University of Reading

GARDEN COURT CHAMBERS

Drone incidents and misuse:
Legal considerations

Anna Jackman and Louise Hooper

December 2023

TABLE OF CONTENTS

DRONE INCIDENTS AND MISUSE: LEGAL CONSIDERATIONS

Summary and how to use this document

In January 2023, the Civil Aviation Authority (CAA) estimated that 500,000 drone operators and flyers were registered under its Drone and Model Aircraft Scheme, and that it processes 7,000 operational authorisations per year. This number is expected to rise as the technology becomes more affordable and as initiatives and investment supporting the technology continue. Alongside their popularity as hobbyist devices, drones are increasingly adopted across civil and commercial sectors and applications as tools enabling aerial imagery and data gathering, and carrying and transport roles. Herein, drones are associated with a range of safety, efficiency and environmental benefits. However, the drone's growing embrace also raises challenges and concerns. From flights in proximity to manned aircraft, the transporting of contraband into prisons, to the presence of camera-laden and noisy drones, concerns continue to be raised about the safety, security, and privacy implications of drone use and misuse. While many drone incidents are accidental, drones have also been purposively and maliciously misused. In each case, drones harness the potential for injury and damage.

This report explores the **legal dimensions and potential harms associated with drone incidents and misuse.** In recognition that drone incidents and misuse involve diverse actors, actions and contexts, and cross-cuts diverse legal specialisms, Dr Anna Jackman (University of Reading) and Barrister Louise Hooper (Garden Court Chambers) co-delivered interactive focus groups bringing together lawyers from diverse specialisms to explore the legal dimensions of drone incidents and misuse. This report acts as both a summary of focus group discussions and as a space to link these discussions back to potentially relevant areas of regulation and guidance. Collectively, it highlights both that drone use, incidents and misuse raise important and complex legal questions, and that these cut across multiple areas and specialisms of law. To aid the reader, we have used bookmarks and hyperlinks to refer back to relevant information. The report is set out in 5 sections:

- Introduction to drones and drone use: Provides an overview of drone technology.
- The regulatory framework: Provides an overview of current and relevant regulation.
- Enforcing the regulations: Provides an overview of current approaches to enforcement.
- The workshops: Sets out the focus group activities and reports on key issues raised.
- Implications and recommendations: Identifies key considerations for lawyers working on cases involving drones, and offers recommendations for regulators and policy-makers.

Report methodology

The report's examination of the legal dimensions and potential harms associated with drone incidents and misuse was underpinned by the co-delivery of three interactive focus groups bringing lawyers from diverse legal specialisms into dialogue. Focus groups were held between September 2022 and March 2023, including: two focus groups with lawyers in the UK (one hybrid focus group in London; one in-person focus group in Manchester), and one online focus group with international participants from 7 countries. A total of 20 participants participated in the focus groups. Participant specialisms were wide-ranging in both legal practice and research, including: Asylum and trafficking, Autonomy, Aviation and Aerospace, Crime, Company and commercial employments, Constitutional and new law, Data protection, Family and Domestic violence, Gender equality, Immigration and Nationality, National Security, Protest, Public, and Regulation of emerging technologies.

The focus groups were structured around interactive activities exploring: the categorisation of drone incidents and misuse; how participants might proceed if they were handed particular drone incident cases (with a focus on classification and process challenges); and the potential

harms and legal questions accompanying the advent of technology advancements and/or approaches to future airspace.

This report forms part of Dr Jackman's Economic and Social Research Council funded *Diversifying Drone Stories* project (ES/W001977/1).

Key findings

- While associated with a range of benefits and opportunities, so too are drones associated with accidents, purposive and malicious misuse. The **potential threats** accompanying drone incidents and misuse include: Image and video capture (e.g., of critical and sensitive sites or activities; intrusion of privacy); Transport and carrying (e.g., outfitting drones with weaponry; transportation of contraband); Data collection (e.g., cyber attacks, corporate espionage); and disruption (e.g., flown to disrupt particular events, spaces or proceedings such as political, sport, or emergency service activities).
- Following the grouping of examples of drone incidents and misuse, we identified **key themes** from the discussions: Intention (referring to intentional and non-intentional actions and incidents, and the challenges of determining intent); Actor (reflecting on the alleged victim and perpetrator); Nature of Criminality (using drones to commit an existing criminal act versus using a drone for novel criminal activity); Legal context (whether the incident may be understood as criminal or civil); Nature of threat/ consequence (distinguishing between a drone posing the threat versus as a carrier of threat, and reflecting on levels of risk associated with particular incidents); Regulatory context (distinctions between recreational and commercial flyers, and airspace categories).
- Six **case studies of alleged drone incidents and misuse** were introduced and discussed. Across the discussions, participants raised questions about: intention (including challenges of determining), attribution (including challenges of determining, and challenges around remote operation and actors), evidence (chain of evidence, drone ownership and use, and evidence from the drone/ drone forensics), the potential of drones to enable the perpetration of existing crimes and/or enact novel criminal activity, the challenges of placing the case study (i.e., not falling neatly into particular areas of law), and the application and implications of drones in relation to existing laws and legal processes (e.g., trespass, nuisance, weaponisation, protective and non-molestation orders).
- Discussions of **emerging capabilities** (e.g., livestreaming, facial recognition) highlighted important legal questions around data (e.g., privacy rights, intellectual property, data servers, and consent), damage and liability (e.g., determining intention, securing damages and uninsured operators). In discussion of drone futures, participants also highlighted concerns around artificial intelligence (e.g., responsibilities, meaningful control, culpability, attribution), automation and autonomy (e.g., definitions, implications of different levels and forms, implications for data protection).
- Discussions of the potential legal dimensions of **proposed models of future airspace** (e.g., BVLOS, highways, integration) focused on issues of: drone routing, implications on existing planning laws, drone noise, service costs, insurance, liability and enforcement.
- Key **considerations for lawyers working on drone-related cases** include: identifying the offences or claim; understanding drone regulations; considering the actors, intention, role, context and effects of the drone; standard of proof; and wider evidentiary questions around: remoteness, accessing drone footage and information, drone forensics, enforcement powers, defences, and third party liability and indemnity.
- Our **recommendations** include: further attention to information provision and presentation; review of existing offences; guidance and resources for lawyers; training and guidance related to drone use, incidents, misuse and enforcement; consideration of potential legal challenges accompanying drone futures; inclusive consultation on regulation and policy; and understanding the potential for drone-enabled or assisted discrimination.

1. INTRODUCTION TO DRONES AND DRONE USE

What are drones?

Unoccupied Aerial Vehicles (UAVs) or Remotely Piloted Aircraft Systems (RPAS), more commonly known as drones, are aircraft without a pilot on board and which can be 'controlled remotely' by a pilot on the ground or fly with 'various levels' of automation or autonomy (POSTnote 2020: 1). Aerial drones 'come in a variety of shapes and sizes', including rotary and fixed-wing platforms, and range in size from 'small hand-held' devices to large aircraft (Haylen 2019: 4; POSTnote 2020: 1). Figure 1 provides an indication of the range of drones and their comparative capabilities.

Fig 1. In general, the larger/heavier a drone is, the greater its capability.

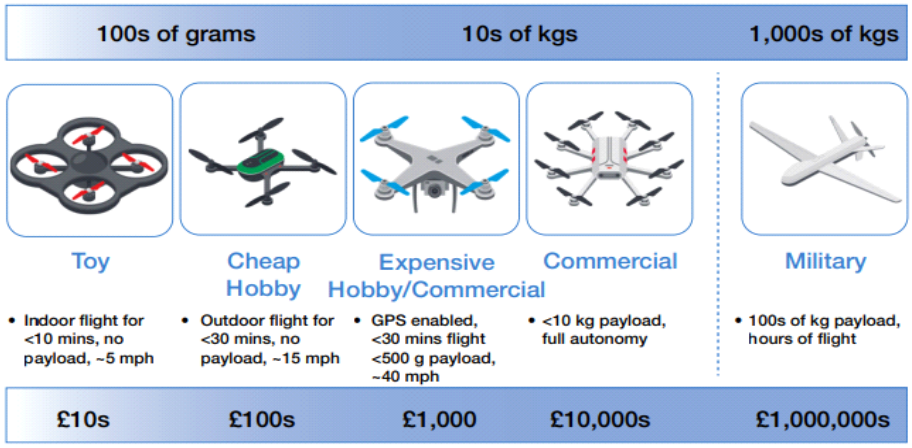

Figure 1: Range of drones. Source: UK Counter-Unmanned Aircraft Strategy (HM Government 2019: 8) https://assets.publishing.service.gov.uk/media/5dad91d5ed915d42a3e43a13/Counter-Unmanned_Aircraft_Strategy_Web_Accessible.pdf

While aerial drones are deployed in diverse civil and military contexts and applications (HM Government 2022; POSTnote 2015), this report focuses on the growing use of drones for both recreational and commercial purposes, and explores the emergent legal dimensions and questions accompanying their use and misuse.

Both commercially available off-the-shelf consumer drones and proprietary platforms developed for commercial applications are growing in number, popularity, and sophistication (POSTnote 2020; HM Government 2022). In January 2023 the UK's aviation regulator, the Civil Aviation Authority (CAA), stated that it has 500,000 drone 'operators and flyers' registered under its Drone and Model Aircraft scheme, processes 7,000 operational authorisation applications per year, and that the total number of drone pilots and aircraft are already '80% larger than the General Aviation and commercial air sector added up' (Civil Aviation Authority at Westminster Business Forum 2023). It is estimated that approximately 96% of drone flyers in the UK identify as male, and 4% as female (DronesDirect 2017; COPTZ 2021). Data from a 2017 survey suggests that 'the majority of drone users in the UK (31%) are aged 55 and over, compared to just one in ten aged 18-24. Those aged 45-54 are the age group that is next most likely to own a drone (28%) while just 12% of 25-34 year olds own this type of technology' (DronesDirect 2017).

Figure 2: Drone. Source: © Colin.C.Ja https://www.flickr.com/photos/141650854@N03/30756188415/ *(CC BY 2.0)*

What are drones used for?

Drones enable the capture of aerial imagery and data, as well as the carrying and transport of items or goods. Central uses include:

Aerial Imagery capture	Drones commonly feature integrated cameras and are used to gather aerial imagery and data for applications including mapping, inspection, monitoring, surveillance and videography. From the surveillance of national infrastructure and site monitoring to Covid-19 response, drones are increasingly embraced as 'eyes in the sky' for asset management and security (HM Government 2022) and as tools for the monitoring of regulatory compliance (Environment Agency 2021; UK Drone Watch 2020).
Aerial Data gathering	Given that the value of the drone lies 'in the data' it gathers (PricewaterhouseCoopers 2022: 42), drones are used in a growing range of data collection roles. Alongside optical cameras, drones can be outfitted with sensors, including thermal sensors (for use cases such as missing persons, fire response, equipment and infrastructure monitoring), multispectral sensors (use cases including agricultural monitoring, vegetation and water quality assessment), hyperspectral sensors (for use cases including material composition surveys and emissions monitoring), and LiDAR (for use cases including the 'generation of 3D models of man-made structures') (Precision Hawk n.d).
Carrying and Transport	Drones are increasingly deployed in transport and carrying applications. These include agricultural spraying and the dispersal of pesticide, as well as the 'last mile and intra-depot delivery' of medical and commercial goods and matter (Connected Places Catapult 2022; HM Government 2022).

Growth of drone use in the UK

As the UK's drone sector grows, drone usage spans increasingly diverse sectors, from agriculture to energy and utilities, construction and manufacturing to emergency services, and local administration to last and middle mile delivery (HM Government 2022; PricewaterhouseCoopers 2022). Drones are associated with the carrying out of 'tasks faster, safer, cheaper and with less impact on the environment than traditional methods' (HM Government 2022: 6). To this end, a 2022 report by the Department for Business, Energy & Industrial Strategy (BEIS) and the Department for Transport (DfT) outlined a vision 'that by 2030

commercial drones will be commonplace in the UK in a way that safely benefits the economy and wider society' (HM Government 2022: 10). This is echoed in wider market forecasting, which estimates that by 2030 'drones could contribute up to £45bn to the UK economy; more than 900,000 drones could operate in UK skies; £22bn in net cost savings may be realised; carbon emissions could be reduced by 2.4M tons; and 650,000 jobs could be associated with an economy that fully adopts drones' (PricewaterhouseCoopers 2022: 2). Initiatives such as Skyway, the UK Government green-lit project proposing to 'build 165 miles (265km) of drone superhighways connecting airspace' above 6 UK towns and cities (Altitude Angel 2022a) aim to realise such visions. However, it is important to note that there remain a series of ongoing challenges around the drone's growing adoption, from public perception and regulation, to the technology itself (PricewaterhouseCoopers, 2022: 6; see also Jackman 2023). For example, while national surveys demonstrate levels of public support, particularly around the use of drones for risky jobs (BT 2023) and for emergency response (PricewaterhouseCoopers 2019), members of the UK general public have also expressed concerns around privacy, safety and security, as well as the potentially disruptive implications of drones on visual and noise landscapes, and wildlife.

Emerging concerns

In a 2022 'mini dialogue' (a 'public dialogue' where 'members of the public interact with scientists, stakeholders and policy makers to deliberate on issues relevant to future policy and research decisions') exploring 'future flight technologies' including drones, participant members of the public highlighted concerns around the potential for 'collisions in the air' and 'risk to people and property below', as well as the 'privacy implications' of drones accessing and 'recording personal spaces' and potentially intruding 'into people's private and domestic lives' (Camilleri et al. 2022). It also highlighted noise and visual implications, with participants 'living near a busy road' expressing concerns 'that the visual and aural disruption' they already experience 'at ground level would be duplicated in the air above their homes', and participants living 'in less built-up areas' expressing concern that 'the peacefulness of green spaces' 'could be spoilt by sights and sounds' of future flight technologies such as drones (Camilleri et al. 2022). Further, while many drone flyers fly responsibly and adhere to relevant rules (see Domestic framework: Rules and regulations for drones in the UK), concerns remain around the potential risks associated with both reckless and negligent, and criminal and malicious drone misuse (see Drone incidents, misuse and threats). In this vein, members of the public expressed concerns around 'drone misuse' (BT 2021), 'risk of improper' and 'criminal' use, and risks to 'public safety' (PricewaterhouseCoopers 2019). To this end, the Civil Aviation Authority suggests that while that they 'expect the adoption' of drones to 'increase significantly' in the 'next decade', the accompanying 'safety and security risks' require further 'mitigation' (CAP 2569: 3). Thus, while drones continue to grow in popularity across commercial, civil and citizen contexts, they remain complex and contested tools and objects.

Drone incidents, misuse and threats

From flights in proximity to manned aircraft, drones transporting contraband into prisons, to the outfitting of drones with weaponry and the attempted assassination of political leaders, both 'careless and inconsiderate' drone use and the 'more deliberate' misuse of drones 'for criminal acts' continues to cause safety, security and nuisance concerns, and to garner 'significant media attention' globally (HM Government 2019: 1; House of Commons 2019: 7; see also POSTnote 2020; Home Office 2019; Jackman 2019; Defence Committee 2019; Rogers 2021). Given the widespread availability and accessibility of drones, their comparatively 'low cost', their 'flight range' and capacity for remote and/or pre-programmed operation, drones can make 'attractive' tools for malicious misuse and/or 'criminal intent' (POSTnote 2020: 3).

Reports of potential threats associated with drone use have varied globally, but broadly fall under four categories:

Image and video capture	• Of critical and sensitive infrastructure (e.g., Government and military facilities) • Of commercial sites and activities (e.g., sporting events, TV and film sets, rural farms) • Of emergency service operations (e.g., by media or members of the public) • Reconnaissance to facilitate further actions (e.g., burglary) • Intrusion of privacy • Spying, stalking and domestic abuse of individuals (e.g., ex partners)
Transport and carrying	• Outfitted with weaponry (such as explosives, handguns, tasers and chainsaws; assassination attempts of political leaders; gang attacks on police and security forces) • Modified to transport, carry and/or drop contraband or potentially harmful items (e.g., into prisons; across borders; by drug cartels)
Data collection	• Cyber-attacks and/or corporate espionage (e.g., corporate facilities, networks and technology)
Disruption	• Flown by criminal actors and citizens at particular sites, spaces and events, with the aim of disrupting proceedings (e.g., airports, political events, sporting events, emergency service operations).

Such incidents highlight that drones are inherently 'malleable' technologies (Jackman 2019), open to modification, repurposing and misuse. To this end, drones provide both 'a new way to commit acts that are already criminal' (Home Office 2019: 29) and introduce and enable novel criminal acts. While drones can be considered within the context of 'technology-enabled crimes' more widely, the growing popularity of drones can be understood as 'enabling a number of emergent user groups' and 'posing its own unique risks and rewards to crime organisers and crime controllers' (Coliandris 2023: 300). Both reckless and negligent, and criminal and malicious drone use and misuse are thus associated with a range of potential threats and raise ongoing concerns around and 'consequences' for privacy, safety and security alike (Home Office 2019: 15).

2. THE REGULATORY FRAMEWORK

The regulatory framework: Summary table	
International: International Civil Aviation Organization (ICAO)	• The Convention on International Civil Aviation (known as the Chicago Convention) was signed on 7 December 1944 by 52 States • ICAO is responsible for developing global standards and recommended practices, procedures and guidance materials related to unmanned aviation (drones) • Assists Contracting States to the Chicago Convention. Article 8 'provides that no aircraft capable of being flown without a pilot shall be flown without a pilot over the territory of a Contracting State without special authorisation by that State' and requires that 'each contracting State undertake to insure that the flight of such aircraft without a pilot in regions open to civil aircraft shall be so controlled as to obviate danger to civil aircraft'.
National: The UK Government, Civil Aviation Authority (CAA) (national aviation regulator), and police	• The UK Government is responsible for laws governing drones • The national aviation regulator, the Civil Aviation Authority (CAA) work to ensure the aviation industry meets the highest safety standards • The police lead on action against the misuse of drones • Drones fall under two separate legislative frameworks: • (1) The Basic Regulation, which outlines the common rules for civil aviation within the UK, makes provisions for Implementing Regulations or Delegated Regulations, and includes a 'UAS regulation package' • (2) The Air Navigation Order 2016 (as amended), within the *Civil Aviation Act* 1982. The ANO covers airspace in the UK (excluding flight indoors), sets out the main civil requirements for UK aviation, and provides regulatory and enforcement powers for the CAA in relation to retained aviation safety legislation. Articles 240 and 241 are particularly pertinent • Regulatory requirements are supported by Acceptable Means of Compliance and Guidance Material, and the CAA also provides guidance on regulation through Civil Air Publication (CAP) documents • Existing drone regulations and legislation have a focus on safety.
Privacy and data protection: The CAA, Information Commissioner's Office (ICO), Biometrics and Surveillance Camera Commissioner	• The Civil Aviation Authority's remit is limited to safety and does not include concerns over privacy, though advises that pilots using drones with cameras should be aware of relevant Data Protection Regulation. The Drone and Model Aircraft Code offers multi-faceted advice regarding respecting people and their privacy • The Information Commissioner's Office (ICO) is an independent body responsible for upholding information rights. The ICO recognises that drone flight can involve collecting, using and/or sharing personal data, and poses the potential for collateral intrusion. The ICO distinguishes between hobbyists and professional or commercial flyers, describing compliance with data protection law (e.g., provision of privacy information, undertaking a Data Protection Impact Assessment) and asserting that where required, drone pilots must comply with the Surveillance Camera Code • The Biometrics and Surveillance Camera Commissioner advise that the use of drones with cameras by 'relevant authorities' is covered by the Surveillance Camera Code. The Code is not technology specific, rather is principles based and applies to the use of

	surveillance cameras in public places. It encourages other operators and users of surveillance camera systems to adopt voluntarily. The code specifies that covert surveillance by public authorities is not covered and is instead regulated by Regulation of Investigatory Powers Act 2000.

International framework

Globally, the International Civil Aviation Organization (ICAO), a United Nations agency, is responsible for 'developing global Standards and Recommended Practices (SARPs), Procedures, and Guidance material for unmanned aviation with the goal to facilitate a safe, secure, and efficient integration of unmanned aircraft into the global aviation system' (ICAO, n.d). As a 'signatory to the Chicago Convention of 7 December 1944 and a member of ICAO, the United Kingdom undertakes to comply with the provisions of the Convention' (CAP 722: 14). Of particular relevance is Article 8 of the Chicago Convention, which 'provides that no aircraft capable of being flown without a pilot shall be flown without a pilot over the territory of a Contracting State without special authorisation by that State' and also requires that 'each contracting State undertake to insure *sic* that the flight of such aircraft without a pilot in regions open to civil aircraft shall be so controlled as to obviate danger to civil aircraft' (CAP 722: 14).

The 19 annexes to the Chicago convention contain the International Standards and Recommended Practices (SARPS) upon which regional (e.g., European Union) and national regulations are created (CAP 722:14).

While ICAO advises on global standards, regulation and legislation are administered nationally. While the UK Government is responsible for 'proposals for new laws governing drones' and the police lead on 'action against the misuse of drones', the UK's aviation regulator, the Civil Aviation Authority (CAA) works to ensure that the 'aviation industry meets the highest safety standards' (Civil Aviation Authority, n.d).

Domestic Framework: Rules and regulations for drones in the UK

As is expanded upon below:

- The Civil Aviation Authority (CAA) regulates drone use in the UK.
- Drones are divided into different operation categories: Open, Specific and Certified.
- In the UK, drones fall 'under two separate legislative frameworks', namely:
  - 'Regulations within the framework of UK Regulation (EU) 2018/1139 (the Basic regulation)' and
  - 'The Air Navigation Order 2016, as amended, within the framework of the Civil Aviation Act 1982' (CAP 722: 14-15).

Civil Aviation Authority (CAA)

The Civil Aviation Authority is the UK's aviation regulator, a public corporation established by Parliament in 1972 and working to ensure that the 'aviation industry meets the highest safety standards' (Civil Aviation Authority n.d). Regarding drones, the CAA's responsibilities include 'providing permissions for drone operators when required', 'providing advice to the general public and industry on how to fly drones safely and reduce risk to aviation', and ensuring that 'any risks' that potential 'future uses pose to aviation are managed effectively and proportionately' (Civil Aviation Authority n.d). The CAA is not responsible for 'proposals for new laws governing drones' which are a 'matter for Government', nor for 'action against the misuse of drones', which the police lead on (Civil Aviation Authority n.d) (see Enforcement).

The Civil Aviation Authority provide a range of information on flying drones safely, including rules around drone flight which are 'based on the risk of the flight – where you fly, the proximity to

other people, and the size and weight of your drone' (Civil Aviation Authority n.d.a). The drone rules are based around the three categories set out in the Basic regulation at Articles 4-6 (the open category, specific category and certified category) (CAP 1789A). There is 'no distinction between flying commercially and flying for pleasure or recreation', i.e. an 'approval just to operate commercially is not required' (Civil Aviation Authority n.d.a).

Understanding Drone Categories

Summary: Drone operation categories	
The Open Category	• **Low-risk drone flights** • Guidance: Drone and Model Aircraft Code; CAP 2012 Drone rules: Requirements for flying in the open category; CAP 722 Unmanned Aircraft Systems in UK airspace; the CAA's webpage under 'Flying in the Open Category'
The Specific Category	• **Higher risk drone flights** • Requires operational authorisation from the CAA • Guidance: CAP 722 Unmanned Aircraft System Operations in UK airspace; the CAA's webpage under 'Flying in the Specific Category'
The Certified Category	• **Large drones** which have to meet specific safety certifications along the lines of aircraft • Regulations under development and not yet published • Guidance: CAP 722 Unmanned Aircraft System Operations in UK airspace; the CAA's webpage under 'Flying in the Certified Category'

The Open Category
The Open Category is 'intended for low-risk drone flights' and covers drones weighing both under 250 grams and between 250 grams and 25 kilograms (Civil Aviation Authority n.d.a). There are various requirements and restrictions for flights in the Open category. These depend on the drone's weight, when the drone was built and/or placed on the market, and whether the drone has a camera onboard. Drones are divided into three categories – A1, A2 and A3, depending on these factors (CAP 2012). If a drone weighs over 250 grams, drone users are required to obtain a 'flyer ID' which shows they have passed a 'basic flying test' and are responsible for 'flying safely and legally' (Drone and Model Aircraft Code n.d). If a drone weighs under 250 grams and has a camera, or weighs over 250 grams, drone users also need to obtain an 'operator ID' which must be labelled on the drone and indicates that they are 'responsible for the drone or model aircraft, and who they allow to fly it' (Drone and Model Aircraft Code n.d). Drones flying in the Open Category must not exceed 120 metres (400 feet), are not permitted to drop articles nor to carry dangerous goods, must be kept within the operator's visual line of sight, and must adhere to all applicable airspace restrictions (CAP 2012). In addition to flight restrictions and requirements around 'prisons, military ranges, royal palaces, government buildings' and 'emergency service incidents', drone flyers are required to stay 'well away' from 'airports, airfields or spaceports' as most of these 'have a flight restriction zone (FRZ)' and permitted flight therein would likely require permissions (Drone and Model Aircraft Code n.d; see also CAP 722). Flights in the Open Category are also subject to further restrictions around proximity to 'uninvolved persons' and distance from residential, commercial, industrial or recreational areas (Drone and Model Aircraft Code n.d.; CAP2012). Guidance can be found in the **Drone and Model Aircraft Code**, on the CAA's website, in CAP722 Unmanned Aircraft System Operations in UK airspace, and in CAP2012 Drone rules: Requirements for flying in the open category.

The Specific Category
The Specific category is intended for 'higher risk flights' and/or for those that fall outside the boundaries of the open category (Civil Aviation Authority n.d.a). In distinction to the Open Category, operations in the Specific Category require an '**operational authorisation**' issued by the CAA (Civil Aviation Authority n.d.b). This authorisation is based upon the CAA's 'evaluation of a safety risk assessment' (Civil Aviation Authority n.d.b). It is also 'only permissible to carry dangerous goods by drone in the Specific catgeory', wherein operators need 'approval to carry items that are classified as dangerous goods' (CAP 2248: 2).
The Certified Category
The Certified category is 'for large drones which have to meet specific safety certifications along the lines of' manned aircaft and aviation (Civil Aviation Authority n.d.a). It 'covers operations that present an equivalent risk to that of manned aviation' and are 'subjected to the same regulatory regime' (Civil Aviation Authority n.d.c). The UK's regulations for drone flights in the certified category 'are still being developed are **not yet published**' (Civil Aviation Authority n.d.c).

Domestic legislative framework

As above, in the UK, drones fall under two separate legislative frameworks: 'Regulations within the framework of UK Regulation (EU) 2018/1139 (the Basic regulation)' and 'The Air Navigation Order 2016, as amended, within the framework of the Civil Aviation Act 1982' (CAP 722: 14-15). Regulations are supplemented with Acceptable Means of Compliance and Guidance Materials, and the CAA provides guidance on regulation through Civil Air Publications (CAPs).

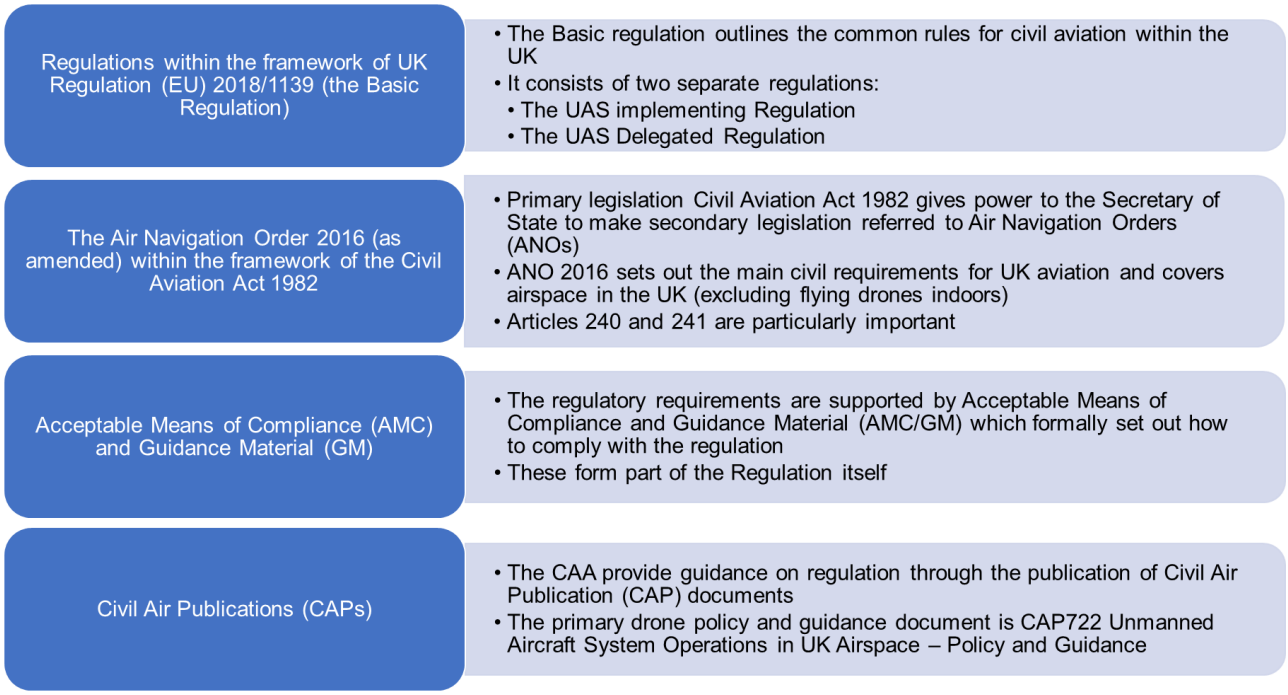

Figure 3: UK regulatory framework. Source: Author's own (see also CAP 722)

The 'Basic regulation'

The 'Basic Regulation' outlines the 'common rules for civil aviation within the UK' (CAP722: 16). Delegated legislation from the Basic Regulation (BR) is referred to as the 'UAS regulation package' (UAS, or Unmanned Aerial Systems, is another term for aerial drones), which consists

of ‘two separate but interlinked regulations’ that were ‘transferred into UK law at the end of the EU exit transition period’ (CAP 722: 17). These include:

- “Regulation (EU) 2019/947 as retained (and amended in UK domestic law) under the European Union (Withdrawal) Act 2018 on the procedures and rules for the operation of unmanned aircraft” (known as the ‘**UAS Implementing regulation**’ and is found in CAP1789A), and
- “Regulation (EU) 2019/945 as retained (and amended in UK domestic law) under the European Union (Withdrawal) Act 2018 on unmanned aircraft and on third country operators of unmanned aircraft systems”’ (known as the ‘**UAS Delegated Regulation**’ and found in CAP1789B) (CAP 722: 17).

The relevant EU regulations were transferred across into UK domestic law, as UK regulations. These regulations became ‘retained EU law’ after the end of the EU-UK transition period following Brexit (Practical Law 2023: 8), and will be ‘amended as necessary’ (CAP 722: 15). Changes made by the EU are not automatically adopted by the UK and both the EU and UK have amended both regulations since their adoption (CAP 722: 17).

The Air Navigation Order 2016

Under UK primary legislation the Civil Aviation Act 1982 gives ‘power to the Secretary of State to make secondary legislation referred to as Air Navigation Orders’ (Feild 2019). The ‘key legislation is the Air Navigation Order 2016 (S.I. 2016/765), which ‘replaced the Air Navigation Order 2009’, and has subsequently been amended (Feild 2019).

The ANO 2016 sets out the main civil requirements for UK aviation and covers airspace in the UK (excluding flying drones indoors). The ANO 2016 also provides ‘regulatory and enforcement powers for the Civil Aviation Authority needed in respect of retained aviation safety legislation’ (House of Commons 2022). The ‘provisions in the ANO concerning equipment requirements, operational rules, personnel licensing, aerodrome regulation and regulation of air traffic services apply to all non-military aircraft, organisations, individuals and facilities’ (CAP 722: 18). Of particular note are Articles 240 and 241:

- ‘Article 240 applies to all persons and stipulates that a person must not recklessly or negligently act in a manner likely to endanger an aircraft or a person within an aircraft’ and
- ‘Article 241 applies to all operating categories and stipulates that a person must not recklessly or negligently cause or permit an aircraft (manned or unmanned) to endanger any person or property (which includes other aircraft and their occupants)’ (CAP 722: 18).

With regards to drones specifically, the ANO provides additional regulatory content that is either:

- ‘not covered by other regulations– for example, specific national requirements such as carriage of radio equipment, endangerment regulations and legal penalties for breaches of these regulations; or
- in support of a more general requirement stated within other regulations – for example, airspace restrictions around aerodromes and other ‘protected’ locations’ (CAP 722: 18).

It can be noted that ‘only certain parts of the ANO apply to UAS [drones] within the Specific and Open categories’ whereas ‘Certified category operations and certified unmanned aircraft are subject to the whole of the ANO, unless specifically exempted by the CAA’ (CAP 722: 18-19).

The ‘regulatory requirements are supported by Acceptable Means of Compliance and Guidance Material (AMC/GM)’ which ‘formally set out how to comply with the regulation’ (CAP 722: 18). These form part of the Regulation itself.

The Civil Aviation Authority also provides guidance on regulation through the publication of Civil Air Publication (CAP) documents. The 'primary' drone 'policy and guidance document' is CAP722 Unmanned Aircraft System Operations in UK Airspace – Policy and Guidance, which 'provides policy and guidance in relation to the operation of UAS [drones] to assist in compliance with the applicable regulatory requirements' (CAP 722: 6). The CAA underscores that CAP documents are not regulation, rather they summarise and reference regulation throughout (CAP 722: 6). Further information about drone-related publications and can be found in the CAA's publications library (Civil Aviation Authority n.d.i).

In August 2023, the Civil Aviation Authority launched a call for input into its review of UK drone regulations (CAP 2569). The review sought feedback on wide-ranging issues, including 'standards adoption' and 'operational categories', including current 'exclusions for users of UAS [drones] weighing below 250 grams' (CAP 2569). On November 22 2023, the CAA published the Call for Input Response Summary (CAP 2609). This document details that the Call for Input received '2,629 responses in total' and that analysis of these responses validated the CAA's 'view that there are opportunities to improve, simplify and strengthen UAS regulation. However, there was limited support for overhauling existing regulatory frameworks, such as operational categorisations and class-marking, due to the cost and wider impacts of change. Collectively, this feedback enabled us [the CAA] to develop a set of proposals that make incremental and targeted improvements to the regulations, while maintaining stability in the overall regulatory framework where possible'. Further information can be found in the Review of UK UAS Regulation Consultation (CAP 2610).

Privacy and data protection

Drone regulation globally has historically 'been focused primarily upon safety considerations' but as drone usage grows and is anticipated to scale, 'increasing attention will need to be paid to privacy and data protection laws' (Clyde & Co 2022).

UK Data Protection Act 2018 and General Data Protection Regulation 2016

Post Brexit, data protection and privacy in the UK is governed by the Data Protection Act 2018 (as amended) and the version of the General Data Protection Regulation (EU) 2016/679 'EU GDPR' as retained in domestic law which is known as the 'UK GDPR' (as amended by Schedule 1 to the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019, (SI 2019/419)). The Government intends to replace this with new legislation currently before parliament as the Data Protection and Digital Information Bill (No. 2) 2023 (Parliamentary Bills n.d).

The UK data protection laws apply to information processed through the use of drones, although exceptions may apply to hobbyists. Where data protection law does apply, strict adherence to the data protection principles must be ensured. In some limited cases, an exemption from compliance with GDPR may apply. These are considered on a case-by-case basis and include, for example, provisions relating to:

- Crime, law and public protection
- Regulation, parliament and the judiciary
- Journalism, research and archiving
- Health, social work, education and child abuse
- Finance, management and negotiations
- References and exams
- Subject access requests where information about other people is requested
- National security and defence

(Information Commissioner's Office n.d.a).

See also Annex 1: Further information about Data Protection law in the UK.

UK GDPR Guidance: The Information Commissioner's Office (ICO)

In the UK, the Information Commissioner's Office (ICO) is the independent body set up to 'uphold information rights in the public interest' (Information Commissioner's Office n.d.b). The ICO has produced UK GDPR Guidance relating to CCTV and video surveillance and included within this is Additional Considerations for Technologies other than CCTV.

The ICO observes that drone flight 'can result in the collection, use, or sharing of **personal data**, including information about individuals who are not the intended focus of the recordings' (Information Commissioner's Office n.d.c). The ICO notes that the growing popularity of drones has 'raised privacy concerns due to their manoeuvrability and enhanced capabilities of taking photos, videos and sensing the environment' and that drones pose the "potential for 'collateral intrusion' by recording images of other individuals unnecessarily", including indirect or inadvertent identification as individuals can 'still be identified through the context they are captured in or by using the device's ability to zoom in on a specific person' (Information Commissioner's Office n.d.c).

The ICO observe a '**distinction** between...individuals who can be considered as **hobbyists** and are therefore generally using their device for purely personal activities, and those individuals or organisations who use the device for **professional or commercial** purposes' (Information Commissioner's Office n.d.c). They specify that 'organisations using drones are clearly **controllers** for any personal data that the drone captures, and therefore are required to comply with data protection law' (Information Commissioner's Office n.d.c).

The ICO explains the requirement to provide **privacy information**. They note that a 'key issue with using drones is that, on many occasions, individuals are unlikely to realise they are being recorded or be able to identify who is in control. If you are a controller, you must address the challenge of providing privacy information if you decide to purchase and use such surveillance systems' (Information Commissioner's Office n.d.c). They add that innovative ways of providing this information such as 'placing signage in the area you are operating a drone explaining its use' or having a 'privacy notice...so individuals can access further information' may be needed (Information Commissioner's Office n.d.c). The ICO also suggest that 'if doing that is very difficult or would involve disproportionate effort, document this information in a way that is readily available' (Information Commissioner's Office n.d.c).

