Mapping the complexity of legal challenges for trustworthy drones on construction sites in the United Kingdom

Joshua Krook *

School of Electronics and Computer Science, University of Southampton, J.A.Krook@soton.ac.uk

David Bossens

Center for Frontier AI Research, Agency for Science, Technology and Research, David_Bossens@cfar.a-star.edu.sg

Sergio Araujo-Estrada

Department of Aeronautics and Astronautics, University of Southampton, S.Araujo-estrada@soton.ac.uk

Peter Winter

School of Sociology, Politics and International Studies, University of Bristol, Peter.Winter@bristol.ac.uk

John Downer

School of Sociology, Politics and International Studies, University of Bristol, John.Downer@bristol.ac.uk

Shane Windsor

School of Civil, Aerospace and Design Engineering, University of Bristol, Shane.Windsor@bristol.ac.uk

Drones, unmanned aircraft controlled remotely and equipped with cameras, have seen widespread deployment across military, industrial, and commercial domains. The commercial sector, in particular, has experienced rapid growth, outpacing regulatory developments due to substantial financial incentives. The UK construction sector exemplifies a case where the regulatory framework for drones remains unclear. This article investigates the state of UK legislation on commercial drone use in construction through a thematic analysis of peer-reviewed literature. Four main themes, including opportunities, safety risks, privacy risks, and the regulatory context, were identified along with twenty-one sub-themes such as noise and falling materials. Findings reveal a fragmented regulatory landscape, combining byelaws, national laws, and EU regulations, creating business uncertainty. Our study recommends the establishment of specific national guidelines for commercial drone use, addressing uncertainties and building public trust, especially in anticipation of the integration of 'autonomous' drones. This research contributes to the responsible computing domain by uncovering regulatory gaps and issues in UK drone law, particularly within the often-overlooked context of the construction sector. The insights provided aim to inform future responsible computing practices and policy development in the evolving landscape of commercial drone technology.

CCS CONCEPTS • Applied computing --> Law, social and behavioural sciences • Computing Methodologies --> Artificial Intelligence • Social and professional topics

Additional Keywords and Phrases: Unmanned Aerial Vehicles, Drones, Artificial Intelligence, Construction Sites, Trustworthy Autonomous Systems

---

* This research was funded by the UKRI Trustworthy Autonomous Systems Hub EP/V00784X/1 and the UKRI Trustworthy Autonomous Systems Node in Functionality (EP/V026518/1).

1 Introduction

The construction industry literally and figuratively shapes the fabric of our society. From the homes we live in to the places we work, we are shaped by our built environment just as we shape it around us. So it is, as the United Kingdom (UK) Government has declared, that construction affects "every person in Britain" [1]. The introduction of new technologies into the construction industry, therefore, has the potential to affect everyday people, depending on how these technologies are used. The vision of Industry 4.0, imagined by the International Business Machines (IBM) corporation and others [2], includes big data, surveillance, and drones, or unmanned aerial vehicles (UAVs), creating a different kind of society.[1] A 'digital' society where technology constructs our environment, and therefore, our experience of that environment.

Emerging technologies present great opportunities for society, and yet pose distinct risks depending on how they are used, misused, and regulated. The use of drones in construction exemplifies this tension as we will present in the following article.

The UK government has expressed interest in harnessing the benefits of the so-called "Third Aviation Revolution": the revolutionary changes in new technology that have allowed for autonomous flight of drones and other unmanned aircraft, including their potential commercial use [3]. So far, public consultations have been held by the UK government on the future of drone use across a range of sectors and circumstances, in both rural and urban settings [4, 5]. However, the UK regulatory regime remains a patchwork of competing byelaws, national laws, and incorporated European Union (EU) regulations. While the EU is imagining a "Single European Sky," the UK has created a bottleneck approval system for the commercial use of drones, on a case-by-case basis, through the Civil Aviation Authority (CAA). Some commentators describe UK drone laws as "chaotic," [6] while others have pressed for closer cooperation between industry and regulators to create a clearer legal framework for commercial drone deployment [7].

In this article, we conduct a literature synthesis that covers both dialogic formats and research in order to examine the legal challenges of using drones in the UK. We consider the following research questions, with a specific focus on the UK with the overall goal of informing legal and policy interventions:

> (1) *What is the state of UK legislation with regard to ensuring trustworthiness of drones on construction sites?*
>
> (2) *What changes are required in the UK's legal and policy landscape to ensure that the use of drones on construction sites remain safe and adhere to privacy principles?*
>
> *(3) How do varying degrees of automation influence law and policy in and around drones on construction sites?*

These questions are reviewed with an eye on deployment contexts in construction, including on-site transportation of materials, monitoring for security purposes, safety inspection, and trespasser detection.

This article begins by outlining how we selected our literature and the research question (Section 2), before moving onto a thematic analysis of the literature where we present the main themes (Section 3). These include: (i) Opportunities for construction; (ii) Privacy Risks; (iii) Safety Risks; and (iv) Regulatory Context in the UK (Section 4), along with twenty-one sub-themes. We then discuss these findings (Section 5), drawing out common themes across the literature. In doing so, we also identify specific gaps and recommendations in national law. Section 6 then presents our main conclusions and explores the potential for future research in this area.

---

[1] The movement towards Industry 4.0 involves "integrating new technologies, including Internet of Things (IoT), cloud computing and analytics, and AI and machine learning" - *What is Industry 4.0? IBM* (2022) <https://www.ibm.com/uk-en/topics/industry-4-0>.

