th Century, was the architectural design of a prison in which the inmates could be ubiquitously watched by one prison guard, without knowing that they are being watched.[1] Now, what if the panopticon concept was combined with wings, a high-tech camera and the latest software capabilities?

Unmanned Aerial Vehicles (UAVs), also referred to as 'drones', are used by law enforcement for many different purposes, from searching for missing people, through to monitoring migrants at borders. It is not very difficult to understand the swift transition of police aviation from helicopters to UAVs, as time and cost are of the essence in everyday policing. Drones are merely one tool within the law enforcement toolkit of technologies *inter alia* Bodycams, Closed-Circuit Television (CCTV), Automated Number Plate Recognition (ANPR), crime-mapping algorithms, and ShotSpotter technologies. The use of these technologies has not been without controversies, owing to their common inaccuracies, biases, and privacy issues, all of which implicate civil liberties. In short, drones are a widespread phenomenon in today's world, with hobbyist, commercial and law enforcement users being able to purchase and use the technology with relative ease.

The ongoing work towards my thesis mainly examines what are the possible human rights implications of the use of police drones. Furthermore, through a socio-legal analysis and, by adopting an empirical approach, further analyses whether these issues are appropriately reflected in the policy documentation used by police forces. The primary aim of the thesis is to create a national framework for the use of police drones in England and Wales. This paper is based on some of the key findings of the thesis project so far. The paper first reflects upon the lessons which can be learned from the empirical methodology. This is beneficial in understanding policing research, and how this process can be improved. Following this, two of the policy documents requested from the police during the empirical research stage, are examined.

[1] Greg Elmer, 'Panopticon – Discipline – Control' in Kirstie Ball et al (eds), *Routledge Handbook of Surveillance Studies* (Routledge 2012), 28; David Lyon et al., *Routledge Handbook of Surveillance Studies* (Taylor & Francis Group 2012), 4; Kevin D. Haggerty and Richard V. Ericson, 'The Surveillant Assemblage' (2000) 51 *British Journal of Sociology*, 606-607.

Methodological Findings

As indicated earlier, there are regular reports from the media on the use of police drones by police forces in England and Wales, for numerous uses such as missing person searches, crime scene investigations, firearm incidents, counter-terrorism efforts, and public order monitoring.[2] However, there is very little information available on a national level on these deployments. Furthermore, although there are many controversies surrounding the use of drones, especially from civil liberties campaigners, there are currently no explicit national policies which specifically deal with how drones should be used by the police in England and Wales. There is no obligation on police forces to provide information on their policies and guidelines. Therefore, there is a gap in the knowledge pertaining to this. As a result, it was decided that there needs to be direct research conducted with all 43 territorial police forces, to gain up-to-date information.

For this project, two empirical methods were employed; survey questionnaires and FOI requests. For the survey questionnaire, an online anonymised survey was designed, with the aim for it to be distributed to the 43 territorial police forces (Table A) in England and Wales. This distribution proved to be unsuccessful, as will be discussed in the next section. The FOI requests were distributed to the 43 territorial police forces, and also to the Ministry of Defence, Police Service Northern Ireland (PSNI), Police Scotland and the British Transport Police. Table B summarises the response rate for these two empirical methods.

Table A: The Territorial Police Forces

Country	Police Forces
England	Avon and Somerset; Bedfordshire; Cambridgeshire; Cheshire; City of London; Cleveland; Cumbria; Derbyshire; Devon and Cornwall; Dorset; Durham; Essex; Gloucestershire; Greater Manchester;

[2] Brian Anderson, 'Criminals are using Heat-Seeking Drones to Sniff Out Weed – and Steal it' *VICE* (19 April 2014) <https://www.vice.com/en/article/nzezjw/criminals-are-using-heat-seeking-drones-to-sniff-out-weedand-steal-it> accessed 10 March 2023; BBC, 'North Wales Police Use Drones to Fight Crime' (10 January 2018) <https://www.bbc.com/news/uk-wales-42636797> accessed 10 March 2023; Harriet Agerholm, 'Drones: Six Positive Ways They Can Be Used' *BBC* (13 March 2019) <https://www.bbc.com/news/uk-46829931> accessed 10 March 2023; Oprah Flash, 'Police Drones Swoop on £75K Cannabis Farm in West Bromwich' *Birmingham Live* (25 February 2021) <https://www.birminghammail.co.uk/black-country/police-drones-swoop-75k-cannabis-19912997> accessed 10 March 2023; BBC, 'Drones Used to Police Illegal Water Abstraction in Lincolnshire' (13 August 2022) <https://www.bbc.com/news/av/uk-england-lincolnshire-62527171> accessed 10 March 2023; Isabelle Bates, 'Police Drone Used in Smethwick Cannabis Factory Bust as Man Arrested' (18 October 2022) <https://www.birminghammail.co.uk/black-country/police-drone-used-smethwick-cannabis-25293362> accessed 10 March 2023.