In discussion of **data security**, the ICO urges a consideration of whether the drone 'connects or interfaces with other systems', highlighting measures such as 'encryption or another appropriate method of restricting access to the stored information', and of the retention period requirements to 'ensure that you retain data for the shortest time necessary for its purpose and dispose of it appropriately, when you no longer require it' (Information Commissioner's Office n.d.c).

The ICO provides a checklist for drone flyers to consider to help them comply with data protection law, including:

- 'We have considered whether there is a genuine need for us to use a drone, if alternative systems or methods of surveillance are not suitable to solve a particular problem;
- We have conducted a **Data Protection Impact Assessment (DPIA)** which includes the risks associated with recording at altitude, and capturing footage of individuals that are not intended to be the focus of our surveillance;
- We have registered our drone if the system falls within the specific criteria set by the Civil Aviation Authority (CAA);

- We have robust policies and procedures in place for the use of drones, and our operators are appropriately trained, with documented credentials;
- We inform individuals that we are using a drone where possible, and we have an accessible privacy notice that individuals can read to learn more about our use; We comply with the Surveillance Camera code of practice where required'

Source: Information Commissioner's Office (n.d.c)

The ICO's guidance on drones sits under its wider **CCTV and Video Surveillance Guidance**, which includes information on 'handling personal information using video surveillance' from a range of technologies, including CCTV, automatic number plate recognition, smart doorbell cameras, and drones (see Video surveillance (including guidance for organisations using CCTV) on Information Commissioner's Office n.d.d). The ICO recognises that as video surveillance 'becomes more mainstream and affordable' some uses 'can be particularly intrusive' and confirms 'organisations using surveillance systems that process the personal data of identifiable individuals need to comply with the UK GDPR and DPA [Data Protection Act] 2018' (Information Commissioner's Office n.d.d). The ICO highlights that drone flyers must 'comply with the Surveillance Camera code of practice where required' (Information Commissioner's Office n.d.c) (see Biometrics and Surveillance Camera Commissioner).

Further information about **personal data, data subjects, data controllers** and **data processors**, and **Data Protection Impact Assessments (DPIAs)** and the requirements of data protection laws generally can be found in Annex 2: UK GDPR guidance: The Information Commissioner's Office.

Biometrics and Surveillance Camera Commissioner

The Biometrics and Surveillance Camera Commissioner (BSCC) is 'an independent monitoring body of the Home Office' and the BSCC's role is to 'encourage compliance with the surveillance camera code of practice' (Gov.UK n.d). The BSCC observed that from 'drones to body worn video, dashcams and doorbells', 'in recent years we have seen an explosion of surveillance technology in the public and private realms' (Gov.UK 2023). They advise that where drones include cameras, they "are necessarily involved in the 'surveillance' of public space" and as such, 'their use by relevant authorities will often be covered by the provisions of the SC [Surveillance Camera] Code' (Office of Biometrics and Surveillance Camera 2023: 78-79).

The **Surveillance Camera Code** presents a 'single set of guiding principles that are applicable to all surveillance camera systems in public places' and 'allows a system operator to establish a clear rationale' for deployment 'which helps ensure compliance with other legal duties' (Home Office 2021: 8). This 'covers technology systems that are associated with, or otherwise connected with, surveillance cameras' and 'applies to the use of surveillance camera systems as defined by Section 29(6)' of the Protection of Freedoms Act 2012 (Home Office 2021: 6, 7).[1] Wider discussions of the Code specify both that specific technologies (such as drones) are 'already covered under the general definition of surveillance camera systems' and that 'the fact

[1] The Protection of Freedoms Act 2012 defines surveillance camera systems as: '(a) closed circuit television or automatic number plate recognition systems, (b) any other systems for recording or viewing visual images for surveillance purposes, (c) any systems for storing, receiving, transmitting, processing or checking images or information obtained by systems falling within paragraph (a) or (b), or (d) any other systems associated with, or otherwise connected with, systems falling within paragraph (a), (b) or (c)' (Protection of Freedoms Act 2012).

that **the Code is principles based rather than technology specific** helps to ensure it does not rapidly get out of date as technologies and use cases develop' (Gov.UK 2021).[2]

The Code 'provides guidance on the appropriate and effective use of surveillance camera systems by **relevant authorities**' (Home Office 2021: 6).[3] It also states that 'other operators and users of surveillance camera systems in England and Wales are *encouraged to adopt the code voluntarily*' (Home Office 2021: 6, emphasis added).

The Code applies to overt surveillance, and notes that the 'government is fully supportive of the use of overt surveillance camera systems 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' (Home Office 2021: 6).

The Code specifies that 'covert surveillance by public authorities (as defined in Part II of RIPA 2000) is not covered by this code but is regulated by RIPA 2000' (Home Office 2021: 7).

The Civil Aviation Authority (CAA), data protection and privacy

CAP722 Unmanned Aircraft System Operations in UK Airspace notes that the 'CAA's remit is limited to safety' and 'does not include concerns over privacy or broadcast rights' (CAP 722: 23). It continues that while the 'capture of images or other data solely for the use of controlling or monitoring the aircraft is not considered to be applicable to the meaning of 'a sensor able to capture personal data'', drone flyers should 'be aware that the collection of images of identifiable individuals, even inadvertently, when using surveillance cameras mounted on [drones], may be subject to the General Data Protection Regulation and the Data Protection Act 2018' (CAP 722: 20). It advises that 'further information about these regulations and the circumstances in which they apply can be obtained from the Information Commissioner's Office' (CAP 722: 20).

In the **Drone and Model Aircraft Code** (applying to flights in the Open category, A1 and A3), the CAA provides guidance on 'protecting people's privacy', advising flyers to:

- 'Respect other people and their privacy: If your drone or model aircraft is fitted with a camera or listening device, you must respect other people's privacy whenever you use them. If you use these devices where people can expect privacy, such as inside their home or garden, you're likely to be breaking data protection laws', adding that 'it's against the law to take photographs or record video or sound for criminal or terrorist purposes' and 'any photos or recordings you take may be covered by the General Data Protection Regulation (GDPR)';
- To understand what your camera 'can do and the kind of images it can take' (e.g., 'what quality you can record, how close your camera can zoom in, if you can start and stop recording when you are flying'), a step which it states 'will help reduce the risk of taking photos or recording videos that invade privacy';

---

[2] The 12 principles of the Surveillance Camera Code concern: use for a 'specified purpose' in 'pursuit of a legitimate aim', taking 'into account' the 'effects on individuals and their privacy', 'transparency' around the deployment and a 'published contact point for access to information and complaints', 'clear responsibility and accountability' for 'system activities', 'clear rules and procedures in place', 'no more images and information should be stored than that which is strictly required for the stated purpose', access restricted to 'retained images and information', a consideration of any relevant 'approved operational, technical and competency standards', 'security measures' in place to 'safeguard against unauthorised access and use', 'mechanisms to ensure legal requirements, policies and standards are complied with in practice', the use should be 'in pursuit of a legitimate aim', and information supporting a surveillance camera system should be 'accurate and kept up to date' (Home Office 2019: 10).

[3] Relevant authorities are defined in Article 33(5) in the Protection of Freedoms Act 2012, and includes entities such as (but not limited to): local authorities, 'a police and crime commissioner', 'any chief officer of a police force in England and Wales', and any 'person specified or described by the Secretary of State in an order made by statutory instrument' (Protection of Freedoms Act 2012).

- Alongside being ‘clearly seen when you’re outside flying’ so that people are aware of who is ‘responsible for’ the drone, flyers should ‘let people know’ before they ‘start recording or taking pictures’, though acknowledge that this can be ‘less practical’ in some instances;
- That flyers should ‘think before sharing photos and videos’ (e.g., to ‘social media’), and ‘avoid sharing anything that could be unfair or harmful to anyone’
- And that drone imagery should be ‘stored safely’ and anything that is not needed should be deleted, adding that ‘if you record images for commercial use, you’ll need to meet further specific requirements as a data controller’.

Source: Drones and Model Aircraft Code (n.d).

Figure 4: Drone. Source: © Miki Yoshihito https://www.flickr.com/photos/mujitra/19440078509/ (CC BY 2.0)

3. ENFORCING THE REGULATIONS

Drone misuse: The CAA and UK Police	• The CAA's remit is safety. While the CAA will investigate where someone has flown not in accordance with their operational authorisation, and will seek to prosecute in cases where dangerous and illegal flying takes place, action against the misuse of drones is led by the Police • The CAA urges citizens to report the misuse of drones to local police • The Air Traffic Management and Unmanned Aircraft Act 2021 provides Police with powers to respond to drone misuse. Where officers suspect a drone could be involved in the commission of an offence, they can: instruct a pilot to land, stop and search people or vehicles to find drones/equipment, confiscate drones/equipment found during a search, require pilot to show registration details and other information (e.g., permissions) and check a drone to see which rules apply to it. It also introduces a fixed penalty system, which is presently under development • In October 2023, the Government announced new legislation in relation to drone use and prisons (Gov.UK 2023a). Building upon the Air Traffic Management and Unmanned Aircraft Act 2021 and the Prison Act 1952, the Air Navigation (Restriction of Flying) (Prisons and Young Offenders Institution) (2023/1101) now details restrictions in relation to the flying of drones in the vicinity of prisons and young offenders institutions in England and Wales (as specified in the schedule) and comes into force on 25 January 2024. • There have been a range of drone-related prosecutions in the UK.

Drone incidents and misuse

A Freedom of Information request submitted to all UK police forces and yielding responses from 20 of 48 Forces described '2,435 reports of incidents involving drones in 2018', representing a 42% increase in the number of reports to police in 2016 (Mercer 2019). Forces received wide-ranging complaints, including drones used to 'film a cash machine', flown over and falling onto busy roads, drone activity linked to 'harassment / stalking crimes', drones flown in proximity to airports and aircraft, being used to drop paintballs, and 'devices being operated over schools or nurseries' (Mercer 2019). A particularly significant area is the use of drones to deliver items to UK prisons, with 'a single attempted drone delivery in May 2022 containing a payload of over £35,000 worth of illicit substances and contraband' (Gov.UK 2023a).

While noting that 'the vast majority of users possess and operate drones for perfectly lawful reasons', analysis on the 'threat from drones in the UK' suggests that 'during 2021 over 6000 incidents involving drones were reported to the police' (Protect UK 2022). It continues that roughly '10% of all reports related to drones flying at or close to airports', that 'nearly 4% of reports related to drone activity in and around prisons' and that roughly 3% of activity was 'reported in the vicinity of sensitive or military sites' (Protect UK 2022). While suggesting that 'only a small proportion' of these reported incidents 'constituted offences', Protect UK (2022) add that it remains difficult to know the 'true scale of illicit drone activity in the UK'. It can be noted that a 'malicious drone incident' entry was added to the UK Government's National Risk Register, 2023 edition (HM Government 2023).

Enforcement scope and response

The CAA recognises that 'despite current regulation', some drones are 'used unlawfully' (CAP 2569: 20). The Drone and Model Aircraft Code (n.d) states that 'it is against the law to fly a drone or model aircraft without having the required IDs. You can also be fined for breaking the law when flying. In the most serious case, you could be sent to prison'. It adds that 'if you endanger

the safety of an aircraft you could go to prison for five years' (Drone and Model Aircraft Code n.d) (see Domestic framework: Rules and regulations for drones in the UK).

While the Civil Aviation Authority 'takes breaches of aviation legislation seriously and will seek to prosecute in cases where dangerous and illegal flying has taken place' (CAP 722: 23), it highlights that responsibility for 'action against the misuse of drones' is led by the police (Civil Aviation Authority n.d). Per a 'signed Memorandum of Understanding' the CAA has agreed 'that the Police will take the lead in dealing with UAS misuse incidents, particularly at public events, that may contravene aviation safety legislation or other relevant criminal legislation' (CAP 722: 23). To this end, the CAA urge citizens to report any misuse of drones to their local Police force. The CAA add that their 'remit is limited to safety and also to investigate where someone is operating, or has operated, in a manner that is not in accordance with their operational authorisation', i.e. this 'does not include concerns over privacy or broadcast rights' (CAP 722: 23).

Of particular importance to the Police's enforcement of drone regulations and the tackling of drone misuse is the **Air Traffic Management and Unmanned Aircraft Act 2021**, which is designed to 'clamp down on the illegal use of unmanned aircraft' by 'giving police officers the necessary powers' to respond (Department for Transport 2021).

- Schedule 8 gives the police and prison authorities powers relating to unmanned aircraft
- Schedule 9 makes provision about powers of police officers in relation to requirements of the ANO 2016
- Schedule 10 makes provision about fixed penalties for certain offences relating to unmanned aircraft (*Source: Air Traffic Management and Unmanned Aircraft Act 2021*).

Per Schedule 8, where officers suspect a drone could be 'involved in the commission of an offence', they are permitted to: instruct a pilot to 'land their drone, stop and search people or vehicles to find drones or drone equipment, and confiscate drones or drone equipment found during a search' (Thames Valley Police n.d). In addition, officers can require pilots to show 'registration details and other information, evidence of permission to fly (where necessary)' and can 'check a drone to understand which rules apply to it' (Thames Valley Police n.d). Per schedule 10, it also introduces the 'creation of a fixed penalty system' enabling police officers to 'issue on the spot fines for set types of offence' – a system which is presently under development (Geeksvana 2023).

In August 2023, the CAA launched a '**Call for Input**' regarding a 'Review of UK UAS Regulations', seeking feedback from drone 'stakeholders...on how CAA can make UAS [drone] regulation fit for the future – effectively mitigating risks, whilst still delivering user needs and enabling the sector to grow' (CAP 2569: 3). Therein, the CAA note that 'the police currently have a limited ability to identify the person responsible for a UAS's operation at the time of an incident', adding that 'in the future, technology' such as 'remote ID' 'will enable UAS to transmit operator and flight data during flight' and 'allow police to identify malicious and/or incompetent operators, both in real-time and historically – leading to re-education, fines, or convictions' (CAP 2569: 20). In this vein, it notes that 'UK Regulation (EU) 2019/945 sets out a requirement to implement Remote ID in the UK by January 2026, through manufacturer requirements and operational requirements' and that the CAA is 'exploring how Remote ID could be implemented in the UK' (CAP 2569: 20).

Air Navigation offences

It is the responsibility of the drone operator to fly within the law. If any provision of the Air Navigation Order 2016/765 is contravened this may result in a criminal offence being committed pursuant to article 265. In preparation for Brexit, an amendment to the Order inserted the

offence of 'Contravention of Commission Implementing Regulation (EU) 2019/947 on the rules and procedures for the operation of unmanned aircraft – UAS operator' at articles 265A and 265B. Schedule 13 of the Air Navigation Order 2016 sets out the penalties for the provisions referred to in paragraph 265(5).

The Air Traffic Management and Unmanned Aircraft Act 2021 introduced the power to make secondary legislation to provide for the police to issue fixed penalties for certain offences where the officer believes that the offender did not cause or intend to cause various types of harm or damage:

- Endanger another aircraft
- Cause harm, harassment, alarm or distress,
- Cause any person occupying any premises nuisance or annoyance relating to their occupation of the premises,
- Under some security or good order and discipline in any prison or in any other institution where persons are lawfully detained,
- Disturb public order, or
- Damage property (including land and buildings) when committing the fixed penalty offence.

Source: Air Traffic Management and Unmanned Aircraft Act 2021.

Further, in October 2023, in recognition of and response to an estimated '504 drones' being 'sighted, intercepted or seized around prisons in England and Wales' between 2019 and 2021, it was announced that new legislation 'will make it an automatic offence to fly drones within 400 metres of any closed prison or young offender institution in England and Wales' (Gov.UK 2023a). While the announcement noted that 'police and prison staff have worked together to help secure more than 70 convictions since June 2016' and that 'those sentenced are serving more than 240 years in prison', the announcement continued that 'drone operators that break the rules could face fines of up to £2,500 while those found smuggling illicit items will face up to 10 years in prison' (Gov.UK 2023a). It added that 'by creating a virtual 'no-fly zone' around prison airspace, the new restrictions mean police and prison staff will be able to act quickly to identify suspicious drones and take swift action against suspected criminal activity, as well as enhancing security by preventing illegal filming'. These new measures 'build upon current legislation, including the Air Traffic Management and Unmanned Aircraft Act 2021....as well as any use of drones which break the Prison Act 1952' (Gov.UK 2023a). The Air Navigation (Restriction of Flying) (Prisons and Young Offenders Institution) (2023/1101) details restrictions in relation to the flying of drones in the vicinity of prisons and young offenders institutions in England and Wales (as specified in the schedule) and come into force on 25 January 2024.

In addition, drones may be used to commit offences under other criminal laws.

Police drone use

Alongside tackling drone misuse, at least 40 of the UK's 48 police forces also use drones as operational policing tools (Jackman 2023a). Police drones are used for a growing range of applications, including aerial searches, securing buildings, and thermal flyovers, and UK Police associate drones with a range of benefits, including the rapid provision of situational awareness, enabling access to dangerous and remote sites, reducing risks to officers on the ground, and offering cost saving aerial support (Jackman 2023a).

While valuable operational tools, a 2023 'survey of law enforcement use of uncrewed aerial vehicles' (drones) by the Biometrics and Surveillance Camera Commissioner (2023) identified several areas of concern around police drone use, including a 'lack of awareness of risks to the security of data recorded when drones are deployed and how, or whether, such risks are

mitigated', as well as a 'lack of consistency of approach to how police use of drones is scrutinised to try and ensure it is appropriate and ethical'. They continue with a series of recommendations, including that 'guidance is needed on how to mitigate UAV-specific security risks, such as hacking and the use of counter-UAV technology', that 'Chief officers should consider a standardised and documented procedure for assessing sensitivity, whether that relates to a geographical site or a more transient operation' involving the use of a drone, and that 'guidance on the assessment and measurement of sensitivity is urgently needed' (Biometrics and Surveillance Camera Commissioner 2023).

Prosecutions

To date, there have been a range of **drone-related prosecutions in the UK**. These include prosecutions 'for the breach of ANO [Air Navigation Order] provisions' (Mouhinso 2022: 502). Examples include 'UK CAA v. Robert Knowles' wherein in August 2013, a drone 'was found and recovered from the waters near the BAE Systems submarine nuclear testing facilities at Barrow-in-Furness in the UK' (Mouhinso 2022: 502). The drone was 'rescued' and 'passed on to the police who traced it back to Mr Robert Knowles' and the 'images recorded from the [drone's] camera later revealed' the aircraft's route, which 'entered restricted airspace' around the facility (Mouhinso 2022: 502). The CAA ultimately prosecuted Mr Knowles for two offences, namely 'flying a UAS within 50m of a structure (in contravention of Article 167(2)(c) of the ANO 2009) and; flying a UAS over Barrow-in-Furness nuclear installation, which is a restricted fly-zone, in breach of Regulation 3(2) of the Air Navigation (Restriction of Flying) (Nuclear Installations) Regulations 2007' (Mouhinso 2022: 502). Mr Knowles plead guilty, 'was convicted on both accounts' and was fined £800 and 'ordered to pay £3,500 in costs' (Mouhinso 2022: 502). Further examples include 'UK CAA v Mark Spencer' (flying a drone over a theme park), and 'NPAS and UK CAA v. Sergej Miann' (drone flying 'under a National Police Air Service helicopter while it was on a search and rescue mission to help locate a missing person') (Mouhinso 2022: 502-503).

Figure 5: Drone. Source: Chandler Cruttenden, Unsplash https://unsplash.com/photos/person-holding-white-and-black-drone-wrwSAEcT94M

Private actions in civil law

In addition to the criminal justice response to drone use, private individuals or companies may seek remedies under civil law including claims for negligence, nuisance, harassment, breach of privacy and misuse of private information.

The issue of what rights a landowner has in respect of airspace above their property and whether a person who flies over the land of a private individual is committing a trespass or some other form of tort has been debated since at least 1815 when Lord Ellenborough in *Pickering v Rudd (1815) 4 Camp 216* said it would not be a trespass to pass over a man's land in a balloon. Summarising the problem in *Berstein v SkyViews Ltd [1978] 1 QB 479*, at 487-488 Griffiths J, there considering whether the taking of a photograph of the claimant's home from the air constituted a trespass, held:

"*I can find no support in authority for the view that a landowner's rights in the air space above his property extend to an unlimited height... The problem is to balance the rights of an owner to enjoy the use of his land against the rights of the general public to take advantage of all that science now offers in the use of air space. This balance is in my judgment best struck in our present society by restricting the rights of an owner in the air space above his land to such height as is necessary for the ordinary use and enjoyment of his land and the structures upon it, and declaring that above that height he has no greater rights in the air space than any other member of the public."*

Applications for court orders preventing both named individuals and, increasingly, 'persons unknown' from flying drones over property have been made, particularly in cases involving protestors. This has resulted in the Courts giving careful consideration to the balance between the right to privacy and the right to protest. For example, an attempt to ban defendants from flying drones over a site was rejected in *MBR Acres v Free the MBR Beagles (see both [2021] EWHC 2996 (QB) and [2022] EWHC 3338 (KB)* on the grounds that the law in respect of trespass and its application to drones was not clear. A full analysis of civil law in respect of drones is outside the scope of this study but we highlight a few issues below.

Negligence

Using drones may cause harm or damage to people, property or animals, for example as a result of crashing, parts or additions such as cameras falling off while in flight, noise and other reasons. This can either be as a result of negligence or accident. Note that where material loss or damage is caused as a result of 'an article, animal or person falling from an aircraft' there is no requirement on the injured party to show negligence, instead loss or damage is assessed as if caused by 'the wilful act, neglect or default of the owner of the aircraft' (Civil Aviation Act 1982 s76(2)). However if legal liability is created in some person other than the owner of the aircraft, for example, if an aircraft was hit by a drone, although the aircraft owner would still be liable for the damage they would be entitled to be indemnified by the drone owner against any claim for loss or damage (if they could be found) (Civil Aviation Act 1982 s76(3)).

Note that this indemnity provision does not appear to apply to the drone itself falling out of the sky, merely things falling from the drone.

Trespass

Research has reflected on the potential legal dimensions and implications of drones flown 'over private property', a scenario which it is argued 'the tort of trespass may become relevant'. Trespass is defined 'as the unjustifiable interference with the possession of land'. Hartman et al. (2022) continue that 'unlike the other forms of tort, trespass is actionable in the courts whether or not the claimant has suffered any damage. Thus, it would not need to be shown that any damage was attributable to the drone'. They continue that 'trespass can also be committed by entering another person's airspace', providing the example of a 'leading case concerning the erection of an advertising sign that extended a mere eight inches over the neighbour's land' and which was ascertained as trespass. They add, however, that the 'law is uncertain in relation to drones', giving the

example of a case that 'was held not to be trespass if an aircraft flies high enough above the level of ordinary use of land...more than thirty metres above the property', a decision which they add was 'influenced by the Civil Aviation Act, which specifically states that a trespass is not committed if an aircraft flies above property at a "reasonable height" having regard to the prevailing conditions'. They conclude that there remain 'questions about whether the operator of a drone might be responsible for committing the tort of trespass and be liable for damages to the landowner, even if the drone has flown through the landowner's airspace without intention'. *Source: Hartman et al. 2022*

Section 76(1) of the Civil Aviation Act 1982 provides that there is no trespass 'by reason only of the flight of an aircraft over any property at a height above the ground which, having regard to wind, weather and all the circumstances of the case is reasonable, or the ordinary incidents of such flight'. To benefit from this protection the drone operator must be complying with all ANO requirements. Moreover, S76 applies only to the flight itself and not to other actions incidental to the flight, for example taking video or photos. In those circumstances, 'best practice therefore is to ensure that the landowner's permission is obtained' (Practical Law 2023: 22).

In two relatively recent cases in which the court was considering whether to grant an injunction to restrict drone flying over property, different outcomes were reached. The 'question of whether flying a drone over a piece of land (and if so, at what height) is an actionable trespass appears, surprisingly, to be one that the law has yet definitively to answer.' (Nicklin J in *MBR Acres Ltd v Free the MBR Beagles* [2021] EWHC 2996 (QB) at para 111).

Nicklin J, refusing relief in respect of drone flying in that case commented at para 113:

"113. This is an interesting question, and it is one that is best left to be resolved in a case when it actually falls for determination. I venture to suggest that the law of trespass may not be the only relevant tort, and that it is better for the coherent development of the law if the full range of potential causes of action is considered. It can hardly be doubted that the law would provide a remedy against someone who used a drone to obtain (a fortiori , to publish) footage of a person getting undressed in the bedroom of his/her home. The entitlement to a remedy would not depend upon whether the drone was trespassing in the airspace of the homeowner's land. It would appear to be a straightforward claim for misuse of private information".

However, in *Anglo International Upholland Ltd v Wainwright [2023] 5 WLUK 613* an interim injunction was granted to prevent the defendant and persons unknown from trespassing onto the site of a dilapidated building and from flying drones over the site and photographs being taken (see Case study 4 for further discussion of *Anglo International Upholland Ltd v Wainwright*). The basis for the decision appears to be that on at least one occasion trespass took place when a person attempted to retrieve a drone that had fallen into the site and that photographs or videos taken by drones may encourage others to trespass.

It would seem most likely that simple flying of a drone, provided at reasonable height and in accordance with the Regulations, would not constitute a trespass even if used for taking pictures or video unless part of a course of conduct resulting in physical trespass. Using a camera or taking video may be better considered under misuse of private information or data protection law. Depending on the circumstances, intrusive and persistent drone use may also be considered harassment.

Nuisance

Whether or not a landowner has right in the airspace above their property and to what height has been the subject of legal commentary, and is often based on consideration of cases relating to 'overlooking' which generally does not count as a nuisance absent exceptional circumstances.

In *Bernstein v Skyviews Ltd* (above) Griffiths J noted that if a person "was subjected to the harassment of constant surveillance of his house from the air, accompanied by the photographing of his every activity" he was "far from saying that the court would not regard such a monstrous invasion of his privacy as an actionable nuisance for which they would give relief' [para 489G].

In a much more recent development, the Supreme Court recognised that visual intrusion could constitute nuisance in *Fearn and ors v Board of Trustees of the Tate Gallery [2023] UKSC 4* [2-23] 2 WLR 339. In that case relating to the panoramic viewing platform of the Tate Modern gallery Lord Leggat JSC held: "in an age when most people carry a smartphone with a high powered camera it is a natural and foreseeable consequence of allowing thousands of visitors a week to look out from a viewing gallery from which they get a clear view of the claimants' living accommodation that a significant number will take photographs of the interiors of the flats" [para 49].

The law has not definitively determined what constitutes a 'reasonable height above ground' or the point at which intrusive viewing becomes nuisance. As with trespass, in our view this is sensible as it will depend on the circumstances.

Note there are also common law and statutory offences of causing public nuisance.

Misuse of private information

The tort of the misuse of private information was confirmed in *Vidal Hall v Google Inc [2015] EWCA Civ 311 [2016] QB 1003* and includes unwanted intrusion into one's personal space. This emerged in various cases considering disclosure and repeat disclosure of private information in print and internet media from 2011 onwards such as *CTB v News Group Newspapers Ltd and Imogen Thomas* [2011] EWHC 1326 and [2011] EWHC 1334 (QB). The correctness of this case was expressly confirmed in the landmark Supreme Court decision in *PJS v News Group Newspapers Ltd [2016] UKSC 26, [2016] AC 108.*

The principal test for determining whether or not information is private is to assess whether in respect of the disclosed facts the person had a reasonable expectation of privacy (Lord Nicholls in *Vidal Hall* at para 21). It is possible to have a reasonable expectation of privacy in a public place.

Breach of Data Protection Law

A civil claim can also be brought under the Data Protection Act 2018 for contravention of the GDPR for material or non material damage including distress (see in particular section 180). See also the prior discussion of the Data Protection Act 2018 and General Data Protection Regulation 2016.

Duty of Care

Finally, there has been a suggestion that drones may affect duties of care imposed on local authorities and others (Greenberg 2022). In *Holmes v Medway Council [2018] 6 WLKUK 702* Medway County and Family Court sitting at Canterbury Combined Court Centre stated that 'drones may change the parameters of what is reasonable to expect by way of surveillance and monitoring'.

4. THE WORKSHOPS

Part 4.1. Grouping drone incidents and misuse

The focus groups were opened with an activity familiarising all participants with examples of reports of drone incidents and misuse, and encouraging a discussion of how we might group such incidents. Participants were provided with a list of reported drone incidents (Figure 6) and tasked to work in small groups to discuss these and develop categories in which to group them. Given the cross-jurisdictional nature of drone incidents, we were interested in bringing together lawyers with diverse expertise to understand whether they took different approaches to the issues.

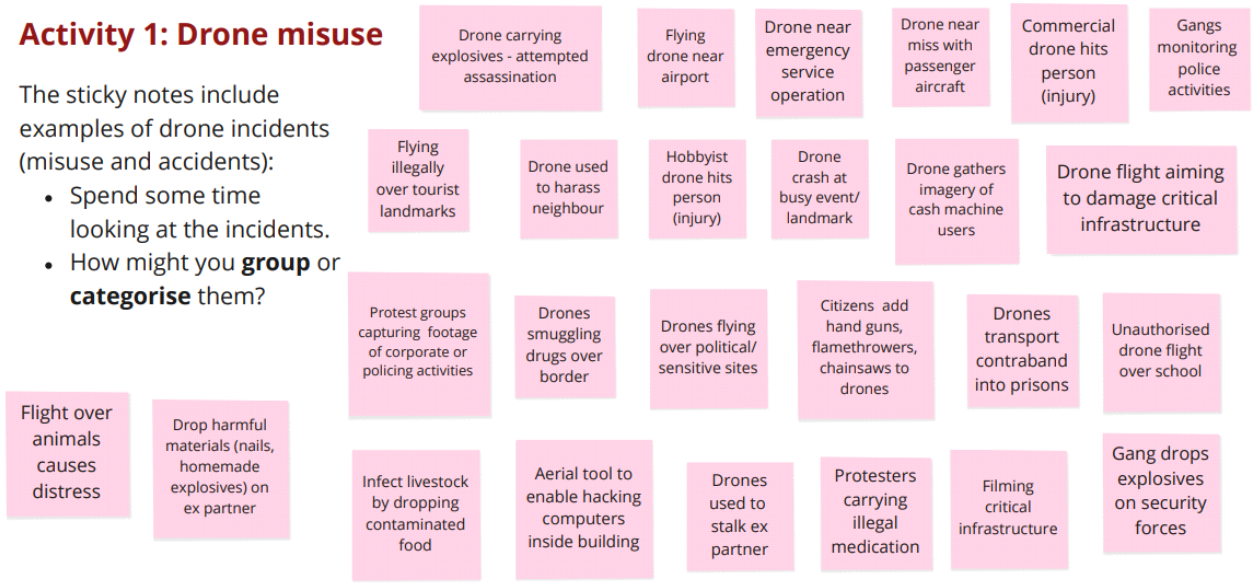

Figure 6: Examples of drone incidents. Source: Author's own

Participants then developed a range of categories in which to group examples of drone incidents and misuse (Figure 7). As is discussed below, participants viewed a number of these groups as linked and/or overlapping, rather than as separate categories. We combine the outcomes of the three workshops below:

Intention:

- Accidental (e.g., hobbyist hits person; flight disturbs nesting birds)
- Reckless/ negligent (e.g., flight near airport; hobbyist hits person; flying illegally over tourist landmark)
- Intentional/ deliberate (e.g., unauthorised flight over school; flight near airport; gangs monitoring police activities)
- Criminal (e.g., flying drone near airport; carrying explosives)
- Experimental (e.g., citizens add handguns, flamethrowers, chainsaws to drones).

Actor:

- Commercial (e.g., commercial drone hits person)
- Hobbyist (e.g., hobbyist drone hits person)
- Protester (e.g., protest groups capturing footage of corporate or policing activists; protesters carrying illegal medication)
- State (e.g., Filming critical infrastructure)
- Non-state actor (e.g., drone carrying explosives; gang drops explosives on security forces)
- Public versus State (e.g., protest groups capturing footage of corporate or poling activities)

- Public versus private (e.g., drone used to harass neighbour)
- Public versus business (e.g., protest groups capturing footage of corporate or policing activities)
- Remote actor (e.g., tool to enable hacking computers).

Action:
- Harassment (e.g., harass neighbour; stalk ex-partner)
- Domestic/ gendered violence (e.g., stalk ex-partner; drop harmful materials on ex-partner)
- Infringement of personal liberties (e.g., harass neighbour)
- Invasion of privacy (e.g., harass neighbour)
- Surveillance (e.g., filming critical infrastructure; gangs monitoring police activities; imagery cash machines)
- Inadvertent capture (e.g., imagery of cash machine users)
- Interpersonal (e.g., harass neighbour; stalk ex-partner).

Nature of Criminality:
- Way to facilitate an existing crime (e.g., drones transport contraband into prisons; drop harmful materials on ex-partner)
- Enabling / enabling a potentially criminal act (e.g., filming critical infrastructure; imagery of cash machine users)
- Novel (e.g., unauthorised flight over schools; near emergency service operation; drop harmful materials on ex-partner; capturing footage of farming activities)
- Using to evade laws (e.g., protesters carrying illegal medication).

Legal context (criminal or civil):
- Criminal (e.g., flight aiming to damage critical infrastructure)
- Civil (e.g., harass neighbour).

Rationale/ Context:
- Defensive or counter-surveillance (e.g., drones flying over political / sensitive sites)
- Facilitating or enabling harmful crimes (e.g., carrying explosives)
- Data (access, capture) (e.g., tools to enable hacking; drones flying over political/ sensitive sites).

Implication / consequence:
- Harm (e.g., drop harmful materials on ex-partner; hobbyist drone hits person; gang drops explosives on security forces; flight over animals causes distress)
- Security (e.g., flying over political/ sensitive sites; flight aiming to damage critical infrastructure; gang drops explosives on security forces; tool to enable hacking computers inside building)
- Safety critical (e.g., near miss with passenger aircraft)
- Non-safety critical (e.g., flight over animals causes distress)
- Categorising by risk (e.g., low risk, medium risk, high risk) (e.g., high risk – near miss with passenger aircraft)
- Nature of threat (drone as carrier of threat, or as threat) (e.g., carrier – explosives; as threat – near miss with passenger aircraft).

Regulatory context:
- Regulations/ flight category (open, specific, certified) (e.g., hobbyist drone hits person; commercial drone hits someone)
- Illegal/ unauthorised drone flight (e.g., drone near airport/ aircraft; transport contraband into prisons)
- Liability (e.g., hobbyist drone hits person; commercial drone hits someone).

Figure 7: Participant categorisations of drone incidents and misuse. Source: Author's own

Discussion of grouping drone incidents and misuse

Based upon the participant's grouping of drone incidents, we developed a series of common themes, including: Intention (referring to intentional and non-intentional actions and incidents, and the challenges of determining intent); Actor (reflecting on the alleged victim and perpetrator, and exploring different configurations of actor; Nature of Criminality (distinguishing between using drones to commit an existing criminal act versus using a drone for a novel criminal activity); Legal context (referring to whether the incident may be understood as criminal or civil); Nature of threat/ consequence (distinguishing between a drone posing the threat and as a carrier of threat, and reflecting on levels of risk associated particular incidents); Regulatory context (distinctions between recreational and commercial flyers, and airspace categories).

Each theme is unpacked below, highlighting key points from participant discussions. As is evident, participants did not understand these categories as separate, but rather as overlapping. As one participant explained, rather than discrete groups, we might better approach categorising incidents of drone misuse by using a 'Venn diagram' of separate but overlapping categories.

Summary of key themes from incident categorisation	
Intention	Participants identified a distinction between 'intentional' and 'non-intentional' acts and incidents, discussing mens rea (see below). In addition to discussing the challenges of determining intention and motive, participants also reflected on intention as it related to an action, and intention as it related to an outcome.
Actor	Participants considered categorising drone incidents in relation to the alleged victim and perpetrator, exploring categories such as 'public versus public', 'public versus commercial' and 'public versus state' and issues such as insurance and compensation. They also explored examples where the actors may be 'blurred' (e.g., private companies acting on behalf of the state).
Nature of criminality	Participants discussed categorising drone incidents in relation to the nature of criminality enabled by the drone, distinguishing between using drones to commit an existing criminal act (e.g., drones transporting contraband into prisons) versus using a drone for a novel criminal activity (e.g., unauthorised flight over a school).
Legal context (criminal or civil)	Participants suggested categorising drone incidents as 'criminal' or 'civil'. However, they noted that this distinction may not always be clear, raising the example of privacy incidents (e.g., drones used to harass a neighbour or to stalk an ex-partner), adding that there may be both criminal and civil dimensions to these incident types.
Nature of threat/ consequence	Participants discussed the nature of the threat itself, making a distinction between a drone posing the threat (e.g., drone crashes as part of normal operation) and a drone as a carrier of the threat (e.g., drone carries explosives or contraband). They extended conversation regarding the nature of the threat to consider the (potential) consequence, proposing categorisation around 'low, medium and high risk' incidents and/or 'safety critical' or 'non safety-critical' activity.
Regulatory context	Participants discussed regulatory context, both in relation to distinctions between recreational and commercial flyers, and in relation to different airspace categories. Participants were interested in whether there was any difference in the regulatory regime in relation to liability and/or civil wrongs. They also discussed potential differences in operational responsibilities (e.g., of operator and pilot) in relation to different regulatory airspace categories.

Intention

A central theme across discussions of identifying and grouping drone misuse was the theme of intention. By way of context, for a criminal offence to exist there will need to be an 'act' (*actus reus)* and an 'intention' (*mens rea*).