2. Methodology

The authors conducted a literature synthesis on the topic of regulating drones on construction sites. A literature synthesis, also known as a ‘rapid review’, is a type of literature review suitable for emerging research topics where systematic reviews are not yet feasible [65 - 67]. Instead of comprehensively mapping a field, a rapid review attempts to gather disparate, emergent sources on a topic [65]. The state of the literature on drones working on construction sites is still in its infancy, hence a rapid review is productive in this context. Given the limited literature on the topic we drew from a range of different sources (law, computer science, robotics, policy, and safety). Such transdisciplinary engagement works well for a new and emerging field with fewer sources because it can help “grasp the complexity of the problem” [68] by providing insights of potential and current drone use in diverse contexts.

We chose to focus on the UK as our source of law for multiple reasons. The review required a country where the deployment of drones on construction sites was viewed as a foreseeable event and eventual reality. For instance, the UK government has already commissioned reports, guidelines, and community consultations on drone safety. Such steps may be read as precursors to future commercial drone regulation [29]. Indeed, the UK is placed at the top of the ‘Drone Readiness Index’ for regulation from Drone Industry Insights (a global data company on commercial drone use based in Hamburg, Germany) (2022) [69]. The UK has an existing private drone market (for private use, such as filmmaking and research), a small commercial market (for commercial filming and surveying), and a strong capacity for commercial drone uptake in the future [70]. The UK government is actively pursuing a strategy to increase the uptake of drones for commercial purposes across a variety of sectors, including construction, agriculture, real estate, film and entertainment, and delivery services [29]. Our literature synthesis also includes peer reviewed sources from the United States and Australia where drone use and safety are an ongoing concern, in order to supplement the UK sample.

2.1 Literature Search Strategy

A search strategy was developed and an electronic database search of ACM Digital Library, Google Scholar, GOV.UK, and websites such as the UK Civil Aviation Authority was conducted from 1 Jan 2002 until 20 March 2023, with early dates used for context, background and case law. The key search terms included the following: (1) ‘drones on construction sites’, ‘the regulation of drones’, ‘drone safety in construction’, ‘drone privacy’, ‘drone safety’ and ‘unmanned aerial vehicles (UAVs)’. We looked for UK government policy documents on drones, regulation, legislation and cases pertaining to ‘drone safety’, ‘drone privacy’ and ‘risks of harm from drone usage’. Our search output identified 93 studies of which 90 were appropriate for full review. Our search strategy is compiled in Table 1, and a complete list of sources is in the bibliography. Note that sources relating to methodology and relevant law sources (e.g., Lifting Operations and Lifting Equipment Regulations 1998 (LOLER)) are not included in the overall count.

Table 1: Search Strategy

Sources Considered	Type:	Academic journal articles, government reports, legislation, cases, media reports
	Language:	English or English translation
	Issuer:	Academic journals, government or affiliated institutions, media organisations or consultancies
Sources Included	Which refer to:	“drones on construction sites,” “the regulation of drones in construction,” “drone safety in construction,”

		or thematically equivalent.
	Which refer to:	“Unmanned Aerial Vehicles (UAVs) on construction sites,” or thematically equivalent.
	Which refer to:	“drone safety,” “drone privacy,” “risk of harm by drones,” or thematically equivalent.

2.2 Data Extraction

Data extraction was achieved through full text reading by the first author via a systematic mapping of drones in the construction site landscape. Each of the co-authors supported the extraction process and organised the literature into categories of ‘opportunities’ and ‘risks’ which were checked and modified in an iterative process. In a final set of data extraction, categories (e.g. regulations, drone policy) were reviewed by the team of co-authors who provided verification of categories, sub categories and the inclusion of a new, emergent category: ‘gaps in the law (UK)’. In this assessment, perspectives of the authors and findings from the literature were included in our discussion section. We found the existing literature on drone use more broadly to be especially useful when writing the discussion section given the lack of empirical research on drones in the context of construction sites.

2.3 Thematic Analysis of the literature

After we categorised the literature according to their opportunities and risks, we counted the number of categories and built them up into common themes, as shown by the results of Table 3: Thematic Analysis of the Literature. This process revealed a narrow range of conceptual and empirical studies on the topic of drones on construction sites. Consequently, we drew on the wider drone literature in law, computer science, engineering, and related fields to help answer our research questions and applied these findings to the context of construction sites - an important yet under researched space to understand opportunities and legal problems especially between and among states, countries and national jurisdictions. Indeed, the literature was enriched by considering different jurisdictions. Different jurisdictions allowed us to see how other major economies around the globe are tackling problems associated with drones across numerous sites and contexts, especially when it came to addressing our related research questions on drone regulation. Having analysed the literature, we identified four major themes: (1) opportunities for construction; (2) privacy risks, (3) safety risks, and (4) the regulatory context. These themes were broken down into sub-themes (such as cost savings, privacy regulations, cybersecurity etc) and presented in Table 3. The rest of the article has been broken down into opportunities (Section 3.1), Risks (Section 3.2), and a comprehensive analysis of the UK regulatory context (Section 4), bringing together the various sub-themes in each category for the sake of readability. In addition, a new finding emerged from our analysis of theme 4 (‘Regulatory context’), which we label as ‘Gaps in UK Law’ and presented in column four in Table 3.