	Hampshire; Hertfordshire; Humberside; Kent; Lancashire; Leicestershire; Lincolnshire; Merseyside; London Metropolitan; Norfolk; Northamptonshire Northumbria; North Yorkshire; Nottinghamshire; South Yorkshire; Staffordshire; Suffolk; Surrey; Sussex; Thames Valley; Warwickshire; West Mercia; West Midlands; West Yorkshire; Wiltshire.
Wales	Dyfed-Powys; Gwent; North Wales; South Wales.

Table B: Empirical Method Response Rates

Type of Empirical Method	Number of Responses
Anonymised Questionnaires	3
Freedom of Information (FOI) Request	31*

* This is excluding the additional forces (Ministry of Defence, PSNI, Police Scotland, British Transport Police).

Issues Encountered in Research with the Police

Reiner and Newburn have categorised individuals who conduct research with the police into four categories: inside insiders; outside insiders; inside outsiders; and outside outsiders.[3] The authors use this categorisation to display the relationships, or lack of relationships for that matter, that researchers can have with police forces, which can then influence the ease or difficulty at which policing research can be conducted. For instance, "inside insiders" are those who still work in the police, and "inside outsiders" are individuals who used to be police officers, and as a result researchers who fall into these two categories are likely to find it easier to conduct research with the police.[4] "Inside outsiders" are usually individuals who are not police officers, but they work closely with police forces, whilst "outside outsiders" have no connection with police forces.[5] As an academic, with connections to some inside insiders and inside outsiders, I fall into the "outside outsiders" category.

[3] Robert Reiner and Tim Newburn, 'Policing Research' in King and Wincup (eds), *Doing Crime and Justice* (Oxford University Press 2008, 2nd ed), 355-357.
[4] Ibid.
[5] Ibid.

The difficulty in conducting policing research as an academic was evident through the questionnaire process of this study, as it was not distributed to the 43 police forces as planned. It was expected that a senior member of a police force, a drone lead for England and Wales, or a higher policing body would be able to facilitate the distribution of the questionnaire. However, these requests were refused, with the justification that they receive many research requests, and cannot prioritise one researcher over another. The questionnaires were designed in a manner in which there was complete anonymity for the police force, as data was to be aggregated. The questionnaires also had a great degree of flexibility, as each question had a "prefer not to say" option, which was in place to assess what information different police forces are comfortable with providing. Albeit, the College of Policing agreed to post the survey information to their 'knowledge hub' which can be accessed by many police officers if they wish to do so.

Although there were not a high number of responses, the few responses received were proven to be useful as the online survey allowed for many open questions to be asked. Consequently, the questionnaire also had questions outside of just drone technology, including some questions on the use of biometric technologies within the police force. However, if the questionnaire distribution had been facilitated, there would have been a significant level of data on the various aspects of police drones. It is to be noted that there was a survey by the Surveillance Camera Commissioner (SCC) conducted in June 2022 on the use of overt surveillance camera systems in public places by police forces in England and Wales[6], which is around the same time that the current project's empirical research also began. This survey was not limited to drones, as it also covered CCTV, ANPR, body-worn cameras, helicopter-borne cameras, and facial recognition technologies.[7] This survey revealed that 31 forces responded that they used drone cameras; however, this included the non-territorial police forces as well. Therefore, this is a similar response rate to my FOI requests. In the Commissioner's report, 15 respondents stated that their drones can record video, and 2 stated that their drones can record audio.[8] This report, however, only had a small section on drones, and focused more on their manufacturers and network topology, when compared to this project's empirical research which is centred on human rights implications. The higher response rate for the commissioner's survey indicates the relative difficulty faced when conducting an academic survey when compared to a governmental survey.

FOI requests can be a competent way of conducting research in the social sciences[9], especially for academic researchers. Although FOI requests were an effective way to ensure responses, as

[6] Office of the Biometric 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) <https://www.gov.uk/government/publications/police-survey-2022-responses-and-key-findings> accessed 13 March 2023.
[7] Ibid.
[8] Ibid.
[9] Raymond M. Lee, 'The UK Freedom of Information Act and Social Research' (2005) 8 *International Journal of Social Research Methodology*, 4; Kevin Walby and Alex Luscombe, 'Ethics Review and Freedom of Information Requests in Qualitative Research' (2018) 14 *Research Ethics*, 2-3.

evident from the high response rate, there were some issues in terms of inconsistencies on how FOI exemptions were applied by police forces. This is more of an issue surrounding how there needs to be a consensus amongst the police forces on how they answer certain questions, rather than an issue with the method of data collection. This discrepancy was evident in how all the FOI questions were answered across the board. The FOI act exemptions allow public officials to withhold information, and the exemptions used by the police forces in this study included:

> *"Section 23 Information Supplied by, or concerning, certain Security Bodies;*
>
> *Section 24 National Security;*
>
> *Section 31(3) Law enforcement"*[10]

Understandably, police forces are likely to withhold or redact any information which would hinder their police tactics. However, when one force openly reveals information surrounding their use of a certain technology, which another force completely withholds, it is a clear indication of different standards of transparency. It is also questionable why there would be different standards of transparency for the same technology which is used for the same purpose. Figure A, Table C and Table D display examples of these discrepancies encountered. Out of the 31 forces who responded, 2 did not actually answer any of the questions and used the exemptions to withhold all information on drones.