> ***Mens rea:*** Properly translated the term means “criminal intention” or an intention to do the act which is made penal by statue or the common law. However, the term is used to embrace any mental element that may be an ingredient of a criminal offence, e.g. recklessness, knowledge. It is necessary to turn to the definition of the particular offence to ascertain the mens rea which must be proved. The mental and other components of a criminal offence can, however, on occasions be difficult to distinguish, e.g. “possessing”, “keeping”, “permitting”. These terms import both physical and mental elements (LexisNexis n.d).

Following a distinction around ‘legitimate and non-legitimate' drone uses (i.e., incidents such as ‘gang drops explosives on security forces’ or ‘drones used to stalk an ex-partner', which participants felt would ‘categorically never have a legitimate use’), participants turned attention to the question of intention. Here, they identified a division between ‘intentional versus non-intentional' acts and incidents (i.e., ‘some of them are intentional acts, and some of them are potentially unintentional but reckless’), while also raising the challenges of determining intention and/or identifying whether a drone incident was deliberate, reckless, or accidental.

One participant described the example of flying in restricted airspace such as an airport Flight Restriction Zone (FRZ) (see Civil Aviation Authority n.d.d), adding that this could be intentional (e.g., flown in an attempt to disrupt airspace or to gather aerial/imagery data), or could be unintentional (i.e., the pilot may not be aware of relevant rules around airspace restrictions). In the latter case, the drone flight may be understood as non-intentional, but nonetheless as constituting reckless flight. Here, participants raised *mens rea*. One participant distinguished between ‘mens rea to do something which is a criminal offence’ versus ‘some of them [the incidents]’ as ‘accidental, some things can happen unintentionally’.

Some participants also raised motive, discussing the challenges associated with determining different motives in the case of different incidents. For example, one participant raised the question ‘is there a difference between artists adding tasers to drones’ and the wider addition of weaponry to a drone, adding that in the former example ‘that’s artistic’ and in the latter it’s ‘more a weapon for the sake of being a weapon’?

Participants reflected on intention as it related to action (e.g., flying a drone over a landmark, or flying over a cash machine) versus intention as it related to outcome (e.g., a drone crashing into a landmark, or gathering imagery of cash machine users). In the case of the drone flying over a cash machine, while it is possible the flyer may be deliberately seeking to capture the imagery with the intention of utilising information from the footage for criminal purposes, a participant highlighted that this could ‘potentially be an innocent flight that just caught’ this information inadvertently. Another participant understood this example as highlighting the need to consider the ‘potential consequences’ of the retention and/or sharing of drone imagery or data more broadly. Reflecting on the example of ‘protestors capturing imagery of illegal farming activities’, participants similarly raised the question of whether the flyer had intended to capture this imagery or whether the capture might instead be inadvertent. Participants also discussed whether ‘a right to public’ land, ‘capturing this footage’ and subsequently seeing ‘this mistreatment’ may constitute a ‘reasonable excuse’ defence.

Lastly, participants also briefly discussed the relationship between intention and the legality of the incident. One participant highlighted 'flight over animals causing distress' as an example of a non-intentional action which may not constitute 'doing anything wrong' in the eyes of the law.

Examples of relevant regulation and guidance

- Up to date CAA guidance on drones can be found on the Civil Aviation Authority's website https://www.caa.co.uk/drones/rules-and-categories-of-drone-flying/introduction-to-drone-flying-and-the-uk-rules/ (see also Domestic framework: Rules and regulations for drones in the UK).

With regard to **intention**

- The Air Traffic Management and Unmanned Aircraft Act 2021 enables the use of penalty notices where intention is not present for breaches of the Air Navigation Order 2016 (see Air Navigation Offences, and Enforcement).

With regard to **dangerous items (goods and/or cargo)**:

- The CAA's Drone and Model Aircraft Code states that 'you must never carry any cargo on your drone or model aircraft that could be dangerous to people, property or the environment if there was an accident' and provides the examples of poisonous, corrosive and flammable cargo (Drone and Model Aircraft Code n.d)
- CAP 2248 and CAP 2555 provide guidance on the carriage of 'dangerous goods', which it clarifies is 'currently only possible in the Specific category' (CAP 2248: 2) and requires application 'approval' by 'the CAA Dangerous Goods Flight Operations Inspectorate' (CAP 2555: 4)
- CAP 2555 defines 'dangerous goods' as 'articles or substances which are capable of posing a hazard to health, safety, property, or the environment and which are shown in the list of DG in the Technical Instructions, or which are classified according to the Technical Instructions' (CAP 2555: 7; see also CAP 1789A for further information)
- The CAA advise that a key distinction is 'whether the items are carried as cargo, or are fitted equipment on the aircraft. Dangerous goods regulations generally refer to carriage of those goods as cargo, i.e., packed in the aircraft for transport, not for use. There's a proviso in the Air Navigation (Dangerous Goods) Order which states that anything that is 'consumed or used' or words to that effect during the flight isn't dangerous goods. The simple example would be fuel; if you carry it as cargo, it's Dangerous Goods, if it's in fuel tanks to be used during the flight, it's not' (personal correspondence with CAA 2023)
- When asked whether 'weapons (e.g. tasers, guns, bombs) and/or improvised weaponry (e.g. chainsaws) count as 'dangerous goods' (per specific category language) and/or 'dangerous cargo' (per drone and model aircraft code)?', we received advice that 'to your specific example, improvised or actual weapons attached to a drone and intended to be used wouldn't be classed as DG [dangerous goods]. Whether or not they'd be DG if carried as cargo would depend on the exact type and how they appear in the ICAO TIs' (personal correspondence with CAA 2023). They added that 'if someone was to attach some sort of weapon to their drone and cause harm with it, we'd expect a Police prosecution under Article 241 of the Air Navigation Order, which states that it's an offence to recklessly or negligently permit an aircraft to endanger persons or property' (personal correspondence with the CAA 2023).

With regard to **wildlife**:

- The Drone and Model Aircraft Code (n.d) advises pilots 'do not fly where you'll disturb or endanger animals and wildlife'.

- In discussion of the 'avoidance of other aircraft', CAP 722 (2022: 27) states that 'UK Regulation (EU) 2019/947 sets out, in UAS.OPEN.060 (2)(b), that: the remote pilot shall maintain a thorough visual scan of the airspace surrounding the unmanned aircraft in order to avoid any risk of collision with any manned aircraft. The remote pilot shall discontinue the flight if the operation poses a risk to other aircraft, people, animals, environment or property'.

Actor

A further way that participants approached categorising drone misuse was to 'categorise in terms of **who is the victim** and **who is the alleged perpetrator'**, identifying combinations of actors such as '**public versus public**', '**public versus commercial**', and '**public versus state**'. Participants moved on to discuss examples of each of these categories, such as 'harassing a neighbour and stalking a partner', which they identified as 'public versus public'.

In discussion of different actors, participants focused in on 'the victim'. Adopting the 'perspective of the victim' in discussion of the scenario of a manned aircraft 'plane full of people' that 'gets hit by a drone and then crashes', one participant raised that their 'primary position' after such an incident 'is to try and find some form of compensation for the families, for the individuals that have suffered injury'. Here they highlighted existing UK aviation regulation on drones and insurance requirements (see table below).

In continuing to discuss this incident example, the participant added that extant insurance requirements may cause issues. They stated that if the drone crashing into the manned aircraft was 'operated criminally' (i.e., with intent to cause harm), that 'anyone who's operating a drone criminally' is unlikely to 'bother to get insurance since they set out to do the harm'. They continued that conversely, if the drone was flown negligently by a hobbyist (i.e., not intending to cause harm) the hobbyist 'may have some insurance', but that the size of the claims would be considerable. The participant then extended this point, applying it to other scenarios in the list. In the case of a 'drone hitting a person that's operated by a hobbyist' and causing an injury, if the drone weighs under 20 kilograms (as the vast majority of off-the-shelf consumer drones do), this incident 'could cause claims' that may be 'in excess of one million pounds' which the majority of hobbyists 'would not have the assets themselves to pay', should they have opted not to insure their drone. As is detailed further below, the Drone and Model Aircraft Code (n.d) states that while 'insurance is optional if you only fly for fun, recreation, sport, or as a hobby' you remain 'responsible for your actions' and thus 'could be held personally liable for any injury or damage you cause'. As such, they add that 'you may want to consider getting third party liability insurance'.

In a further discussion about drones and insurance, a participant was asked whether they felt 'there should be a scheme for uninsured drone users in the same way there is for uninsured car drivers'. The participant responded that they 'completely agreed with that', identifying some 'problems' associated with 'drones impacting aircraft'. They continued that under the 'Montreal Convention, a drone impacting an aircraft is likely to fall into Article 21' part 2 (specifying that 'the carrier should not be liable for damages arising under paragraph 1 of Article 17 to the extent that they exceed for each passenger 100,000 Special Drawing Rights if the carrier proves that: (a) such damage was not due to the negligence or other wrongful act or omission of the carrier or its servants or agents; or (b) such damage was solely due to the negligence or other wrongful act or omission of a third party') (The Carraige by Air Acts 2002), wherein 'an airline can argue that the accident was solely caused by the act of a third party' as there may currently be 'really no way of them being able to avoid a drone', the result of which 'means you end up with limited recovery for passengers', as 'they would have to go after the drone user'. The participant continued that 'even if you had an insured drone user, the reality is that those insurance policies' also have

‘problems’. They added that the first problem ‘is that almost all drone insurance policies exclude cover when a drone user is operating the drone outside of the drone code or rules or regulations, which means that the cover is in any event excluded’. They continued that ‘even if it wasn't’, ‘the limit of liability under those drone policies’ remains ‘maybe 10 million’, but that the ‘average passenger aircraft could be £300 million, and full of losses in there. So the actual money available is totally inadequate’. As such, they argued that ‘there needs to be some other form of protection’ to account for both ‘criminal users’ or ‘exclusions within insurance for domestic drone operators’ (Under domestic law see also liability and indemnity provisions of Section 76 of the Civil Aviation Act 1982, further discussed under Private actions in civil law, and Case study 1: Drones used to monitor an ex-partner).

Participants also offered challenges and complications to a categorisation approach based on actors. For example, a participant raised the issue of private companies acting on behalf of the state. Here, they gave the example of HS2, the high-speed railway UK infrastructure project, wherein ‘private companies’ are subcontracted to act on behalf of ‘the Government’. They continued that drones have been flown ‘from private land’ and have been used by such companies to obtain imagery of and ‘to film’ individuals such as ‘activists’ on ‘public highways and public land’, with drone imagery then utilised in cases seeking ‘injunctions of persons unknown’. The participant argued that the use of a drone for surveillance ‘by a private company but on behalf of the state’ was significant as it could be understood as an attempt to use Government surveillance ‘via private companies’ to ‘curtail’ public movement ‘along the public highway’, adding that the mobilisation of this drone imagery to seek ‘injunctions of persons unknown’ meant people ‘risk losing their liberty’. They continued that when they ‘wrote and asked for the [drone] footage’, they were ‘passed away, these people are so far removed from the state that by the time you get to them, they say the time has lapsed’ and the footage has been ‘deleted, because no one asked for it, so we haven’t got it anymore’. In discussing the ‘blurring’ of categories between different actors (such as the state and private companies sub-contracted to act on its behalf), the participant argued that **this blurring both highlights and feeds into evidentiary challenges** around ‘tracking this through, who holds the data and the imagery’, and raises questions of data rules more broadly, which ‘apply in different ways’ to these different actors. This remains a live and pertinent issue.

In September 2022 a ‘high court judge granted a route-wide injunction to HS2 to prevent environmental protesters from accessing hundreds of miles of land earmarked for the controversial route. *It is thought to be one of the largest injunctions of its kind against protesters granted by a court’* (Taylor 2022) (see *High Speed Two (HS2) Limited and Secretary of State for Transport v Persons Unknown and Ors* [2022] EWHC 2360). HS2 have issued a comment on the scope and nature of the injunction, stating that ‘the High Court has imposed an injunction to restrain unlawful trespass on and obstruction of access to land on the route of the HS2 Scheme’ and that ‘the injunction will not, and is not intended to, stop legitimate protest. Instead, we hope the injunction will prevent the violence, intimidation, and criminal damage that protests have frequently caused, harming the HS2 project and those working on it, and costing the UK taxpayer millions of pounds’ (HS2 2023).

Examples of relevant regulation and guidance
With regard to **insurance:** • The Civil Aviation Authority states that it is ‘the responsibility’ of every drone ‘operator to ensure they have appropriate insurance coverage’ (CAP 722: 21). • The CAA note that ‘the insurance you need depends on the size of your drone’ and ‘what you use it for’ (Drone and Model Aircraft Code n.d). For drones weighing over 20kg, you ‘must always have third party insurance, no matter what you use your aircraft for’ (Drone and Model Aircraft Code n.d). • The CAA require that ‘all commercial drone flights’ to hold ‘valid insurance cover’ (Civil

Aviation Authority n.d.a) and specify that you 'must have third party liability insurance' if you receive payment for your drone use or 'use your drone for work' (Drone and Model Aircraft Code n.d).

- For drones weighing 'below 20kg' and flown 'for fun, recreation, sport, or as a hobby, you can choose whether or not to have insurance', whereas if you 'fly for any other reason, you must have third party liability insurance' (Drone and Model Aircraft Code n.d).
- CAP 722 (2022: 21) states that the 'UK Regulation (EU) 785/2004 as retained (and amended in UK domestic law) under the European Union (Withdrawal) Act 2018 which came into force on 30 April 2005, requires most operators of aircraft, irrespective of the purposes for which they fly, to hold adequate levels of insurance in order to meet their liabilities in the event of an accident'. It continues that 'UK legislation which details insurance requirements is set out in Civil Aviation (Insurance) Regulations 20052. Article 2(b) of UK Regulation (EU) 785/2004 states that the regulation does not apply to 'model aircraft with an MTOM of less than 20kg', but the term 'model aircraft' is not defined within the regulation itself. Therefore, for the purposes of interpretation within the insurance regulation only, its use of the term 'model aircraft' should be taken to mean: 'Any unmanned aircraft which is being used for sport or recreational purposes only'. For all other types of unmanned aircraft operation, whether commercial or non-commercial, appropriate cover that meets the requirements of UK Regulation (EU) 785/2004 is required' (CAP 722: 21).

Nature of criminality

Participants also discussed categorising the drone incidents in relation to the nature of criminality enabled by the drone. Here, they distinguished between 'using drones' to commit 'an existing criminal act' (i.e., something that 'is clearly already a criminal offence' and 'using a drone to do something that is clearly already a criminal offence') versus a drone being utilised as and/or for a 'novel criminal activity where this is really a policy or criminal issue that's arisen because people now have access to use drones'. This distinction is echoed in research, with Coliandris (2023: 300) noting that 'aerial and remotely piloted drones possibly alter the conduct of crime by augmenting 'conventional' modes or by creating entirely novel ones.'

Here, participants identified examples (from the incident list provided) of drones used to commit an existing crime, including using drones to 'transport drugs into prisons', and 'using drones to infect cattle with diseases', whereby the drone is 'a mechanism allowing you to do it' but is 'one' of a number of ways 'to do it'. Where a drone was 'used to do something that is clearly already a criminal offence' or 'a matter where it attracts civil liability', participants felt such incidents were 'quite legally unambiguous'.

They continued that other incidents may constitute or 'fall into a grey area'. For example, in discussion of 'novel criminal activity' where a 'criminal issue has arisen because people now have access to drones', participants cited incidents such as 'unauthorised flight over a school', 'illegal footage over private land', and 'flights near emergency service operations', which they felt 'previously without a drone would have been unlikely' to occur. They continued that in distinction to drones being used to commit an existing crime, where drones enable novel criminal activity, the drone could be understood as 'intrinsic to the act', rather than 'being a facilitator'. In discussion of such incidents as potential 'grey areas', participants highlighted 'debates within that', raising questions of whether 'a drone was an offensive weapon which you could add a charge' [to the indictment] for.

In discussion of the nature of criminality, a participant also drew attention to the theme of 'remoteness', noting that in cases across both categories (i.e., using drones to commit an existing criminal act versus using a drone for a novel criminal activity), drones could also be understood in relation to a desire to 'evade laws', i.e., drones emerge as a tool flown remotely in an attempt to 'get around a framework', rather that perpetrating an act 'directly'.

Lastly, one participant noted that while their group had 'used the word criminal' when describing the initial distinction (between drones used to commit criminal acts versus using drones for novel criminal activity), they had also considered 'civil wrongs as well', giving the example of 'privacy' focused incidents. In this vein, in discussion of 'novel acts' that drones may more widely enable, one participant noted that some of the incidents 'are novel acts' but 'wouldn't necessarily be criminal acts'.

Legal context (criminal or civil)

In discussing the categorisation of drone incidents, participants also suggested and explored categorising the incidents as 'criminal' or 'civil'. Here, participants made reference to the distinction between criminal and civil law. For further information see Annex 3: Definitions: Criminal and Civil law.

In discussion of categorising drone incidents as criminal or civil, participants identified incidents such as 'stalking an ex-partner' and 'protestors capturing imagery of illegal farming activities' as 'civil wrongs' that 'wouldn't necessarily be criminal'.

Participants also noted examples where the distinction between criminal and civil may be unclear. For example, in discussion of incidents that may be related to 'privacy' (such as 'drones used to harass neighbour' or 'drones used to stalk ex-partner'), a participant highlighted the 'criminal aspect of it' which police or 'law enforcement will be involved in', while also highlighting the potential civil dimensions around the 'invasion of privacy' and associated 'mental distress' ('manifest as physical symptoms'), for which a claimant may be able to seek remedy (e.g., compensation).

Lastly, one participant also suggested that examples where an 'infringement of personal liberties' may be evident may fall 'somewhere in between civil and criminal', perhaps more appropriately considered under 'human rights'. By this we understand them to mean that there may be an infringement of liberty that is not sufficiently serious to amount to a breach of rights or where any relevant balancing exercise in respect of another person's rights permits the infringement (for example the right to freedom of expression may have more weight than the right to privacy depending on the circumstances, see e.g. *MBR Acres Ltd v Free the MBR Beagles* [2021] EWHC 2996 (QB), discussed under Trespass in Private actions in Civil law.

Examples of relevant regulation and guidance
In relation to **privacy**: • For a full discussion of data privacy and drones see Privacy and Data Protection. A claim for breach of data protection can be made to the County Court or High Court without first raising a complaint to the ICO (s180 Data Protection Act 2018) • See also Private actions in civil law for tort of misuse of private information. • The Civil Aviation Authority's (CAA) remit is limited to safety and does not include concerns over privacy, though it advises that pilots using drones with cameras should be aware of relevant Data Protection Regulation • The Drone and Model Aircraft Code (n.d) states that 'if your drone or model aircraft is fitted with a camera or listening device, you must respect other people's privacy whenever you use them. If you use these devices where people can expect privacy, such as inside their home or garden, you're likely to be breaking data protection laws' It offers multi-faceted advice regarding respecting people and their privacy

- CAP 722 (2022: 20) states that drone operators and pilots 'should be aware that the collection of images of identifiable individuals, even inadvertently, when using surveillance cameras mounted on an unmanned aircraft, may be subject to the General Data Protection Regulation and the Data Protection Act 2018'
- The Information Commissioner's Office (ICO) is an independent body responsible for upholding information rights. The ICO recognises that drone flight can involve collecting, using and/or sharing personal data, and poses the potential for collateral intrusion. The ICO distinguishes between hobbyists and professional or commercial flyers, describing compliance with data protection law (e.g., provision of privacy information, undertaking a Data Protection Impact Assessment) and asserting that where required, drone pilots must comply with the Surveillance Camera Code
- The Biometrics and Surveillance Camera Commissioner advise that the use of drones with cameras by 'relevant authorities' is covered by the Surveillance Camera Code.

Nature of threat / consequence

In discussion of categorising drone incidents, one participant reflected on the implications of beginning with the 'nature of the threat itself'. The participant made a distinction between the drone itself as 'posing the threat', and the drone as 'the carrier' of the threat. They continued that a drone itself might 'crash', and this crash may be associated with its 'normal operation' but occur 'because of a mishap'. In distinction, a drone may be used as a 'carrier', for example of 'explosives or contraband' (see Understanding Drone Categories and Examples of relevant regulation and guidance in Intention for discussion of dangerous goods).

Building on this discussion in the US context, another participant offered a distinction between the flight of the drone (e.g., whether the operation of the 'drone is itself a crime – is it being operated without permission, is it a threat to air navigation, or to persons on the ground?'), and the drone's involvement in criminal activity (e.g., is it being used to 'facilitate a crime like smuggling contraband'?). Here, they continued that the US aviation regulator, the Federal Aviation Administration (FAA), is 'concerned with when the flight itself is illegal because it's a threat to either people on the ground or to other air travel' (i.e., whether the drone flight contravenes aviation legislation), whereas if you are 'flying your drone legally, in other words you have a legal right to be there [in airspace] but you're committing a crime with it [the drone], the FAA doesn't care. It's not up to them. They don't enforce that', rather 'state law' would address this.

Another participant raised considering the nature of the threat as well as its (potential) consequence. They stated 'when it comes to categorisation, I was more focusing on what was the risk' as a 'determining factor'. They continued that 'we can divide these misuses in terms of, for instance, low risk, medium risk, and high risk, considering the impact that will be created by these incidents'. While adding that 'of course intentionality is important' (see Intentions) this participant understood one approach to categorisation in relation to threat as that focused on the potential 'implication of a drone'. Another participant suggested that in following this approach to categorisation, we could ask whether an incident was a 'safety critical' or 'non safety-critical activity', giving the examples of 'interfering with Civil Aviation' (e.g., 'drone near miss with passenger aircraft') as 'definitely a safety critical issue', in comparison to 'flying over animals and disturbing them' which is 'arguably not' safety critical.

Lastly, in relation to categorising via the consequence of a drone incident, a participant also raised the question of liability. Here, the participant gave the example of G4S (a security and facility services company operating several prisons in the UK) coming 'under scrutiny' regarding the ill effects on prisoners of drugs delivered to prisons via drones, adding that G4S had specifically faced scrutiny 'for not adequately policing drones' at their prisons. This issue is

echoed in Watchdog reports revealing that 'the deadly Black Mamba drug' was 'flown into a Staffordshire prison by drones', and that 'in May 2016 six inmates at the G4S-run prison were taken to hospital suffering from the ill effects of legal highs brought in by a drone' (Richardson 2017).

Examples of relevant regulation and guidance
• In the UK, the Civil Aviation Administration, states that responsibility for the 'action against the misuse of drones' is lead by the police (Civil Aviation Authority n.d), 'particularly at public events, that may contravene aviation safety legislation or other relevant criminal legislation' (CAP 722: 23). • For a fuller discussion, see Enforcement.

Regulatory context

In discussion of different approaches to categorising incidents of drone misuse, participants also raised regulatory context, in relation to both distinctions between recreational hobbyist and commercial flyers, and in relation to different airspace categories.

One participant raised whether any regulatory distinctions between a recreational hobbyist flyer who causes a person injury with their drone, and a commercial drone flyer who causes injury with their drone, would impact the regulatory response. The participant was interested in whether there 'might be different regulatory regimes over these two things, different amounts of liability', and the relation to 'tort law' (i.e., concerned with civil wrongs) (see Legal Context). Another participant raised the question of whether it would 'make a difference' if the incidents were to occur in different regulatory categories of airspace (i.e., Open, Specific, and Certified), asking whether this approach to regulation 'comes with different responsibilities for the operator and pilot'. They added that the 'operational requirements and restrictions' detailed in the regulations could 'also be another way of categorizing' drone incidents or misuse.

As is detailed in Domestic framework: Rules and regulations for drones in the UK, the UK's drone rules are based upon the risks associated with the flight (i.e., where you fly, proximity to other people, and the drone's size and weight) and are approached via three categories (Open, Specific and Certified; see Understanding drone categories). In terms of the responsibilities of pilots and operators, the Civil Aviation Authority details requirements in relation to qualifications and competencies, and responsibilities (see CAP 722; Drone and Model Aircraft Code). A distinction between hobbyist and commercial operator does appear in the Data Protection guidance from the ICO.

Examples of relevant regulation and guidance
• The Civil Aviation Authority's drone regulations are based upon 'the risk of the flight – where you fly, the proximity to other people, and the size and weight of your drone' (Civil Aviation Authority n.d.a) and there is 'no distinction between flying commercial and flying for pleasure or recreation', i.e., an 'approval just to operate commercially is not required' (Civil Aviation Authority n.d.a). The insurance requirements depend on both the size of your drone and what you are using your drone for. In relation to **insurance**: • The CAA states that it is 'the responsibility' of every drone 'operator to ensure they have appropriate insurance coverage' (CAP 722: 21). • The CAA note that 'the insurance you need depends on the size of your drone' and 'what you use it for' (Drone and Model Aircraft Code n.d). For drones weighing over 20kg, you 'must always have third party insurance, no matter what you use your aircraft for' (Drone and Model Aircraft Code n.d). • The CAA require that 'all commercial drone flights' to hold 'valid insurance cover' (Civil

Aviation Authority n.d.a) and specify that you 'must have third party liability insurance' if you receive payment for your drone use or 'use your drone for work' (Drone and Model Aircraft Cod n.d).

- For drones weighing 'below 20kg' and flown 'for fun, recreation, sport, or as a hobby, you can choose whether or not to have insurance', whereas if you 'fly for any other reason, you must have third party liability insurance' (Drone and Model Aircraft Code n.d).
- CAP 722 (2022: 21) states that the 'UK Regulation (EU) 785/2004 as retained (and amended in UK domestic law) under the European Union (Withdrawal) Act 2018 which came into force on 30 April 2005, requires most operators of aircraft, irrespective of the purposes for which they fly, to hold adequate levels of insurance in order to meet their liabilities in the event of an accident'. It continues that 'UK legislation which details insurance requirements is set out in Civil Aviation (Insurance) Regulations 20052. Article 2 (b) of UK Regulation (EU) 785/2004 states that the regulation does not apply to 'model aircraft with an MTOM of less than 20kg', but the term 'model aircraft' is not defined within the regulation itself. Therefore, for the purposes of interpretation within the insurance regulation only, its use of the term 'model aircraft' should be taken to mean: 'Any unmanned aircraft which is being used for sport or recreational purposes only'. For all other types of unmanned aircraft operation, whether commercial or noncommercial, appropriate cover that meets the requirements of UK Regulation (EU) 785/2004 is required' (CAP 722: 21).

In relation to **drone operation categories** and associated rules and responsibilities:

- For flights in the Open category, in addition to requirements around obtaining a flyer ID (showing 'you've passed the basic flying test') and registering for an operator ID ('which must be labelled on your drone') (Drone and Model Aircraft Code n.d), CAP 2012 states that drones in the A1 (and weighing 250-500 grams) or A2 (weighing up to 2 kilograms) sub-categories require operators to complete the A2 Certificate of Competency (A2 CoC) theoretical test, with an external provider (CAP 2012). Pilots flying in the Specific category must complete the General VLOS Certificate (GVC) 'as a minimum', which 'is a remote pilot competency certificate' introduced to satisfy 'the remote pilot competency requirements for VLOS [Visual Line of Sight] operations' (CAP 722: 120). The GVC includes a 'theoretical examination and a practical test flight' which are 'conducted at an RAE [Remote Pilots Assessment Organisations] facility' (CAP 722: 120). CAP 722 continues, due to the 'wide-ranging scope of the Specific category, the remote pilot competency requirements will vary widely, dependent on the type of operation being conducted' and 'will be set out in each individual operational authorisation document' (CAP 722: 119).
- In terms of responsibilities, CAP 7222 states that the drone 'operator is responsible for the overall operation of the UAS, and most specifically the safety of that operation. This includes the conduct of any safety risk analysis of the intended operations' and continues that the 'operator's responsibilities that are particular to each operating category are listed within the Annex to UK Regulation (EU) 2019/947'. The document also provides a 'more general set of responsibilities' (CAP 722: 112).
- For a fuller discussion of drone operation categories, see Domestic framework: Rules and regulations for drones in the UK.

Part 4.2. Responding to drone incidents and misuse

In the second activity, the focus group turned attention to specific reports of drone incidents from around the globe, asking participants to reflect on how they might handle them. Participants were assigned specific case studies from the following list:

Surveillance	Case study 1	Drones used to monitor ex-partner
	Case study 2	Drones used by gangs to disrupt policing
Carrying	Case study 3	Drones used to drop harmful materials on ex-partner
	Case study 4	Groups uses drones to infect livestock
Infrastructure	Case study 5	Drone used in attempt to disrupt electrical grid
	Case study 6	Drones used at environmental protest at airport

This section introduces the case studies discussed and details key reflections around the contexts, legal procedures and challenges related to these. Collectively, it identifies three overarching themes: **Surveillance** (case study 1: Drones used to monitor ex-partner, and case study 2: Drones used by gangs to disrupt policing), **Carrying** (case study 3: Drones used to drop harmful material on ex-partner, and case study 4: Group uses drones to infect livestock), and **Infrastructure** (case study 5: Drone used in attempt to disrupt electrical grid, and case study 6: Drones used at environmental protest at airport). Working in small groups, in relation to each case study, participants discussed:

- What is reported to have taken place? Who was involved?
- If you were handed this case, how would you proceed?
- Would you anticipate any challenges or opportunities (e.g., chain of evidence)?
- Are there any areas of law that you might cite, or that might need changing or reviewing to ensure potential drone harms are adequately covered?

Case study analysis

Surveillance: Case studies 1 and 2

Case study 1: Drones used to monitor ex-partner

Case study 1	**Drones used to monitor ex-partner**
	‘For mother-of-three Kim* a small barbecue in her backyard on New Year's Eve was meant to be respite from months of harassment by her ex-husband. That was, until she saw the drone hovering above her head. "I heard fans, or air, and I looked up and I saw a drone right above my head," she said. "It shot up really high and far away and flew to a parked car in one of the side streets." The Western Sydney woman is confident it was the work of her ex-husband who had, that day, been trying to discover her whereabouts. "I knew it was him because he had tried every other means to get near us," Kim said. "My fear was he was going to come through the night under the guise of the local fireworks and take my children." Kim is one of many victims being stalked and harassed using a new generation of technology. She lives in fear, in a virtual prison, to keep her children safe. Six security cameras surround the property, windows are sealed with sensors and the whole family wear personal alarms wherever they go.’
Source:	ABC News (2018) Perpetrators using drones to stalk victims in new age of technology fuelled harassment https://www.abc.net.au/news/2018-10-01/drones-used-to-stalk-women-in-new-age-of-harassment/10297906 (30/09/2018)
Country:	Australia

In discussion of case study 1, participants highlighted several key themes, including **attribution, related evidence, harassment** and **course of conduct**.

In discussion of this reported incident, participants raised questions and challenges around attribution. Participants stated that the 'first thing' that struck them is that they 'don't see it clearly in the facts that it could be determined to be the man' operating the drone, and that there remained a question of 'how they are going to prove that it's him', adding that 'there's an obvious evidential problem'. Other participants supported this, adding that while the victim may be 'confident it's him [the alleged perpetrator]' as 'that day he was trying to discover her whereabouts', the piece does not suggest that 'she [the victim] has seen him' operating the drone, or that 'he [the alleged perpetrator] has some kind of history with drones' such as 'buying a drone' or 'some other contemporaneous evidence' along these lines. In this vein, they stated that while they recognised her confidence in attribution, they were not clear that 'there was anything to connect it [the drone] to him [the alleged perpetrator]'. They also highlighted that context remained important, stating that it was 'New Year's Eve, there's fireworks going on, there's reasons you could imagine drones are in the air'. While continuing that it 'might depend on' whether the drone was 'right up above her head', they added that it could be asserted that that was 'an accident', given how often hobbyists fly 'low' over property and/or in manners or locations more widely that regulations do not permit (see Domestic framework: Rules and regulations for drones in the UK). In this vein, one participant added that even if attribution could be determined, 'what if he [the alleged perpetrator] says well I was just flying it [the drone] over the area, and it meets all the CAA rules?'. Here, they added that it would be important to show that the drone flight was 'causing distress' and this was 'intentional' (see Intentions).

In discussion of how evidence might be obtained more widely, participants added that if 'there was enough to arrest him, then there might be enough to download his phone and other devices', which they continued may be significant if the alleged perpetrator was using their phone to operate the drone or if their 'credit card history' demonstrated that 'he's bought' a drone. Participants also raised the question of the scope and utility of surveillance in this case, adding that while the victim has 'lots of security around her property', even with such 'security measures, somebody can still just fly a drone over and see if you're there or not'. Participants added that given the drone 'flew to a parked car in one of the side streets' that another approach to try and 'show the drone was connected to the individual [the alleged perpetrator]' might be see whether the drone could be a connected to a specific parked car, which could be connected the alleged perpetrator, through the presence of CCTV (e.g., 'from other people's properties' or 'Ring doorbells').

Participants also discussed whether the drone itself could be located and inspected, and whether this might reveal 'who it's registered too', though others added that the individual may simply 'not follow other laws' such as 'registering the drone', and that the ability to bypass such 'aviation laws' remains 'part of the reason why people use these vehicles [drones] to do illegal activities, because of establishing the link...there is a distance and remoteness to it'. This was underscored by another participant who stated that the potential distance between the incident and 'the person flying the drone is obviously evidentially a massive challenge'.

In discussion of relevant areas of law, a participant felt that assertions of attribution (rather than determined attribution) 'might be problematic' for a 'criminal case', though may be 'sufficient' in 'family court'. Here the participants were perhaps thinking of the difference in standard of proof between a criminal and civil case, with crime usually being proved beyond reasonable doubt and a civil case being determined on the balance of probabilities. Other participants suggested that the 'legislation that would probably capture this would be harassment', 'rather than a criminal' approach. Participants stressed that in the case of 'harassment', there 'has to be a course of

conduct'. While participants highlighted that the victim 'does say he [the alleged perpetrator] had been harassing her before...trying to discover her whereabouts, trying to get nearer by other means', they continue that it 'might depend on what existing orders there are in place', as if the drone-related incident was treated as a 'one-off' it may be more 'difficult'. Here, participants stated that even if 'he [the alleged perpetrator] knew she was there [home] already and was trying to see who she was with in the garden, to see if she had a new partner' for example, they were unsure whether he could be 'arrested just for that'. In the event that there were measures such as 'non-molestation orders' (a type of injunction that can be applied for through the family court and granted in order to prevent a partner, former partner or 'associated person' from causing an individual or their child/children harm, including harassment and psychological abuse) in place, participants noted that while these typically include requirements such as to stay '50 metres from the property', the drone somewhat complicated this as its pilot could be 'further, far away'. They continued that while it may be argued that drone flight in proximity to the person and home is 'inherently a form of harassment' and 'would come under a normally worded non-mol [non-molestation order]', it might be beneficial to 'spell' the drone misuse out 'specifically and then have multiple breaches'. They also underscored the importance of demonstrating that the drone flight was causing 'emotional distress' which may enable her to seek 'compensation' for 'psychological damage' (see Legal context).

While focusing attention predominantly on harassment, participants also identified and discussed a range of other relevant areas of law.

In addition to highlighting breaches of aviation law around safety in relation to 'hovering a drone' above the victim's head (see Domestic framework: Rules and regulations for drones in the UK), participants raised questions regarding 'what the law of trespass' says in relation to drones, asking 'if you haven't put a foot on the ground' but were a 'Peeping Tom...getting some kind of access, remote or otherwise' with a drone, for example to see someone or 'see somebody naked', 'would that be prosecutable?'. One participant responded that 'it would' be prosecutable, comparing it to 'voyeurism' and adding that 'the law of trespass may be used for civil action as well, potentially' (see also Trespass).

Participants also raised the question of 'privacy issues arising from the monitoring'. Here, both General Data Protection Regulation (GDPR) and the 'intrusion to private personal privacy' were highlighted, with one participant in the international focus group stating that 'we talk of fundamental rights of individuals, so intrusion into her privacy through surveillance is in itself a breach to her fundamental right, and therefore that is a breach and the ex-partner has had no right probably to use drone just to undertake surveillance without her own express authorization'. In discussion of the 'intrusion to private privacy', they continued that 'though it may not be criminal...a civil suit may ensue specifically for the ex-partner spying on the wife because she has a right, her fundamental right to privacy'. The participant also added that if it was ascertained that the alleged perpetrator 'violated her right to privacy through surveillance', trespass and 'intrusion' may be 'linked', 'one aspect is a civil suit, the other aspect of trespassing and be actually prosecuted under the penal code or the Criminal Court rules'.

In addition to raising the 'property angle' in relation to 'trespass', a participant also raised whether this drone incident 'could come under nuisance'. They also continued to raise a question around 'jurisdiction', asking 'would the family court have jurisdiction in the sky?' (see also Nuisance). Such statements echo questions raised by some lawyers. It is asserted, for example, that 'drones pose complex questions over the torts (legal wrongs) of trespass and nuisance. A person may be able to bring a claim if their right to quiet enjoyment of their property is violated by an intentional or reckless act of a drone user' (Mills & Reeve 2016).

Ultimately, participants reflected that this incident could be considered as or in relation to 'quite a few different things', and that the discussion had highlighted that there were 'multiple overlapping areas' of law relevant to this incident.

Examples of relevant regulations and guidance

In relation to **enforcement:**

- The Air Traffic Management and Unmanned Aircraft Act 2021 provides powers where police officers suspect a drone could be involved in the commission of an offence.
- See Enforcement for a fuller discussion.

In relation to **registration and wider operator and pilot requirements**:

- The registration requirements of the Drone and Model Aircraft Code (n.d), applying to drone flight 'outdoors' and in the Open Category (A1 and A3 categories), 'depend on the weight of your drone or model aircraft, whether it is a toy, and whether it has a camera', with drones weighing below 250 grams with a camera requiring an Operator ID (an 'operator is the person responsible for managing a drone or model aircraft'), and drones weighing over 250 grams requiring both a Flyer ID (obtained by passing the 'CAA's official theory test') and an Operator ID.
- See Domestic framework: Rules and regulations for drones in the UK.