Table 2: Thematic Analysis of the literature

Themes	**Sources**
(1) Opportunities for Construction (n=18)	**Sub-themes** ● Cost Savings [11, 51, 52, 69, 70, 74] ● Time savings [52, 74] ● Safety benefits [52, 69, 70, 74, 97] ● Offshore / remote use cases [77, 78, 79, 80, 81, 82, 83]
(2) Privacy risks (n=34)	**Sub-themes** ● Privacy in Applied Settings [4, 10, 13, 17, 24, 25, 60, 64, 97] ● Data protection [15, 84, 85, 86, 93, 94] ● Privacy breaching incidents [18, 19, 22] ● Human Rights [36, 37, 38, 39, 43]
(3) Safety risks (n=37)	**Sub-themes** ● Construction sector policies [1, 8, 9, 12] ● Adverse Weather [17, 24, 25] ● Drone Safety in Applied Settings [4, 10, 13, 17, 24, 25, 60, 64, 97] ● Cybersecurity [17, 23, 24] ● Interference with Other Aircraft [26, 27, 28] ● UAV Noise Profile [71, 72, 73, 74]
(4) Regulatory Context (n=49)	**Sub-themes** ● Privacy Regulations [14, 16, 20, 21, 36, 37, 38, 39, 40, 41, 42, 75, 76] ● Privacy by design [83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98] ● Health and Safety Regulations [44, 45, 46, 47, 48, 49, 50, 53, 54] ● Lifting, Work and Safety Regulations [55, 56, 57, 58, 59, 62, 63] ● Worker's Rights and Psychological Health [17, 76] ● Drone Policy and Drone Law [3, 4, 5, 6, 28, 29, 30, 31, 32, 33, 34, 35, 61, 71] ● Reports and public sector analysis [2, 7, 69, 70]
Key: **N = The number of identified sources for a particular theme. Note that duplicate sources have not been counted twice.**	

3. FINDINGS

3.1 Drones: Opportunities for the Construction Industry

Results of the literature review indicated a variety of opportunities, echoing future imaginaries inspired by the possibilities of autonomous technology. Given the narrow yet varied literature of drones on construction sites, we must look into the longer-term future of drone technology, the economy and society with the aim of identifying areas of strategic priorities and emerging governmental policy. An interesting observation in this case is the UK government's aim to halve the construction industry's construction time and emissions by 2025 [8]. Fundamental to this vision is the adoption of emerging drone technologies, such as Unmanned Aerial Vehicles (UAVs) [8]. UAVs or drones represent a myriad of opportunities for the construction sector. These included: cheaper and more efficient safety inspections [9], faster construction times [10], and potentially, cheaper delivery of construction materials [11]. As such, drones could be a major economic opportunity for the UK [1].

Drones are also said to provide opportunities that stretch beyond the economy. For example, one of the biggest claims in the literature is that drones have the potential to improve worker safety [9], where workers "falling from a height" account for 51% of construction fatalities in the UK [12]. Given how drones on construction sites have the potential to replace human workers who work at heights, or in tight spaces or other precarious circumstances (such as offshore or in hazardous environments), there is an opportunity to reduce worker fatalities [13]. With a view towards considering how drones might be developed with higher degrees of automation, we might say that 'autonomous' drones have further potential to minimise injury risks and time taken to work in precarious environments. Nevertheless, in the short term, the use of human-controlled drones on construction sites has the potential to improve safety on site, whilst reducing the cost and time of construction.

According to the literature, drones may also offer another means of improving safety and reducing risks on construction sites through monitoring safety compliance and helping to identify defects in a building's foundations [13]. Safety inspections prevent accidents before they occur, and a combination of human-drone teams could make these inspections more efficient and cost-effective [13]. High-definition cameras and the ability to offer aerial perspectives make drones particularly well suited for this task. Drones can provide "safe and direct views of the construction area" from locations which would otherwise be hard to reach, while also helping to monitor "safety hazards such as the status of job transport routes" [9].

The versatility of drones allows for significantly enhanced task monitoring. In some instances, drones can ensure safety compliance over vast quantities of land, as is necessary when inspecting oil and gas pipelines [7]. This reduces the cost of hiring human safety inspectors to cover such a large area, and it allows for human-machine teams to go beyond monitoring merely target areas that are at risk of deterioration or collapse, to other areas of lesser risk. It also allows for the monitoring of trespassers and intruders on a large area of land, without the necessity of hiring costly security [79]. The same is true in the monitoring of shipping and large vessels as they operate at sea [82], which could assist with offshore construction.

Safety and cost could particularly be improved in remote regions and offshore construction, which can often pose higher risks to human workers [82]. Using drones in offshore construction, such as to maintain offshore wind farms or to monitor coastal regions has been shown to decrease costs and safety risks to workers [77]. Drones may, for instance, have the potential to mitigate risks arising from adverse weather conditions during construction at sea. Although there is very little literature on this, analogous use-cases can be found with drones used for coastal water monitoring sending real-time data back to human operators to understand the effectiveness of anti-pollution measures, without risking human lives [78]. While the cited studies relied on humans-in-the-loop and semi-autonomous drones [77, 78], the move towards fully 'autonomous' drones could also have a stronger use-case in remote regions. Current line-of-sight regulations (covered below) mean that humans must be 'present' at least within viewing distance, whereas fully autonomous drones could operate in environments that are dangerous to humans (such as volcanic environments).

Furthermore, drones pose less of a safety risk themselves in offshore or remote environments where fewer humans are around to be hit by a falling or error-prone drone [81]. Although there is minimal literature on this in the construction sector, some literature does exist in the maritime sector [80, 81]. Applying this analogously, the research indicates that drones operating at sea pose less of a safety risk than drones operating in densely populated urban areas, such as London [81]. Maritime drones are also increasingly proving capable of performing complicated tasks at sea, such as collecting and testing large quantities of water samples [80], and have proven their capability to operate offshore in anti-piracy and naval operations [81]. It is foreseeable that these advancements might one day be applied in offshore construction, for example to construct wind turbines, oil platforms and so on. At the same time, offshore construction faces different regulatory challenges, such as the application of environmental law, and jurisdictional challenges, such as when drones operate across international territories or within international waters. Drones operating across territorial lines will face different legal regimes according to where the operator is based and where a drone incident or accident occurs. Remote operations also have to face the logistical hurdles of maintaining communication with a drone, line of sight to the drone or POV of the drone's own visual capacity, which can be impacted by adverse weather conditions [81].