[10] The Freedom of Information Act 2000.

Figure A: Forces' Own Drone Operations Manual (as attached in FOI response)

Police Force 1:

3.10 [redacted]
3.11 Security and Privacy
3.12 Other Documents
Operations
4.1.1 Types Of Operation
4.1.2 Operation Examples
4.1.3. Areas of Operation
4.1.4. [redacted]
4.1.5. [redacted]
4.1.6 [redacted]
4.2 [redacted]
4.3 [redacted]
4.4 [redacted]
4.5 [redacted]
4.6 [redacted]
4.7 [redacted]
4.7.1 [redacted]
4.7.2 [redacted]

15. Pre-Planned Operations Procedure

[redacted]

16. Spontaneous Operations Procedure

Some examples of spontaneous incidents might include:-

[redacted]

Police Force 2:

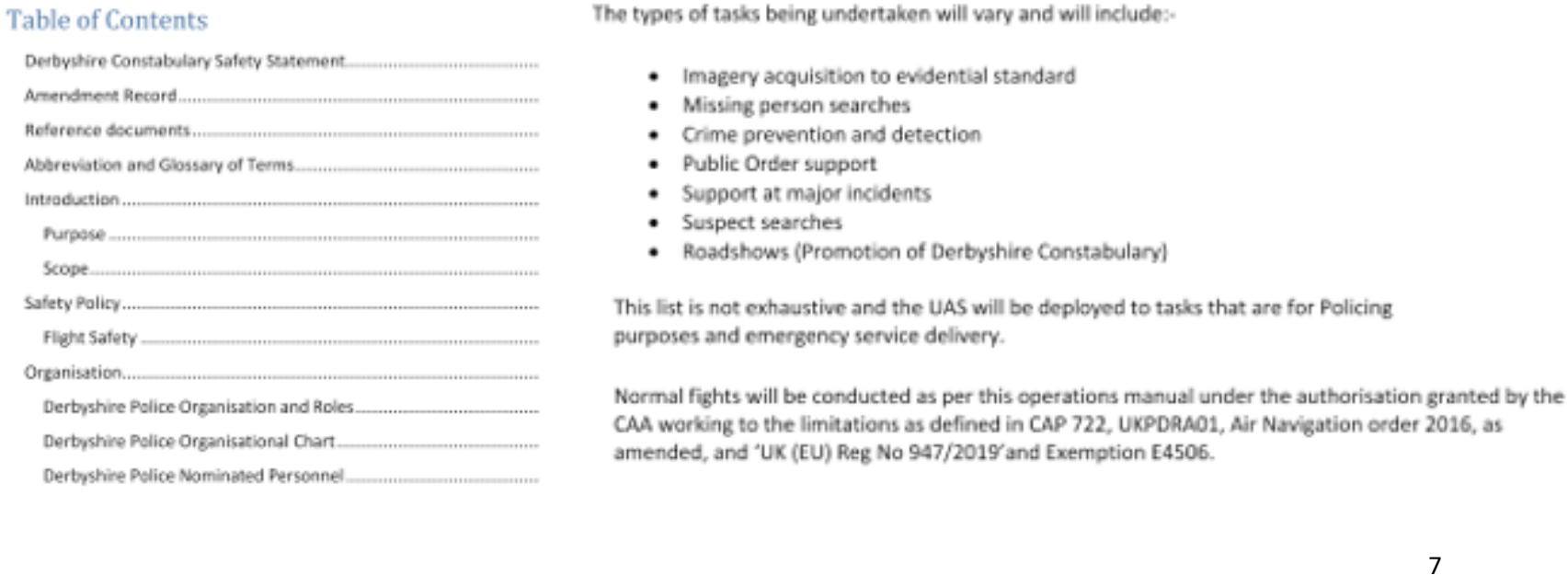

Table of Contents

Derbyshire Constabulary Safety Statement
Amendment Record
Reference documents
Abbreviation and Glossary of Terms
Introduction
Purpose
Scope
Safety Policy
Flight Safety
Organisation
Derbyshire Police Organisation and Roles
Derbyshire Police Organisational Chart
Derbyshire Police Nominated Personnel

The types of tasks being undertaken will vary and will include:-

- Imagery acquisition to evidential standard
- Missing person searches
- Crime prevention and detection
- Public Order support
- Support at major incidents
- Suspect searches
- Roadshows (Promotion of Derbyshire Constabulary)

This list is not exhaustive and the UAS will be deployed to tasks that are for Policing purposes and emergency service delivery.

Normal fights will be conducted as per this operations manual under the authorisation granted by the CAA working to the limitations as defined in CAP 722, UKPDRA01, Air Navigation order 2016, as amended, and 'UK (EU) Reg No 947/2019'and Exemption E4506.