In relation to **drone airspace rules**:

- In the context of the UK, the question of how the drone was permitted to fly in proximity to alleged victim's residential home would depend on the drone's weight, when the drone was built and/or placed on the market, and whether or not the drone has a camera onboard (CAP 2012).
- All flights in the open category must not exceed 120 metres (400 feet), are not permitted to drop articles nor to carry dangerous goods, must be kept within the operator's visual line of sight, and must adhere to all applicable airspace restrictions (CAP 2012). Further, if the drone in question could be identified as a consumer drone weighing under 250 grams (with or without a camera), it falls within the A1 category and is permitted to 'fly over uninvolved people, but not over crowds' and 'at residential, recreational, commercial and industrial sites' (CAP 2012; Drone and Model Aircraft Code, n.d), though the Drone and Model Aircraft Code (n.d) reminds flyers that they 'must never put people in danger. Even small drones and model aircraft could injure people if you don't fly them safely'. Drones weighing between 250 grams and 500g are also part of the A1 category, and while users are permitted to 'fly closer to people than 50m if you get the A2 Certificate of Competency', they are not permitted to intentionally fly over uninvolved persons (Drone and Model Aircraft Code n.d; CAP 2012). If the drone can be identified as weighing between 500 grams and 2 kilograms and the flight is in the Open Category, the flyer is permitted to fly 'no closer than 50m horizontally from uninvolved persons'. If the drone weighs between 2 kilograms and 25 kilograms, the rules are as such: 'No uninvolved people present within the area of flight; Maintain 50 metres separation from any uninvolved people; No flight within 150 metres horizontally of residential, commercial, industrial or recreational areas' (CAP 2012).
- See also Domestic Framework: Rules and regulations for drones in the UK.

In relation to **privacy:**

- While the CAA's remit is limited to safety, it advises that pilots using drones with cameras should be aware of relevant Data Protection Regulation. The Drone and Model Aircraft Code (n.d) also stipulates that 'If your drone or model aircraft is fitted

with a camera or listening device, you must respect other people's privacy whenever you use them. If you use these devices where people can expect privacy, such as inside their home or garden, you're likely to be breaking data protection laws. It's against the law to take photographs or record video or sound for criminal or terrorist purposes. Any photos or recordings you take may be covered by the General Data Protection Regulation (GDPR)'. The Drone and Model Aircraft Code (n.d) offers multi-faceted advice regarding respecting people and their privacy.

- The Information Commissioner's Office (ICO), an independent body responsible for upholding information rights, recognises that drone flight can involve collecting, using and/or sharing personal data, and poses the potential for collateral intrusion. The ICO distinguishes between hobbyists and professional or commercial flyers, describing compliance with data protection law (e.g. provision of privacy information, undertaking a Data Protection Impact Assessment) and asserting that where required, drone pilots must comply with the Surveillance Camera Code.
- See Privacy and data protection section for a fuller discussion.

In relation to **trespass**:

- CAP 722 (2022: 20) states that drone 'operators must be aware of their responsibilities regarding operations from private land and any requirements to obtain the appropriate permission before operating from a particular site. They must ensure that they observe the relevant trespass laws and do not unwittingly commit a trespass whilst conducting a flight'.
- In discussion of 'Airspace restrictions for remotely piloted aircraft and drones' and under 'other considerations before flying', the CAA's website (n.d) states 'the aviation regulations only address the flight safety aspects of the flight' and that in addition to the 'legitimate interests of other statutory bodies', drone operators 'should also be mindful of the requirements of Section 76(1) of the Civil Aviation Act 1982 in relation to trespass and nuisance, noting that they must comply, at all times, with the relevant operating regulations' and that drones "should be flown at a height over the property of another person which is 'reasonable' in all circumstances. Failure to do so could amount to trespass if the flight interferes with another person's ordinary use and enjoyment of land and the structures upon it".
- Article 76 (point 1) of the Civil Aviation Act 1982 relates to 'liability of aircraft in respect to trespass, nuisance and surface damage' and states 'no action shall lie in respect of trespass or in respect of nuisance, by reason only of the flight of an aircraft over any property at a height above the ground which, having regard to wind, weather and all the circumstances of the case is reasonable, or the ordinary incidents of such flight, so long as the provisions of any Air Navigation Order and of any orders under section 62 above have been duly complied with', and section 39 (points 1 and 2) relate to 'trespassing on licensed or authorised aerodromes' state that 'subject to subsection (2) below, if any person trespasses on any land forming part of an aerodrome licensed in pursuance of an Air Navigation Order or authorised by a certificate under the Aerodromes Regulation, he shall be liable on summary conviction to a fine' and '(2) No person shall be liable under this section unless it is proved that, at the material time, notices warning trespassers of their liability under this section were posted so as to be readily seen and read by members of the public, in such positions on or near the boundary of the aerodrome as appear to the court to be proper'.
- For further discussion of Trespass and Nuisance see Private actions in civil law.

Case study 2: Drones used by gangs to disrupt policing

Case study 2	Drones used by gangs to disrupt policing
	'Criminals used drones to disrupt the monitoring of a hostage situation, says the FBI. A top FBI official told a drone conference in Denver that criminals deliberately flew several small drones to block the rescue team's view of an unfolding situation. The drones caused the FBI to lose sight of the attacker. "We were then blind," Joseph Mazel, the FBI's operational technology law unit chief, told the AUVSI drone conference. According to military news site Defense One, which attended the conference, the hostage situation occurred over the winter in the outskirts of a large US city. The FBI had set up an elevated observation post to monitor the hostage situation, and suddenly drones appeared, carrying out a series of "high-speed low passes at the agents in the observation post to flush them [out]," Mr Mazel said.'
Source:	BBC News (2018) Drones used to disrupt FBI hostage situation https://www.bbc.co.uk/news/technology-44003860 (04/05/2018)
Country:	United States of America (USA)

In discussion of this incident, participants focused attention on the **remote obstruction of policing and the complexity of mitigation**.

The participants first introduced the scenario, which they described as 'concerning criminals using drones to disrupt a hostage situation. Basically, drones were used to block the rescue team's view of an evolving situation, in which the FBI lost sight of the attacker'. In discussion of both what was reported to have taken place and relevant areas of law, participants understood the situation as 'almost certainly criminal because it would be obstructing a police operation'. They stated that 'if it wasn't a drone', it sounded like it would 'be tampering or interfering with a police investigation or operation' and that if 'you did that in a non-drone context while the police were trying to pursue someone, they'd just charge you with obstructing'. They understood the actors involved (the gang) as 'criminal already', but as using the drone as a way of doing that [their activities] more effectively' (see Nature of Criminality). Thus, they understood the drone as a facilitator 'being used to very effectively do something that's already illegal'. Participants recognised the drone as a 'double-edged sword', its ability to 'extend the capacity for a human user to achieve certain ends' as applicable to both the police as drone users and for 'prospective criminals' seeking to 'conduct counter-surveillance of police movements' by using drones (Coliandris 2023: 303).

Participants highlighted that in addition to the potential of the drone flight contravening relevant aviation legislation, other legislation around obstructing police activities would also likely be applicable.

Linking back to the discussion of attribution and remoteness in Case study 1, participants also raised the question of 'how the FBI or police forces would deal with drones being used to obstruct investigations', raising that if 'there was someone just standing or driving in a way that could obstruct, I presume the police would stop them or arrest them, but if this is going on [with drones] remotely, presumably it might be quite hard to find them'.

In this vein, some participants raised the issue of 'countermeasures' or 'counter-drone technology' (C-UAS), which refers to 'systems designed to detect, track, identify and/or intercept drones' (Martins et al. 2020: 5). The participants continued that drone misuse was 'difficult to counter' and the 'range of countermeasures' remained relatively limited, with 'a target timely response' potentially 'many, many years away from being developed, or being widely available'. While increasingly trialled and deployed by UK police forces, counter-drone technologies remain

associated with a ‘range of hurdles’ including costs, ‘coordination, planning and safety’ (Martins et al. 2020: 5; see also Jackman 2023a). To this end, the UK Government’s Counter-Unmanned Aircraft Strategy asserts both the importance of police having ‘a full range of powers and technologies to act against malicious drone use’ and their goals around resourcing and ‘empowering’ police to have ‘access to training, technology and legal powers appropriate to their roles and the drone risks they face, so that they can act confidently and decisively to address drone-based threats’ (HM Government 2019: 27).

Lastly, one participant also raised the question around ‘what would happen if the drone fell from the sky in the course of a police operation, if the police brought it down’ utilising a counter-measure such as a ‘net, gun etc’ and the falling drone ‘caused damage to people below, potentially causing risk of physical injury’. They continued to raise a question of ‘who carries the risk of that?’. They asked if hypothetically someone was ‘seriously hurt by a drone falling through the sky', 'could they sue the person who was flying it’, though added that ‘in practice that this might not get much further because it’s in the course of police action’ and as such there ‘might not be very much in the way of damages, or it may not even be traceable’. Information about regulation relevant to the police use of drones can be found in the table below (see also Jackman 2023a).

Examples of relevant regulations and guidance
In relation to **drones near emergency service operations**: • The Civil Aviation Authority states that remote pilots must ensure that the drone ‘is not flown close to or inside any areas where an emergency response effort is ongoing [including ‘activities by police, fire, ambulance, coastguard or other similar services where action is ongoing in order to preserve life, protect the public or respond to a crime in progress’], unless they have permission to do so from the responsible emergency response personnel’ (CAP 722: 11). • The Drone and Model Aircraft Code (n.d) states that ‘you must keep out of the way and not fly in any way that could hamper the emergency services when they’re responding to an emergency incident. If you’re out flying at or near to an emergency incident when it happens, you must safely and immediately stop flying unless the emergency services give you permission to continue’. • In addition to aviation legislation, legislation such as Section 89 of the Police Act 1996, which the Crown Prosecution Service summarises as stipulating that 'the offence of obstructing a police officer is committed when a person wilfully obstructs: a constable in the execution of his duty, or, a person assisting a constable in the execution of the constable's duty' and that 'a person obstructs a constable if he prevents him from carrying out his duties or makes it more difficult for him to do so' may be relevant. It continues that "the obstruction must be 'wilful', meaning the accused must act (or refuse to act) deliberately, knowing and intending his act will obstruct the constable: Lunt v DPP [1993] CLR 534. The motive for the act is irrelevant" (Crown Prosecution Services 2022). In relation to **drone airspace rules**: • The Drone and Model Aircraft Code (n.d) states that ‘it’s against the law to take photographs or record video or sound for criminal or terrorist purposes’. For example, section 58 Terrorism Act 2000 makes it an offence to collect or make a record of information of a kind likely to be useful to a person committing or preparing an act of terrorism. • CAP 722 (2022: 23) states ‘The Police often have greater resources, response times and powers of investigation than the CAA. To support this, the CAA has agreed with

the Police, in a signed Memorandum of Understanding that the Police will take the lead in dealing with UAS misuse incidents, particularly at public events, that may contravene aviation safety legislation or other relevant criminal legislation. Please report any misuse of UAS to your local Police force. The CAA's remit is limited to safety and also to investigate where someone is operating, or has operated, in a manner that is not in accordance with their operational authorisation. This does not include concerns over privacy or broadcast rights'.

In relation to **police use of drones**:

- The Civil Aviation Authority (n.d.a) states that police drone 'operations fall outside the scope of UK Regulation (EU) 2019/947. This is because these activities are outside the scope of the primary legislation that this regulation falls under (UK Regulation (EU) 2018/1139 – 'The Basic Regulation'), as set out in Article 2'. They continue that 'there is, however, a requirement for the CAA to ensure that police UAS operations take due regard of the safety objectives of the Basic Regulation, and that they are separated safely from other aircraft. Additionally, the Air Navigation Order 2016 requirements still apply, including (but not limited to) the requirement to not recklessly or negligently act in a manner likely to endanger an aircraft, and to not recklessly or negligently cause or permit an unmanned aircraft to endanger any person or property. The CAA is actively engaged with the Department for Transport, the National Police Chiefs' Council (NPCC) and other government agencies to establish suitable policy to cover this area' (Civil Aviation Authority n.d.a). The Civil Aviation Authority (n.d.a) add that 'until this policy is in place, police UAS operators are reminded that whilst they do not fall within the scope of the Basic Regulation, current NPCC operational guidance is that all police UAS operations remain within the confines of extant regulation' (Civil Aviation Authority n.d.a).
- Further discussion of the withdrawal of the Small unmanned aircraft – emergency services operations (ORS4 1233) and its present reworking can be found in Jackman's (2023a) report exploring police drone use in the UK.

Carrying: Case studies 3 and 4

Case study 3: Drones used to drop harmful material on ex-partner

Case study 3	Drones used to drop harmful material on ex-partner
	'Drones can be used to help first responders survey an area and better address people in need of immediate assistance. Or drones can be weaponized and used by a vindictive ex-partner who wants to do harm to their former love interest, which is what happened when a Pennsylvania man allegedly used a drone to air-lift explosives onto his ex-girlfriend's property...44-year-old Jason Muzzicato was in possession of a DJI Phantom 3 drone that hadn't been registered with the Federal Aviation Administration (FAA). During his arraignment earlier this week, where he was charged with crimes related to possession of the firearms and explosives, Assistant U.S. Attorney John Gallagher alleged that Muzzicato used the drone to drop explosive devices on his ex-girlfriend's house, according to Pennsylvania newspaper the Morning Call. Muzzicato's attorney denied the charge and said that there hasn't been any "conclusive evidence" to suggest his client attempted to bomb his former partner's home. The court will decide if Muzzicato was behind the alleged bombings, but he was certainly equipped for them. An FBI search of his home and automotive business discovered 10 guns,

	including multiple semi-automatic pistols and AR-15 rifles. The agency also found seven handmade explosives in his possession, according to Lehigh Valley Live. He should not have been in possession of any of the gun, as he had a domestic violence protective order filed against him in 2017 that makes it illegal for him to own firearms...Muzzicato is also accused of being responsible for a number of explosions that have happened within his neighborhood since March. While the explosions have not resulted in any damage or injuries, they have disrupted the community. One neighbor claimed that he saw the autoworker use the drone to drop nails from the sky, according to news station WTAP. Muzzicato also allegedly equipped his car with dashboard switches that, when flipped, would release objects like ball bearings, nails and paint thinner that could be used to damage other cars.'
Source:	MIC (2019) Drones are now being weaponized by abusive exes https://www.mic.com/impact/how-drones-are-being-weaponized-used-to-stalk-harass-people-18784714 (19/09/2019)
Country:	United States of America (USA)

In discussion of case study 3, participants focused attention on **attribution** and **the chain of evidence,** the **pursuit of criminal or civil wrongs,** and **remoteness and its implications** on the scope of existing domestic violence protective orders.

In a discussion mirroring aspects of that related to Case study 1: Drones used to monitor ex-partner, participants gravitated towards questions of the 'evidentiary challenges' of attributing the drone and its activities to the alleged perpetrator, describing this as a 'remote actor problem'. In discussion of evidentiary challenges more widely, participants asserted that it would also be important to 'look at the firearms in his possession' and to determine whether they were 'related in way evidentially, to the explosive devices that were dropped' on the victim's home. The participant added that there were 'quite a few stages of evidence collection' to go through, given that 'an FBI search of his home and automotive business discovered guns'. In discussion of things that 'can connect back to' the alleged perpetrator, participants also raised whether it might be possible to 'trace the explosive devices if there are any serial numbers or anything on those, back to his business', adding that it may be possible to determine 'if forensically there was a link, chemical or otherwise, between whatever was found at the girlfriend's house and his handmade explosives, then that would be good evidence'. For further discussion of drone forensics, see Case study 5: Drone used in attempt to disrupt electrical grid. In continuing the discussion of evidence and reflecting on relevant areas of law, participants first highlighted the relevant 'history' of the alleged perpetrator's actions and 'obsession' with his 'ex-partner', and then second raised that his 'possession of firearms' accounted for a 'breach' of a relevant protective order and that the same order may 'extend to making it illegal for him to have in his possession not just the firearms but the explosives' too. That said, participants expressed uncertainty about whether there may or may not 'be enough to reach the criminal standard' and, as with Case study 1: Drones used to monitor an ex-partner, some felt it may be more appropriate to pursue 'harassment' and the 'civil standard'.

Building on this, participants also raised questions about the actions of the alleged perpetrator and how these fit with the scope of the existing domestic violence protective order. Here, one participant stated that 'what really struck me' was that although the domestic violence protective order 'made it illegal for him to own firearms, it didn't make it illegal for him to own the drone'. They continued that while the fact that the drone 'hadn't been registered' may be sufficient for its use 'to make it a crime', they expressed concerns about the implications of the rise of emerging technology including drones and the scope of existing domestic violence protective orders. Here, we might consider the rise of technology-enabled domestic violence, including acts such as

cyberstalking, more widely (Crown Prosecution Service 2023). Another participant added that they felt that the 'law needs to catch up to modern times' to recognise 'these kind of new ways of causing distress and harm, such as by using drones'.

The Online Safety Act 2023 imposes duties which, in broad terms, require providers of services such as search engines or user to user services [4] (including social media) 'to identify, mitigate and manage the risks of harm', including risks which particularly affect individuals such as children or vulnerable adults from illegal content and activity (Online Safety Act 2023). This may result in service providers having duties or being liable under the Act if illegal content or actions including images or videos are uploaded online or livestreamed. Illegal content is defined at section 59 and schedule 7 of the Act and covers a wide range of offences including harassment, child sex abuse material, public order offences, terrorism, and offences involving drugs or weapons.

While not explicitly raised by participants, an additional relevant dimension is the use of the drone to transport explosives or other weaponry. Alongside the growing use of weaponised off-the-shelf drones in warfare across global battlefields (Jackman 2019), evidence submitted to the 2019 House of Commons Defence Committee inquiry into the 'Domestic threat of drones' highlights videos shared on social media demonstrating that drones have been modified by hobbyists to carry and deploy a range of weapons, including tasers, handguns, flamethrowers and chainsaws (Defence Committee 2019). While 'there was nothing to suggest there was any malicious intent behind these videos, but simply to show what was possible', such citizen-led modifications nonetheless highlight that such drone modifications 'could be used for nefarious purposes' (Protect 2022).

Examples of relevant regulations and guidance

In relation to carrying **dangerous items (goods or cargo)**:

- In the UK context, the Civil Aviation Authority's Drone and Model Aircraft Code (n.d) states that 'you must never carry any cargo on your drone or model aircraft that could be dangerous to people, property or the environment if there was an accident' and provides the examples of poisonous, corrosive and flammable cargo.
- Section 94 (1) of the Air Navigation Order (2016) states that 'a person must not cause or permit any article or animal (whether or not attached to a parachute) to be dropped from a small unmanned aircraft so as to endanger persons or property' (see also Air Navigation Order 2016).
- CAP 2248 and CAP 2555 provide guidance on the carriage of 'dangerous goods' [DG], which it clarifies is 'currently only possible in the Specific category' (CAP 2248: 2). CAP 2555 defines 'dangerous goods' as 'articles or substances which are capable of posing a hazard to health, safety, property, or the environment and which are shown in the list of DG in the Technical Instructions, or which are classified according to the Technical Instructions' (CAP 2555: 7; see also CAP1789A for further information).
- The CAA advise that a key distinction is 'whether the items are carried as cargo, or are fitted equipment on the aircraft. Dangerous goods regulations generally refer to carriage of those goods as cargo, i.e., packed in the aircraft for transport, not for use. There's a proviso in the Air Navigation (Dangerous Goods) Order which states that anything that is 'consumed or used' or words to that effect during the flight isn't dangerous goods. The simple example would be fuel; if you carry it as cargo, it's Dangerous Goods, if it's in fuel tanks to be used during the flight, it's not' (personal correspondence with CAA 2023).
- When asked whether 'weapons (e.g. tasers, guns, bombs) and/or improvised weaponry (e.g., chainsaws) count as 'dangerous goods' (per specific category

[4] *User-to-user service* means an internet service by means of which content that is generated directly on the service by a user of the service, or uploaded to or shared on the service by a user of the service, may be encountered by another user, or other users, of the service (s3 Online Safety Act 2023).

language) and/or ‘dangerous cargo’ (per drone and model aircraft code)?’, we received advice that ‘to your specific example, improvised or actual weapons attached to a drone and intended to be used wouldn’t be classed as DG [dangerous goods]. Whether or not they’d be DG if carried as cargo would depend on the exact type and how they appear in the ICAO TIs’ (personal correspondence with CAA 2023). They added that ‘if someone was to attach some sort of weapon to their drone and cause harm with it, we’d expect a Police prosecution under Article 241 of the Air Navigation Order, which states that it’s an offence to recklessly or negligently permit an aircraft to endanger persons or property’ (personal correspondence with the CAA 2023).

Case study 4: Group uses drones to infect livestock

Case study 4	**Group uses drones to infect livestock**
	‘One of China’s biggest animal feed producers said it had used a radio transmitter to combat crooks using drones to drop pork products contaminated with African swine fever on its pig farms, as part of a racket to profit from the health scare. In July, China’s agriculture ministry said criminal gangs were faking outbreaks of swine fever on farms and forcing farmers to sell their healthy pigs at sharply lower prices. And on Thursday, a state-backed news website, The Paper, reported that a pig farming unit of Beijing Dabeinong Technology Group Co Ltd had run foul of the regional aviation authority, as its transmitter had disrupted the GPS signal in the area. Answering questions from investors on an interactive platform run by the Shenzhen Stock Exchange, Dabeinong confirmed on Friday that its pig farming unit in Heilongjiang province had unwittingly violated civil aviation rules. “Our unit in Heilongjiang province... to prevent external people from using drones to drop pork with African swine fever virus, violated regulations by using a drone control equipment set,” the company said. “We broke related radio regulations, although that was unintentional,” said Dabeinong, adding that it had surrendered the equipment to authorities and was willing to accept a penalty.’
Source:	Reuters (2019) Commercial pig farm in China jams drone signal to combat swine fever crooks https://www.reuters.com/article/china-swinefever-idUSL4N28U0QB (20/12/2019)
Country:	China

In relation to case study 4, participants discussed issues around: **the challenges of identifying and categorising the harm, evidentiary questions** (around the novelty of the drone as an enabler and the reliability of the information), **relevant areas of law** (including the use of drones to drop hazardous goods, and trespass), and the **implications of responding to the drone with radio equipment.**

Participants first raised the challenges of identifying and categorising unlawfulness and harm, expressing that they weren’t ‘immediately’ sure of how to categorise ‘what kind of unlawfulness it [the case study] is’. They continued by pointing to the cross-jurisdictional nature of the drone incident, noting that it could be understood in different ways, including ‘poisoning or biohazard’, ‘damage to private property’ or ‘industrial sabotage as its impacting the profits of the pig farmers’, ‘cruelty to animals’, or ‘environmental protection’, as there are 'some collateral damages out of this practice’.

Participants also returned to discussions in the Grouping drone incidents and misuse activity regarding the nature of criminality enabled by the drone, distinguishing between using drones to commit an existing criminal act, and novel uses of drones (i.e., a criminal activity that has arisen

because of drones) (see Nature of criminality). Here, participants understood case study 4 as ‘kind of like a class industrial scam, but done with new technology’. While some remarked that ‘you don’t necessarily need a drone to create what they said was happening’, others added that drones could be understood as enablers and that ‘drones means on a bigger scale and more easily’. In this vein, ‘with regard to what needs to be regulated or criminalised’, several participants ‘thought that the act itself is probably already caught by some existing framework’ but wondered ‘whether or not you need to extend that because the scale is greater, there’s a greater capacity for disruption by the drone.’

In discussing evidentiary questions, participants raised questions regarding the reliability of the information and the proof of allegation. Taking on the role of ‘a defence’, one participant stated that they would need to ‘ask for’ further information about whether the ‘Government is saying there’s a criminal gang in order to create a diversion’ and to determine whether ‘there is a real outbreak’ or whether ‘there is an engineered outbreak which a criminal gang are using to further their own means’. They continued that they’d need to determine this information, including ‘questioning the reliability of the information from the Government, in order to justify the blanket use of blocking’ technology.

Participants also raised additional questions around evidence. One participant raised questions around how these allegations were being proved, asking ‘how do you prove the drone dropped it?’. They continued that the pig farmers may in fact be ‘more concerned about people flying surveillance drones over to look at unsafe industry practices’ and suggested that further questioning was need about whether this was ‘actually a protection of the industry from being surveilled by activists, rather than people actually dropping contaminated meat’. Another participant described the potential for the drone to be a ‘red herring used by the State’. They continued that ‘bio terrorism has existed long before drones’ and they expressed that there was potential for these allegations ‘being driven to more effectively restrict or limit people’s drone use’. They continued that ‘looking at’ this incident, ‘it seems like the newsworthiness of the story is about the drone itself... the drone is in the headline’. This was significant, they continued, because such headlines can suggest that ‘we could be entering this lawless dystopia that sort of provides the proving ground to set up the legal system where we can use the drones as much as we want, as the police, as the State’, but ‘we don’t want you to use them too much, unless you’re using it for our purposes then we’ll allow it’.

Participants also highlighted areas of law that they felt were particularly relevant, including trespass (see also Trespass and Case study 1: Drones used to monitor ex-partner), the dropping of hazardous items, and interference with the drone.

Participants highlighted that while if you did this act ‘in a pre-drone age, you’d be going into the farm’, a ‘contained place’, so that would be entering private property without permission’, reflecting on whether ‘the sky is different’. They continued to reflect on the rights you have ‘by owning a property’, with one participant adding that while ‘you have easement’, they were unsure whether you ‘actually control the air above you’. Others expressed an ‘understanding of land’ ownership as ‘always being from what is down there up to the skies’. Another participant added that this case may not be understood as ‘trespassing...in the sky, in the same way’ as physically being on the ground, though others added that they wondered ‘whether that is something that will be increasingly questioned, if it’s trespassing in the sky over property’. In discussion of this, one participant stated that ‘if you had to do it [dropping meat] the old fashioned way [i.e., on foot], you’d be trespassing into the property’ and you ‘could be criminalised for that’. They continued that while drones made this action ‘a lot easier’, their alleged usage introduced a ‘question mark about whether the act of flying over private property with intent should be criminalised’ or whether it’s adequately ‘covered by the existing rules’.

Elaborating ‘on the comparisons with trespassing’, another participant highlighted the experience of the farmer. Here they raised that ‘if this was going to be done in a conventional way by foot or by vehicle, the farmer will be able to secure the property, they’d be able to put fences and gates and things, take steps to aim to prevent this happening’, whereas in the case of the drone, ‘they don't have any control over the airspace of their farms, they can't prevent potential civil wrongs by securing their property’ (see by way of example *Anglo International Upholland Ltd v Wainwright [2023] 5 WLUK 613*, discussed in Trespass), where an injunction was granted in part because the judge found there was nothing further the landowner could do to secure their property and prevent risk of injury). While the participant remained unclear whether drones would constitute trespass, they also raised whether drones flying over and ‘making noise and disturbing’ people and animals at the farm might constitute ‘nuisance’ and this might be an avenue for ‘contention’ (see Nuisance, and table below).

Participants also raised the issue of carrying and/or dropping hazardous goods via drone. One participant suggested that ‘hazardous goods are not allowed to be dropped’, and while ‘hazardous goods are primarily chemicals and explosives’ they noted that ‘contaminated meat in this context might be classed’ as hazardous and ‘you might be able to argue’ these rules apply (see table below).

Lastly, participants also raised the issue and potential implications of the act of interference with the drone, via the use of countermeasure equipment. Here, participants focused concerns on the secondary implications of the use of equipment in an attempt to ‘block the drone’, raising that a ‘blanket blocking of an area may both engage human rights and commercial rights being infringed’ as it may impact upon the use or functioning of other equipment, and it may also impact other drone users, leading to their drones ‘becoming uncontrollable, crashing and potentially causing property damage’.

Another participant stated that this aspect of the case might be challenging in an evidentiary sense, and recommended engaging with an ‘expert in inhibiting the drone signal and also the EMP [electromagnetic pulse]’, such as from the ‘International Telecommunications Union’ who could ‘help with radio frequencies’, including whether they ‘jam, match or collide with other frequencies, and to what extent’ we might expect ‘damage’ to ‘other connections, equipment, and tools’. Information about countermeasures or counter-drone technology can be found in Case study 2: Drones used by gangs to disrupt policing. However, in addition to state-led strategy and measures, private actors and individuals have also sought to ‘take matters into their own hands’ by turning to online overseas stores to buy devices such as ‘drone jammers’ (Engineering & Technology 2021).

Examples of relevant regulation and guidance
In relation to **animals**: • The Drone and Model Aircraft Code (n.d) states that flyers should not fly where they will ‘disturb or endanger animals and wildlife’. • CAP722 (2022: 27) states that the ‘remote pilot shall discontinue the flight if the operation poses a risk to other aircraft, people, animals, environment or property’. In relation to **nuisance, trespass and noise**: • While the Drone and Model Aircraft code (n.d) does not mention nuisance, disturbance or trespass specifically, CAP722 (2022: 20) states that drone ‘operators must be aware of their responsibilities regarding operations from private land and any requirements to obtain the appropriate permission before operating from a particular

site. They must ensure that they observe the relevant trespass laws and do not unwittingly commit a trespass whilst conducting a flight.'

- In relation to noise, CAP 1766 (2019: 24) states that 'there are currently no noise specific requirements for UASs in UK. The intent is that UK follows EC regulation'. CAP 1789B (2021: 3) states that 'in order to provide citizens with high level of environmental protection, it is necessary to limit the noise emissions to the greatest possible extent. Sound power limitations applicable to UAS intended to be operated in the 'open' category might be reviewed at the end of the transitional periods as defined in Commission Implementing Regulation (EU) 2019/947'. Part 13 'lays down the basic noise emission standard' and details a 'noise test code' (CAP 1789B: 53). CAP 2505 (2023: 4) states that technologies such as drones raise and pose 'new challenges for noise legislation and understanding of how these types of noise sources may impact people on the ground'.
- For further discussion, see Private actions in civil law (including sections on Trespass and Nuisance), Drones and Noise.

In relation to carrying and/or dropping **hazardous or dangerous items (goods)**:

- The CAA's Drone and Model Aircraft Code (n.d) states that 'you must never carry any cargo on your drone or model aircraft that could be dangerous to people, property or the environment if there was an accident' and provides the examples of poisonous, corrosive and flammable cargo.
- Act 94 (1) of the Air Navigation Order (2016) states that 'a person must not cause or permit any article or animal (whether or not attached to a parachute) to be dropped from a small unmanned aircraft so as to endanger persons or property'.
- CAP 2248 and CAP 2555 provide guidance on the carriage of 'dangerous goods', which it clarifies is 'currently only possible in the Specific category' (CAP 2248: 2). CAP 2555 defines 'dangerous goods' as 'articles or substances which are capable of posing a hazard to health, safety, property, or the environment and which are shown in the list of DG in the Technical Instructions, or which are classified according to the Technical Instructions' (CAP 2555: 7; see also CAP 1789A for further information).
- The CAA advise that a key distinction is 'whether the items are carried as cargo, or are fitted equipment on the aircraft. Dangerous goods regulations generally refer to carriage of those goods as cargo, i.e., packed in the aircraft for transport, not for use. There's a proviso in the Air Navigation (Dangerous Goods) Order which states that anything that is 'consumed or used' or words to that effect during the flight isn't dangerous goods. The simple example would be fuel; if you carry it as cargo, it's Dangerous Goods, if it's in fuel tanks to be used during the flight, it's not' (personal correspondence with CAA 2023).
- When asked whether 'weapons (e.g. tasers, guns, bombs) and/or improvised weaponry (e.g. chainsaws) count as 'dangerous goods' (per specific category language) and/or 'dangerous cargo' (per drone and model aircraft code)?', we received advice that 'to your specific example, improvised or actual weapons attached to a drone and intended to be used wouldn't be classed as DG [dangerous goods]. Whether or not they'd be DG if carried as cargo would depend on the exact type and how they appear in the ICAO TIs' (personal correspondence with CAA 2023). They added that 'if someone was to attach some sort of weapon to their drone and cause harm with it, we'd expect a Police prosecution under Article 241 of the Air Navigation Order, which states that it's an offence to recklessly or negligently permit an aircraft to endanger persons or property' (personal correspondence with CAA 2023).

In relation to **counter-measures or interference with a drone**:

- The Air Navigation Order 2016 (as amended) states that 'a person must not recklessly

or negligently act in a manner likely to endanger an aircraft, or any person in an aircraft' (Air Navigation Order 2016), which has been interpreted to suggest that it is 'illegal to interfere with a flying aircraft in the UK' (ADS 2019).

- CAP722 (2022: 92) discusses 'frequency interference', stating that 'operations close to any facility that could cause interference (such as a radar station) could potentially disrupt communications with the UAS [drone], whatever the frequency in use. GNSS jamming activities may also disrupt communications as well as command and control signals. Information on scheduled GNSS jamming exercises can be found on the Ofcom website. This document does not include information on the UK Counter-Unmanned Aircraft Strategy. Details on this strategy can be found on the gov.uk website'.
- Wider laws cited can depend on the form of countermeasure (i.e., equipment used). Ofcom, the regulator for the UK's communications industries, asserts that 'it is illegal, unless authorised, to use any apparatus for the purpose of interfering with wireless telegraphy' and cites 'section 68(1) of the Wireless Telegraphy Act 2006' (Ofcom n.d). Section 68(1) states that 'a person commits an offence if he uses apparatus for the purpose of interfering with wireless telegraphy' (Wireless Telegraphy Act 2006).
- In relation to 'radio frequency jamming', Ofcom defines a jammer as 'any apparatus designed, constructed, adapted, or intended to be used to block or weaken the reception of wireless telegraphy', though clarifies that 'Ofcom does not authorise or licence the use of jammers' (Ofcom n.d). Rather, jammers 'as described above, are subject to the Electromagnetic Compatibility Regulations 2016' which 'require that equipment does not affect the operation of radio communications' and 'make it a criminal offence to make non-compliant equipment available' (Ofcom n.d).

Infrastructure: Case studies 5 and 6

Case study 5: Drone used in attempt to disrupt electrical grid

Case study 5	**Drone used in attempt to disrupt electrical grid**
	'A DJI Mavic 2 drone approached a Pennsylvania power substation. Two 4-foot nylon ropes dangled from its rotors, a thick copper wire connected to the ends with electrical tape. The device had been stripped of any identifiable markings, as well as its onboard camera and memory card, in an apparent effort by its owner to avoid detection. Its likely goal, according to a joint security bulletin released by DHS, the FBI, and the National Counterterrorism Center, was to "disrupt operations by creating a short circuit." The drone crashed on the roof of an adjacent building before it reached its ostensible target, damaging a rotor in the process. Its operator still hasn't been found. According to the bulletin, the incident, which was first reported by ABC, constitutes the first known instance of a modified, uncrewed aircraft system being used to "specifically target" US energy infrastructure. It seems unlikely to be the last, however.'
Source:	Wired (2021) A Drone Tried to Disrupt the Power Grid. It Won't Be the Last https://www.wired.com/story/drone-attack-power-substation-threat/ (05/11/2021)
Country:	United States of America (USA)

In discussion of case study 5, participants focused attention to **evidentiary challenges (around remoteness, registration and identification), questions of liability** and **determining potential damages,** and the **labelling of critical infrastructure.**

Participants first discussed the evidentiary challenges of remote operation, stating that the problem with incidents such as case study 5 was that 'unless somebody specifically sees the

drone' and 'where it goes, because it's probably going to be flown beyond visual line of sight', it remains 'almost impossible to catch people'. Participants noted that if 'representing the substation', they would seek to 'try and track the drone' in order to obtain relevant information such as the serial number or markings (which may be linked to registration information), or to pursue extracting the 'memory card' as you may be able to 'see where' the drone flew or was 'programmed' to fly, via 'forensic analysis' (see box below).

Participants also discussed how common the practice of police-led drone forensics was, raising that the lack of common access to such techniques may 'feed into why the CPS [Crown Prosecution Service] don't pursue' drone cases, as they can 'seize, but they ask the police officers and they're not sure if they'll get the conviction'. Part of Dr Jackman's wider research project involved engagement with UK police forces both using drones and policing drone misuse. This research found that some participating members of the police desired further access to drone forensics training, and that some officers felt that 'seizing drones' may be additionally challenging due to both the 'paperwork' associated with this and the a potential 'nervousness' from a 'CPS perspective' because of the comparatively low number of barristers, 'district judges or benches' 'that know this [drone] legislation inside out' (Jackman 2023a).

Drone Forensics

Drone forensics refers to the forensic examination of drones. Forensic analysis of a drone can, depending on the type of drone flown, enable the determination of the flight history, geo-locations, waypoints, and altitude, as well as additional information, and can be used to 'build an evidentiary picture to determine if a drone was used in a criminal offence'.

The Forensic Access Group (2023) provide a range of guidance around drone examination, including case background, data acquisition, analysis and reporting. They advise not powering the drone on where possible, and describe 'RF isolating' a drone if it needs to be powered on in order to examine data (e.g., with a Faraday bag, namely an enclosed or sealed unit preventing signals from being sent or received from a device). They also describe 'methods that data may be stored on drones', including internal flash storage and memory cards, and techniques to access this information, including 'JTAG or ISP' and 'Chip Off'. They also advise that there are other devices that may be useful to inspect and 'may contain data of relevance', including smartphones that contain data related to the drone (e.g., in an app, which may contain 'data of relevance'), or the remote control unit or ground control station. They highlight a range of 'data of interest', including two key 'data types', namely GPS data and flight logs, and media files (videos and images). They add that while any media present can be useful to provide data on who is operating the drone, detail in the content of the video/image, as well as metadata, that it's 'not always straightforward to interpret GPS data' so analysis will be needed to present it in a meaningful and useful way (i.e., decoding).