Drones may also change traditional construction practices by replacing existing lifting devices such as cranes or pulley systems. Some commercial drones have the capacity to lift 200 kilos, which is well beyond the limits of a human labourer – meaning that they can serve a range of functions beyond monitoring [7]. Using drones as lifting tools could allow construction projects to replace human workers in hazardous environments [11]. For instance, drones could assist in delivering equipment and materials across landscapes that are difficult or dangerous for humans to traverse [11]. Although commercial drones are currently limited by their carrying capacity, early studies show that they have the potential to reduce delivery times, labour costs and vehicle costs, while bypassing traffic and other obstacles [11].

The use of drone 'swarms' could offer even greater benefits by overcoming limitations faced by individual drones operating in isolation. A drone 'swarm' can be thought of as "a collection of multi-agent robot systems that exhibit emergent behaviour through interactions with each other and the environment" [99]. Drone swarms could conduct activities in concert to effectively coordinate the transportation of goods via emergent behaviour, such as making the fastest route selection. Increased carrying capacity means an increase in efficiency, fewer trips required, and the potential for carrying loads up to greater heights or to harder to access areas. Such coordinated behaviour in the lifting of heavy materials could reduce the risk of lifting injuries in labourers, therefore reducing the cost of healthcare and insurance costs for both companies and their staff. The speed and versatility of drones in everyday construction activities presents an opportunity for the more dangerous forms of construction to occur safely [10].

3.2 Drones: Risks for the construction industry

Our literature review identified a limited range of privacy risks and laws in regard to drone use on construction sites. Consequently, in order to address the dearth of privacy risks, we must turn our attention to existing privacy challenges that drones present in society. It is clear: the use of drones raises significant challenges to the privacy, civil liberties, and agency of individuals in society [14, 15]. For example, the literature highlights how drones have the potential to infringe on privacy laws in new ways, by spying through skylights, upper-level windows, on balconies and rooftops, in a manner that surpasses traditional CCTV equipment. The literature on drones in society also warns of the risk of "paparazzi in the skies," monitoring our daily behaviours [16]. High resolution cameras and real-time data analysis are said to have the potential to exacerbate the risk of privacy violations - including imagined futures with drones on construction sites posing risks to the privacy of workers, neighbours, and passers by. In addition it is not clear whether drones should monitor and feedback real-time information on workers to a control room curating potential punitive responses. Because of this, some authors paint a dystopian picture here of future cities where we live under the ever-watchful flying drones [15]. Drones used for construction surveillance may necessarily record a lot of other data, just by virtue of flying around in cities, and this data will need to be managed carefully to protect privacy.

While at first, this may appear farfetched, construction companies that deploy drones, may, in a similar manner, run the risk of creating their own surveillance system. Although there are many cameras in our environment, from phone cameras to CCTV, drone cameras can operate at height, and remain, therefore, relatively unnoticeable to those far below them. They can also spy through top-floor windows, skylights, and other hard-to-reach areas. This may have an adverse effect on the behaviour and working practices of labourers, through a centrally controlled system [17]. For example, drones that are 'autonomous' could monitor the work of labourers and report back to company bosses about work culture, work performance and worker behaviour [17]. This may lead to the fear of labourers feeling anxious and paranoid, which may be exacerbated if surveillance is conducted covertly. Such thoughts chime with previous studies which have found that the continuous surveillance of workplace practice increases worker stress [17]. Workers who are observed are likely to change their behaviour or suffer from psychological impacts verging on paranoia – which may itself cause accidents to occur [17]. The interference of drones in a worker's line of sight could also cause accidents due to sensory overload [17]. Under the WP29 Guidelines (EU), workplace surveillance might not be legal even if consented to by workers, because consent is not meant to be assumed or given in an employment context due to power differentials between employers and employees.

Any advanced form of workplace surveillance will also very likely face pushback from unions in the UK or work councils in Europe, who see surveillance as a breach of good working conditions [76]. The Trades Union Congress (UK) for example, states that "everyone is entitled to a private life, including at work," and that "monitoring must be done in a way that's not oppressive to staff" [76]. Surveillance that is oppressive and intrusive may fall afoul of various other laws, such as data protection laws, discussed in further detail below.

Members of society who live next to construction sites may also be filmed intentionally or unintentionally by drones. Drones can fly by windows, over balconies and onto rooftops and raise privacy concerns for people in compromising situations [18]. In Australia, in particular, there have been cases of privacy infringement concerning the use of drones in private life. For example, in the city of Darwin in 2017, a drone was caught filming a 27-year-old woman swimming nude in her secluded backyard pool [18]. In Sydney a month later, a drone was caught filming a woman showering in her fifth-floor apartment [19]. In the UK, case law will not necessarily protect those filmed by a drone, especially if the person did not already have "a reasonable expectation that the activity would be kept confidential" [20, 21]. Such an expectation might exist for someone in a fifth-floor apartment; however, the law posits a test for free expression:

> *"Even in cases that may be thought to involve a reasonable expectation of privacy, such as sexual activity, it is possible that there may be a countervailing right to free expression depending on the participants and the context of the relationship, such as where publication corrects a false image of a public figure"* [14].