Human Rights Concerns

(a) Privacy Issues

The panoptic ever-present watchful eye of certain law enforcement technologies, especially in a situation of public surveillance, will always bring into question the possible infringement of the privacy expected by individuals. As per the European Convention on Human Rights (ECHR) and the Human Rights Act, individuals have the right to privacy, which public officials, such as the police, must respect in their law enforcement procedures.[11]

The UK's Data Protection Act (DPA) 2018 follows the obligations under the General Data Protection Regulation (GDPR). The DPA further lists specific 'law enforcement processing' requirements, which is the processing of data concerning the "prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties including... the prevention of threats to public security".[12] The first data protection principle under the DPA states that either the data subject must have given consent to the processing of data, or the processing must be proven to be necessary for the policing task, for that processing to be lawful.[13] Police drones can capture the visual data of individuals, and then that footage can be further used for law enforcement purposes, such as crime scene investigations. Therefore, appropriate data processing safeguards must be in place.

The reason that aerial surveillance methods, whether through the use of helicopters or drones, are deployed is so that there is a large geographical area which can be covered through the aerial surveillance camera. However, unlike a helicopter, which can easily be seen and heard when flown overhead, drones can operate discreetly at certain heights. One police force in the UK, the Derbyshire police, came under scrutiny in the media for its deployment of drones for social distance monitoring purposes during the peak of the COVID-19 pandemic.[14] The police force had used drones to capture individuals in a national park and proceeded to post this footage on their social media, in an attempt to warn others of social distancing rules.[15] In the process, the force captured the visual data of individuals without consent, and further shared it online, again without consent. Although, at certain distances, the facial images of individuals may not be easily

[11] European Convention on Human Rights (ECHR) 1950, Article 8.
[12] Data Protection Act (2018), Part 3 Section 31.
[13] Ibid, Part 3 section 35.
[14] BBC, 'Coronavirus: Peak District Drone Police Criticised for 'Lockdown Shaming' (27 March 2020) <https://www.bbc.co.uk/news/uk-england-derbyshire-52055201> accessed 10 March 2023; Helen Pidd and Vikram Dodd, 'UK Police Use Drones and Roadblocks to Enforce Lockdown' *The Guardian* (26 March 2020) <https://www.theguardian.com/world/2020/mar/26/uk-police-use-drones-and-roadblocks-to-enforce-lockdown> accessed 10 March 2023.
[15] Ibid.

identifiable, their overall body language and physical characteristics could be identified. Thus, it is important to investigate whether the existing policies guiding police drones effectively address privacy concerns associated with the technology.

(b) Social Control

When a drone is flown above a height at which it can be easily seen, this is referred to as the drone operating Beyond Visual Line of Sight (BVLOS). However, drones can also be flown at a visible distance from individuals, as long as it adheres to the Civil Aviation Authority (CAA) guidelines.[16] A panoptic situation is not only one that incorporates ubiquitous surveillance, but this surveillance is also most effective when individuals know that they are being watched. The surveillant assemblage, as coined by Haggerty and Ericson, is a situation in which many surveillance systems come together to create a landscape of ultimate surveillance, and this can be used as a method of social control.[17] Individuals may be likely to change the way that they behave because they are aware of this monitoring. It is this element that makes drones which are used to monitor protests, and similar public order situations, particularly concerning if they are not used appropriately.

Under the ECHR Articles 10 and 11, individuals have the rights to freedom of expression, and freedom of assembly and association, respectively.[18] Police in England and Wales have been reported to have deployed drones in many protests.[19] According to the FOI responses for this study, 21 forces have explicitly stated that drones have been deployed by their force to monitor protests.[20] Due to increased threats of terrorist attacks in public demonstrations, it is a policing duty to be able to monitor these situations, due to public safety fears. If the protest in which a drone is being deployed is a protest against the government or the police, such as the Kill the Bill

[16] According to Civil Aviation Authority guidelines, drones must not operate above 400 feet from the earth's surface. Also see: Bruce Crumley, 'UK Units to Test BVLOS Deployment of Police Drones' (8 February 2022) *Drone DJ* <https://dronedj.com/2022/02/08/uk-units-to-test-bvlos-deployment-of-police-drones/> accessed 8 March 2023; Simon Parkin, 'Police drones offering eye-in-sky 20 miles away to be piloted in Norfolk' *Eastern Daily Press* (7 February 2022) <https://www.edp24.co.uk/news/crime/20633231.police-drones-offering-eye-in-sky-20-miles-away-piloted-norfolk/> accessed 8 March 2023.

[17] Haggerty Ericson (n1), 605-622.

[18] ECHR (n 11), Article 10 and Article 11.

[19] Vikram Dodd, 'Drones Used by Police to Monitor Political Protests in England' *The Guardian* (15 February 2021) <https://www.theguardian.com/uk-news/2021/feb/14/drones-police-england-monitor-political-protests-blm-extinction-rebellion> accessed 13 March 2023; The Voice, 'Police Drones Monitor Asylum Seeker Protest' (26 February 2023) <https://www.voicenewspapers.co.uk/news/police-drones-monitor-asylum-seeker-protest-597529> accessed 13 March 2023.