Alongside depending on the type of drone engaged, drone forensics can also be understood as challenging as it is a 'relatively new' field, 'there is a limited amount of information and specialisation on the matter, and as there is no standardised practice to conduct a forensic investigation around drones' (Mantas and Patsakis 2022: 1). Stating that the forensic analysis of drones is required to comply with the 'Forensic Science Regulator's Code of Practice', which details engaging with drones (see also Forensic Science Regulator 2023), the Forensic Access group add that 'not to comply could potentially lead to implications down the road at court, perhaps not around admissibility, but around the weight of evidence'. *Source: Forensic Access Group 2023*

Lastly, returning to previous discussions regarding whether the drone was used to commit an existing criminal act or to facilitate novel criminal activity (see Nature of Criminality), one participant noted that 'you can achieve the same criminal behaviour by throwing something' over the perimeter fence 'or whatever', while another argued that the 'drone is making these' kinds of actions 'easier to do potentially'.

In further discussing the challenges of identifying drones and their operators, a participant also drew attention to developments in the area of 'remote identification' in the United States.

Remote Identification: Remote identification (known as 'remote ID') refers to the 'ability of a drone in flight to provide identification and location information that can be received by other parties through a broadcast signal' (Federal Aviation Administration n.d). From September 2023, the FAA requires 'all drone pilots who are required to register' their drones to 'operate in accordance with the rules on Remote ID', in order to enable the safe 'integration of drones into the National Airspace System' (Federal Aviation Administration n.d). In the UK, such debates commonly fall under the term 'electronic conspicuity' which can be understood as an 'umbrella term for the technology that can help pilots, remotely piloted aircraft systems and air traffic service providers be more aware of what is operating in surrounding airspace' and which can include technology 'broadcasting flight information' (CAP 1711: 20). Such technology is understood as a 'critical part' of enabling UK airspace to 'become an entirely known environment where integration of all traffic...is made possible because of shared digital information' (NATS 2023: 5). While identifying electronic conspicuity as a 'vital aid', the Civil Aviation Authority (n.d.e) states that it is exploring 'mandating that drones will not be able to fly unless Remote ID is enabled', and that it's Airspace Modernisation Strategy 'will be aligned with the outcome of a study commissioned by the Department for Transport on specifications' and a 'roadmap of electronic conspicuity deployment will be developed in conjunction with the Department for Transport' (CAP 1711: 21). While acknowledging that the technology 'does not come without cost', a report by NATS, the UK's leading provider of air traffic control services, recommended that the UK 'adopt electronic conspicuity by 2025, strengthening the principle of 'see and avoid' by adding the ability to 'detect and be detected' for both crewed and uncrewed aircraft' (NATS 2023: 15, 9). In August 2023 the Civil Aviation Authority launched a call for input regarding a review of UK drone regulations, in which it noted that 'UK Regulation (EU) 2019/945 sets out a requirement to implement Remote ID in the UK by January 2026, through manufacturer requirements and operational requirements' and that the CAA is 'exploring how Remote ID could be implemented in the UK' (CAP 2569: 20).

For further discussion of electronic conspicuity, see Integration.

Liability and damage

Participants also raised questions around liability and determining potential damages. Remarking on the shorthand title of the press article, 'drone used in an attempt to disrupt the grid', the participants returned to the discussion of intention to argue that 'if there's an attempt, it's not an innocent case of someone flying a drone and then making a mistake' (see Intentions). A participant continued that if it had been a mistake 'then we would speak about a civil liability case, intervening with an insurance company and settling the matter outside the court'. Conversely, in the case of a deliberate act to target the substation, ' it seems that there's an intention to damage perhaps or to cause any other harm' and as such 'criminal proceeding' may be more appropriate (see Legal Context). In this event, there is a need to understand 'the loss', and you 'might calculate how much, or up to what extent, all the damages can be monitored and give a value of the damage, and unless the aggressor pays the damage, then the criminal liability is not released at all, at least from a precautionary perspective'. In discussion of the 'responsibilities of the service provider' (i.e., electrical grid), some participants also felt that 'if

you have a facility which is vulnerable... that it's for you to address that vulnerability', asking 'is it ok for you to have something so open to potential terrorist attack?'. Here, one participant suggested that facilities would 'have to take measures', such as encasing or putting a non-conducting 'net over a generator' which 'would stop a drone performing'. Guidance, such as that provided by the National Protective Security Authority (n.d.), the UK government's National Technical Authority for physical and personnel protective security, seeks to 'assist national infrastructure site security managers in developing a C-UAS [counter-drone] strategy' and may be of utility here.

Critical infrastructure

Lastly, one participant expressed concern around the expanding labelling of 'critical infrastructure' in the UK. The participant argued that in the 'last 2 years' the phrase 'critical infrastructure' has been used 'more and more in criminal legislation', particularly in 'anti-protest legislation', 'where it removes the protest' from sites labelled as such. They added that this expansion was notable when compared to wider understandings of critical infrastructure as 'water, gas, electricity, hospitals', and asserted that it was significant because buildings such as 'parliament' are understood as 'critical infrastructure', but the 'public should have a right to access their representatives' and as it is labelled critical infrastructure, 'you cannot have a protest outside'. They added that their concern 'would be the increasing use of the term critical infrastructure in legislation, the government moving quickly to characterise what they see as critical infrastructure' and the potential implications this can bring more widely. As is further discussed in Case study 6: Drones used at environmental protest at airport, these comments may relate to the passing of the Public Order Act 2023, which responds to 'disruption' caused by protestors with a range of 'measures' to 'bolster the police's power to respond' (Home Office 2023) and which makes 'provision for new offences relating to public order; provision about stop and search powers; provision about the exercise of police functions relating to public order; provision about proceedings by the Secretary of State relating to protest-related activities; [and] provision about serious disruption prevention orders; and for connected purposes' (Public Order Act 2023).

Examples of relevant regulations and guidance

In relation to **registration and flight requirements**:

- In the UK, the requirement to register your drone depends on the drone's 'weight of your drone or model aircraft, whether it is a toy, and whether it has a camera' (Civil Aviation Authority n.d.f). The Drone and Model Aircraft Code (n.d) specifies that 'even if you do not need to register, you must still follow the Drone and Model Aircraft Code when you fly' (see Domestic framework: Rules and regulations for drones in the UK).
- With regard to the flight itself, in addition to communicating registration requirements, the Drone and Model Aircraft Code (n.d) continues that flyers must 'follow any flying restrictions' and notes that 'flying may be restricted around some sites, such as prisons, military ranges, royal palaces, and government buildings'. As the Civil Aviation Authority (n.d) notes, a 'number of airspace restrictions exist within the UK and these apply equally to both unmanned and manned aircraft. These areas are referred to as either: Prohibited Areas, Restricted Areas or Danger Areas' and 'apps and online resources' can be used to 'check airspace'.
- It can also be noted that additional regulation may apply in relation to 'restricting flying in the vicinity' of specific forms of infrastructure, such as 'nuclear installations' (The Air Navigation (Restriction of Flying) (Nuclear Installations) Regulation 2016).
- The Air Navigation Order 2016 (as amended) states that 'a person must not recklessly or negligently cause or permit an aircraft to endanger any person or property' (Air Navigation Order 2016).

- The Drone and Model Aircraft Code (n.d) states that if ‘you make a forced landing or crash on private property, you must get the property owner’s permission before retrieving your drone...This is especially important at sites where security services are likely to respond if you enter without permission’.

In relation to key **national infrastructure:**

- In detailing 'interference with use or operation of key national infrastructure', the Public Order Act 2023 defines ‘key national infrastructure’ as: ‘road transport infrastructure, rail infrastructure, air transport infrastructure, harbour infrastructure, downstream oil infrastructure, downstream gas infrastructure, onshore oil and gas exploration and production infrastructure, onshore electricity generation infrastructure, or newspaper printing infrastructure’ (Public Order Act 2023).

Case study 6: Drones used at environmental protest at airport

Case study 6	**Drones used at environmental protest at airport**
	‘Heathrow Pause, a splinter of the Extinction Rebellion movement, intended to fly drones in the airport's 3.1-mile exclusion zone. Climate change activists have failed to cause disruption at Heathrow Airport by flying drones after claiming the gadgets were blocked by "signal jamming". Heathrow Pause - a splinter of the Extinction Rebellion movement - intended to fly the machines in the airport's 3.1-mile (5km) exclusion zone, potentially disrupting hundreds of flights. The protest group said it had attempted three drone flights on Friday, with at least one successful, and 11 activists had been arrested, including former paralympian James Brown. But Heathrow said it was "fully operational despite attempts to disrupt the airport through the illegal use of drones".’
Source:	Sky News (2019) Heathrow protest fails to take off as drones 'blocked by signal jammers' https://news.sky.com/story/heathrow-drone-protesters-blocked-by-signal-jamming-as-two-arrested-11808171 (13/09/2019)
Country:	England

In discussion of the final case study, case study 6, participants discussed the **range of actors involved,** the **challenges of identifying the nature of the violation,** and **evidentiary challenges (e.g. identifying operator and chain of evidence)**.

Participants first noted the range of actors involved, including the activists flying drones, the activist group, the airport, the Met Police, and the Civil Aviation Authority (CAA) (see also Actors). After raising the ‘first lawyer question’ of ‘who is my client?’, they discussed the challenges of proceeding in terms of determining case type. One participant stated that you’d first need to consider are ‘you even competent to proceed with this case, and that might depend on whether it’s a protest law case or civil aviation law case, or a human rights case’ if ‘they’re going to run with freedom of expression’. Another participant noted that this case may not fall neatly within a single category, highlighting that cases involving drone incidents can require cross-jurisdictional or disciplinary legal competency and knowledge.

In this vein, participants also discussed challenges around identifying the nature of the violation. In discussion of representing the airport, participants reflected on what kinds of charges might be made. Here, participants focused attention on aviation safety, stating that ‘there's presumably legal actions against these nine people that have been arrested under the Air Navigation Order

for dangerous operation of a drone', as well as potential 'violations of the drone regulations in the UK' by breaching restrictions and 'limitations' around where flyers can fly their drones.

Participants also described advising on the responsibilities of airports to respond to drone incidents. In discussion of 'advising an airport', one participant suggested a range of questions to be asked, including 'what are your safety obligations as an airport, what obligations do you have to provide a safe airspace? What are your legal risks and obligations if you don't shut the airport down? What kind of steps can you take to shut this down? Can you get an injunction? What kind of claims could you have against you if you close and airlines can't operate?'. They continued that case study 6 was an 'interesting' incident as 'it's a threatened activity that hasn't entirely taken place'.

Participants also identified a 'challenge' around 'separating the potential aviation violations and the non aviation ones'. One participant raised that it may be worth considering 'civil' actions, noting that while 'there doesn't seem to be any loss of income from Heathrow for this activity, this could happen in the future, and this has happened in the past' (e.g., Gatwick airport 2018). In December 2018, reported sightings of a drone (or drones) 'caused the airport to close for two days' (33 hours) with more than '1,000 flights cancelled and more than 140,000 passengers affected' (Shackle 2020). A participant continued that 'splitting the incident in relation to 'the aviation and the non aviation laws' could however raise 'some procedural issues' as they understood that 'in the UK for aviation violations that the Civil Aviation Authority might be the one to do the prosecution and not the Crown Prosecution Service, so there could be an administrative issue' (see Enforcement).

Participants also discussed identifying the nature of the violation in relation to representing and acting on behalf of the activists. A participant suggested that the 'climate change activists would rely upon freedom of expression, freedom to protest', while another noted that while 'there are available rights to them' it would be important to explore whether 'the right to protest covers what they're trying to do'. Others suggested a 'defence of necessity' - namely that the action was 'necessary because of the climate emergency' meaning that 'they have to do this'. Participants also suggested that the activists may be able to suggest that they have 'assessed' the situation and risks and 'knew they weren't going to cause any harm'. In this vein, another participant highlighted that such activist groups 'often put out releases that they are going to' act, 'alerting the authorities', and thus 'the duty is now on you to mitigate'.

Lastly, participants also raised concerns over the ways in which activists may be classified and/or changed. Here, participants stated that the activists and 'climate activism group' may be classified 'as terrorists', with one participant stating that 'that's where we've moved to, where this Government has moved to, where if you're an environmental activist you're a domestic extremist'.

A participant also raised concerns about changes to the UK law in relation to protests and nuisance, stating that police can 'arrest on mass' protesters 'now they'd be covered under public nuisance'. This may refer to both the Public Order Act 2023 and the Police, Crime, Sentencing and Courts Act 2022 (see also Case study 5: Drone used in attempt to disrupt the electrical grid). The Home Office (2023) states that while the Government 'fully supports the right of individuals to engage in peaceful protest', the 'serious disruption caused by a small minority of protestors has highlighted that more needs to be done to protect the public and businesses from these unacceptable actions'. They continue that 'new measures are needed to bolster the police's powers to respond more effectively to disruptive and dangerous protests' and that the 'measures in the Public Order Bill...improve the police's ability to manage such protests and take a proactive approach to prevent such disruption happening in the first place' (Home Office 2023).

The Public Order Act 2023 ‘builds on the public order measures in Part 3 of the Police, Crime, Sentencing and Courts Act 2022 which, amongst other things, update the powers in the 1986 Act enabling the police to impose conditions on a protest, provide for a statutory offence of intentionally or recklessly causing public nuisance and increases the maximum penalty for the offence of wilful obstruction of a highway’ (Home Office 2023). The Public Order Act (2023) makes ‘provision for new offences relating to public order; provision about stop and search powers; provision about the exercise of police functions relating to public order; provision about proceedings by the Secretary of State relating to protest-related activities; provision about serious disruption prevention orders; and for connected purposes’ (Public Order Act 2023). Elements potentially relevant to this case study include 'obstruction etc of major transport works' (section 6), 'interference with use or operation of key national infrastructure' (section 7), ‘key national infrastructure' (Section 8), and the powers in response outlined (Public Order Act 2023). Amnesty International UK (2023) states that the Public Order Act follows 'hot on the heels’ of ‘protest restrictions contained in the Police, Crime, Sentencing and Courts Act 2022. This Act introduced new vague and undefined police and government powers to clamp down on any protests – including by one person. Even without the Public Order bill, protests can now be shut down if they're considered too noisy or likely to be a nuisance' (see also Doughty Street Chambers 2023). Section 78 of the Police, Crime, Sentencing and Courts Act 2022 refers to 'Intentionally or recklessly causing public nuisance’ (Police, Crime, Sentencing and Courts Act 2022).

Participants also discussed evidentiary challenges, including identifying operators and chain of evidence. First, participants asked how, if you’re ‘saying there was 35 people’, it could be determined ‘which individual, precisely who, is flying the drone’. One participant raised questions about piloting the drone, asking ‘is it just one remote control that controls the drone, or could we have 4 remote controls, so 4 of us could control the same drone?’ and about how ‘you attribute to a person’, adding that the group could try to obscure or hide who specifically is piloting the drone’ - ‘it’s almost like I’m Spartacus, if you all say I have the remote control’.

Participants also noted that finding and ‘linking’ drone flight to a specific person can be ‘quite difficult’ because it can be ‘a very remote activity’ (i.e., the drone can be piloted from a distance), and that with 35 people, people could occupy different locations and ‘different positions’ meaning that it’s very challenging to identify who any one drone ‘belongs to’ and to ‘put the evidence together to determine who’s at fault’. Lastly, attribution and responsibilities were raised. A participant raised whether there was a ‘distinction between the pilot and the operator’, asking ‘who would be the responsible liable person?’ and ‘would it be the operator who's essentially in charge of it all or the individual that's controlling the aircraft, which could be more than one person?’ (see table below).

Participants also focused on evidentiary questions. They raised issues around registration as a potential source of information, though added that this would depend on whether the drones were (and/or were required to be) registered. Others also highlighted that the approach to evidence would ‘depend on if you’ve captured the drone’ and if so, what information or data may be determined from this (see both Case study 5: Drones used in attempt to disrupt the electrical grid, and Recommendations for further discussion of drone forensics). If not, participants noted that identifying the specific drone would be challenging because if you’re ‘taking a picture of that drone in the sky’ you wouldn’t be able to determine information on it because of the distance.

Lastly, it can be noted that while beyond the scope of focus group discussions, wider concerns about the risks associated with drone incidents in proximity to airports are reflected through the inclusion of an entry on ‘the malicious use of a drones’ featuring the example of the ‘malicious use of drones at an airport’ in the 2023 edition of the National Risk Register (HM Government

2023: 87). This is the 'external version' of the Government's 'assessment of the most serious risks facing the UK' (HM Government 2023: 6). It 'assesses the likelihood and impact for each risk' following an established methodology (HM Government 2023: 6). Identifying drones as a 'novel vector to commit crimes and attacks', the register describes a scenario wherein a busy and active airport is targeted by a 'perpetrator' with 'malicious intent' (HM Government 2023: 87). In discussion of response, the scenario describes 'specialised police counter-drones capabilities...to respond to the incident', as well as 'police work, alongside further investigative methods (for example forensic scrutiny of a downed drone)...to identify and apprehend malicious users' (HM Government 2023: 88). In the case of malicious risks, the risk scores detailed in the National Risk Register are determined 'via the Professional Head of Intelligence Assessment yardstick' (HM Government 2023: 11). Three 'parameters', namely the 'intent of malicious actors to carry out an attack' 'balanced against an assessment of their capability to conduct an attack' and 'the vulnerability of their potential targets to an attack' are 'collated' to form a 'likelihood score' - i.e., the 'percentage chance of the reasonable worst-case scenario occurring at least once in the assessment timescale' and 'scored on a 1-5 scale' (HM Government 2023: 11). The dot at the centre of the plot (extending outwards in multiple directions) determines a 'malicious drone incident' as a number 2, with a 0 – 2.1% percentage chance likelihood, and a 'moderate' impact (HM Government 2023: 87) (see Figure 8).

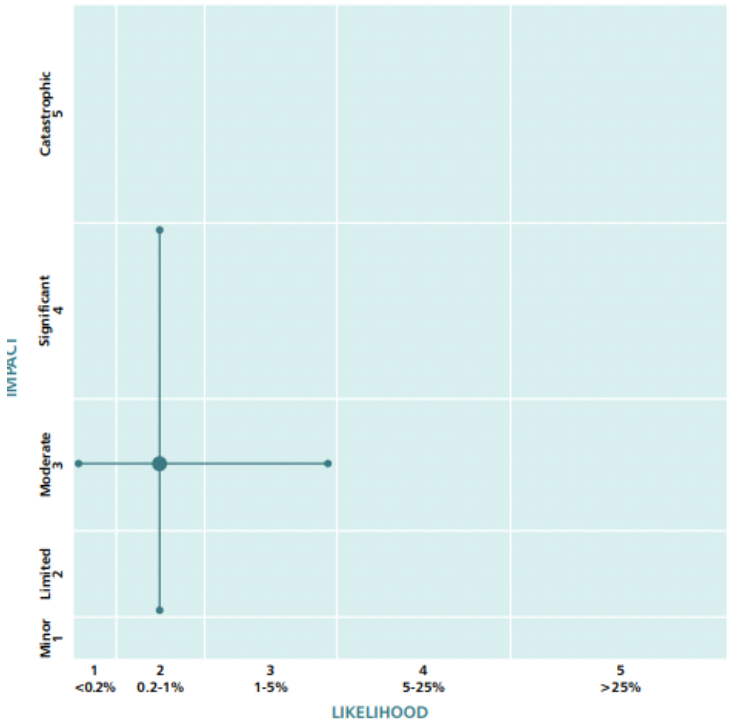

Figure 8: Malicious drone incident. Source: National Risk Register (HM Government 2023: 87) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1175834/2023_NATIONAL_RISK_REGISTER_NRR.pdf

Examples of relevant regulations and guidance
Regarding **airspace restrictions**: • CAP 722 (2022: 47) states that 'as defined in the ANO [Air Navigation Order], FRZs [Flight Restriction Zones] are established around aerodromes, and space sites'. Aerodromes are 'defined areas (including any buildings, installations and equipment) ...intended to be used either wholly or in part for the arrival, departure and surface movement of aircraft' (CAP 1430: 6), and include airports and airfields. • The Drone and Model Aircraft Code (n.d) states that 'most airports, airfields and

spaceports have a flight restriction zone (FRZ)' and drone flyers must 'never fly in this zone unless you have permission from the airport, airfield or spaceport' so as to avoid 'endangering the safety of an aircraft'.

- CAP 722 (2022: 47) confirms that 'aerodrome FRZs are always active', the National Risk Register that it is 'illegal to fly in an airport's flight restriction zone unless specific permissions have been granted' (HM Government 2023: 87), and the Drone and Model Aircraft Code (n.d) adds that 'if you endanger the safety of an aircraft, you could go to prison for five years'.

Regarding **enforcement**:

- See Enforcement for a full discussion.

Regarding **attribution and responsibility**:

- The Drone and Model Aircraft Code (n.d) states that the 'flyer' is 'responsible for flying safely and legally whenever you fly' and the 'operator' is the 'person responsible for managing a drone'. The Operator is responsible for 'making sure that anyone who flies it has a flyer ID' and is 'usually the person or organisation that owns the drone or model aircraft, but not always' (Drone and Model Aircraft Code n.d).
- CAP722 (2022) details a range of responsibilities for drone operators and pilots. The drone operator refers to 'any legal or natural person operating or intending to operate one or more' drones and is 'responsible for the overall operation of the' drone, and the drone pilot refers to 'a natural person responsible for safely conducting the flight of an unmanned aircraft by operating its flight controls, either manually or, when the unmanned aircraft flies automatically, by monitoring its course and remaining able to intervene and change course at any time' (CAP 722: 112, 115).
- In discussion of 'human authority over automated and autonomous' drones, CAP 722 (2022: 106) also states that the 'general principle to be observed is that all UAS [drones] must be under the command of a remote pilot. Dependent on the level of autonomy, a remote pilot may simultaneously assume responsibility for more than one aircraft, particularly when this can be accomplished safely whilst directing the activities of one or more other remote pilots. However, if this option is to be facilitated the applicant will need to demonstrate that the associated human factor issues...have been fully considered and mitigated' (see also Automation and Autonomy).

Part 4.3. Emerging capabilities

In the third activity participants briefly discussed a range of emerging capability developments and reflected on their potential legal dimensions and implications. Participants selected a couple of technological developments from the below list and reflected on:

- What challenges these developments might raise for legal practitioners and/or police involved in a drone-related case;
- What issues these advancements might raise for legislators and/or regulators.

Development	Description
Live streaming drone imagery to social media	Some commercially available / consumer drones have the function to live broadcast drone footage to social media (e.g., Facebook)
Drones paired with other technologies	Drones can be paired with other technologies, such as facial recognition
Intelligent flight	Refers to a flight mode on some commercially available/ consumer drones that enables drones to lock onto and follow particular points, objects, or people, and/or to rapidly ascend or descend from/towards these. These capabilities are marketed as cinematographic techniques
Racing drones	Small drones capable of high speed flight (e.g., over 100 miles per hour), flown as part of the recreational activity or sport of drone racing

Drone swarms	Development of groups of drones that fly collectively, in collaboration and communication with each other

Across these discussions, three central themes emerged around: **Data, Damage and Liability,** and **Fun and Games**.

Key themes explored in emergent technology discussion	
Data	In relation to **livestreaming**, participants focused on: • Regulation and obligations • Privacy, privacy rights and civil liberties • Intellectual property and monetisation • Data storage and servers • Right to be forgotten In relation to **facial recognition**, participants focused on: • Questions of consent • Distinctions between overt and covert surveillance • The potential for group harm rather than individual harm
Damage and liability	• Determining intention • Securing damages • Uninsured operators
Fun and games	In discussion of **drone racing**, participants focused on: • Drone speed limits and potential damages

Data

Across the discussions, participants identified a range of challenges raised by drones (see Drone incidents). This included a range of challenges related to data. In a European Parliament discussion of 'Privacy and Data Protection Implications of the Civil Use of Drones', Marzohhi (2015: 21-22) argues that drones 'change and transform the nature of surveillance, magnifying it, when compared to other similar tools'. The report continues that drones can be understood as complicated as they 'can be non-detectable (they are not always visible or heard, like aircrafts, helicopters, CCTV)', they enable a 'mobile view' and the 'access' of /to 'more locations (such as private properties, across fences or through windows)', 'can observe in detail (more than the naked eye, through zooms)' and sensors, and can 'follow persons' (e.g., through intelligent flight modes) (Marzohhi 2015: 21-22). Collectively, these attributes that a range of readily available consumer or off-the-shelf drones possess 'simplify and improve covert and overt surveillance and tracking of individuals or groups' (Marzohhi 2015: 22).

In discussion of the data dimensions and concerns raised by the aforementioned technology capabilities and developments, participants focused on the theme of **livestreaming**, reflecting on the data-related implications for regulation and obligations, privacy, privacy rights and civil liberties; intellectual property and monetisation, data storage and servers, and the right to be forgotten. In discussion of **facial recognition technology**, they also drew attention to questions and implications around overt and covert surveillance, and group harm.

Livestreaming

With regard to regulation, several participants discussed whether someone 'livestreaming drone footage to social media' who doesn't 'have a locked account' and the footage is thus 'visible to a public audience' and that footage contains personal data (e.g., an identifiable individual), would be determined as collecting or 'processing personal data' (i.e., a data controller) (see UK GDPR guidance: Information Commissioner's Office). Another participant raised 'another issue' of 'whether the [drone] operator' has been informed by the drone manufacturer 'about his or her obligations when doing the livestream', expressing concern about uncertainty around what 'obligations' both lie with or have been 'passed on to the ultimate operator'.

Participants also focused discussion around **privacy, privacy rights and civil liberties**. Here, participants drew attention to the potential impacts of livestreamed drone imagery (e.g., to an unlocked/ 'visible to a public audience' social media account and featuring identifiable individuals) on privacy rights. They raised the existing definition of 'personal data' as 'something that can plausibly reveal who you are' and highlighted that drone footage such as 'a video where you can see your face' could be 'construed as personal data'.

Participants also expressed caution around the **'live' sharing element,** as no 'thoughtful review' of the footage had taken place. Here, a participant suggested that if they were approached and asked about livestreaming they would 'under most circumstances, unless it's someplace where you're in a controlled environment and you know who's there' suggest that 'you'd be a lot better off filming it and then reviewing it and then figuring out what it is you're going to broadcast because you could easily invade someone's privacy...before you have time to even realize what it is you're doing'. Here, the participant provided the example of footage capturing someone 'nude sunbathing in their backyard' and continued that while you may not 'intentionally invade someone's privacy, you could'. With regard to the potential invasion of privacy, the international focus group participant also raised the potential for 'extensive civil liability', given the 'reasonable expectation of privacy' such as 'in places that you own that are not visible from the street'.

Participants also focused on the potential wider implications of livestreamed drone footage, raising a range of concerns. One participant noted that if a drone livestreamed footage at 'concerts or events' it may capture imagery of 'people smoking weed' or the like, and asked 'what are the implications of the recording?'. Here, another participant suggested that if someone attended a concert they may not 'realise' that they are being filmed and there are 'privacy rights implications' to this. Others raised potential implications of livestreamed drone footage in relation to potential 'claims or remedies' where a 'drone operation is determined as having breached privacy laws', asserting that the sharing, visibility and accessibility of drone footage via the social media platform 'means that the extent of violation has been broadened and that will have implications on how much a person can claim, if this were to be a quantifiable'. Lastly, in discussion of wider data-related implications of livestreaming, a participant raised the issue of the potential for drones to amplify or extend existing issues around livestreaming footage. Here, they raised the example of 'amateur detectives and paedophile hunter' groups 'knocking on the wrong door and confronting someone who is an innocent person' but because they are livestreaming, this has resulted in an individual experiencing property damage, and them 'bringing a civil action against them [the 'hunters'] because the damage to his house and car was a result of them publishing his data'.

As is discussed in Domestic framework: Rules and regulations of drones in the UK, advice on drones and privacy has been issued by the Information Commissioner's Office (ICO). This advice distinguishes between hobbyists and 'individuals or organisations' using drones for 'professional or commercial purposes', and provides information on responsibilities in relation to personal data (i.e., as data controllers or data processors) (Information Commissioner's Office n.d.c). They add that where drones are used for professional or commercial purposes, those 'using drones are clearly controllers for any personal data that the drone captures, and therefore are required to comply with data protection law' (Information Commissioner's Office n.d.c). Relevant UK law includes the Data Protection Act 2018, which is the 'implementation of the General Data Protection Regulation (GDPR)' (Gov.UK n.d.a).

The 'Data Protection Act 2018 controls how your personal information is used by organisations, businesses or the government' (Gov.UK n.d.a). Those 'responsible for using personal data' must 'follow strict rules called data protection principles', which ensure that 'the information is: used fairly, lawfully and transparently; used for specified, explicit purposes; used in a way that is adequate, relevant and limited to only what is necessary; accurate and, where necessary, kept

up to date; kept for no longer than is necessary' and 'handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage' (Gov.UK n.d.a). In relation to rights, 'under the Data Protection Act 2018, you have the right to find out what information the government and other organisations store about you' (Gov.UK n.d.a). It should be noted that while the GDPR 'does not apply to: the processing of personal data by an individual in the course of a purely personal or household activity' (Regulation (EU) 2016/679), and the Information Commissioner's Office (n.d.a) adds that 'if you only use personal data for such things as writing to friends and family or taking pictures for your own enjoyment, you are not subject to the UK GDPR', questions could nonetheless be raised around if and/ or when a hobbyist drone user could be understood as a data controller, depending on the specific circumstances and context of the data processing. It should also be considered that if the drone is livestreaming (irrespective of whether the video is recorded to be played back or not), that if carried out by a data controller this still constitutes the processing of personal data if individuals can be identified directly or indirectly, per the Information Commissioner's CCTV and Video Surveillance guidance (n.d.f). This guidance states that live streaming functions, even those that 'do not necessarily record any footage or save any data to a storage device or the cloud' and instead 'stream footage over the internet in real-time' also 'qualifies as processing' and 'constitutes the processing of personal data if you can identify individuals directly or indirectly' (Information Commissioner's Office n.d.d). It continues that this 'live streaming of images of identifiable individuals is still subject to the requirements of the UK GDPR and DPA 2018' (Information Commissioner's Office n.d.d).

Participants also highlighted potential issues around **intellectual property and monetisation**. Here, they raised the issue of someone 'livestreaming drone footage to social media' which is 'visible to a public audience' and the question of 'image reuse and IP [intellectual property]'. Others raised questions 'as to who owns the data' and 'the intellectual property rights that come with it'. Another participant also raised a question as to whether the IP might 'transfer to the social media platform', or whether it 'stays with person taking it [the drone footage]' and whether 'you lose control of where it's stored'.

Others also raised a question about the distinction between hobbyist and professional or commercial drone flyers (a distinction which the ICO makes) (see GDPR guidance: Information Commissioner's Office). They began by returning to the UK's drone regulations around insurance. The CAA states that 'the insurance you need depends on the size of your drone' and 'what you use it for' (Drone and Model Aircraft Code n.d), adding that for both drones weighing over 20 kilograms and drones used 'for work' you must have 'third party insurance', whereas for drones flown 'for fun, recreation, sport or as a hobby, you can choose whether or not you have insurance' (Civil Aviation Authority n.d.a; Drone and Model Aircraft Code n.d) (insurance is explored under Damage and Liability, below). The participant raised whether a hobbyist flyer who livestreams drone footage to social media introduces 'a chance that this can be monetized' and therefore may 'not be considered' as a hobbyist flyer but rather 'a commercial operator'. This potential of 'becoming a commercial entity' raises a range of potential 'legal considerations', including around insurance, as well as around 'privacy aspects' such as GDPR and data protection regulation adherence. Another participant raised a question about the need for closer attention to drone insurance policies and what they may cover and/or exclude in relation to 'any kind of privacy advertising liability losses', noting that particularly in the case of the 'hobbyist drone user' that does opt to get insurance, 'if there was some kind of loss that somebody incurred as a consequence of that [drone hobbyist's] surveillance, then there may be no redress or no money at the end of the rainbow for that because of those insurance policies'.

In relation to the example of **activist drone use**, per the above questions around regulation, it may also be important to consider whether the activist group could be considered as a data controller. If the ICO were to receive a complaint about an activist group recording with a drone,

they would first determine if the recording was carried out by a data controller, per their guidance and considering who decided to record and what the purpose of the recording was (Information Commissioner's Office n.d.e). If the processing is carried out by a data controller, then broader questions around what lawful basis they are relying on, and how they are meeting their requirements under the transparency principle would come into scope. As the UK GDPR is a principles-based legislation, the same rules apply irrespective of the device used to process the personal information (such as drones, body worn cameras or smart phones).

Participants also discussed **data storage and servers**. Here, they raised potential issues around the jurisdiction of servers, which 'may be in another jurisdiction' from where the footage is obtained and may raise evidentiary issues. In discussion of an example of activists using a drone to livestream footage of a protest, one participant stated that they 'don't use twitter or Facebook', but instead use 'their own servers' based overseas 'and the live stream is streamed directly to that server' rather than onto 'your phone'. The participant continued that this livestreamed drone footage can be significant. They described an example where drone footage livestreamed directly to a server was used in a case related to a police officer 'hitting a chap in the mouth' 'with a riot shield, breaking his teeth', and where the police officer had 'turned off' their body cam 'because he thought it was faulty'. The participant added that 'it was a drone that enabled the man, many years later, to recover the costs of all his dental work'. In discussion of activist drone use more widely, the participant also noted that where footage was stored outside of the UK (i.e., overseas), it was difficult for UK police to obtain it.

It can be noted that the issue of drone data servers and storage has also received considerable attention in the press. For example, Chinese drone manufacturer DJI were reportedly subject of the US Army 'banning service members' from using their drones due to 'increased awareness of cyber vulnerabilities' (Daniels 2017) and have more widely been subject to concerns around 'security threats', with the Pentagon (United States) 'issuing a special statement reaffirming its view that DJI systems are potential threats to national security' and the 'Treasury Department banning US investment in DJI' (Weitz 2023). In addition, DJI was added by the United States Government to the 'Department of Commerce's Entity List' and the 'Non-SDN Chinese Military-Industrial Complex Companies (NS-CMIC) List' due to the company's 'active support' of the 'biometric surveillance and tracking of ethnic and religious minorities in China' (Lawler 2021). In this vein, the Office of the Biometrics and Surveillance Camera Commissioner (2023: 79) expressed 'concerns around the human rights and ethical considerations' of 'procuring and developing surveillance technology from companies with concerning trading history'.

Lastly, participants raised the issue of **the right to be forgotten**. Here, in discussion of drone livestreamed footage (recorded and replayable), participants raised a potentially 'bigger implication' that once 'it's there, it's there, it's going to populate everywhere' and may impact ongoing debates and struggles around 'the right to be forgotten'.

Under Article 17, the 'UK GDPR introduces a right for individuals to have personal data erased' and this right to erasure is also known as 'the right to be forgotten' (Information Commissioner's Office n.d.f). This right 'is not absolute and only applies in certain circumstances' (Information Commissioner's Office n.d.f). The Information Commissioner's Office (n.d.f) advises 'individuals have the right to have their personal data erased if: the personal data is no longer necessary for the purpose which you originally collected or processed it for; you are relying on consent as your lawful basis for holding the data, and the individual withdraws their consent; you are relying on legitimate interests as your basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing; you are processing the personal data for direct marketing purposes and the individual objects to that processing; you have processed the personal data unlawfully (i.e., in breach of the lawfulness requirement of the 1st principle); you have to do it to comply with a legal obligation; or you have

processed the personal data to offer information society services to a child' (Information Commissioner's Office n.d.f). It also highlights that 'there is an emphasis on the right to have personal data erased if the request relates to data collected from children. This reflects the enhanced protection of children's information, especially in online environments, under the UK GDPR' (Information Commissioner's Office n.d.f).

Facial recognition

In discussion of drones paired with other technologies, participants focused on facial recognition. Facial recognition technology 'identifies or otherwise recognises a person from a digital facial image' taken by a camera (Information Commissioner's Office n.d.c). Facial Recognition technology 'software measures and analyses facial features' and 'typically enables the user to identify, authenticate or verify, or categorise individuals' (Information Commissioner's Office n.d.c). Facial recognition can be based on 'digital images' that are either 'still or from live camera feeds' (College of Policing 2022). Live facial recognition refers to a type of facial recognition technology that is 'used in public spaces in real time' (Information Commissioner's Office n.d.c). While a range of legal questions and concerns surround facial recognition have been raised, including around 'protection afforded to privacy rights, and other human rights of those subject to police facial recognition technology' (Purshouse and Campbell 2019), there is nonetheless growing interest in the use of facial recognition technologies in the UK. For example, in October 2023, the Policing Minister for the UK in a letter urged police 'forces to increase their use of artificial intelligence crime-fighting' tools, challenging UK police to 'double the number of searches they make using retrospective facial recognition technology to track down known offenders by May 2024' (Gov.UK 2023b). Facial recognition, and particularly live facial recognition technology (LFRT), is highly contentious and there have been widespread calls for it to be banned (see Access Now 2022). A recent case in the European Court of Human Rights, *Glukhin v Russia* No. 11519/20 (2023) held that the use of LFRT to identify, locate and arrest a peaceful protestor was not simply a breach of the individual's right to privacy but also capable of having a chilling effect on the rights to freedom of expression and assembly more generally. In respect of facial recognition powers Chris Philip the policing minister stated in October 2023 that he wanted police to be able to search the passport database containing millions of images (BBC News 2023). The vast majority of these are people who have neither been suspected nor convicted of any crime. There is also increasing concern in the UK that private facial recognition technology providers are collaborating with and exploring methods of sharing information with the police, which has the potential to circumvent the safeguards the police are required to adhere to (Big Brother Watch 2023; Privacy International 2020).