The expectation of our private life remaining private is protected by certain legal frameworks. However, drones may bypass these frameworks due to technical loopholes in existing legislation – where certain circumstances have not been accounted for. Existing laws may focus on street-level surveillance by traditional CCTV cameras, rather than cameras in the sky. This means that companies or operators who obtain footage of people engaging in private actions or private spaces might be used, displayed or transmitted without consent. In 2014, Edward Snowden revealed that National Security Agency (NSA) workers frequently passed nude photos around the office [22]. These photos had been captured by government surveillance, and were not meant to be viewed publicly, but they were nevertheless shared amongst colleagues [22]. Snowden's discussion reveals the very human and social aspects of privacy violations, where authority figures succumb to moral failures and fail to treat their jobs, and the general public, with respect and dignity.

He described the situation as follows:

> "*You've got young, enlisted guys, 18 to 22 years old. They've suddenly been thrust into a position of extraordinary responsibility where they now have access to all of your private records. [They] stumble across something that is completely unrelated to their work [such as a nude photo of someone] in a sexually compromising situation. So, what do they do? They turn around in their chairs and they show their co-worker"* [22].

It is easy to imagine a similar situation arising on a construction site. For instance, workers in construction settings can collect nude images (photos or videos) of a nearby neighbour and pass these images around the working environment. Even if the law bans this practice, it is reasonable to presume that it may still occur, and that privacy violations could lead to actionable harm for neighbours. The use of drones in busy urban environments, such as London, raises the risk profile of these incidents occurring, particularly as drones can operate at heights that are unusual for other, more common-place surveillance, such as CCTV cameras. Drones can therefore spy on neighbours at unique angles, from harder-to-reach places, such as fifth-floor balconies, and are able to have a kind of versatility to monitor people's movements beyond static cameras (albeit static cameras can act in concert).

Cybersecurity is also an issue here – where unauthorised access to data could lead to the leaking of footage that was previously thought to be private, through password sharing or hacking attempts. In general, drones are vulnerable to hacking, interference, or software error, all of which could lead to accidents and/or breaches of privacy. For example, there is a potential for drones to be hacked for "nefarious purposes" [17, 23]. As drones operate via GPS and a Wi-Fi network to communicate, it is possible that "these navigation and communication networks are vulnerable to security breaches" [17, 23]. There have already been instances of drones being hacked or subjected to malicious attacks, such as "GPS spoofing attacks" [17, 23], for the purpose of "stealing sensitive information, spreading malicious programs, or UAV footage interception" [17].

More mundane interference, such as electromagnetic waves could also interfere with a drone's operations [24]. This risk becomes significant, for instance, for a commercial drone carrying up to 200 kilos of construction materials. In such a circumstance, safety features and/or criminal laws must exist to prevent a significant potential for injury. Electromagnetic interference can come from "cell phone towers, power lines, or steel structures, and might affect the drones' compass and GPS signal, which can cause errors or complete data loss" [24]. Other forms of nefarious interference include dangerous pranks. The use of lasers by teenagers to interfere with aircraft, for example, may transfer over to drone interference.

On a building site, drones can cause disruption to a worker's job by making unexpected noises or unexpected movements, falling from a height, or causing other objects to fall [17]. A study in Chile, for example, identified a major risk of drones falling on workers and colliding with building elements or other moving elements on site [24]. This is particularly significant in adverse weather conditions, such as heavy winds, rain or snow, or poor lighting conditions [17, 24, 25]. Drones that move very fast can generate gusts of wind, resulting in "particulate emissions from loose soil, dirt, sand or gravel stockpiles, which are quite common on construction sites" [17]. Any adverse conditions run the risk of disrupting the drone's sensors, causing potential harm to humans or damage to the drone itself [17]. The presence of numerous drones on construction sites might also distract workers, causing them to fall or injure themselves if working at a height [17]. There is currently limited research regarding the noise signature of UAVs, which are different in character from traditional forms of machinery. The public perception has, however, raised concerns of UAVs causing significant noise disruption of operating in swarms at low heights in urban areas [71, 72], and some research has tried to model software for optimal paths to reduce noise [72].The research indicates a mixed perception of drone noise and distraction on site. For workers, some perceived drones to be "obnoxious" while others reported they did not "feel the drones distract much since there are so many other noises on jobsites" [73]. Other researchers pointed out that drones can disrupt a worker from selective attention to a task that requires concentration [74]. There is a need for future research to classify the noise profile of UAVs to ascertain safe levels of noise, particularly for drones operating in swarms.

Drones may also pose an existential risk to civilian or military aircraft that fly above or near construction sites where drones are operating, such as near airports or urban centres. A joint study by the Department for Transport, Military Aviation Authority and the British Airline Pilots Association modelled the impact a drone would have if colliding with a windscreen of manned aircraft, including helicopters and commercial airlines [4]. The study found that even small drones of 400g could pose "a critical risk to the windscreens and tail rotors of helicopters" [4]. For commercial planes, the results were less severe, with only a drone of above 2kg causing "critical damage and only when airliners fly at higher speeds, which is commonly done at heights where these drones are not flown or can easily reach" [4]. Commercial airlines above 40,000 feet are well beyond the reach of a drone, and commercial airlines are already instructed to fly well above the London skyline, for example. Nevertheless, the study revealed that the risks to planes - at runways and other lower-level areas - are real and significant.