[20] Out of the 27 forces that own drones: 21 forces have specified they have used drones for protests; 1 force does not; 2 did not disclose whether they do; and 2 did not specify they use it for drones; and 1 has stated their drone has been grounded.

protests (which were protests for the freedom to protest itself)[21], there may be a fear of their freedom of expression being suppressed.[22] As mentioned, drones can be flown at a height which is within people's visual line of sight. Therefore, a protestor seeing that a drone is being operated at a protest, and that their visual data is being captured by this drone, could deter the protestor.

Owing to the advancements in drone technology, it is not only the video footage captured that allows for a protestor to be identified at a protest. This is because drones are mostly equipped with Global Positing Service (GPS) technology, which can identify the geographical location of where the drone footage was taken from.[23] Furthermore, drones can also be combined with an International Mobile Subscriber Identity (IMSI) catcher, which is a technology that tricks mobile phones by imitating a cell tower, to track and intercept the phones.[24] In the United States, IMSI catchers have been reported to be used by the US police to spy on BLM protestors.[25] It is likely that the UK follows or is likely to follow, the US. In fact, a British company, which markets technologies to UK police forces, has advertised their innovative portable IMSI catcher, which can be easily mounted to existing drones.[26] This is an example of surveillant assemblage, as firstly there is an overall movement towards limiting freedom of speech and protest, as seen in the 'Kill the Bill' demonstrations, which is then furthered by the use of technology that can influence human behaviour through mass surveillance.

---

[21] Gracie Mae Bradley, 'How the British Government is Trying to Crush our Right to Protest' *The Guardian* (15 December 2020) <https://www.theguardian.com/commentisfree/2020/dec/14/british-government-right-to-protest-limitations-freedoms-pandemic-legislation> accessed 13 March 2023; The Economist, 'An Illiberal Bill to Suppress Protest in Britain' (18 March 2021) <https://www.economist.com/leaders/2021/03/18/an-illiberal-bill-to-suppress-protest-in-britain> accessed 13 March 2023.

[22] Anthony McCosker, 'Drone Vision, Zones of Protest, and the New Camera Consciousness' (2015) 9 *Media Fields Journal*, 1-14; Finn and Wright, 'Unmanned Aircraft Systems: Surveillance, Ethics and Privacy in Civil Applications' (2012) 28 *Computer Law and Security La*w, 188; Neil J. Waghorn, 'Watching the Watchmen: Resisting Drones and the Protestor Panopticon' (2016) 71 *Geographica Helvetica*, 99.

[23] McCosker (n22), 2.

[24] James Rippingale, 'As UK Cracks Down on Protests, Surveillance Tech Market Grows' *Al Jazeera* (5 October 2021) <https://www.aljazeera.com/news/2021/10/5/surveillance-tech-centre-stage-at-international-security-expo> accessed 10 March 2023; Eyako Heh and Joel Wainwright, 'No Privacy, No Peace: Urban Surveillance and the Movement for Black Lives' (2012) 3 *Journal of Race, Ethnicity and the City*, 124-125; Privacy International, 'How Police Drones Technology Can Be Used at a Protest' (5 May 2021) <https://privacyinternational.org/explainer/4498/how-police-drones-technology-can-be-used-protest> accessed 10 March 2023.

[25] Heh and Wainwright (n24), 124-125; Kim Zetter, 'How Cops Can Secretly Track Your Phone' *The Intercept* (31 July 2020) <https://theintercept.com/2020/07/31/protests-surveillance-stingrays-dirtboxes-phone-tracking/> accessed 13 March 2023; Sam Briddle, 'U.S. Marshals used Drones to Spy on Black Lives Matter Protests in Washington, D.C.' *The Intercept* (22 April 2021) <https://theintercept.com/2021/04/22/drones-black-lives-matter-protests-marshals/> accessed 13 March 2023.

[26] Rippingale (n24); Mike Ball, 'IMSI & WIFI Catcher Surveillance Devices for Drones' *Unmanned Systems Technology* (27 May 2022) <https://www.unmannedsystemstechnology.com/2022/05/imsi-wi-fi-catcher-surveillance-devices-for-drones/> accessed 12 March 2023..

(c) Biometric Concerns

When drones are being deployed for surveillance purposes, for example at a large sporting event, or for monitoring public disorder, the main purpose of the deployment would be to identify the activity of individuals. This is also the case when observing a crime scene, as they may look for suspects in that area. Even in the case of a missing person search, they would be using the drone to search an area to find an individual who matches the profile of the person that is missing. Therefore, there is a process of identification using the footage captured by the drone. A camera technology which is used for similar purposes would be Closed-Circuit Television (CCTV) cameras, and the UK has one of the highest numbers of public CCTV cameras in the world.[27] This is not surprising, as CCTVs have proven to be an effective police investigation method in the UK.[28] However, combining CCTV footage with biometric technologies such as facial recognition and Automated Number Plate Recognition (ANPR) has received criticism for human rights violations.[29] Facial recognition technologies have especially been criticized for their disproportionate impacts on non-White individuals, and such biases would be a violation of Article 14 of the ECHR, on the prohibition of discrimination.[30] Drones also capture video footage and can be even more invasive as they can cover a large amount of area, whilst CCTV cameras are in one fixed location. It is, thus, important to consider the possible discriminatory effects of using facial recognition to analyse drone footage for law enforcement purposes.