While not a widespread practice, there is growing interest in drone-assisted facial recognition. For example, police in 'Sharjah, the third-most populous city in the United Arab Emirates, are using drones with facial recognition technology to track wanted criminals' (Singh 2021). Here, 'facial recognition drones take to the skies and scan crowded public spaces' and if 'any matches are found, the ground units of the police force move in to make the arrest' (Singh 2021). It is also believed drones used to surveil people in China may have been equipped with cameras designed to detect race (Zeeberg 2023).

In discussion of the potential of drone-enabled facial recognition, participants raised **questions around consent**. While noting that it was their understanding that UK police had not yet used facial recognition with a drone, they mused that 'what you're going to get with these types of hybrids merging together through different technologies is compounding effects and greater complexity'. Here, the participant focused on concerns that if drones were used for facial recognition, 'and there's been some forces tempted by the idea', that police 'may have quite a lot of discretion and latitude to use that because it would technically be classified as overt surveillance'. They continued that 'under the current legal framework, following the case of

Bridges' they understood that such a usage 'would be classed as overt surveillance and so covered by really basic common law powers, very easy to satisfy the test for using it'. In this vein, they raised concerns regarding consent, stating that 'that's not based on whether someone knows they are being watched. Whether it's covert is based on whether the user is trying to hide it or not, so I think that's an issue where you've got an intrusive surveillance measure being used on a population - how do you know you're being subject to facial recognition via drone?'. They added that they felt it was 'under regulated because of creative judicial reasoning about what is overt and covert surveillance'. Reflecting on the police understanding of 'overt' technology usage, they added that 'by the time you got to the sign' stating that this technology is in use 'you've been scanned' already, i.e., it's not effective as a form of consent. The participant continued that per 'Bridges versus South Wales police' their understanding was that facial recognition as it 'was used was an overt form of surveillance so it didn't need any RIPA [Regulation of Investigatory Powers Act] oversight or authorisation and that wasn't based on people knowing it was there or consenting to having it used in that area, it was based on the fact that the police were using it – their intentions were not to hide or conceal it'. Here, the participant referred to the Ed Bridges versus South Wales Police case.

Ed Bridges versus South Wales Police: In summary, Ed Bridges 'challenged South Wales Police's use of live facial recognition in public' in 'the world's first legal challenge to police use of this technology' (Liberty n.d). Bridges asserted that by using the technology 'on more than 60 occasions since May 2017' and potentially taking 'sensitive facial biometric data from 500,000 people without their consent', the Police Force were 'breaching rights to privacy, data protection laws, and equality laws' (Liberty n.d). While 'in September 2019, the High Court decided that while facial recognition does interfere with the privacy rights of everyone scanned, the current legal framework provides sufficient safeguards', Bridges appealed and in August 2020 the 'Court of Appeal agreed' and 'found South Wales Police's use of facial recognition technology breaches privacy rights, data protection laws and equality laws. The judgment means the police force leading the use of facial recognition on UK streets must halt its long-running trial' (Liberty n.d.). The Court added "that there were 'fundamental deficiencies' in the legal framework and that Ed Bridges' rights were breached as a result" (Liberty n.d).

Regarding UK regulation more widely, facial regulation technology 'involves processing personal data, biometric data and, in the vast majority of cases seen by the ICO, special category personal data. Biometric data is a particular type of data that has a specific definition in data protection law' (Information Commissioner's Office n.d.c). Biometric data refers to 'personal data resulting from specific technical processing relating to the physical, physio-logical or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic (fingerprint) data, as defined at Article 4(14) UK GDPR' (Information Commissioner's Office n.d.c). The Information Commissioner's Office (n.d.c) continues that 'under the UK GDPR, processing biometric data for the purpose(s) of uniquely identifying an individual is prohibited unless a 'lawful basis' under Article 6 UKGDPR and a 'condition' in Article 9 UKGDPR can be satisfied. It also further links to 'additional guidance regarding facial recognition technology in public spaces' (Information Commissioner's Office n.d.c).[5]

Lastly, participants also briefly discussed the potential for '**group harm**, rather than individual harm' by which they referred to the potential for the surveillance to harm the collective interests

[5] Five of the 'conditions' for processing are provided solely in Article 9 of the UK GDPR. The other five require authorisation or a basis in UK law. This means you need to meet additional conditions set out in section 10 and Schedule 1 of the DPA 2018, depending on the Article 9 condition relied upon' (Information Commissioner's Office n.d.g).

of a group even if targeted solely at one individual. One participant stated that ‘it’s definitely there – it seems like it’s something that the legal framework is really not well equipped to recognise or deal with because the framework is such that that police can do what they want as long as they can say it’s necessary or proportionate – it broadly complies with these vaguely defined principles, and the courts always have to play catch up’. They continued that ‘you’re not only waiting years for that process to work...The court’s structure is not designed to vindicate collective harms or the creeping normalisation of a surveillance society so it has to be done through a political process’.

Figure 9: Drone. Source: Watts, Flickr https://www.flickr.com/photos/watts_photos/14807508737/ (CC) PDM 1.0 DEED

Damage and liability

A second theme cutting across focus group discussions was that of damages and liability. Across a range of discussions, participants raised concerns around **determining intention, securing damages** and **uninsured operators**. Potentially relevant regulations and guidance are also highlighted.

In discussions of drone use and incidents, participants distinguished between **intentional acts and non-intentional** or reckless acts (see Intentions) and the potential implications of this upon criminal or civil wrongs (see Legal Context). In the case of ‘a deliberate act’ participants added that ‘criminal proceedings’ may be more appropriate, and in the case of a non-intentional act, a ‘civil liability case, intervening with an insurance company and settling the matter outside the court’ may be more appropriate.

Participants described potential challenges around **securing damages** in relation to UK drone insurance requirements. Participants noted that if a drone was ‘operated criminally’, i.e., with intent to cause harm and perpetrating harm, ‘anyone who’s operating a drone criminally’ is unlikely to ‘bother to get insurance since they set out to do the harm’. They continued that if the drone was flown negligently by a hobbyist (i.e., not intending to cause harm), even in the event that the hobbyist had insurance, the potential size of the claims could be considerable and beyond the scope of the insurance policy (see Actor for a fuller discussion).

Potentially relevant regulations and guidance include those around responsibility, liability and insurance.

With regards to **responsibility**, Civil Aviation authority regulations and guidance describe responsibilities in relation to category (see Understanding drone categories), and flyer (operator or pilot). The Drone and Model Aircraft (n.d) states that 'you're responsible for flying safely whenever you fly' and advises that flyers must 'follow this Code to make sure you never put people in danger' and that 'you could be fined for breaking the law when flying your drone or model aircraft. In the most serious cases, you could be sent to prison' (see Domestic framework: Rules and regulations for drones). CAP 722 provides further information about responsibilities for both drone 'operators' and drone 'pilots', making a distinction between these roles. CAP 722 (2022: 112) refers to the drone 'operator' as 'any legal or natural person operating or intending to operate one or more UAS'. In discussion of the responsibilities of the drone operator, CAP 722 (2022: 112) states that the drone 'operator is responsible for the overall operation of the UAS, and most specifically the safety of that operation. This includes the conduct of any safety risk analysis of the intended operations'. It adds that the 'operator's responsibilities that are particular to each operating category are listed within the Annex to UK Regulation (EU) 2019/947' while including a 'more general set of responsibilities' around 'Operational Procedures Development/ Operations Manual, Remote Pilots and Other Operations and Maintenance Personnel, Use of Contracted Remote pilots, and Unmanned Aircraft and Associated Supporting Systems' (CAP 722: 112-113). With regard to the 'remote pilot', CAP 722 (2022: 115) defines the remote pilot as 'a natural person responsible for safely conducting the flight of an unmanned aircraft by operating its flight controls, either manually or, when the unmanned aircraft flies automatically, by monitoring its course and remaining able to intervene and change the course at any time'. It continues that the 'remote pilot is nominated for each flight by the UAS operator [per above] and is responsible for the overall conduct of that flight, with safety obviously being the primary consideration' (CAP 722: 115). It adds that the 'remote pilot's responsibilities that are particular to each operating category are listed in the Annex of UK Regulation (EU) 2019/947', while also providing a 'more general set of responsibilities' around 'General Requirements, Pre-flight Responsibilities, In-flight Responsibilities, Competency Requirements, Medical Requirements, and Radio Licensing' (CAP 722: 115).

With regard to drone flight, CAP 722 (2022: 27) continues that 'there are no right-of-way rules set out in regulation between unmanned aircraft and other airspace users, however it is likely that the unmanned aircraft remote pilot will identify other airspace users before they identify the unmanned aircraft, and therefore the remote pilot will usually be first to manoeuvre away from any conflicting aircraft'. It adds that 'UK Regulation (EU) 2019/947 sets out, in UAS.OPEN.060 (2)(b), that: the remote pilot shall maintain a thorough visual scan of the airspace surrounding the unmanned aircraft in order to avoid any risk of collision with any manned aircraft. The remote pilot shall discontinue the flight if the operation poses a risk to other aircraft, people, animals, environment or property' and clarifies that a 'similar requirement is set out within UAS.SPEC.060(3)(b), for the Specific Category' (CAP 722: 27). The CAA underscores that 'although this places a responsibility for collision avoidance on the remote pilot, it does not absolve other airspace users from their own collision avoidance responsibilities. Neither does it imply any 'right of way' over UAS, by other airspace users' (CAP 722: 27).

With regards to '**liability** for damages caused by a small drone', the UK 'follows the same rules of the system established for other aircraft' (European Parliament 2018: 47). General rules are contained in the Article 241 of the Air Navigation Order 2016 and it introduces a **fault-based liability,** stating that 'a person must not recklessly or negligently cause or permit an aircraft to endanger any person or property' (European Parliament 2018: 47).

With regards to **insurance**, Civil Aviation Authority guidance states that it is 'the responsibility' of every drone 'operator to ensure they have appropriate insurance coverage' (CAP 722: 21). They continue that 'the insurance you need depends on the size of your drone' and 'what you use it

for' (Drone and Model Aircraft Code n.d). For drones weighing over 20 kilograms, you 'must always have third party insurance, no matter what you use your aircraft for' (Drone and Model Aircraft Code n.d). The Civil Aviation Authority rules also require 'all commercial drone flights' to hold 'valid insurance cover' (Civil Aviation Authority n.d.a) and specify that you 'must have third party liability insurance' if you receive payment for your drone use or 'use your drone for work' (Drone and Model Aircraft Code n.d). For drones weighing 'below 20kg' and flown 'for fun, recreation, sport, or as a hobby, you can choose whether or not to have insurance', whereas if you 'fly for any other reason, you must have third party liability insurance' (Drone and Model Aircraft Code n.d). The Drone and Model Aircraft Code (n.d) does however add that while 'insurance is optional if you only fly for fun, recreation, sport, or as a hobby' you remain 'responsible for your actions' and thus 'could be held personally liable for any injury or damage you cause', and as such, 'you may want to consider getting third party liability insurance'.

CAP 722 states that the 'UK Regulation (EU) 785/2004 as retained (and amended in UK domestic law) under the European Union (Withdrawal) Act 2018 which came into force on 30 April 2005, requires most operators of aircraft, irrespective of the purposes for which they fly, to hold adequate levels of insurance in order to meet their liabilities in the event of an accident' (CAP 722: 21). It continues that 'UK legislation which details insurance requirements is set out in Civil Aviation (Insurance) Regulations 20052. Article 2(b) of UK Regulation (EU) 785/2004 states that the regulation does not apply to 'model aircraft with an MTOM of less than 20kg', but the term 'model aircraft' is not defined within the regulation itself. Therefore, for the purposes of interpretation within the insurance regulation only, its use of the term 'model aircraft' should be taken to mean: 'Any unmanned aircraft which is being used for sport or recreational purposes only'. For all other types of unmanned aircraft operation, whether commercial or noncommercial, appropriate cover that meets the requirements of UK Regulation (EU) 785/2004 is required' (CAP 722: 21).

With regard to manufacturers and liability, CAP 1789B (2022), which is a 'consolidated version' of Regulation (EU) 2019/945 as retained (and amended in UK domestic law) under the European Union (Withdrawal) Act 2018 (known as Delegated Regulation) (see Domestic framework: Rules and regulations for drones in the UK) states that 'products shall only be made available on the market if they satisfy the requirements of this Chapter and do not endanger the health or safety of persons, animals or property'. It also discusses the 'obligation of the manufacturers' with regard to 'conformity assessment' (and that 'Conformity assessment bodies shall take out liability insurance') and discusses 'CE Marking' (CAP 1789B).

In December 2022, the Civil Aviation Authority (n.d.g) issued a news item that 'from 23 December 2022, there will be no UAS in the UK which are class marked in accordance with UK Regulation (EU) 2019/945'. They continued that drones 'in the Open Category may continue to be used, as they have been so far, within the legacy and transition provisions, and the basic open category limitations. Following the UK Civil Aviation Authority's (CAA) consultation on whether to extend the legacy and transitional provisions for drones operating in the open category, and after a formal decision from the Department for Transport (DfT), it has been decided that the transition and legacy provisions will now be extended to 1 January 2026. The DfT will also remove the automatic recognition of class marks issued within the EU, as equivalent to UK Class marks, from the 23rd December 2022, in The Aviation Safety and Air Traffic Management (Amendment) Regulations 2022' (Civil Aviation Authority n.d.g). They confirmed that 'there are currently no designated standards, Market Surveillance Authority, or conformance assessment bodies established in the UK under UK Regulation (EU) 2019/945, therefore it will not be possible for manufacturers to comply with the UK class marking requirements of this regulation. As such, there will be no UAS which are able to make use of the Open Category class mark provisions in UK Regulation (EU) 2019/947. Any UAS operated

within the Open Category, regardless of whether it holds a class mark issued in the EU, should be flown to the 'non-class mark' open category limitations and conditions' (Civil Aviation Authority n.d.g).

In recognition that in spite of 'current UAS [drone] regulation', drones can still be used 'unlawfully for smuggling, harassment, and infringement of sensitive sites', the Civil Aviation Authority continues to look at risk mitigation (CAP 2569: 20). Noting that 'UK Regulation (EU) 2019/945 sets out a requirement to implement Remote ID in the UK by January 2026, through manufacturer requirements and operational requirements', the CAA adds that they are 'exploring how Remote ID could be implemented in the UK' (CAP 2569: 20). They continue that while 'regulations exist today to prohibit UAS flying in airspace restriction zones, including airspace above aerodromes, prisons, and high-security buildings... in the future, UAS should be manufactured with mitigations in place that make it easier for users to comply with these restrictions' (CAP 2569: 21). They add that 'could include functionality on UAS [drone] controllers that alert users when they are flying in restricted airspace ('geoawareness'), or that prevent UAS from entering restricted airspace altogether ('geofencing')', adding that while some drones 'have this functionality today', there remain 'limitations in how this functionality is implemented in practice' (CAP 2569: 21). Collectively, the CAA recognises that current drone regulation 'mitigates most risks through placing requirements' on drone users, and suggests that, following UK Regulation (EU) 2019/9453, in future they plan to 'shift mitigations, in part, to UAS themselves – ensuring UAS are safe and secure by design' (CAP 2569: 3).

Figure 10: Drone. Source: Nihon Graphy, Unsplash https://unsplash.com/photos/white-and-gray-robot-toy-zfxgGX6yaNU

Fun and games

Drones are increasingly utilised in entertainment applications. Entertainment emerged as a theme cutting across discussions. Here, participants largely focused discussion around racing drones. **Drone racing** using First Person View (FPV) is a 'competition where pilots control drones equipped with cameras while wearing goggles that stream the live video feed from the drones so they feel like they're flying from inside the drone. The goal is to complete a complex race course as quickly as possible and ahead of the other pilots' (Drone Racing League n.d). The aerial sport of drone racing has emerged as increasingly popular around the globe (see for

example the Drone Racing League and the British Drone Racing Association). Drone racing involves using 'lightweight crafts that can reach speeds of over 100mph' (BBC Science Focus n.d). Flying outside of a drone racing setting, a 'custom drone builder now holds the Guinness World Record for 'Fastest ground speed by a battery-powered remote-controlled (RC) quadcopter', flying his drone at 224 miles-per-hour (MPH) (Liszewski 2023).

In discussion of drone racing, participants first raised questions regarding **drone speed limits.** One participant remarked that they have 'built a novice drone' and when they were doing their required CAA training they couldn't determine a 'speed limit on these drones' and had concerns that 'you can just make one for yourself and the speed you fly that'. They continued that 'if that collided with someone...it could lead to pretty horrific damage'. While noting their smaller size, other participants shared concerns around the speed of racing drones and the potential for collisions at speed to result in injury and damage. Participants did not think there was currently a speed limit in place applying to drones, but reflected that 'there's a position on being reckless' and that 'if you were flying around a park' or a place more broadly 'at 100mph', it could be argued that 'that's reckless'. Other participants asserted that they saw an 'argument for having an imposed speed limit', and argued that the 'thing to do' is to consider 'the capability of the drone, to set a parameter within its manufacture that it can't go faster than X' or that you can use it 'over 100mph' but only in particular contexts (e.g., 'drone racing locations', 'defined tracks' or in 'confined empty airspace'). Lastly, participants also raised the potential implications of racing drones on 'the birds in the sky'.

With regard to relevant regulation, Article 241 of the Air Navigation Order 2016 'stipulates that a person must not recklessly or negligently cause or permit an aircraft (manned or unmanned) to endanger any person or property (which includes other aircraft and their occupants)' and article 240 'that a person must not recklessly or negligently act in a manner likely to endanger an aircraft or a person within an aircraft' (CAP 722: 18). The Drone and Model Aircraft Code covers the flight of drones (Open A1 and A3 categories) 'outdoors' only (the rules 'don't apply if you're flying indoors'), and mentions speed in relation to 'keeping a safe distance' and states: 'If you fly at high speeds, fly further away to give yourself more time to react' (Drone and Model Aircraft Code n.d; CAP 2004). In discussion of the 'protection of third parties', CAP 722 (2022: 41) states 'Do not fly at excessive speeds when close to people'. In discussion of the 'overflight of uninvolved persons', CAP 722 (2022: 32) states 'think before flying towards people, especially at higher speeds as the aircraft's trajectory while falling may present a danger to people on the ground'. The CAA states that their drone rules 'don't apply if you are flying indoors. Flights within buildings, or within areas where there is no possibility for the drone to escape into the open air (such as a closed netted structure) are not subject to aviation legislation' (Civil Aviation Authority n.d.a). Guidance suggests that 'Persons intending to operate drones indoors should refer to the appropriate Health and Safety at Work regulations' (Drone Safe Register 2018). The 'Health and Safety Executive is responsible' for drones 'used at work on the ground', and 'from a health and safety perspective...employers will need to ensure that they comply with their duties under the Health and Safety at Work Act of 1974 and related health and safety legislation' (Mouhinso 2022: 501).

Part 4.4. The Future?

In addition to discussing emerging capabilities (part 4.3), we were interested in exploring legal questions that may also emerge in relation to potential future developments. Here, discussions were two-fold, first on identifying key future technologies and examining their implications (wherein participants focused on artificial intelligence and autonomy), and second, on identifying the potential legal dimensions of different proposed models of future airspace (including Beyond Visual Line of Sight flight (BVLOS), drone highways or corridors, and drone integration).

Technology futures

In discussion of key technology developments that may impact the functioning, regulation and enforcement of drones, participants identified and focused upon artificial intelligence (AI), and automation and autonomy.

Summary of technology future themes discussed	
Artificial intelligence	• AI can be defined in a range of ways, but might be understood as 'an umbrella term for a range of algorithm-based technologies that solve complex tasks by carrying out functions that previously required human thinking' (Information Commissioner's Office n.d.h). • AI takes a range of forms, including AI Chatbots such as ChatGPT. • Researchers at Microsoft have experimented with the use of ChatGPT to control robots, such as drones. • In discussion of the potential legal considerations surrounding AI Chatbot controlled drones, participants raised questions around understandings of the drone operator and pilot and their responsibilities; notions of meaningful control; questions around culpability; and attributing the drone's action. • The ICO has issued guidance on AI and data protection.
Automation and autonomy	• In discussion of automation and autonomy, participants discussed intelligent flight modes, the implications of different actors involved in automated systems upon responsibility and liability, and the challenges of definitions and their implications. • Regarding intelligent flight (i.e., flight modes that particular off-the-shelf consumer drones are equipped with), participants raised the question of who or what is at fault if an accident happens. • Participants discussed more widely the complexity around the different actors involved in automated systems, and the implications of this upon responsibility and liability. • Participants also centred on the importance of, and implications for, definitions of automation and autonomy. Here, participants reflected on the ways in which regulatory frameworks (from around the world) distinguished between automation and autonomy, and the implications for what they identified as both a lack of nuance with regard to differing levels or forms of autonomy (including in the context of commercial drone operation), and in some cases, a mismatch across different areas of regulation (e.g., third party liability regulation on AI).

Artificial intelligence (AI)

Artificial intelligence refers to 'the use of digital technology to create systems capable of performing tasks commonly thought to require intelligence' (HM Government 2019a). The Information Commissioner's Office (n.d.h) notes that while AI 'can be defined in many ways', it can be understood as 'an umbrella term for a range of algorithm-based technologies that solve complex tasks by carrying out functions that previously required human thinking'.

In relation to drones, it is asserted that artificial intelligence 'could enable drones to make decisions usually taken by a human pilot' and that 'AI may also enable systems to learn without being explicitly programmed' (POSTnote 2020: 4). While artificial intelligence takes a range of forms, it is asserted that the 'promises and perils of AI' have 'of late, taken a pivotal turn — with the emergence of AI chatbots such as Chat GPT' (Nawaz 2023).

In this vein, participants were asked about 'ChatGPT being attached to drones, so Chat GPT deciding on what your drone's going to do'. ChatGPT refers to 'a natural language processing (NLP) AI Chatbot driven by AI technology developed from Open AI. The chatbot has a language-

based model that the developer fine-tunes (with help from user feedback) for human interaction' (PC Guide 2023). While AI Chatbots have been (re)launched under different additions, these 'AI models are basically trained on large datasets to learn the relationship in sequential data — pretty much like words in a sentence. It helps them in recognizing, summarizing, predicting, or generating human language' (Nawaz 2023). As such, they 'can answer an ever-increasing array of questions and reply to 'prompts' on request' (PC Guide 2023). ChatGPT has become extremely popular version, with over '100 million users globally' as of 1 July 2023 (PC Guide 2023).

While often popularly associated with 'writing essays and answering questions', researchers at Microsoft have also used 'the chatbot to control robots' (Kan 2023). In early 2023, researchers from Microsoft 'published a paper on how ChatGPT can streamline the process of programming software commands to control various robots, such as mechanical arms and drones' (Kan 2023). Rather than relying 'on hand-written code to control robots', the researchers turned to ChatGPT 'to write some of the computer code' (Kan 2023). The researchers noted that while 'ChatGPT can do a lot by itself, it still needs some help', adding that they provided a 'text prompt for ChatGPT which describes the task goal while also explicitly stating which functions from the high-level library are available. The prompt can also contain information about task constraints, or how ChatGPT should form its answers' (Kan 2023). After feeding ChatGPT a 'long prompt laying out the computer commands', they could 'make requests to instruct ChatGPT to control the robot in various ways' and found that 'ChatGPT asked clarification questions when the user's instructions were ambiguous' and was able to write 'complex code structures for the drone such as a zig-zag pattern to visually inspect shelves' (Kan 2023). While acknowledging that the use of ChatGPT in this context remains limited in the sense that 'the chatbot can only write the computer code for the robot, based on the initial "prompt" or text-based request the human gives it', the research nonetheless demonstrated 'Chat GPT's potential in robotics' (Kan 2023). Microsoft have released video footage demonstrating the research into 'how ChatGPT can help a user control a real drone with only language instructions' (Microsoft 2023).

In discussion of using AI such as ChatGPT 'to operate drones', participants reflected on the implications on understandings of the drone operator and pilot and their responsibilities, remarking that 'there's no operator really' and raising questions of 'meaningful control', including who and how 'would you be culpable?'. They continued that this kind of development might be understood as raising challenges around 'how to attribute the action of the drone to somebody' and 'lead to a situation where you divorce the culpability'. In discussion of AI more widely, the Information Commissioner's Office (n.d.h) states that "decisions made using AI are either fully automated, or with a 'human in the loop'. As with any other form of decision-making, those impacted by an AI supported decision should be able to hold someone accountable for it".

AI and Data protection

The growth of AI and 'the new data processing opportunities it brings' is also said to 'challenge fundamental data protection principles' (International Working Group on Data Protection in Telecommunications 2018: 8).

With regard to **AI's impacts on data protection** in the context of the UK, the Information Commissioner's Office (n.d.h) in 2023 updated 'guidance on AI and data protection', covering both how they 'interpret data protection law as it applies to AI systems that process personal data' and 'best practice for data protection-compliant AI' with the aim of 'mitigating the risks to individuals that AI may cause or exacerbate' (Information Commissioner's Office n.d.h). While noting that there are a range of 'other legal frameworks and obligations relevant to organisations developing and deploying AI that will need to be considered', the ICO notes that the guidance focuses 'on data protection compliance' and is 'restricted to data protection law' (Information Commissioner's Office n.d.h). While noting that 'data protection law does not use the term 'AI',

so none of your legal obligations depend on exactly how it is defined', the ICO notes that more widely the 'umbrella term' of "AI has a variety of meanings, including: In the AI research community, it refers to various methods 'for using a non-human system to learn from experience and imitate human intelligent behaviour'; or in the data protection context, 'the theory and development of computer systems able to perform tasks normally requiring human intelligence'" (Information Commissioner's Office n.d.h). It notes that given the prominence of 'machine learning', the guidance 'focuses on the data protection challenges that ML-based AI may present, while acknowledging that other kinds of AI may give rise to other data protection challenges' (Information Commissioner's Office n.d.h). The guidance highlights 'the most relevant piece of UK legislation' as 'the Data Protection Act 2018 (DPA 2018)' (Information Commissioner's Office n.d.h). The guidance adopts a 'risk-based approach to AI' and is divided into 'several parts covering...the foundational principles of data protection: lawfulness, fairness, and transparency; purpose limitation; data minimisation; accuracy; storage limitation; and security and accountability', while also providing 'more in-depth analysis of measures to comply with people's individual rights' (Information Commissioner's Office n.d.h).

The guidance touches upon issues such as the requirements to undertake a data protection impact assessment (DPIA), and information on data controller and processor roles and responsibilities. Regarding the discussion of how data controllers and processors should be understood in the context of AI, the ICO states that while 'often, several different organisations will be involved in developing and deploying AI systems which process personal data', the 'UK GDPR recognises that not all organisations involved in the processing will have the same degree of control or responsibility. It is important to be able to identify who is acting as a controller, a joint controller or a processor so you understand which UK GDPR obligations apply to which organisation' (Information Commissioner's Office n.d.h). While the guidance provides information regarding determining data controllers and processors, it also notes that 'when AI systems involve a number of organisations in the processing of personal data, assigning the roles of controller and processor can become complex. For example, when some of the processing happens in the cloud. This can raise broader questions outside the scope of this guidance' (Information Commissioner's Office n.d.h).

With regard to 'ensuring individual rights' in relation to AI, the ICO raises the issue of ensuring rights 'relating to solely automated decisions with legal or similar effect' (Information Commissioner's Office n.d.h). The ICO continues that there 'are specific provisions in data protection law covering individuals' rights where processing involves solely automated individual decision-making, including profiling, with legal or similarly significant effects. These provisions cover both information you have to provide proactively about the processing and individuals' rights in relation to a decision made about them' (Information Commissioner's Office n.d.h). They continued that "Under Articles 13 (2)(f) and 14 (2)(g), you must tell people whose data you are processing that you are doing so for automated decision-making and give them 'meaningful information about the logic involved, as well as the significance and the envisaged consequences' of the processing for them. Under Article 15 (2)(h) you must also tell them about this if they submit a subject access request. In addition, data protection requires you to implement suitable safeguards when processing personal data to make solely automated decisions that have a legal or similarly significant impact on individuals" (Information Commissioner's Office n.d.h). It continues that 'for processing involving solely automated decision-making that falls under Part 3 of the DPA 2018, the applicable safeguards will depend on regulations provided in the particular law authorising the automated decision-making' (Information Commissioner's Office n.d.h). The ICO offers guidance regarding 'solely automated' and 'partly automated decision-making', adding that 'in solely automated contexts, human intervention is only required on a case-by-case basis to safeguard the individual's rights,

whereas for a system to qualify as not solely automated, meaningful human intervention is required in every decision' (Information Commissioner's Office n.d.h).

It should be noted that in 2022 the Law Commission launched 'Aviation Autonomy', a programme set to examine the 'existing legal framework to identify the challenges and opportunities linked to the introduction of highly automated systems into the aviation sector' and undertaking a review of 'existing legislation to identify any legislative blocks, gaps or uncertainties' (Law Commission 2022).

Automation and autonomy

In discussion of key technology developments that may impact the functioning of drones and their regulation and enforcement, participants relatedly focused on automation and autonomy, reflecting on **intelligent flight,** the implications of **different actors involved** in automated systems upon **responsibility and liability,** and the **challenges of definitions** and their **implications**.

In discussion of intelligent flight, namely modes of flying that some commercially available or off-the-shelf consumer drones possess (including follow me, course lock, waypoints, home lock, and points of interest, (DJI n.d)), which are primarily marketed as cinematography techniques that enable drones to lock onto and follow particular points, objects, or people, and/or to rapidly ascend or descend from/towards these, participants raised the question of who or what is 'at fault if an accident happens?'.

This related to a wider discussion around the 'complexity' accompanying different actors involved in automated systems. Here, a participant raised the range of actors 'in the chain' and the question of 'who in that chain is the one responsible or liable for any issues?', flagging the need to consider 'the main manufacturer of the aircraft', those 'supplying...particular technology for the automation', as well as the 'operator, the pilot, the entity offering the C2 links' and 'USpace' or 'UTM [Unmanned Traffic Management]' (see below). This concern was echoed by other participants who said that a key issue was that of 'liability', and expressed concerns regarding understandings of autonomy involving a person ('pilot') that 'is able to press the big red button' and is thus liable, because 'that's just intervention, that's not control'. They continued that lessons could be learned from the wider context of manned aviation, wherein greater amounts of automation are being 'introduced' to manned aviation and have prompted debates around 'reduced' crewing (see Freed and Lampert 2023). They described these kinds of 'human factor' issues as important areas of consideration, particularly in light of ongoing developments around detect and avoid, namely the 'the capability to see, sense or detect conflicting traffic or other hazards and take the appropriate action' (CAP 1861a: 3), because as these approaches are 'being automated or autonomised, or whatever you want to call it', questions remain about the place of the human and their ability and liability to react in this way.

Such discussions prompted debates around definitional issues surrounding automation and autonomy. In addition to observations that 'humans are the primary subject and object of norms that are created, interpreted and enforced by other humans' and that as 'machines become ever more intelligent and autonomous, lawmakers and courts will face increasingly complex dilemmas when regulating the autonomous conduct of these machines' (Hartman at al. 2022: 7), participants in the international focus group raised the issue of definitions. Here, one participant noted key 'differences between these two terminologies [automation and autonomy] technically' and suggested that while the 'regulation aims to dichotomize these two kind of operations', there remains a lack of clarity around these terms. The participant continued that 'the way it [regulation] defines autonomous operation is by setting a bar too high, where anything could be fully autonomous or not at all, whereas we know that there are different levels of autonomy,

within which a technology could operate.' They continued that it was significant that this 'emphasis' or nuance was 'missing at this point', in part because commercial drone operations with 'increasing automation' have been 'dubbed as autonomous, where the human is not there in the operation' but still has 'supervisory control'.

In this vein, another participant echoed a lack of definitional clarity around automation and autonomy, stating that the 'regulations have created the dichotomy between autonomous and the flights where the remote pilot is on the ground and any point where that remote pilot can interfere with the flight, such as doing a kill switch, meaning it cannot be autonomous. So autonomous is only where there's no pilot involved at all, which there is no cases of this at the moment, as far as I know it'. This was significant, they continued, because 'this definition that we have in law doesn't match the technology', but it 'also doesn't really match the regulations as well because if we look what the safety regulators are doing also on AI', they have a 'four stage approach' (though they added 'arguably the first three are not really AI anyways, they're just levels above increasing complex algorithms'), with 'the proposal for third Party liability regulation on AI. That's still a proposal and that will set out liability rules for the use of drones, because they've explicitly mentioned the Montreal Convention and the Rome Convention in it, which is aviation liability. So they're linking it to drones, and that definition of AI does not match this autonomous or remotely piloted dichotomy, so even in terms of the technology or the regulation, they are mismatched'.

Examples of relevant discussion in regulation or guidance
• Section 4.5 of CAP 722 contains a discussion around **automation and autonomy**. The document states that the guidance 'relates to the regulatory interpretation of the term "autonomous" and provides clarification on the use of high authority automated systems in civil UAS' (CAP 722: 105). The guidance states that while the 'dictionary definition of autonomy is "freedom from external control or influence"', the 'need to meet safety requirements, defined in the various Certification Specifications under CS XX.1309/ CS XX.2510, for "Equipment, Systems and Installations" means that at this point in time all UAS systems are required to perform deterministically' (CAP 722: 105). This means that the response of drones 'to any set of inputs must be the result of a pre-designed data evaluation output activation process' and as a result 'there are currently no UAS related systems that meet the definition of autonomous' (CAP 722: 105). • The guidance distinguishes 'automated' drones into two categories, (1) **'highly automated'**, referring to systems that 'still require inputs from a human operator (e.g. confirmation of a proposed action) but which can implement the action without further human interaction once the initial input has been provided', and (2) **'High authority automated systems'**, namely those which 'can evaluate data, select a course of action and implement that action without the need for human input'. It adds that the concept of an autonomous drone 'is a system that will do everything for itself using high authority automated systems. It will be able to follow the planned route, communicate with Aircraft Controllers and other airspace users, detect, diagnose and recover from faults and operate at least as safely as a system with continuous human involvement' (CAP 722: 105). • Regarding 'learning, or self-modifying systems', which the CAA describes as a system 'that uses data related to previous actions to modify its outputs such that their results are closer to a previously defined desired outcome', CAP 722 (2022: 106) states that while learning systems 'do have potential to be used in UAS' the aforementioned 'safety requirements...still apply', meaning that 'it may not be possible to use these systems to their full potential'. They add that it remains 'possible that, at some point in the future, the aviation industry may consider the use of non-deterministic systems to

improve overall system flexibility and performance. Whilst there are no regulations that specifically prohibit this, the use of non-deterministic systems will drive a number of system and operational safety assessment issues that will need to be addressed before the use of this type of technology could be accepted for use in aviation' (CAP 722: 106).

Airspace futures

In addition to exploring the legal dimensions of potential technology futures, we were also interested in participant views regarding the potential legal dimensions of different proposed models of future airspace, including Beyond Visual Line of Sight flight (BVLOS), drone highways or corridors, and drone integration.

Adopting a focus on airspace management, discussions sought to account for airspace change in the context of ongoing UK Government interest and investment into commercial drone activities. To this end, a 2022 report by the Department for Business, Energy & Industrial Strategy and the Department for Transport outlined a vision 'that by 2030 commercial drones will be commonplace in the UK in a way that safely benefits the economy and wider society....while sharing airspace equitably and safely with other users' (HM Government 2022: 10). In launching a review of current drone regulations in the UK in August 2023, the Civil Aviation Authority stated that it is 'committed to enabling the safe and secure adoption of drones...at scale', continuing that 'through effectively mitigating the safety and security risks associated with mass uptake of UAS [drones], we [the CAA] intend to unlock the significant public value from UAS and enable the UAS sector to grow' (CAP 2569: 7).

Visual Line of Sight (VLOS)

As is outlined in Domestic framework: Rules and regulations for drones in the UK, existing drone regulations in the UK largely centre on Visual Line of Sight (VLOS) operations. When operating in the Open Category, or 'when set out within the terms of an operational authorisation for the specific category', drones must be 'operated within visual line of sight of the remote pilot' (CAP 722: 25). Operating Visual Line of Sight (or VLOS) is 'defined within UK Regulation (EU) 2019/947 as: a type of UAS operation in which, the remote pilot is able to maintain continuous unaided visual contact with the unmanned aircraft, allowing the remote pilot to control the flight path of the unmanned aircraft in relation to other aircraft, people and obstacles for the purpose of avoiding collisions' (CAP 722: 25). Operating VLOS 'ensures the remote pilot can monitor the aircraft's position, orientation, and the surrounding airspace at all times. This is important in order to ensure the UA [drone] can be manoeuvred clear of anything that might pose a collision hazard' (CAP 722: 25). For flight within the Open Category, 'operations are limited to a maximum distance of 400 feet (120 metres) from the closest point of the surface of the earth' (CAP 722: 26; Drone and Model Aircraft Code n.d).

CAP 722 (2022: 25-26) adds that the 'maximum distance from the remote pilot at which this can be safely achieved depends on a number of factors and may change from flight to flight'. It continues that the 'maximum VLOS distance varies for every operation, and will include such considerations as: The size of the aircraft (and its 'visual conspicuity'); Any lighting onboard the UA to aid in orientation and navigation; The weather conditions (fog, sun glare etc.); The remote pilot's eyesight; Terrain and obstacles that may obscure the view between the RP [remote pilot] and the UA [drone]'. The guidance notes that it is 'for the remote pilot to satisfy themselves, after careful consideration of the above guidance, the maximum horizontal distance that can be safely achieved whilst still maintaining unaided visual contact with the UA [drone]' (CAP 7222: 26). It should be noted that 'while corrective lenses may be used, the use of binoculars, telescopes, or any other forms of image enhancing devices are not permitted', though 'provision is made within

UK Regulation (EU) 2019/947 for the use of FPV equipment within the Open Category, providing an observer is used' (CAP 722:25-26; see also CAP 1861 for information on Extended Line of Sight or EVLOS).