In late 2018, illegal drone activity near Gatwick Airport in the UK led to days of delays, cancellations of 800 flights and impacted 100,000 passengers [26]. Although no culprit was ever found, and the actual veracity of the drone sightings was never proven, the effects of the sightings were significant [27]. The Gatwick drone sighting has led to a generation of 'restriction zone' rules around airports in the UK, where drones are now unable to fly "within one kilometre of airport boundaries," and five kilometres from the ends and sides of a runway (Art. 94A(4) ANO) [14, 28]. Commercial drones can get permission from flight control to bypass these restrictions [29]. However, an imagined future of ubiquitous commercial drone use of delivering goods and services, would raise the risk of accidental entry into airport boundaries causing disruption to flights, damage to aircraft, and potential loss of life.

4. Regulatory Context

4.1 Drone Law and Policy

Despite the benefits and risks of drones, the UK's current regulatory regime has been described as "chaotic", with a pastiche of local byelaws, national laws, and leftover EU laws, all having slightly different guidelines and standards [6]. A move away from EU regulations may also occur in future, due to Brexit. Some scholars claim there is currently "overregulation, inconsistent regulation and regulatory disharmony" [6]. The book *Drone Law and Policy* goes into some of these arguments at length [4]. Patrick Slomski, a contributor to the book, and an expert in drone law at Clyde & Co law firm, suggests that a restrictive regulatory approach to drones has been a "barrier to widespread use", but there are efforts accelerating on the regulatory front, and that "we're at a tipping point [and we are likely to see progress] proceed much faster in the next couple of years" [7]. However, regulating millions of drones is no easy task given their diversity of form and function – spanning air, underwater, interior use, and underground – and the complex risks involved in each form of deployment [7].

The Civil Aviation Authority (CAA) manages the certification, licensing, and permit process for commercial aerial drone use in the UK. However, a lack of clarity and transparency on the requirements for commercial use creates a bottleneck where the CAA must approve diverse use-cases one by one. Commercial drone pilots can get exemptions for closeness restrictions, building inspections and first-person-view use, for example, but it is unclear when these exemptions will be given, and for what reasons. Maurice Thompson, editor of *Drone Law and Policy*, notes that regulators are aware of the lack of commercial guidance, but "there's an openness with industry… a lot of our clients have been surprised that when they turn up to a regulator's doorstep and say, 'we want to do this,' they actually get a pretty good dialogue to guide them" [7]. At the same time, this raises concern for why this guidance is not already public, in the form of norm-setting regulation.

In public consultations, the UK government has hinted at creating new regulatory frameworks for commercial drone usage, and yet, no new law is forthcoming [4, 5]. In 2017, the Department for Transport held a public consultation that aimed at "stimulating drone innovation and enterprise in the UK, ensuring safety and operation within the law [and] laying the foundations for a developed drone market" [4]. This mainly focused on remote-controlled, or semi-autonomous drones [4]. The Government acknowledged the risks posed by drones "to safety, security and privacy, which rightly cause the public much concern" [4]. In 2022, the UKRI and Sciencewise, a UK-based deliberative public dialogue platform, funded a joint public dialogue on three types of "future flight technologies for civilian use – drones, advanced air mobility ('air taxis') and regional air mobility ('eco-planes')" [5]. Fully autonomous drones were considered as part of this discussion [5]. The consultation focused on the benefits and disadvantages (including risks) of using new aerial technologies and relevant infrastructure and included discussion of what a future "Skyways Code" for governance of these technologies would look like [5]. Participants suggested a "cautious and measured approach to governance before public investment in these technologies' development is accelerated" [5]. Despite the development of a "Skyways Code" and list of potential rules, the public consultation has not as yet led to any new regulatory proposals. As suggested above, however, these might be expected in the next couple of years [7]. For the construction industry, an enforced Skyways Code would make clear, for example, how drones could operate in public spaces near or between construction sites.

At present, the interpretation of UK drone laws for drones operating in the construction sector require a broad understanding of the role of the CAA, including data protection laws, lifting regulations and civil aviation orders. Even then, the law is in a state of flux. While the EU is currently creating laws for a "Single European Sky" for 2024 and beyond [30], it is unclear if the UK will adopt these rules, or whether they will partake in future single sky arrangements. The CAA notes on the topic, for example, that "references to EU regulations or EU websites in our guidance will not be an accurate information or description of your obligations under UK law" [30]. As a result, commercial drone operators may soon face competing regulatory regimes across the channel, adding further confusion to the existing legal framework. This would be exacerbated if the expected commercial drones will one day be expected to operate autonomously across borders, rather than in their current manually operated form. "The need for global consensus is critical", says Professor Julie-Anne Tarr [7]. Without new regulations and guidance however, the current uncertainty is expected to continue.

4.2 Air Navigation Order

The CAA have published a set of guidelines for drone use, called the Drone and Model Aircraft Code (Updated July 2022) and operate in accordance with the Air Navigation Order (2016) (As amended). The Air Navigation Order sets out the basic regulatory framework for UK drone operation and relates to "small unmanned aircraft" (SUA) [14]. An SUA is defined (sch 1, art 1) as "any unmanned aircraft… having a mass of not more than 20kg" [28]. According to the Air Navigation Order, the Drone and Model Aircraft Code gives details regarding drone registration, licensing, and piloting requirements.

The Air Navigation Order also covers both “remote pilots” and “SUA operators” [28]. A remote pilot is defined as someone who operates the flight controls of an SUA by manual use of remote control, “or who is able to intervene by operating the flight controls when the SUA is flying automatically” [28]. An SUA operator is someone “who has the management of the SUA” [31]. These are often the same person, but they can be different, as in the case of a child remote pilot and an adult SUA operator, who supervises the flight operation. The SUA may also be envisaged as semi-autonomous in their control - for instance, a person giving orders to a drone but not flying it directly.