The *Bridges* case explored the human rights violations associated with the police's use of facial recognition technologies, as the claimant asserted that the footage of him from a protest,

[27] Craig Williams, 'Glasgow's 5,352 CCTV Cameras Makes it the 'Most Surveilled' City in UK' *GlasgowLive* (1 February 2022) <https://www.glasgowlive.co.uk/news/glasgow-news/glasgows-5352-cctv-cameras-make-22929514> accessed 14 March 2023; Matthew Chandler, 'Gwynedd CCTV has Increased by More than 350 Percent since 2019, Figures Show' *North Wales Chronicle* (17 October 2022) <https://www.northwaleschronicle.co.uk/news/23054822.gwynedd-cctv-increased-350-per-cent-since-2019-figures-show/> accessed 14 March 2023; Amy Fanworth, 'People in East Lancashire Being Watched by Hundreds of CCTV Cameras' *Lancashire Telegraph* (11 November 2022) accessed 14 March 2023.

[28] Mark Townsend, 'How CCTV Played a Vital Role in Tracking Sarah Everard – and Her Killer' *The Guardian* (3 October 2021) <https://www.theguardian.com/uk-news/2021/oct/02/how-cctv-played-a-vital-role-in-tracking-sarah-everard-and-her-killer> accessed 14 March 2023; BBC, 'Lincoln CCTV Cameras Lead to Seven Arrests in First Month' (24 June 2022) <https://www.bbc.com/news/uk-england-lincolnshire-61916283> accessed 14 March 2023.

[29] Emine Sinmaz, 'Sadiq Khan Faces Legal Challenge Over Traffic Camera Surveillance' *The Guardian* (4 August 2022) <https://www.theguardian.com/uk-news/2022/aug/03/sadiq-khan-faces-legal-challenge-over-traffic-camera-surveillance> accessed 14 March 2023; Ivana Davidovic, 'Should We Be Worried by Ever More CCTV Cameras' *BBC* (18 November 2019) accessed 14 March 2023.

[30] Pete Fussey and Daragh Murray, 'Independent Report on the London Metropolitan Police Services' Trial of Live Facial Recognition Technology' *The Human Rights Big Data and Technology* (July 2019), 22; Joe Purshouse and Liz Campbell, 'Automated Facial Recognition and Policing: A Bridge Too Far?' (2022) 42 *Legal Studies*, 209-227; Joy Buolamwini, 'Artificial Intelligence has a Problem with Gender and Racial Bias' *Time* (17 February 2019) <https://time.com/5520558/artificial-intelligence-racial-gender-bias/> accessed 14 March 2023.

captured by a CCTV, was used in facial recognition software.[31] The Court held that the police force's use of facial recognition was partially unlawful, as its use on an ongoing basis violated Article 8 of the ECHR.[32] The case also refers to the Surveillance Camera Commissioner's (SCC) Code of Practice, and the need for police to complete the SCC 'Self-Assessment Tool' as a risk assessment.[33] Furthermore, the Court ruled that the police force did not comply with their Public Sector Equity Duty, under the Equality Act 2010. This is because they did not assess any indirect discrimination, on the grounds of sex or race, which could result from the use of facial recognition technology. The implications of biometric technologies are closely linked to the phenomenon described by Lyon as "surveillant sorting", which looks at the relationship between digital surveillance and social segregation.[34] In this surveillance process, the personal data of individuals is collected, which can then be used to sort people into certain categories, which can have discriminatory effects.[35] Likewise, biometric technology may sort individuals into categories based on the colour of their skin. As a similar surveillance camera technology, it should be expected that SCC guidelines and other important risk assessments on facial recognition should be investigated when it comes to drone technology as well.

As mentioned earlier, although the faces of the data subjects may not be clear in the footage, the overall mannerisms and physical characteristics can be identified. This is especially relevant in the discussions of the merging of biometric technology and drones because facial recognition is not the only biometric analysis used by law enforcement, there is also gait recognition.[36] Gait recognition refers to a technology which can identify an individual through the manner of their body movements, especially when walking.[37] Out of the 3 questionnaire responses, two responded that they have not trialled or used gait recognition technology, and 1 force said they are unsure whether gait recognition technology has been trialled or used. This is however limited data, due to the unsuccessful distribution of the questionnaires. However, if drones are flown close to the data subject, they could likely be identifiable.