Lastly, CAP722 (2022: 27) asserts that there are 'no right-of-way rules set out in regulation between unmanned aircraft and other airspace users, however it is likely that the unmanned aircraft remote pilot will identify other airspace users before they identify the unmanned aircraft, and therefore the remote pilot will usually be first to manoeuvre away from any conflicting aircraft'. It adds that per 'UK Regulation (EU) 2019/947' in 'UAS.OPEN.060 (2)(b), that: the remote pilot shall maintain a thorough visual scan of the airspace surrounding the unmanned aircraft in order to avoid any risk of collision with any manned aircraft. The remote pilot shall discontinue the flight if the operation poses a risk to other aircraft, people, animals, environment or property' (CAP 722: 27; see also UAS.SPEC.060(3)(b) for the Specific Category). The CAA underscores that 'although this places a responsibility for collision avoidance on the remote pilot, it does not absolve other airspace users from their own collision avoidance responsibilities. Neither does it imply any 'right of way' over UAS, by other airspace users' (CAP 722: 27). The range of legal considerations identified for VLOS flying are extensively covered earlier in the report (e.g., see parts 4.1 Grouping drone incidents and misuse, 4.2 Responding to drone incidents and misuse, and 4.3 Emerging Capabilities) and as such will not be repeated here.

Beyond Visual Line of Sight (BVLOS)

In recognition of changing airspace in the UK, in this short activity we introduced discussions around Beyond Visual Line of Sight (BVLOS) flight. While operating in VLOS is 'adequate for many businesses', the Civil Aviation Authority recognise that there are 'significant opportunities of greater efficiency, productivity, safety and economic value' in operating a drone Beyond Visual Line of Sight (CAP 1861). To this end, a range of drone operators in the UK, from emergency services to commercial operators, continue to explore operating BVLOS (HM Government 2022).

BVLOS refers to 'an operation in which the remote pilot or RPA [drone] observer does not use visual reference to the remotely piloted aircraft in the conduct of flight' (CAP 1861). CAP 722 (2022: 28) adds that 'BVLOS operations will require either: a technical capability which has been accepted as being at least equivalent to the ability of a pilot of a manned aircraft to 'see and avoid' potential conflictions' such as Detect and Avoid ['the capability to see, sense or detect conflicting traffic or other hazards and take the appropriate action'], which 'would be expected to comply with Regulation (EU) 923/2012 as retained (and amended in UK domestic law) under the European Union (Withdrawal) Act 2018: The Standardised European Rules of the Air (SERA) chapter 2 (avoidance of collisions), as adjusted by Rule 8 of the Rules of the Air Regulations 2015 (Rules for avoiding aerial collisions)', or 'an operational mitigation, which reduces the likelihood of encountering another aircraft to an acceptable level, which may be achieved either using airspace segregation, or another suitable method of ensuring such segregation' (CAP 722: 28).

CAP 722 (2022) states that the 'primary means of achieving BVLOS operations without using a technical DAA [detect and avoid] capability, is using airspace segregation'. CAP 1861 (2020) clarifies that BVLOS operations today 'are most commonly conducted in segregated airspace which is typically provided by a Temporary Danger Area (TDA)'. A Temporary Danger Area refers to 'temporary airspace which has been notified as such, within which activities dangerous to the flight of aircraft may take place or exist, at such times as may be notified' (CAP 1616). The CAA acknowledges that 'for a sustainable BVLOS business model, the TDA is not a practical long term solution, due to its 90-day validity and inability to re-establish without significant changes once expired' (CAP 1861; see also Jackman 2023).

To this end, in ‘describing its vision for the integration of Beyond Visual Line of Sight’ drones into UK airspace, the Civil Aviation Authority’s Airspace Modernisation Strategy outlines a series of phases, including atypical air environment, segregation, accommodation, and integration, to describe ‘a transition from the use of segregated airspace (i.e., temporary danger areas (TDAs)), towards operations in unsegregated airspace supported by transponder mandatory zones (TMZ)’, towards integration. They continue that ‘given the limitations of today’s technology and ‘ruleset’, an incremental approach is required to transition from segregated airspace to unsegregated airspace’ (CAP 2533: 7). For future developments, see Integration below.

Figure 11: Drone silhouette. Source: Goh Rhy Yan, Unsplash https://unsplash.com/photos/silhouette-of-quadcopter-drone-hovering-near-the-city-p_5BnqHfz3Y

Drone highways

In seeking to open drone discussions in relation to evolving UK airspace, we introduced participants to one emergent area of development, namely drone highways or corridors.

A UK-based example of such a development is Project Skyway, ‘the world’s largest and longest network of drone superhighways’ proposed and planned to be comprised of 165 miles of drone corridors or highways linking six ‘towns and cities across the UK’ (including Reading, Oxford, Milton Keynes, Cambridge, Coventry, and Rugby) (Altitude Angel 2022). The consortium underpinning the project is led by ‘Unified Traffic Management software provider Altitude Angel’, and the under-development highway ‘network’ is designed to ‘help unlock the huge potential offered by unmanned aerial vehicles’ and to ‘be a catalyst to enable growth in the urban air mobility industry’ (Altitude Angel 2022, 2022a). Plans for Project Skyway were submitted under a ‘Department for Business, Energy & Strategy (BEIS) InnovateUK programme...to support business growth through the development and commercialisation of new products, processes, and services’ and the UK Government in July 2022 gave ‘the go-ahead' for the plans (Altitude Angel 2022a). BT subsequently ‘invested £5M’ in the project, and ‘will provide connectivity and network infrastructure to allow Altitude Angel to roll out its software’ (The Guardian 2023).

In discussion of airspace changes such as the proposed drone highway or corridor, participants raised questions around locating the corridors, and how the development of such airspace models might fit with existing planning processes. In discussion of locating such corridors, participants suggested that they could be located ‘along existing transport corridors’, such as ‘above highways’, though acknowledged that while potentially assisting with the mitigation of some impacts (such as noise), this may create other knock-on issues, as ‘highways have to be

accessible by helicopters'. In discussion of where the 'route would go', participants also raised issues around the question of 'competing interests', from those of the drone providers and supporters, to 'NIMBYs, people who in the wealthy areas who can perhaps get their MPs to lobby the Government more, they're not going to have drone corridors in the same way that they don't have wind farms or anything that effects the local environment'.

While drones are associated with a range of benefits - from rapid data gathering, increasing operational safety (e.g. reducing workers at height), to enabling connection and access (e.g., delivery to remote areas) (Jackman 2023), the growing use of drones remains associated with a range of challenges and risks. As introduced in the report's opening (Introduction), research into the perception of drones by members of the UK general public demonstrates concerns around privacy, safety and security, as well as the potentially disruptive implications of drones on visual and noise landscapes, and wildlife alike. Social science research has found that some members of the UK public are concerned about issues such as drone noise, with participants in a mini dialogue exercise 'living near a busy road' expressing concerns 'that the visual and aural disruption' they already experience 'at ground level would be duplicated in the air above their homes', and participants living 'in less built-up areas' expressing concern that 'the peacefulness of green spaces' 'could be spoilt by sights and sounds' of future flight technologies such as drones (Camilleri et al., 2022).

In this vein, one participant likened the discussion to 'living under the flight path' and suggested that drone innovation required further attention the range of issues and legal implications accompanying this.

Lastly, participants added that such innovations 'won't necessarily fit into existing planning regulations', with a participant suggesting that such developments might require a 'complete rewrite of planning law in terms of extending it into airspace'. In this vein, it has been more widely acknowledged that drones raise both opportunities and challenges for statutory bodies such as Local Authorities. For example, in 2020 research undertaken by barrister Richard Ryan and Safer Drones Trustee Chris Gee with 350 UK local authorities reportedly found that 'councils do not have appropriate policies in place for drones and where there is a policy in place, it is not consistent with CAA regulations' (Local Government Lawyer 2020). They continue that they 'did not find a single policy that was accurate, up to date or enforceable' (Local Government Lawyer 2020). In this vein, in their review of UK local authority drone rules, McLachlan et al. (2022: 1) argue that these can presently be understood as a 'patchwork of inconsistent' rules. In relation to 'public open and green spaces', they continue that 'many local authorities are unaware of the issues being created through: (i) inappropriately couched or poorly framed byelaws; (ii) multiple byelaws covering the same area by virtue of overlapping jurisdictions; or (iii) the lack of readily identifiable policies for drone use on public land'. They conclude that 'overregulation, inconsistent regulation and regulatory disharmony are causing confusion for recreational drone enthusiasts such that it is never clear which public- or crown-owned open and green spaces they are allowed to, or prohibited from, flying' (McLachlan et al. 2022: 1).

The sentiment that local authorities require further resourcing in this area was also echoed in January 2023 at the Westminster Business Forum (2023) event 'next steps for drone regulation in the UK', at which Councillor Keith Artus of the Strategic Aviation Special Interest Group (SASIG), a 'special interest group of the Local Government Association', discussed the role, interests and concerns of local authorities in relation to drones. While outlining a range of benefits of drone use and integration, the Councillor also raised 'issues impacting adoption', including that local authorities have 'little understanding of the sector and its potential relevance to them, they have no systematic assessment of the issues they give rise to, they have no unified strategy for use/control of drone operations, they may not have the availability of human

and financial resources to implement, and they do not have training regimes or the drones knowledge base', adding that further reflection is required on the 'infrastructure needed' (Westminster Business Forum 2023). The Councillor added that local authorities will be key 'facilitators of drone use' and thus 'need an overarching approach' (Westminster Business Forum 2023). In response to such issues, in October 2023, the AAM Academy for UK City and Local Governments launched the first courses on its learning platform (AAM4Gov), which is supported by the UK Research and Innovation Future Flight Challenge, and is designed to support understanding and training in the area of advanced air mobility, including drones (ARPAS-UK 2023; AAM4Gov 2023).

Integration

Presently, many 'small RPAS [drone] operations are restricted to Class G airspace below 500ft above ground. While this is not formally segregated, it is largely free of normal aircraft traffic' (House of Lords 2015: 15). In its development of strategy around the evolution of UK airspace, the Airspace Modernisation Strategy outlines four stages (atypical air environment, segregation, accommodation, and integration), with integration referring to BVLOS drones 'capable of operating in the same environment as other airspace users, without the need for additional requirements to be placed upon them to address their specific operating characteristics (CAP 2533: 26).

In discussion of drones being further integrated into UK airspace, participants raised a range of questions regarding costs, insurance, liability, noise and security. For example, participants raised questions of the costs associated with the development of air traffic management technologies, systems and infrastructures, asking 'who's going to pay for it, who's going to run it?' and how might 'private industry', 'government' and/or 'access' and/or 'user fees' fit within this. They also raised the question of whether the 'unmanned traffic management system' should be 'allowed to collect and sell data as a way to pay for the system', returning briefly to prior discussions around the implications of technological development on data regulations (see Data). Others raised questions around insurance, asking what the mandated 'insurance requirements' would be as airspace evolved (see Damages and Liability).

Participants also raised related questions about enforcement and liability in relation to both enforcing aviation rules (e.g., 'how do you merge in and out of those, like if you're breaking the traffic laws who enforces that?'), and liability in relation to potential detect and avoid technology failure. They also returned to discussions around noise, stating that drones can be 'so loud' and if you were living below them, 'they'd be annoying, so bad' (see Drones and noise below). Some participants also returned to discussions around the potential implications of drones upon areas of law such as nuisance (see Nuisance, and Responding to drone incidents and misuse).

Lastly, participants also raised issues around 'security', raising questions such as 'what kinds of drones are you letting fly in this system?'. Others added that while 'it depends' on the airspace infrastructure 'being rolled out', each 'will have its own vulnerabilities', which will 'also affect the safety and security of civilian airspaces'. Raising the question of what happens if the communications between aircraft are 'hacked' or 'hijacked', the participant continued that this issue could be further complicated where communications are 'automated'. Such issues have been raised more widely (Defence Committee 2019), including questions of the 'hacking' of popular consumer drones, with researchers demonstrating that they can 'reverse engineer the radio signals of drones' to see drone 'communications' such as 'its own GPS location and a unique identifier for that drone' and 'the GPS coordinates of its operator' (Greenberg 2023).

In discussion of aspirations around the 'future integration of air traffic', the Airspace Modernisation Strategy states that the 'strategy aims to safely facilitate access by diverse

airspace users, with a transition towards greater integration of air traffic, where it is safe to do so' (CAP 1711: 20). In discussion of 'future integration', the CAA adds that 'in terms of determining a path through the accommodation phase towards integration, detect-and-avoid (DAA) systems (ground-based, air-based or a combination of both) are likely to be a critical enabling technology. At this stage, electronic conspicuity is considered very likely to be an essential enabler for DAA [detect and avoid] and is therefore likely to be essential for operations within TRAs that are established for the purpose of integrating BVLOS operations' (Civil Aviation Authority n.d.h). Electronic conspicuity can be understood as an 'umbrella term for the technology that can help pilots, remotely piloted aircraft systems and air traffic service provides be more aware of what is operating in surrounding airspace' (CAP 1711, see also Civil Aviation Authority 2021).

The CAA adds that 'once it can be demonstrated that the developments are sufficiently mature and there is data available to support safety arguments, that will start to signal the closure of the accommodation phase' and then we will 'start to see RPAS [drones] integrated within standard classifications of UK airspace, permitting them to operate BVLOS without the need for additional requirements to be placed upon them to address their specific operating characteristics' (Civil Aviation Authority n.d.h). The CAA understands drones in 'non-segregated airspace' as 'operations within airspace that is shared with other aircraft', and adds that 'in order to authorise BVLOS operations in non-segregated airspace, the maturity of technological and operational mitigations requires significant work' (CAP 1861). With regard to security, the CAA outlines a concept of a 'Detect & Avoid Ecosystem', which includes detecting both 'cooperative' and 'non-cooperative' drones (CAP 1861; CAP 1861A). Cooperative aircraft (including drones) refer to those 'broadcasting their position, speed, direction and altitude (CAP 1861) and providing 'either actively or upon interrogation, their position, speed, altitude and heading as a minimum, but may also include their planned route and destination' (CAP 1861A). Conversely, non-cooperative aircraft (including drones) refer to 'aircraft that are not proactively broadcasting any information' (CAP1861; see also CAP 1861A).

Drones and noise

With regard to the issue of drone noise, the Civil Aviation Authority 'recognises that the noise footprint of new and novel aircraft will be one of the factors that will determine the level of public support for these new operations, along with other considerations, such as carbon footprint, privacy and visual pollution' (CAP 2296: 19). In discussion of eVTOL (electric vertical take-off and landing) craft, including drones, the Civil Aviation Authority notes that such technologies 'present new challenges for noise legislation and understanding of how these types of noise sources may impact people on the ground' (CAP 2505: 4). Adding that 'this is a relatively new research area', the CAA note that 'studies into the effects of this type of noise include the development of exposure-response relationships for annoyance and perceptions of noise characteristics. The impact on sleep disturbance will need to be understood more clearly, as well as the role non-acoustic factors will play with this type of noise exposure and response' (CAP 2505: 30).

With regard to the regulation of drone noise in the UK, as is discussed in Case study 4, CAP 1766 (2019: 24) states that 'there are currently no noise specific requirements for UASs in UK. The intent is that UK follows EC regulation'. Drone noise is discussed within both the Implementing Regulation (CAP 1789A) and the Delegated Regulation (CAP 1789B). Alongside describing the responsibilities of drone operators in the specific category to 'minimise nuisance, including noise and other emissions-related nuisances, to people and animals', CAP 1789A (2022: 31, 4) states that drone 'noise and emissions should be minimised as far as possible taking into account the operating conditions and various specific characteristics of individual Member States, such as the population density, where noise and emissions are of concern'. CAP 1789B (2021: 3) states that 'in order to provide citizens with high level of environmental

protection, it is necessary to limit the noise emissions to the greatest possible extent. Sound power limitations applicable to UAS intended to be operated in the ‘open’ category might be reviewed at the end of the transitional periods as defined in Commission Implementing Regulation (EU) 2019/947’. Part 13 'lays down the basic noise emission standard' and detailed 'noise test code' (CAP 1789B: 53).

Given both the range of ‘different operators’ and ‘variety of types of operators over a range of different communities living in different environments’, the CAA has raised the regulatory challenges associated with ‘setting limits specifically to accommodate these different circumstances’ (CAP 2296: 19). They also highlight that drones can introduce complexities around identifying ‘which operators are responsible’ for ‘noise disturbance’, which ‘differs from current aviation noise activity, where it is largely clear that the noise originates from aircraft using a specific airfield’ (CAP 2296: 19). As such, the CAA has previously expressed that their ‘preferred approach would be to draw from the ICAO Balanced Approach to Aircraft Noise Management’ which ‘consists of identifying the noise problem at a specific airport and analysing various measures [including ‘Reduction of Noise at Source (Technology Standards); Land-use Planning and Management; Noise Abatement Operational Procedures; and Operating Restrictions’] available to mitigate noise’ (CAP 2296: 19-20). While this approach is ‘currently applied on an airport-by-airport basis, making it relevant, as it stands, for new and novel aircraft launch/landing sites’, the CAA notes that drones present a ‘greater potential for en-route noise disturbance to occur...if they are to operate at lower altitudes than civil aircraft, in greater volumes, and over-populated areas’, adding that ‘elements of the approach may require adaptation’ (CAP 2296: 20).

It can be noted that the ‘transition and legacy provisions will now be extended to 1 January 2026’ (Civil Aviation Authority n.d.g) and the implications for this in relation to drone noise in the UK may be understood as unclear.

5. IMPLICATIONS AND RECOMMENDATIONS

The final section of the report includes:

- (5.1) Key considerations for lawyers working on drone-related cases;
- (5.2) Key questions or themes;
- (5.2) Recommendations moving forward.

(5.1) Key considerations for lawyers working on drone-related cases

In this section we provide a practical summary of some key considerations for lawyers involved in a drone-related or drone featuring case, building upon the testimony of participants in the focus groups.

Key considerations for lawyers working on drone-related cases

- **Identify offences or claim:** Consult relevant aviation regulation (see Domestic framework: Rules and regulations for drones in the UK) and the different avenues for enforcement, prosecution or remedy (see Enforcement).
- **Drone Regulations**: Consider whether the individual and/or group meets and/or has met requirements under drone regulation with regards to registering their drone (see Domestic framework: Rules and regulations for drones in the UK), while recognising that some actors may opt not to register their drone and/or to use second hand devices.
- **Actors:** Consider the question of which actors are involved in the case and who might have access to relevant drone footage. Participants distinguished, for example, between public versus private, public versus state, and public versus business, noting that data rules may apply differently depending on the actors involved. They also highlighted that this may be complicated in some cases (e.g., where a private company may be contracted to act on behalf of the state; See Actor).
- **Role of the drone:** Consider the nature of the case and whether or not to prioritise the drone aspect. For example, one participant described the use of drones to transport contraband into prisons (a significant issue in the UK – see Drone incidents, misuse and threats). They described focusing on other charges (e.g., the supply of drugs) as they were concerned that the Crown Prosecution Service 'rarely ventured into drones'. Another participant gave the example of driving offences and the dominant focus on driving without a license, rather than driving without insurance, as the former has a higher penalty as an offence.
- **Context:** Consider the context of the action (e.g., if a taser is added to a drone, was it added by an artist, or by an individual or group who may be intending on inflicting harm).
- **Consider consequential effects:** For example, if an individual flies a drone over a cash machine user, this may be deliberate (e.g., to capture data), or unintentional (e.g., inadvertently captured information). Nonetheless, there may be additional consequences (e.g., retention and/or sharing of drone imagery or (personal) data) (see GDPR guidance: Information Commissioner's Office, and Data).
- **Expertise:** Participants foregrounded that drone incidents and misuse are often cross-jurisdictional, can be interpreted differently by lawyers with different specialisms, and can require multiple forms of legal expertise. Do you need to seek expert technological, forensic or legal advice?
- **Standard of proof**: In relation to how you may be approaching the drone incident, e.g., as criminal or civil (see Legal Context), consider the impacts of this in relation to both the elements that must be proved, who by and to what standard.
- **Intention:** Was the drone use, incident and/or misuse intentional (e.g., deliberate) or unintentional (e.g., negligent or reckless)? In some cases, it may be difficult to determine intention.

Evidence

- **Consider evidence and evidentiary challenges at an early stage:** Ensure the available evidence was lawfully collected, that the drone is secured and/or available for inspection and that any item attached to the drone is identified. Pay attention to any footage, weapon, data, or other related object or item and what evidence links them to the drone and/or the individual or the offence or wrongdoing.
- **Remoteness:** The potential remoteness of the drone flyer from the drone itself requires consideration.
- **Accessing drone footage and information:** Explore whether it is possible and/or permitted to gather information about or from a drone. For example, if a drone is captured, some information may be visible on the drone itself (e.g., flyer or operator IDs; serial numbers). Further information may, if appropriate, be ascertained via the use of drone forensics. Drone forensics refers to the forensic examination of a drone, and may, depending on type of drone flown, be able to determine a range of information about the drone flight to build an evidentiary picture (see Drone forensics discussion in Case study 5: Drone used in attempt to disrupt the electrical grid).
- **Drone Forensics:** It should be noted that drone forensics remains a relatively nascent field and participants expressed concerns that drone forensics was not yet commonplace and this may be impacting Crown Prosecution Service (CPS) pursuit of drone cases (see also Jackman 2023a). As such, it is important to consider both the potential for, scope and reliability of forensic evidence, and to note that drone litigation will likely require technical expertise (e.g., sourcing and hiring a drone expert).
- **Enforcement powers:** Were any powers exercised lawfully? Is it possible and/or permitted to locate, apprehend or seize the drone? Consider the police powers detailed in the Air Traffic Management and Unmanned Aircraft Act 2021 (see Enforcement).
- **Defences:** Consider any available defences.
- **Third party liability and indemnity:** Where relevant consider any third party liability or indemnity.

* Further information on all themes in this condensed action-oriented list can be found throughout the wider report.

(5.2) Key questions or themes

As part of the final activity, participants were encouraged to share key questions or themes they'd like to raise to and share with legislators, regulators and policy-makers. Here, we highlight *several themes* participants drew attention to. We then think across the report as a whole to provide a series of *overarching recommendations* moving forward.

Key questions of themes highlighted by participants	
Approaching regulation	• Participants suggested that they'd like to know more about 'what regulators actually want from drones...what is the end goal of drone regulations' because they were unsure about 'whether the best approach' was to 'look at examples of things going wrong and address each of those, like whackamole, or whether there's a need for another approach'. • In discussion of 'causes versus harms' a participant reflected on whether it may be best to 'focus on harm... as the causes can change over time' and the 'harms you're seeking to prevent are perhaps less likely to change as quickly'. While noting that 'in this country' they 'wondered if you risk almost giving too much power to the executive...to update quite regularly if you go for a causes rather than harms based approach', they added that 'there might come a point where technology has moved on quite a lot and the harms being caused have changed and shifted so much in a way that

	power delegated to the executive to make what initially seemed to be incremental changes actually ended up being, over the course of years, a big policy shift that parliament didn't necessarily envisage and that de facto don't necessarily have the executive powers to do'. • In recognition of the complexity of drone use and misuse, one participant called for a 'meta regulatory approach to regulate drone operations and curb drone misuse'. They continued that 'the regulation does not really sit' and is not in the sole 'jurisdiction' of aviation authorities, rather it 'overlaps' with communication authorities, the Information Commissioner's Office and others, and as such there is a 'need for a meta regulatory approach'. • Participants also raised the question 'when you regulate, what are you regulating?' in relation to Artificial Intelligence specifically. A participant continued that this is an important question in the field of AI, where questions arise around whether you are 'regulating input' or whether you 'should actually be regulating harm, or the cause of the harm'.
Pace of regulatory change	• Participants suggested that there remained challenges with the pace of regulatory change impacting the potential for regulations to become 'redundant', and the challenges of 'future proofing' of regulations, which remained 'years behind'.
Insurance and compensation	• Participants returned to issues around insurance and compensation, including the implications of uninsured operators, the coverage of insurance, and the potential knock on impacts on accident reporting. • Participants highlighted insurance concerns both around drone flyers that are 'uninsured' because they are 'intentionally' misusing drones, and around hobbyists either being uninsured or having 'insufficient insurance' (i.e., insurance 'excludes coverage' in particular circumstances). They continued that 'however you look it', circumstances could emerge where a drone flyer 'causes damage either to an individual or going through the windscreen of a plane and cause losses which they are not insured to cover'. Here, participants again returned to the potential to create 'something similar to the Motor Insurance Bureau – MIB coverage' in order to accommodate 'circumstances where people are injured' or harmed and to ensure 'protections in place for them' (see Damages and Liability). • In discussion of insurance, a participant stated that 'one big concern is ensuring that those people who are injured, whether under civil or criminal law are well treated, for example, if you're physically injured, you get compensation for this'. They continued that while they thought this was 'an important thing to guarantee', 'coming from the aviation domain...where safety is always the number one priority', they had concerns that 'if we have such a tort based focus or a criminal based focus, this could bring imbalance to what we often call the just culture approach where we want people to come forward and those who have potentially caused an incident or an accident to share information, so lessons can be learned and things can be fixed, so this doesn't happen again'. They continued that 'if we go down the route of tort or focusing on criminal, which I think could

	happen with this new proposal of third party AI liability in aviation, this could impact people's willingness to come forward because of their fear to be prosecuted or sued', and add such 'concern for legislators, policymakers, regulators is to ensure that the just culture approach that aviation has benefited from the very beginning is maintained'. • A 'just culture' can be understood as one promoting 'continuous learning' from mistakes and encouraging 'pilots to openly and freely share essential safety related information' including the 'reporting of occurrences' (Civil Aviation Authority n.d.i). The Civil Aviation Authority (n.d.i) pursues this through treating people 'fairly' and where appropriate 'not punishing' them for 'actions, omissions or decisions taken by them that are commensurate with their experience and training'. It does add that 'to maintain or improve aviation safety in cases of, for example, gross negligence, wilful violations and destructive acts, further action may be necessary' (Civil Aviation Authority n.d.i). CAP 722 provides further information regarding accidents and 'occurrence reporting'.
Automation, autonomy and responsibility	• Participants highlighted the 'complexity' of automated and autonomous systems, adding that the range of actors 'in the chain' prompted and complicated the question of 'who in that chain is the one responsible or liable for any issues?'. • Here, participants raised questions about both human factors and potential distinctions between 'supervision', 'intervention' and 'control', reflecting on the implications of different forms and relations of operation to questions around human ability and liability. • See Automation and Autonomy for a full discussion.
Managing deviant drones	• Participants raised concerns around the 'push for drone integration' and the ongoing question of how to 'stop' devious, malicious, or reckless drones. They continued that at present the technology was not 'adequate' and as such, they felt further attention was needed to drone misuse 'as drones are normalised in our civilian airspace'.

(5.3) Recommendations

In the report's final section, we develop key recommendations applicable to lawyers working on drone cases and relevant to wider drone decision-makers (e.g., regulators, legislators and policy-makers). In providing these recommendations, we recognise both the importance and challenges of balancing the benefits of drone innovation with safety, privacy, and wider considerations. This report demonstrates that drone incidents and misuse both evoke and engage with various areas of law. As such, we make the following recommendations:

Information provision and presentation: While recognising the scope of existing information provided by UK regulators (see Domestic framework: Rules and regulations in the UK).

I. Further information and guidance should be developed to enable drone users to more fully understand their legal obligations and responsibilities (e.g., around insurance and liability, including the extent to which they may be liable in the case of an accident or incident and in relation to indemnity provisions, e.g., in the Civil Aviation Act section 76 in the unlikely event a drone comes into contact with an aircraft) and the potential outcomes if these are not appropriately met (e.g., Enforcement, Legal context);

II. Further information should be developed in specific areas to aid clarity (e.g., around the weaponisation of drones; around designated Standards and secure by design/ manufacturing drones with mitigations, see Damage and Liability);
III. Existing information could be more clearly presented, for example via a maintained table containing links to and summaries of key relevant legislation, regulation and guidance targeted to key drone user groups (e.g., hobbyists, commercial flyers, local authorities, emergency services) and enabling easier access to and awareness of key information;
IV. Additional clarification could be provided where regulators employ different distinctions (e.g., CAA does not distinguish between hobbyists and commercial users (see Understanding drone categories), whereas with regard to data protection, the ICO does distinguish between hobbyist, and professional or commercial, uses (see UK GDPR Guidance: The Information Commissioner's Office), in order to minimise the potential for user confusion.

***Review of existing offences*:** Criminal law should be reviewed to explore whether it adequately covers (new) offences committed using drones as opposed to existing offences facilitated by drones (see Nature of criminality). We also suggest that the result of any such review should not seek to criminalise actions more appropriately dealt with in the civil courts and in particular should be taken not to criminalise legitimate expressions of opinion or protest.

Legislation has the potential to be applied in a discriminatory manner and should be subject to monitoring and evaluation to ensure it is fairly applied. For example, fixed penalty notices, although not discriminatory in themselves may be applied in a discriminatory manner.

Moreover, particular care should be taken in respect of any offences proposed by way of secondary legislation to ensure legality, non-discrimination and fairness.

Ensure any legislative changes or enforcement actions take into account the benefits of information sharing following an accident to enable lessons to be learnt: Over-regulation, enforcement or high penalties inconsistent with the severity of an accidental event may result in individuals not reporting accidents. This should therefore be taken into account when seeking to regulate new forms of harms committed by or through drone use. An appropriate balance should be drawn and the current approach of the Civil Aviation Authority (n.d.i) of treating people 'fairly' and where appropriate 'not punishing' them for 'actions, omissions or decisions taken by them that are commensurate with their experience and training' should be maintained.

Guidance and resources for lawyers: Resources should be developed in order to build capacity amongst law enforcement and lawyers in respect of both criminal drone incidents, and civil actions related to drones. There remains a notable lack of information about drones and drone-related criminal offences in the standard criminal and civil practitioner textbooks or Crown Prosecution Service (CPS) guidance. The report identifies some of the different forms of specialist knowledge that may be required.

Criminal guidance: Guidance in respect of the most likely offences under the ANO 2016 and the general criminal law should be provided. This could perhaps take the form of a table of statutory and common law offences (perhaps akin to the CPS entry on trespass – including the actus reus, mens rea, and any statutory liability or defence, preconditions, allocation and penalty). In particular, guidance should be produced in respect of the offences referred to in the Air Traffic Management and Unmanned Aircraft Act 2021 that may be subject to a fixed penalty notice to enable the individual served with the notice to make a reasoned choice about whether to accept the notice or not:

- endanger another aircraft
- Cause harm, harassment, alarm or distress,
- Cause any person occupying any premises nuisance or annoyance relating to their occupation of the premises,

- Under some security or good order and discipline in any prison or in any other institution where persons are lawfully detained,
- Disturb public order, or
- Damage property (including land and buildings) when committing the fixed penalty offence (Air Traffic Management and Unmanned Aircraft Act 2021).

Evidence: Consider whether information or guidance is required in respect of evidence obtained by, from and about drones including, for example, technical matters, airspace matters and where that evidence is located overseas (see discussion of drone forensics in Case study 5).

Training and guidance related to (the legal dimensions of) drone use, incidents, misuse and enforcement: Further resources should be developed to support key drone stakeholders (e.g., police, local authorities) in building awareness and capacity around both drone usage (e.g., applications), potential drone incidents and misuse (e.g., incident types), and the routes and mechanisms for enforcement. This report has sought to demonstrate that drone use, incidents and misuse variously intersect and engage with diverse areas of law. Consultation with legal practitioners in the development of such forms of resource and guidance may aid in building awareness and capacity in relation to pertinent legal questions (e.g., Trespass, Nuisance, Noise) and practice (e.g., informing public messaging on drone policies in local authorities; understanding the implications of drones upon planning law – see Drone highways). It may also prove useful to undertake monitoring and evaluation in relation to how key stakeholders deploy relevant enforcement measures.

Consideration of potential legal challenges accompanying drone futures: Further research is needed to consider potential future harms and legal challenges arising from drone technology, both in relation to emerging technological developments (see Emerging capabilities and Technology Futures), and in relation to the anticipated scaling of drone activity (see Airspace Futures). The following areas are of particular concern:

- Data protection in the context of emerging capabilities such as livestreaming and facial recognition,
- Responsibility and liability in relation to autonomy and artificial intelligence (see Artificial Intelligence, and Automation and Autonomy).
- Liability in relation to the potential failure of remote identification and electronic conspicuity technologies, and in relation to regulation around drone noise (e.g., in relation to nuisance, see Drones and noise).

We recognise that a number of these considerations are highlighted in ongoing and wider work around Airspace Modernisation and Future Flight, but are of the view that there remains further scope to explore legal challenges and modes of enforcing drone use and misuse specifically (e.g., considering the implications of technological advancements such as miniaturisation as a potential challenge to a weight-based categorisation approach; considering site specific forms of drone zoning, perhaps akin to the height restrictions adopted in the Air Navigation (Restriction of Flying) (Prisons and Young Offenders Institution) (2023/1101)). The speed with which new technology develops means that any legislative framework developed to cover these harms should have sufficient flexibility to take into account new risks and ways of operating drones.

Inclusive consultation on regulation and policy: Consultation around new regulation and policy work should be more inclusive in order to reduce the potential of contributing to existing forms of inequity. For example, while some consultations have sought to include a diverse range of voices (e.g., Future Flight Mini Dialogue), further work should aim to ensure representation of different voices (e.g., women, minority communities, residents in diverse geographical areas and contexts), consideration of different priorities, concerns and level of awareness of the potential benefits or harms arising from drone use, and reflection on how these may intersect with

different legal questions and challenges. This may also extend to seeking further consultation with commercial female drone flyers, who remain typically under-represented in consultation exercises.

Understanding the potential for drone-enabled or assisted discrimination: Further resources should be dedicated to understanding the potential for drones to enable or assist in diverse forms of discrimination. Given that drones are predominantly owned and used by men (see What are drones), we suggest that particular attention is paid to the potential for drones to be used for gender-based harassment in both civil and criminal contexts.

Reference list

AAM4Gov (2023) The AAM Academy for UK City and Local Government https://aam4gov.com/

ABC News (2018, 30 September) Perpetrators using drones to stalk victims in new age of technology fuelled harassment https://www.abc.net.au/news/2018-10-01/drones-used-to-stalk-women-in-new-age-of-harassment/10297906

Access Now (2022, 29 Sept) The Geneva Declaration on Targeted Surveillance and Human Rights https://www.accessnow.org/press-release/geneva-declaration-on-targeted-surveillance-and-human-rights/

ADS (2019, 13 Feb) Countering the malicious usage of drones https://www.adsgroup.org.uk/blog/countering-the-malicious-usage-of-drones/

Air Navigation Order (2016) https://www.legislation.gov.uk/uksi/2016/765/part/10/chapter/1/made?view=plain

Air Navigation (Restriction of Flying) (Prisons and Young Offenders Institution) (2023/1101) https://www.legislation.gov.uk/uksi/2023/1101/introduction/made#:~:text=The%20Secretary%20of%20State%20has,prisons%20and%20young%20offender%20institutions.

Air Navigation (Restriction of Flying) (Nuclear Installations) Regulation 2007 https://www.legislation.gov.uk/uksi/2007/1929/contents/made

Air Traffic Management and Unmanned Aircraft Act 2021 (2021) https://www.legislation.gov.uk/ukpga/2021/12/contents

Altitude Angel (2022, 24 March) UK consortium reveal blueprint to build 165 mile drone 'Superhighway' https://www.altitudeangel.com/news/uk-consortium-reveal-blueprint-to-build-165-mile-drone-superhighway

Altitude Angel (2022a, 18 July) UK Government gives the green light for World's longest drone 'superhighway' https://www.altitudeangel.com/news/uk-government-gives-the-green-light-for-worlds-longest-drone-superhighway

Amnesty International UK (2023, 26 April) The Public Order Bill: Explained https://www.amnesty.org.uk/blogs/campaigns-blog/public-order-bill-explained

Anglo International Upholland Ltd v Wainwright [2023] 5 WLUK 613 https://caseboard.io/cases/d85da422-03dd-4265-9a5c-1f146c26eadf

ARPAS UK (2023, 24 Oct) Is your council ready for the growth of drones and air taxis? https://www.arpas.uk/is-your-council-ready-for-the-growth-of-drones-and-air-taxis/

BBC News (2023, 4 Oct) Police access to passport photos 'risks public trust' https://www.bbc.co.uk/news/technology-67004576

BBC News (2018, 4 May) Drones used to disrupt FBI hostage situation https://www.bbc.co.uk/news/technology-44003860

BBC Science Focus (n.d) Want to be a drone racer? The sport's world champ explains how to launch your career https://www.sciencefocus.com/future-technology/how-to-make-it-in-drone-racing-from-the-world-champion (last accessed 12 Dec 2023)

Bernstein v SkyViews Ltd [1978] 1 QB 479 https://www.bailii.org/cgi-bin/redirect.cgi?path=/ew/cases/EWHC/QB/1977/1.html

Big Brother Watch (2023, 25 May) Biometric Britain: the expansion of facial recognition surveillance https://bigbrotherwatch.org.uk/wp-content/uploads/2023/05/Biometric-Britain.pdf

Biometrics and Surveillance Camera Commissioner (2023) 2023 survey of law enforcement use of uncrewed aerial vehicles https://www.gov.uk/government/news/2023-survey-of-law-enforcement-use-of-uncrewed-aerial-vehicles

British Drone Racing Association (n.d) About the BDRA https://bdra.uk/who-are-the-bdra/

BT (2023, April) Perceptions of drone technology https://www.bt.com/content/dam/bt-plc/assets/documents/newsroom/public-perceptions-of-drones-research-report.pdf

BT (2021, 23 November) Nearly 7 in 10 Brits believe drones will positively impact their future https://newsroom.bt.com/nearly-7-in-10-brits-believe-drones-will-positively-impact-their-future/

Camilleri E, Gisborne J, Mackie M, Patel R, and Reynolds M (2022, June) Future Flight Challenge – Mini Public Dialogue https://www.ukri.org/wp-content/uploads/2022/07/UKRI-120722-FutureFlightChallengeMiniPublicDialogueReport.pdf

CAP1430 (2016) UK Air Traffic Management Vocabulary https://publicapps.caa.co.uk/docs/33/CAP1430_UK%20ATM%20Vocabulary_5JAN2017.pdf

CAP1616 (2021) Airspace Change http://publicapps.caa.co.uk/docs/33/CAA_Airspace%20Change%20Doc_Mar2021.pdf

CAP1711 (2023) Airspace Modernisation Strategy 2023–2040 Part 1: Strategic objectives and enablers https://publicapps.caa.co.uk/docs/33/CAP%201711%20ed2%20Airspace%20Modernisation%20Strategy%20Part%201%20(24%20Jan).pdf

CAP 1766 (2019) Emerging Aircraft Technologies and their potential noise impacts http://publicapps.caa.co.uk/docs/33/CAP1766EmergingAircraftTechnologiesandtheirpotentialnoiseimpact.pdf

CAP 1789A (2022) Unmanned Aircraft Systems - Consolidated version of Regulation (EU) 2019/947 as retained (and amended in UK domestic law) under the European Union (Withdrawal) Act 2018 https://publicapps.caa.co.uk/docs/33/CAP_1789A_UAS_IR2019_947.pdf

CAP 1789B (2022) Unmanned Aircraft Systems - Consolidated version of Regulation (EU) 2019/945 as retained (and amended in UK domestic law) under the European Union (Withdrawal) Act 2018 https://publicapps.caa.co.uk/modalapplication.aspx?appid=11&mode=detail&id=9655

CAP1861 (2020) Beyond Visual Line of Sight in Non-Segregated Airspace https://publicapps.caa.co.uk/modalapplication.aspx?appid=11&mode=detail&id=9294#:~:text=Description%3ARegularly%20operating%20unmanned%20vehicles,that%20this%20technology%20can%20deliver.