From 30 November 2019, all drones over 250g must be registered, and all pilots of these drones must also be registered, via a testing system [28]. Testing requirements apply for both commercial and private drone operators [28]. According to the CAA, the test covers “safety, security and privacy issues” [4]. It therefore covers the most basic risks associated with drone use. Pilots must attain a Flyer ID to show they’ve passed the basic flying test, as issued by the CAA [32]. They must also obtain an Operator ID, and this ID must be displayed on their drone at all times [32]. From 1 Jan 2023, new drones need to have a “class marking” (C0 - C4) and also have to meet mandatory product safety standards, based on their weight and capacity [32]. This may reduce the risk of drones malfunctioning due to technical or hardware problems.

The regulators provide further basic restrictions for drone operation. A small unmanned aircraft must fly below the legal height limit of 400 feet (120 metres) above the surface [28]. They must fly at a distance of at least 50m from humans, including in buildings and transport [32]. They must never fly over people who are crowded together, such as in shopping areas, sporting events or religious gatherings [32]. They must be kept at least 150m away from residential, recreational, commercial and industrial areas (although exceptions exist for drones lighter than 250g, and commercial drone operators can apply for an exemption from the CAA) [32]. Small unmanned aircraft must also not be flown in “restricted airspace, within one kilometre of airport boundaries,” and five kilometres from the ends and sides of a runway [28, 29]. Again, exemptions to this rule can apply for commercial operations, for inspections of buildings, for example, with permission from flight control [29].

Drones that are equipped or mounted with video cameras face further restrictions [28]. They must not be flown over or within 150m of any congested area, over or within 150m of an organised open-air assembly of more than 1,000 people, within 50m of any vessel, vehicle or structure not under control of the SUA operator, and within 50m of any person (except when taking off or landing, which can be within 30m) [28]. This places greater regulatory hurdles for surveillance and monitoring drones, especially in highly congested areas, such as major cities.

4.3 Commercial Use Regulations

In 2017, the Ministry of Defence (MoD) published guidance on the safe and legal flight of drones, stating that the use of drones commercially required direct permission from the CAA [33]. Commercial operators had to pass a mandatory accredited course that would train and assess their ability to safely operate drones [33]. “The courses include flying competence, knowledge of the law, risk assessments, decision making and more” [33].

On 1 January 2021, new EU regulations governing the use of drones came into force in the UK [34].[2] Developed by the EU Aviation Safety Agency (EASA), the regulations adopted a risk-based approach, no longer distinguishing between leisure and commercial use. Anyone flying a drone commercially must still obtain permission for operations from the CAA by passing a theory and flight test [34]. An operations manual must also be developed and approved by the CAA, detailing every aspect of the proposed drone operation, including risk assessment, insurance, maintenance and safe flying within the required visual line of sight limits [34].

In order to obtain an operational authorisation, unless the planned operation can be covered by a Predefined Risk Assessment (PDRA), the UAS operator must first conduct a risk assessment of the proposed operation and submit this as part of their application [32, 35]. The risk assessment must: outline the proposed operation (what the operator wants to do); describe the operational process (how the operator will do it); describe the technical aspects of the UAS to be used (what technology the operator will do it with); and then demonstrate that it can be done safely (safety and risk assessment) [32, 35].

---

[2] Note that the UK and EU are to some extent, still collaborating regarding matters related to navigation. See, for example, the section on aviation in ‘Part 2, Heading 2, Title 2,’ *EU-UK Trade Cooperation Agreement* (24 Dec 2020).

A ‘Certified’ category of drone use covers operations that present an equivalent risk to that of manned aviation. Such operations are subject to the same regulatory regime (i.e. certification of the unmanned aircraft, certification of the UAS operator, licensing of the remote pilot). UK regulations relating to the Certified category are still being developed and are not yet published [32]. Until these regulations are available, principles should be followed as established in the relevant “manned aviation regulations for airworthiness, operations and licensing, and this will be used as the basis for regulating the Certified category” [32]. The same requirements that relate to manned aircraft are applicable [35].

4.4 Privacy Regulations

Privacy regulations in the UK cover a wide range of scenarios and legal actions. These include a general right to privacy, a tort of misuse of private information, protection from harassment and data protection. Some of these regulations may impact the use of drones, particularly when drones operate in busy commercial centres and threaten the privacy of workers or the general public.

As a starting point, the UK Human Rights Act 1988 obliges the courts to follow the European Convention on Human Rights (ECHR), which includes Article 8, the right to privacy [36, 37]. This does not, however, create a general tort of privacy in the UK [38]. There may nevertheless be some form of protection against intrusion [39]. When balancing the right to privacy with the right to free expression, the courts have established a two-stage test [20]. First, a determination must be made as to whether the person “publishing the information knows or ought to know that there is a reasonable expectation the information in question will be kept confidential [20]. Second, once that bar is passed, there needs to be a balancing, “as a matter of fact and degree, the interest of the recipients in publishing the information” [20]. This includes recognizing free expression, and in the case of the media, “with a measure of latitude shown for the practical exigencies of journalism,” such as tight deadlines [20]. These rules and restrictions are generally relating to the publication of information, which may not be necessary in the case of drones filming on construction sites.