---

[31] R (Bridges) v Chief Constable of South Wales & Others [2020] EWCA Civ 1058, paragraph 28-30.
[32] Ibid.
[33] Ibid, page 57.
[34] David Lyon et al., *Routledge Handbook of Surveillance Studies* (Taylor & Francis Group 2012), 5; David Lyon, *Surveillance Society* (McGraw-Hill Education 2001), 25, 27, 52.
[35] Ibid.
[36] Elise Thomas, 'New Surveillance Tech Means You'll Never be Anonymous Again' *Wired* (16 September 2019) <https://wired.co.uk/article/surveillance-technology-biometrics> accessed 13 March 2023; City Security, 'Gait Recognition: A Useful Identification Tool' (13 July 2018) https://citysecuritymagazine.com/security-management/gait-recognition-identification-tool/> accessed 13 March 2023; Home Office and the National Police Chief's Council, 'Law Enforcement Facial Images and New Biometrics Oversight and Advisory Board: Terms of Reference' (July 2018) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/784855/Facial_Images_Board_TOR_Final_Version.pdf> accessed 13 March 2023.
[37] City Security (n 36); Privacy International, 'How Gait Recognition Technology can be Used at a Protest' (5 May 2021) <https://privacyinternational.org/explainer/4496/how-gait-recognition-technology-can-be-used-protest> accessed 13 March 2023.

Policies and Procedures Related to Police Drones

The key human rights concerns about police drones have now been examined, and the next step would be to investigate whether the policies and guidelines followed by police forces effectively mitigate these issues. This paper will subsequently discuss two key UK guidelines identified; the Surveillance Camera Commissioner (SCC) Self-Assessment Tool, and the Data Protection Impact Assessment (DPIA). These are two documents that the FOI requests sought from the police forces that own drones. Table C and Table D provide an overview of the responses to the SCC and DPIA questions.

Table C: FOI responses on SCC Self-Assessment Tool

Response	Number of Forces
Attached SCC Self-Assessment Tool	9
In Progress	3
FOI Exemptions	3
Information not held/SCC not completed	10
Drones owned but have been grounded/have not been used	2
Total Number of Police Forces with Drones	**27**

Table D: FOI responses on DPIA

Response	Number of Forces
Attached DPIA	12
In Progress	4
FOI Exemptions	4
Information not held/DPIA not completed	6
Drones owned but have been grounded/have not been used	1
Total Number of Police Forces with Drones	**27**

The element of drones which embody privacy, social control, and the possibility of biometric convergence is its visual element. It is therefore vital that the police forces have policies and procedures in place that specifically address these human rights implications. The recently revised SCC Code of Practice, under the Protection of Freedoms Act 2012, acts as guidance to public officials in England and Wales for the appropriate usage of any surveillance camera

systems that they deploy, including drones.[38] The purpose of the principles of the code is stated to be to achieve "the most appropriate balance between public protection and individual human rights" which helps the authority to "establish a clear rationale for any overt surveillance camera deployment in public spaces" whilst complying with legal duties.[39] The Code has principles which address the camera systems' impact on privacy, and the need for clear policies and procedures for the system.[40] The Code also states that the use of any biometric recognition systems must be justified and proportionate for the purpose.[41] The Code makes specific reference to all four of the ECHR articles mentioned in this paper (Articles 8, 10, 11 and 14).[42] As a part of this code, the SCC Self-Assessment Tool is a check that police forces can carry out to assess whether they are complying with the principles of the Code. Thus, it is concerning that only 9 forces hold a completed SCC Assessment Tool. One force stated:

> *"Please note that, in relation to Question 5, the Surveillance Camera Commissioner's (SCC) Self-Assessment Tool is a guidance tool and not a requirement under any legislation and has not been used"*

Although the SCC Code or Tool are not legally binding, it is one of the only guidance that explicitly addresses surveillance camera systems. If completed, it is a sufficient way to make the public aware that a force's camera technology is being used with the appropriate safeguards in place, and some forces publish their completed Self-Assessment Tools on their official websites.

The SCC Self-Assessment Tool has sections in which the police force can check whether they comply with each of the principles of the SCC Code of Practice. Principle 2 of the SCC Code of Practice states that "the use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified".[43] The section of the Self-Assessment Tool which assesses forces' compliance with Principle 2 of the Code asks whether a Data Protection Impact Assessment (DPIA) has been completed. The Tool also asks for a justification of why a DPIA has not been completed for the camera technology. Although the FOI request has asked police forces to attach their SCC Self-Assessment Tool, it was assumed that some forces who have not completed the tool may still have a DPIA. This proved to be true.

---

[38] Biometrics and Surveillance Camera Commissioner, 'Update to Surveillance Camera Code of Practice' *GOV.UK* (22 November 2021) <https://www.gov.uk/government/publications/update-to-surveillance-camera-code> accessed 26 March 2023.
[39] Ibid, 8.
[40] Ibid, 9.
[41] Ibid, 12, 20.
[42] Ibid, 11.
[43] Ibid, Principle 2.