CAP1861a (2020) Innovation Hub: Detect & Avoid Ecosystem For BVLOS in Non-Segregated Airspace https://publicapps.caa.co.uk/docs/33/CAP%201861a%20DAA%20Annex%20to%20BVLOS%20Fundamentals.pdf

CAP2004 (2020) Flying as a hobby and at a club https://publicapps.caa.co.uk/docs/33/CAP2004_EU_Drone_Rules_Factsheet_V7%202.pdf

CAP2012 (2022) CAP2012: Drone Rules: REQUIREMENTS FOR FLYING IN THE OPEN CATEGORY https://publicapps.caa.co.uk/modalapplication.aspx?appid=11&mode=detail&id=9954

CAP2248 (2021) Carraige of dangerous goods by Remotely Piloted Aircraft Systems. The Civil Aviation Authority https://publicapps.caa.co.uk/modalapplication.aspx?appid=11&mode=detail&id=10842

CAP 2296 (2021) CAA Response to 2021 Government Consultation on the Future of Transport Regulatory Review: Future of Flight https://publicapps.caa.co.uk/docs/33/CAA%20Response%20to%20Future%20of%20Flight%20Consultation%20(CAP2296).pdf

CAP 2505 (2023) Emerging Technologies: The effects of eVTOL aircraft noise on humans https://publicapps.caa.co.uk/modalapplication.aspx?appid=11&mode=detail&id=11972

CAP 2533 (2023) Airspace Policy Concept: Airspace Requirements for the Integration of Beyond Visual Line of Sight (BVLOS) Unmanned Aircraft https://publicapps.caa.co.uk/docs/33/Airspace_Policy_Concept_BVLOS_UA_Integration(CAP2533)-20230403.pdf

CAP 2555 (2023) Guidance on the Carriage of Dangerous Goods as Cargo for UAS/RPAS Operators in the Specific Category https://publicapps.caa.co.uk/docs/33/CAP2555.pdf

CAP 2569 (2023) Call for Input: Review of UK UAS Regulations https://publicapps.caa.co.uk/modalapplication.aspx?catid=1&pagetype=65&appid=11&mode=detail&id=12283

CAP2609: Call for Input Response Summary https://publicapps.caa.co.uk/modalapplication.aspx?catid=1&pagetype=65&appid=11&mode=detail&id=12449

CAP2610: Consultation Review of UK Unmanned Aircraft Systems (UAS) Regulations https://publicapps.caa.co.uk/modalapplication.aspx?catid=1&pagetype=65&appid=11&mode=detail&id=12450

CAP 722 (2022) CAP 722: Unmanned Aircraft System Operations in UK Airspace - Guidance https://publicapps.caa.co.uk/modalapplication.aspx?appid=11&mode=detail&id=415#:~:text=Description%3ACAP%20722%20provides%20guidance,development%20and%20operation%20of%20UAS.

Civil Aviation Act 1982 https://www.legislation.gov.uk/ukpga/1982/16/contents

Civil Aviation Authority (2021, 26 October) Task force on electronic conspicuity https://www.caa.co.uk/newsroom/news/task-force-on-electronic-conspicuity/

Civil Aviation Authority (n.d.) Our role (drones) https://www.caa.co.uk/our-work/about-us/our-role/ (last accessed 18 July 2023)

Civil Aviation Authority (n.d.a) Introduction to drone flying and the UK rules https://www.caa.co.uk/drones/rules-and-categories-of-drone-flying/introduction-to-drone-flying-and-the-uk-rules/ (last accessed 18 July 2023)

Civil Aviation Authority (n.d.b) Flying in the specific category https://www.caa.co.uk/drones/rules-and-categories-of-drone-flying/flying-in-the-specific-category/ (last accessed 10 July 2023)

Civil Aviation Authority (n.b.c) Flying in the certified category https://www.caa.co.uk/drones/rules-and-categories-of-drone-flying/flying-in-the-certified-category/ (last accessed 10 July 2023)

Civil Aviation Authority (n.d.d) Airspace restrictions for remotely piloted aircraft and drones https://www.caa.co.uk/drones/airspace-and-restrictions/airspace-restrictions-for-remotely-piloted-aircraft-and-drones/ (last accessed 10 July 2023)

Civil Aviation Authority (n.d.e) Remote ID https://www.caa.co.uk/drones/updates-and-publications/remote-id/ (last accessed 1 December 2023)

Civil Aviation Authority (n.d.f) Registration requirements for drones and model aircraft https://register-drones.caa.co.uk/registration-requirements-for-drones (last accessed 10 December 2023)

Civil Aviation Authority (n.d.g) News for remote pilots https://www.caa.co.uk/drones/updates-and-publications/news-for-drone-and-remote-pilot-operators/ (last accessed 5 December 2022)

Civil Aviation Authority (n.d.h) Airspace policy concept for BVLOS flying https://www.caa.co.uk/drones/rules-and-categories-of-drone-flying/airspace-policy-concept-for-bvlos-flying/ (last accessed 10 December 2023)

Civil Aviation Authority (n.d.i) Drone and remote piloted aircraft publications https://www.caa.co.uk/drones/updates-and-publications/drone-and-remote-piloted-aircraft-publications/ (last accessed 10 July 2023)

Clyde & Co (2022, 23 March) Global Regulation of Drones https://www.clydeco.com/en/insights/2022/03/global-regulation-of-drones

Coliandris M (2023) Chapter 17, Drones as disruptive socio-technical systems: A case study of drone crime and control, in Housley W, Edwards A, Roser Beneito-Montagut R, Fitzgerald R (ed) The SAGE Handbook of Digital Society. Sage, pp.298-313

College of Policing (2022, 21 March) Terminology (live facial recognition) https://www.college.police.uk/app/live-facial-recognition/terminology#facial-recognition

Connected Places Catapult (2022) The case for drones in UK agriculture https://cp.catapult.org.uk/news/the-case-for-drones-in-uk-agriculture/

COPTZ (2021, 25 August) Women in Drones https://coptrz.com/blog/women-in-drones/

Crown Prosecution Service (2023, 24 April) Stalking or Harassment https://www.cps.gov.uk/legal-guidance/stalking-or-harassment

Crown Prosecution Services (2022, 4 August) Public Justice Offences incorporating the Charging Standard https://www.cps.gov.uk/legal-guidance/public-justice-offences-incorporating-charging-standard#:~:text=A%20person%20obstructs%20a%20constable,DPP%20%5B1993%5D%20CLR%20534

CTB v News Group Newspapers Ltd and Imogen Thomas [2011] EWHC 1326 https://www.bailii.org/cgi-bin/format.cgi?doc=/ew/cases/EWHC/QB/2011/1326.html

CTB v News Group Newspapers Ltd and Imogen Thomas [2011] EWHC 1334 (QB) https://www.bailii.org/cgi-bin/format.cgi?doc=/ew/cases/EWHC/QB/2011/1334.html

Daniels J (2017, 4 August) US Army reportedly bans Chinese-made drone, citing 'cyber vulnerabilities'. CNBC https://www.cnbc.com/2017/08/04/us-army-bans-chinese-made-drone-citing-cyber-vulnerabilities.html

Data Protection Act 2018 https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Defence Committee (2019) Domestic Threat of Drones inquiry https://committees.parliament.uk/work/2150/domestic-threat-of-drones-inquiry/publications/

Department for Transport (2021) Bill to modernise airspace and tackle illegal use of unmanned aircraft receives Royal Assent https://www.gov.uk/government/news/bill-to-modernise-airspace-and-tackle-illegal-use-of-unmanned-aircraft-receives-royal-assent

DJI (n.d.) Intelligent flight modes https://www-v1.dji.com/intelligent-flight-modes.html (Last accessed 18 August 2023)

Doughty Street Chambers (2023, 15 August) The use of the new statutory public nuisance offence to prosecute political and environmental protest https://insights.doughtystreet.co.uk/post/102iagn/the-use-of-the-new-statutory-public-nuisance-offence-to-prosecute-political-and-e

Drone and Model Aircraft Code (n.d) The Drone and Model Aircraft Code. The Civil Aviation Authority https://register-drones.caa.co.uk/drone-code/the_drone_code.pdf

Drone Racing League (n.d) What is drone racing? https://thedroneracingleague.com/about-drl/

Drone Safe Register (2018) Indoor drone flights https://dronesaferegister.org.uk/blog/drone-flights-indoors-caa-provide-clarification-on-recent-changes

Drones Direct (2017) UK Drone Users Survey 2017 https://www.dronesdirect.co.uk/files/pdf/drones-report-2017.pdf

Engineering & Technology (E&T) (2021, 19 March) How illegal drone jammers are sold to Europe https://eandt.theiet.org/content/articles/2021/03/how-drone-jammers-are-sold-to-europe-and-the-uk/

Environment Agency (2021, 30 September) Environment Agency takes to the air https://environmentagency.blog.gov.uk/2021/09/30/environment-agency-takes-to-the-air/

European Parliament (2018) Artificial intelligence and civil law: liability rules for drones https://www.europarl.europa.eu/RegData/etudes/STUD/2018/608848/IPOL_STU(2018)608848_EN.pdf

Federal Aviation Administration (n.d) UAS remote identification https://www.faa.gov/uas/getting_started/remote_id#:~:text=What%20is%20it%3F,parties%20through%20a%20broadcast%20signal.

Fearn and ors v Board of Trustees of the Tate Gallery [2023] UKSC 4, [2023] 2 WLR 339 https://www.bailii.org/cgi-bin/format.cgi?doc=/uk/cases/UKSC/2023/4.html

Feild P (2019) Drones & Enforcement 2019 Legal Framework https://www.rtpi.org.uk/media/4069/paul-field-drones-royal-town-planning-2019.pdf#:~:text=Drones%20are%2C%20in%20the%20UK%20unmanned%20aircraft%20controlled,set%20out%20in%20the%20Civil%20Aviation%20Act%201982.

Forensic Access Group (2023) Drone Analysis in Digital Forensic Investigations. Hosted by Forensic Access Group, Jake Blythe, Ahzim Mir. Online webinar, 13 July 2023 https://www.forensic-access.co.uk/cpd-training-and-events/webinars-and-events/drone-analysis-in-digital-forensic-investigations/?utm_source=website&utm_medium=intaforensics+article&utm_campaign=drone+webinar&utm_id=webinar

Forensic Science Regulator (2023) Forensic Science Regulator: Code of Practice (accessible) https://www.gov.uk/government/publications/statutory-code-of-practice-for-forensic-science-activities/forensic-science-regulator-code-of-practice-accessible

Freed J, Lampert A (2023, 6 February) European Aviation Regulators Shut Down Proposal to Fly With Just One Pilot. Skift https://skift.com/2023/02/06/european-aviation-regulators-shut-down-proposal-to-fly-with-just-one-pilot/

GDPR-info.eu (n.d.) General Data Protection Regulation https://gdpr-info.eu/

Geeksvana (2023, 16 June) Fixed Penalties COMING for UK DRONES! Youtube https://www.youtube.com/watch?v=V7UEvwG3vx4

Glukhin v Russia No. 11519/20 (2023) European Court of Human Rights https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-225655%22]}

Gov.UK (n.d.) Biometrics and Surveillance Camera Commissioner https://www.gov.uk/government/organisations/biometrics-and-surveillance-camera-commissioner

Gov.UK (n.d.a) Data Protection https://www.gov.uk/data-protection

Gov.UK (2023) Drones, DNA losses and mission creep feature in OBSCC annual report https://www.gov.uk/government/news/drones-dna-losses-and-mission-creep-feature-in-obscc-annual-report

Gov.UK (2023a, 23 October) New prison ‘no-fly zones’ for drug-delivering drones https://www.gov.uk/government/news/new-prison-no-fly-zones-for-drug-delivering-drones#:~:text=By%20creating%20a%20virtual%20'no,security%20by%20preventing%20illegal%20filming.

Gov.UK (2023b, 29 October) Police urged to double AI-enabled facial recognition searches https://www.gov.uk/government/news/police-urged-to-double-ai-enabled-facial-recognition-searches

Gov.UK (2021) Surveillance Camera Code – summary of consultation responses https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1035078/SC_Code_-_summary_of_consultation_responses_2021.pdf

Greenberg A (2023, 2 March) This Hacker Tool Can Pinpoint a DJI Drone Operator’s Exact Location. Wired https://www.wired.com/story/dji-droneid-operator-location-hacker-tool/

Greenberg D (2022) Drones, Overview. Thompson Reuters https://uk.westlaw.com/Document/I4588F0F01FCD11E9907CE38C3F60FB33/View/FullText.html

Hartmann, J., Jueptner E, Matalonga A, Riordan J, White S (2022) Artificial Intelligence, Autonomous Drones and Legal Uncertainties. European Journal of Risk Regulation, 1–18 doi:10.1017/err.2022.15

Haylen A (2019) Civilian Drones. House of Commons Library https://commonslibrary.parliament.uk/research-briefings/cbp-7734/

High Speed Two (HS2) Limited *and Secretary of State for Transport v Persons Unknown and ors* [2022] EWHC 2360) https://www.bailii.org/cgi-bin/format.cgi?doc=/ew/cases/EWHC/KB/2022/2360.html

HM Government (2023) National Risk Register, 2023 edition https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1175834/2023_NATIONAL_RISK_REGISTER_NRR.pdf

HM Government (2022) Advancing airborne autonomy Commercial drones saving money and saving lives in the UK https://www.gov.uk/government/publications/advancing-airborne-autonomy-use-of-commercial-drones-in-the-uk

HM Government (2019) UK Counter-Unmanned Aircraft Strategy. CP 187 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/840789/Counter-Unmanned_Aircraft_Strategy_Web_Accessible.pdf

HM Government (2019a) A guide to using artificial intelligence in the public sector https://www.gov.uk/government/collections/a-guide-to-using-artificial-intelligence-in-the-public-sector

Holmes v Medway Council [2018] 6 WLUK 702 https://uk.westlaw.com/Document/I4588F0F01FCD11E9907CE38C3F60FB33/View/FullText.html

Home Office (2023) Public Order Bill: factsheet https://www.gov.uk/government/publications/public-order-bill-overarching-documents/public-order-bill-factsheet

Home Office (2021) Surveillance Camera Code of Practice https://assets.publishing.service.gov.uk/media/619b7b50e90e07044a559c9b/Surveillance_Camera_CoP_Accessible_PDF.pdf

Home Office (2019) UK Counter-Unmanned Aircraft Strategy https://www.gov.uk/government/publications/uk-counter-unmanned-aircraft-strategy

House of Commons (2022) Draft legislation: The Air Navigation (Amendment) Order 2022 https://www.gov.uk/government/speeches/draft-legislation-the-air-navigation-amendment-order-2022

House of Lords (2015) Civilian Use of Drones in the EU - European Union Committee Contents https://publications.parliament.uk/pa/ld201415/ldselect/ldeucom/122/122.pdf

HS2 (2023) HS2 route-wide injunction https://www.hs2.org.uk/in-your-area/hs2-route-wide-injunction/

ICAO (n.d.) The International Civil Aviation Organization. Drone enable https://www.icao.int/safety/ua/Pages/default.aspx

Information Commissioner's Office (n.d.a) A guide to the data protection exemptions https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/exemptions/a-guide-to-the-data-protection-exemptions/

Information Commissioner's Office (n.d.b) What we do https://ico.org.uk/about-the-ico/what-we-do/

Information Commissioner's Office (n.d.c) Additional considerations for technologies other than CCTV https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/guidance-on-video-surveillance-including-cctv/additional-considerations-for-technologies-other-than-cctv/#uas

Information Commissioner's Office (n.d.d) CCTV and Video Surveillance https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/

Information Commissioner's Office (n.d.e) A guide to controllers and processers https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/controllers-and-processors/controllers-and-processors-a-guide/

Information Commissioner's Office (n.d.f) Right to erasure https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/right-to-erasure/#:~:text=individual%20for%20ID%3F-,What%20is%20the%20right%20to%20erasure%3F,time%20the%20request%20is%20received.

Information Commissioner's Office (n.d.g) Special Category data https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/lawful-basis-for-processing/special-category-data/

Information Commissioner's Office (n.d.h) Guidance on AI and data protection https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/

Informational Commissioner's Office (n.d.i) What is personal data? https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/personal-information-what-is-it/what-is-personal-data/what-is-personal-data/ (last accessed 14 August 2023)

Information Commissioner's Office (n.d.j) Key data protection terms you need to know https://ico.org.uk/for-organisations/sme-web-hub/key-data-protection-terms-you-need-to-know/ (last accessed 15 August 2023)

Information Commissioner's Office (n.d.k) What is a DPIA? https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/what-is-a-dpia/ (last accessed 4 August 2023)

International Working Group on Data Protection in Telecommunications (2018) Working paper on privacy and artificial intelligence https://www.bfdi.bund.de/SharedDocs/Downloads/EN/Berlin-Group/20181130_WP_Artificial-Intelligence.html?nn=355094

Jackman A (2023) UK Commercial Drone Industry: Professional, responsible and considerate drone use https://research.reading.ac.uk/drone-geographies/wp-content/uploads/sites/271/2023/10/Industry_report.pdf

Jackman A (2023a) Police Drones: Uses, Challenges, Futures https://research.reading.ac.uk/drone-geographies/wp-content/uploads/sites/271/2023/09/Police-report.pdf

Jackman A (2019) Consumer drone evolutions: trends, space, temporalities, threats. *Defense & Security Analysis*, 35 (4), 362-383

Kan M (2023, 21 February) Microsoft Researchers Are Using ChatGPT to Control Robots, Drones. PC Mag https://uk.pcmag.com/news/145540/microsoft-researchers-are-using-chatgpt-to-control-robots-drones

Law Commission (2022) New project to examine the legal implications of increased autonomy in aviation https://lawcom.gov.uk/new-project-to-examine-the-legal-implications-of-increased-autonomy-in-aviation/

Lawler R (2021) US Treasury claims DJI assists Chinese surveillance of Uyghurs and blocks investments https://www.theverge.com/2021/12/16/22839970/dji-chinese-military-industrial-complex-investment-blacklist

LexisNexis (2023) Mens rea definition https://www.lexisnexis.co.uk/legal/glossary/mens-rea#:~:text=What%20does%20Mens%20rea%20mean,statute%20or%20the%20common%20law.

Liberty (n.d.) Legal Challenge: Ed Bridges v South Wales Police https://www.libertyhumanrights.org.uk/issue/legal-challenge-ed-bridges-v-south-wales-police/#:~:text=The%20judgment%20means%20the%20police,were%20breached%20as%20a%20result

Liszewski A (2023) Man Sets New Speed Record for the World's Fastest Drone https://gizmodo.com/ryan-lademann-new-record-for-the-worlds-fastest-drone-1850000565#:~:text=The%20FAA%20limits%20the%20speed,or%20drone%2C%20to%20100%20MPH.

Local Government Lawyer (2020) Will local authorities become airspace planners? https://www.localgovernmentlawyer.co.uk/regulatory-and-enforcement/190-regulatory-features/42706-will-local-authorities-become-airspace-planners

Mantas E, Patsakis C (2022) Who watches the new watchmen? The challenges for drone digital forensics investigations. Array, 1000135, 1-8

Martins BO, Holland Michel A, Silkoset A (2020) Countering the Drone Threat: Implications of C-Uas Technology for Norway in an EU and NATO Context. PRIO Paper. Oslo: PRIO https://www.prio.org/publications/12245

Marzohhi O (2015) Privacy and Data Protection Implications of the Civil Use of Drones https://www.europarl.europa.eu/RegData/etudes/IDAN/2015/519221/IPOL_IDA(2015)519221_EN.pdf

MBR Acres v Free the MBR Beagles (2021) EWHC 2996 (QB)https://www.bailii.org/cgi-bin/format.cgi?doc=/ew/cases/EWHC/QB/2021/2996.html

MBR Acres v Free the MBR Beagles (2022) WWHC 3338 (KB) https://www.bailii.org/cgi-bin/format.cgi?doc=/ew/cases/EWHC/KB/2022/3338.html

McLachlan S, Dube K, Schafer B, Gillespie A, Fenton N (2022) The Chaotic State of UK Drone Regulation https://arxiv.org/ftp/arxiv/papers/2205/2205.01041.pdf

Mercer D (2019, 23 February) Revealed: Drones used for stalking and filming cash machines in the UK. https://news.sky.com/story/police-warn-drone-users-after-incidents-soar-by-40-in-two-years-11637695

MIC (2019, 19 September) Drones are now being weaponized by abusive exes https://www.mic.com/impact/how-drones-are-being-weaponized-used-to-stalk-harass-people-18784714

Microsoft (2023, 21 February) ChatGPT + Real Drone. Youtube https://www.youtube.com/watch?v=i5wZJFb4dyA

Mills & Reeve (2016, 2 December) Drones - the key legal issues https://www.mills-reeve.com/insights/blogs/technology/december-2016/drones-the-key-legal-issues

Mousinho, IA (2022) Chapter 41: United Kingdom, in Scott, BI (ed) The Law of Unmanned Aircraft Systems, second edition. Wolters Kluwer, pp.497-506

National Protective Security Authority (n.d.) Countering Threats from Unmanned Aerial Systems https://www.npsa.gov.uk/countering-threats-unmanned-aerial-systems-uas (last accessed 09 August 2023)

NATs (2022) South of the clouds: The next generation of uncrewed aviation. Prepared by BVLOS Operations Forum https://www.nats.aero/wp-content/uploads/2023/03/WhitePaper_South_of_the_clouds_March23.pdf

Nawaz SA (2023, 9 August) Hallucinations and Existential Threats — Yet More Power to AI. PRIO blogs https://blogs.prio.org/2023/08/hallucinations-and-existential-threats-yet-more-power-to-ai/

Ofcom (n.d) Rules on using radio equipment https://www.ofcom.org.uk/spectrum/rules

Office of the biometrics and surveillance camera commissioner (2023) Commissioner for the Retention and Use of Biometric Material Annual Report January 2021 – March 2022 And Surveillance Camera Commissioner Annual Report March 2021 – March 2022 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1135384/Biometrics__Surveillance_Camera_Commissioner_Annual_Report_21-22.pdf

Online Safety Act 2023 https://www.legislation.gov.uk/ukpga/2023/50/enacted

Parliamentary Bills (n.d) Data Protection and Digital Information (No. 2) Bill https://bills.parliament.uk/bills/3430

PC Guide (2023, 1 December) What is Chat GPT? Everything you need to know https://www.pcguide.com/apps/what-is-chat-gpt/

Pickering v Rudd (1815) 4 Camp 216 https://www.bailii.org/cgi-bin/format.cgi?doc=/ew/cases/EWHC/KB/1815/J43.html

PJS v News Group Newspapers Ltd [2016] UKSC 26 https://www.bailii.org/cgi-bin/format.cgi?doc=/uk/cases/UKSC/2016/26.html

Police Act 1996 https://www.legislation.gov.uk/ukpga/1996/16/section/89/enacted

Police, Crime, Sentencing and Courts Act 2022 https://www.legislation.gov.uk/ukpga/2022/32/part/3/crossheading/public-nuisance/enacted

POSTnote (2020) Misuse of civilian drones, 610 https://researchbriefings.files.parliament.uk/documents/POST-PN-0610/POST-PN-0610.pdf

POSTnote (2015) Automation in military operations, 511 https://post.parliament.uk/research-briefings/post-pn-0511/#:~:text=This%20POSTnote%20outlines%20current%20and,future%20lethal%20autonomous%20weapons%20systems

Practical Law (2023) Drones: Law in the UK. Simon Phippard, Bird & Bird https://uk.practicallaw.thomsonreuters.com/8-618-5239?transitionType=Default&contextData=(sc.Default)&firstPage=true

Practical Law (n.d.) Mens Rea https://uk.practicallaw.thomsonreuters.com/w-002-9006?transitionType=Default&contextData=(sc.Default)#:~:text=Latin%20for%20%22guilty%20mind.%22,Knowingly.

Precision Hawk (n.d.) Beyond the edge https://www.precisionhawk.com/sensors/advanced-sensors-and-data-collection/

PricewaterhouseCoopers (2022) Skies without limits v2.0 https://www.pwc.co.uk/intelligent-digital/drones/skies-without-limits-2022.pdf

PricewaterhouseCoopers (2019) Building Trust in Drones https://www.pwc.co.uk/intelligent-digital/drones/building-trust-in-drones-final.pdf

Privacy International (2020) King's Cross has been watching you – and the police helped (25 June 2020)

Protect UK (2022) Threat from Drones in the UK https://www.protectuk.police.uk/threat-risk/threat-analysis/threat-drones-uk

Protection of Freedoms Act (2012) https://www.legislation.gov.uk/ukpga/2012/9/contents

Public Order Act 2023 https://www.legislation.gov.uk/ukpga/2023/15/enacted

Purshouse J, Campbell L (2019) Privacy, crime control and police use of automated facial recognition technology. Criminal Law Review, 2019(3), 188-204. Accepted manuscript accessible via: https://research-portal.uea.ac.uk/en/publications/privacy-crime-control-and-police-use-of-automated-facial-recognit

Regulation of Investigatory Powers Act (2000) https://www.legislation.gov.uk/ukpga/2000/23/contents

Reuters (2019, 20 December) Commercial pig farm in China jams drone signal to combat swine fever crooks https://www.reuters.com/article/china-swinefever-idUSL4N28U0QB (20/12/2019)

Richardson A (2017, 16 August) Deadly Black Mamba drug being flown into Staffordshire prison by drones. Birmingham Live https://www.birminghammail.co.uk/news/midlands-news/deadly-black-mamba-drug-being-13485473

Rogers J (2021) Future Threats: Military UAS, Terrorist Drones, and the Dangers of the Second Drone Age, in A comprehensive approach to countering unmanned aircraft systems https://www.japcc.org/chapters/c-uas-future-threats-military-uas-terrorist-drones-and-the-dangers-of-the-HYPERLINK "https://www.japcc.org/chapters/c-uas-future-threats-military-uas-terrorist-drones-and-the-dangers-of-the-second-drone-age/"second-drone-age/

Shackle S (2020, 1 December) The mystery of the Gatwick drone. The Guardian https://www.theguardian.com/uk-news/2020/dec/01/the-mystery-of-the-gatwick-drone

Singh I (2021, 26 April) AI-powered facial recognition drones track criminals in UAE. DroneDJ https://dronedj.com/2021/04/26/facial-recognition-drones-sharjah-police/

Sky News (2019, 13 September) Heathrow protest fails to take off as drones 'blocked by signal jammers' https://news.sky.com/story/heathrow-drone-protesters-blocked-by-signal-jamming-as-two-arrested-11808171

Taylor, D (2023, 20 September) HS2 granted route-wide injunction to tackle environmental protests. The Guardian https://www.theguardian.com/uk-news/2022/sep/20/hs2-high-speed-rail-route-injunction-to-tackle-environmental-protests

Thames Valley Police (n.d.) Drones https://www.thamesvalley.police.uk/advice/advice-and-information/drones/drones/ (Last accessed 8 June 2023)

The Air Navigation (Restriction of Flying) (Nuclear Installations) Regulations 2016 https://www.legislation.gov.uk/uksi/2016/1003/made

The Air Navigation (Restriction of Flying) (Prisons and Young Offenders Institution) (2023/1101) https://www.legislation.gov.uk/uksi/2023/1101/contents/made

The Carraige by Air Acts (2002) https://www.legislation.gov.uk/uksi/2002/263/contents/made

The Guardian (2023) BT invests £5m in plan for ‘drone superhighway’ across southern England https://www.theguardian.com/business/2023/jan/04/bt-invests-5m-in-plan-for-drone-superhighway-across-southern-england (04 January 2023)

UK Drone Watch (2020, 2 November) Benchmarking police use of drones in the UK https://dronewars.net/2020/11/02/benchmarking-police-use-of-drones-in-the-uk/

Vidal Hall v Google Inc [2015] EWCA Civ 311, [2016] QB 1003 https://www.bailii.org/cgi-bin/format.cgi?doc=/ew/cases/EWCA/Civ/2015/311.html

Weitz R (2023, 12 January) More can be done to ban US government use of Chinese drones. Defense News https://www.defensenews.com/opinion/commentary/2023/01/12/more-can-be-done-to-ban-us-government-use-of-chinese-drones/

Westminster Business Forum (2023, 31 January) Next steps for drone regulation and use in the UK https://www.scotlandpolicyconferences.co.uk/forums/agenda/Drones-23-agenda.pdf

Wheldon Law (n.d) The fundamental differences between criminal law and civil law in the UK https://wheldonlaw.co.uk/the-fundamental-differences-between-criminal-law-and-civil-law-in-the-uk/ (last accessed 03 August 2023)

Wired (2021, 5 November) A Drone Tried to Disrupt the Power Grid. It Won't Be the Last https://www.wired.com/story/drone-attack-power-substation-threat/

Wireless Telegraphy Act 2006 https://www.legislation.gov.uk/ukpga/2006/36

Zeeberg A (2023, 4 April) A tiny blog took on big surveillance in China – and won. Wired (April 4 2023) https://www.wired.com/story/surveillance-china-security-camera-giant-ipvm/

Annex

Annex 1: Further information about Data Protection law in the UK

- The General Data Protection Regulation 'lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data' and 'protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data' (Article 1, Regulation (EU) 2016/679). The GDPR 'does not apply to: the processing of personal data by an individual in the course of a purely personal or household activity' (Article 2, Regulation (EU) 2016/679) (GDPR-info n.d).
- In the context of drones, the Data Protection Act 2018 adds that 'part 2 supplements the GDPR' and 'applies a broadly equivalent regime to certain types of processing to which the GDPR does not apply (see Chapter 3)'. Chapter 3 (21) states that 'this Chapter does not apply to the processing of personal data by an individual in the course of a purely personal or household activity' (Data Protection act 2018).
- The 'Data Protection Act 2018 controls how your personal information is used by organisations, businesses or the government' (Gov.UK n.d.a). Those 'responsible for using personal data' must 'follow strict rules called data protection principles', which ensure that personal data is used:
    - fairly, lawfully and transparently;
    - for specified, explicit purposes;
    - in a way that is adequate, relevant and limited to only what is necessary;
    - accurate and, where necessary, kept up to date;
    - Kept in a form which permits identification of the data subject for no longer than is necessary and
    - handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage.

(Gov.UK n.d.a, (Article 5 GDPR)).

- As with GDPR, under the Data Protection Act 2018, 'you have the right to find out what information the government and other organisations store about you' (Gov.UK n.d.a). This includes the right to:
    - Be informed about how your data is being used
    - Access your personal data
    - Have incorrect data updated
    - Have data erased
    - Stop or restrict the processing of your data
    - Data portability
    - Object to how your data is being processed.
- There are additional rights where data is being used for automated processing or profiling.
- Where an exemption applies, compliance with GDPR is not required. Whether or not you can rely on an exemption often depends on why you process personal data' and 'if no exemption covers what you do with personal data, you need to comply with the UK GDPR as normal' (Information Commissioner's Office n.d.a). Exemptions are considered on a case by case basis and include provisions relating to:
    - Crime, law and public protection
    - Regulation, parliament and the judiciary
    - Journalism, research and archiving
    - Health, social work, education and child abuse
    - Finance, management and negotiations
    - References and exams

- Subject access requests where information about other people is requested
- National security and defence.

(Information Commissioner's Office n.d.a).

The exemptions most likely to affect drone usage are those relating to journalism, academia, art and literature and research.

Annex 2: UK General Data Protection Regulation (GDPR) guidance: The Information Commissioner's Office

- '**Personal data**' is 'information relating to an identified or identifiable natural person ('data subject')'. An 'identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person" (Information Commissioner's Office n.d.i). (UK GDPR article 4(1)).
- A '**data subject**' refers to 'someone who can be identified from personal data', they are the 'subject of that data' (Information Commissioner's Office n.d.j) (UK GDPR Article 4(1), Data Protection Act 2018 section 3(5)).
- The Information Commissioner's Office (ICO) distinguishes between a 'data controller' and a 'data processor'. A data controller 'has the responsibility of deciding how personal data is processed and protecting it from harm' (Information Commissioner's Office n.d.j). The data processor processes the data 'on behalf of the data controller', but still needs to 'protect people's private data' (Information Commissioner's Office n.d.j). 'Controllers can delegate the processing of personal data to data processors, but the responsibility for keeping it safe will still rest with the controller' (Information Commissioner's Office n.d.j).
- The ICO provides further information about **Data Protection Impact Assessments** (DPIA), stating that 'a DPIA is a process designed to help you systematically analyse, identify and minimise the data protection risks of a project or plan. It is a key part of your accountability obligations under the UK GDPR, and when done properly helps you assess and demonstrate how you comply with all of your data protection obligations' (Information Commissioner's Office n.d.k). Crucially, conducting a DPIA is 'a legal requirement for any type of processing, including certain specified types of processing that are likely to result in a high risk to the rights and freedoms of individuals. Under UK GDPR, failure to carry out a DPIA when required may leave you open to enforcement action' (Information Commissioner's Office n.d.c). Undertaking a DPIA and 'considering the risks related to your intended processing before you begin' supports compliance with another general obligation under UK GDPR: data protection by design and default, which per article 25 states that: 'the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures… and… integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects' (Information Commissioner's Office n.d.k). Please note that the proposed Data Protection and Digital Information (No. 2) Bill would replace DPIAs with risk assessments, but at present the law remains DPIAs.

Annex 3: Definitions: Criminal and civil law

Criminal law refers to 'the activities that UK Acts of Parliament have prescribed as either acceptable or unacceptable' and 'relates to offences that have a negative impact on society as a whole rather than on a single individual' (Wheldon Law n.d). When an individual is suspected of

‘committing a criminal offence’ they will typically be ‘investigated by the police’, which ‘could result in a criminal prosecution’ (Wheldon Law n.d). Criminal proceedings can be ‘brought by the Crown Prosecution Service (CPS)’ or relevant ‘parties with specific interests’, and if a ‘defendant is found guilty, the court will impose a penalty’ per relevant ‘sentencing guidelines’ (Wheldon Law n.d).

Civil law typically involves ‘disputes between individuals or between individuals and organisations’ and ‘relates to offences that harm another person and their rights or property’ (Wheldon Law n.d). Civil cases seek to ‘settle disputes and establish whether the defendant [accused] had a responsibility or duty of care towards the claimant [bringing the claim]’ (Wheldon Law n.d). Following a civil case, ‘no one is sent to prison’, however if ‘found liable’ ‘in a court or tribunal’ (as initiated by the claimant, a private party) the defendant ‘may be ordered to pay compensation in the form of damages’ (Wheldon Law n.d).

In sum, criminal law can be understood as ‘seeking to punish for an offence’ and civil law as seeking to ‘achieve a remedy (e.g. compensation) for the injured party’ (Slater and Gordon Lawyers n.d). It should be noted that an individual can face both criminal and civil action at the same time.

Figure list

About the authors
Dr Anna Jackman is Lecturer at the University of Reading.
Louise Hooper is a Barrister at Garden Court Chambers.

Acknowledgements
This report forms part of Dr Jackman's Diversifying Drone Stories research grant (ES/W001977/1). Funded by the *Economic and Social Research Council (ESRC),* the project explored the use, perception and impact of drones in changing UK airspace, engaging with diverse stakeholders (including lawyers, emergency services, industry, pilots, air traffic controllers, local authorities, regulators, policy-makers, and members of the public) to understand different uses and experiences. The report's authors would like to sincerely thank the participants from the legal community that gave their time to contribute to the research. This work is available under a Creative Commons Attribution CC-BY License (information about CC licenses).

Citation
Any material quoted from the report should cite the report's source. To cite the report, please use the following citation: Jackman A, Hooper L (2023) Drone incidents and misuse: Legal considerations, https://research.reading.ac.uk/drone-geographies/wp-content/uploads/sites/271/2023/12/Drone-incidents_Jackman-Hooper.pdf