Completing a DPIA is also an obligation, under the UK's Data Protection Act 2018, for the types of law enforcement processing that "is likely to result in a high risk of the rights and freedoms of individuals".[44] As evidenced by the human rights concerns discussed in this paper, drones would indeed be a technology for which a DPIA should be completed. According to the Data Protection Act, there are four elements that must be included in a DPIA:

> *"1) A general description of the envisaged processing operations;*
>
> *2) An assessment of the risks to the rights and freedoms of data subjects*
>
> *3) The measures envisaged to address those risks*
>
> *4) Safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Part, taking into account the rights and legitimate interests of the data subjects and other persons concerned"*[45]

The SCC provides a camera-specific DPIA template, which is available on the government's website.[46] The technologies listed in this DPIA template include fixed CCTV; Automated Number Plate Recognition (ANPR); stand-alone cameras; body-worn video; drones; and redeployable CCTV.[47] Out of the 12 forces that attached their DPIA, the SCC's camera-specific template was not completed by any of the forces. The DPIAs attached by the forces are very detailed, and follow a similar format as the Home Office's, and Information Commissioner's Office's, suggested templates.[48] The DPIAs provided in the responses also do follow the elements set out by the Data Protection Act. However, the SCC's DPIA template is unambiguously for surveillance camera technologies, which include drones. For instance, the template states that if the surveillance camera used involves "systematic and extensive profiling", "public monitoring", "data matching", "innovative technology, and/or "biometrics", the SCC DPIA should be completed. As discussed, these are the most prominent implications of police drones. These are implications distinctive to camera technologies, such as drones, when compared to other technologies that may be

[44] Data Protect Act 2018, Section 64.
[45] Ibid, Section 64(3).
[46] Biometrics and Surveillance Camera Commissioner, 'Data Protection Impact Assessment for Surveillance Cameras' *GOV.UK* (22 October 2018) <https://www.gov.uk/government/publications/data-protection-impact-assessments-for-surveillance-cameras> accessed 26 March 2023.
[47] Ibid.
[48] Information Commissioner's Office, 'Data Protection Impact Assessment' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/> accessed 10 Match 2023; Information Commissioner's Office, 'Sample DPIA Template' (9 February 2018) <https://ico.org.uk/media/2258461/dpia-template-v04-post-comms-review-20180308.pdf> accessed 10 March 2023; Home Office, 'National ANPR Service: Data Protection Impact Assessment' *GOV.UK* (31 May 2022) <https://www.gov.uk/government/publications/national-anpr-service-data-protection-impact-assessment> accessed 10 March 2023.

deployed by the police, such as predictive algorithms. Therefore, it is expected that a police force using drones should have completed this assessment.

Out of the forces that attached their DPIA, some provided redacted versions to ensure that no tactics have been provided. However, as shown by table D, 4 forces applied FOI exemptions. One force provided a completed SCC Self-Assessment Tool which stated that a DPIA had been completed, but they went on to clarify in their FOI response that this was incorrect. Now that this has been brought to their attention, they will be working towards preparing a DPIA. It could be that the forces that have said that a Self-Assessment Tool or DPIA is in progress have only started this process since the FOI request brought it to their attention. These are, however, documents that should be in place before any deployments.

Looking Forward: The Need for a National Framework

In conclusion, it can be seen that there are many human rights implications associated with police drones, particularly concerning the right to privacy, freedom of speech, and protection from discrimination, and these should be guaranteed to all individuals. At present, there is not a definite indication to the public that these human rights issues are being addressed by police forces in their deployment of drones. The relationship between law, technology and criminal justice is an active area of research in academia, and therefore creating a better opportunity for academics to conduct policing research can mitigate some of the transparency issues identified in this paper. Ultimately, it is of benefit to law enforcement bodies to ensure public trust is secured in their policing operations, as this can in turn ensure the controversy-free continuation of their day-to-day work.

As explored in this paper, under laws such as the Data Protection Act, the ECHR, and the Protection of Freedoms Act, there are some procedures which must be followed by public officials when handling the personal data of individuals. Furthermore, there are various technologies used in law enforcement in England and Wales; however, there are no specific national guidelines for each of them. Since we are scrutinising a surveillance camera technology in this study, I have focused on the overarching guidelines provided for such technologies, which are mainly the Surveillance Camera Commissioner's (SCC) guidelines. As a part of this guidance, there are assessment templates which are easily available to all police forces, including the SCC Self-Assessment Tool and associated Data Protection Assessments. However, according to the responses received in this study, not all the police forces who own drones have completed such assessments. Therefore, it is difficult for the public to understand how police forces have ensured that their legal duties have been fulfilled in the process of deploying drone technologies.

My thesis aims to use the information gathered from the socio-legal analysis and empirical research, to create a national framework for the use of drones. This will have step-by-step guidelines for the legal checks that should be in place, ensuring that the deployments for the intended policing purposes are legitimate, necessary and proportionate. Within this framework, there will be in-depth information on legal obligations; what to include in operational guidelines; as well as the key assessments that should be conducted. Although the framework in this project focuses on drone technologies, the lessons learned can be used for similar law enforcement technologies as well. It is also important to understand that each technology has its unique capabilities, which are what help the police with their operations, and this also means it has its unique implications which should be addressed in their associated guidelines.