The UK also has a tort regarding the misuse of private information. For example, if a drone is used to “record footage of private activities such as topless sunbathing, skinny-dipping or sexual activity” and this material is shared on social media, courts will consider “whether the filmed person had a reasonable expectation that the activity would be kept confidential” [14, 20, 21]. Even in situations where this bar is passed, it’s possible that a greater “right to free expression” exists, “such as where publication corrects a false image of a public figure” [14]. Construction workers who share captured private footage of neighbours on social media, for example, may be subject to this law. Construction companies may also face liability from this type of activity regarding their employees in terms of unauthorised disclosure. For example, if private footage is published by the company in some form, such as on their website or product videos [75]. It should also be noted that a range of hacking and spoofing software exists for drones. For example, a malicious third party may use this software and take over the drone’s operational function [97], creating a scenario, which could damage a construction company’s reputation.

The Protection from Harassment Act 1997, likewise raises certain actionable harms that may occur by drone filming. The Act prohibits a person from harassing another when they know “or ought to know [that their course of conduct, on at least two occasions] amounts to harassment of the other” (s. 1(1)) [40]. This form of harassment is a crime (s. 2) [40], but it also may give rise to a civil remedy for damages for “anxiety… and any financial loss resulting from the harassment” (s. 3(2) [40]. A single instance of a drone spying on a neighbour (and causing anxiety), would therefore not be sufficient – the statute requires repeated behaviour [14]. It’s possible that repeated monitoring of a construction site – with a private view of a neighbour, may be sufficient in particular circumstances.

Finally, the Data Protection Act 2018 governs the processing (including the collection, use, storage and disclosure) of “personal data,” including any information related to an “identifiable living individual” (s. 3(2)) [41]. For visual imagery: this includes car registration numbers, a person’s face, or other data / information that identifies an individual. The Act acknowledges the GDPR (EU) as binding in the UK. The GDPR Article 5 says that personal data should be processed “lawfully, fairly and in a transparent manner [and] collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes” [42]. According to Article 13, when personal data is collected the "controller” of the data should provide information to the data subject (i.e. the person who’s data is being collected), including the “identity and contact details of the controller” [42]. Article 4(7) defines “controller” as “natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data" [42].

A private use exception exists in the DPA (UK) for processing data for personal use and household activity within one's own private home, for family and friends, etc. (with the exception of spying on sexual activity) [14]. A public interest exception also exists where "the processing is being carried out with a view to the publication by a person of journalistic, academic, artistic or literary material, and ... the controller reasonably believes that the publication of the material would be in the public interest" (sch 2, pt 5, para 26) [41].

Privacy regulations adopted from the EU are now subject to revision and replacement, or revocation, depending on the actions of the UK government following Brexit. There has been some suggestion in the media, for example, that the current UK government may withdraw from the European Convention on Human Rights [42], which may subsequently revoke application of Article 8 (the right to privacy) in the UK.

4.5 Privacy by design

The broader literature on drones, new technologies and legal frameworks makes frequent reference to privacy by design, a solution where privacy is built into a product or service from the start. 'Privacy by Design' (PBD) has a considerable body of research that focuses on the complex social, technical, legal and ethical aspects of privacy requirements in systems engineering [83]. The privacy by design framework devised by Cavoukian [83] calls for privacy to be built "directly into the design and operation, not only of technology, but also of operational systems, work processes, management structures, physical spaces and networked infrastructure" from the outset [83]. The framework supports the inclusion of a proactive and preventive approach to privacy rather than a reactive one, where privacy is viewed as the "default" position and embedded into the design process from the outset [83]. In doing so, privacy by design respects individuals rights while also considering the social, legal and ethical aspects of data processing, end-to-end privacy, and user-centric considerations [83].

A detailed analysis of the literature shows a shift away from the more technical and reactive aspects of privacy to a more proactive interest in the design of social, ethical and legal aspects of privacy [83, 85, 95, 98]. The law has adopted privacy by design as the default position, particularly when it comes to the processing of personal data or consumer information. In 1995, the concept was adopted into the European context in the data protection directive (RL 95/46/EC) [84]. The directive mandated that technical, social, and organisational steps be taken into account in order to protect data privacy during the planning phase of a processing system (Recital 46) [84].

The General Data Protection Regulation (GDPR, (2018) now mandates a form of "data protection by design and by default," (Article 25), including taking appropriate technical and organisational steps at the time of processing data to implement data protection principles, such as data minimisation or pseudonymisation. Article 25(2) states that furthermore, the controller of the data must, by default, only process personal data necessary for the specific purpose of the processing, and by default, not make this data widely accessible. The general data protection principles mention that cost, nature, scope and context of data processing can however be considered as well as the risks of that particular dataset (Article 25(1)).

In general, aside from a suggestion of pseudonymisation and data minimisation, the law leaves it up to individual designers and companies to themselves come up with the exact method by which data can be privatised. As an EU law, it is also up to the member states (and now the independent UK), to come up with their own data protection policies with their own Data Protection Agencies (DPAs).

In the UK, the Information Commissioner's Office (ICO) has produced guidance on the UK GDPR, including the principles of data minimisation, purpose limitation, storage limitation, accuracy, fairness and confidentiality, among others [85]. Checklists are provided on each item, making sure that companies only collect data that is specifically relevant to their stated purpose, relevant, limited and secure in nature [85]. Applying these principles to the construction site examples, it is clear that certain types of data collection, for example on neighbours or overheard conversations, would be beyond the scope of commercial operations, and therefore unlawful under the UK's GDPR. Drone operators must also conduct privacy impact assessments (PIAs) before the deployment of drones, to prevent privacy breaches [86]. This includes mapping out potential risks to privacy ahead of time and planning ahead the mitigation of these risks. These must be submitted to the ICO which will respond in eight weeks, or fourteen weeks for complex cases [85].

Adopting a data minimisation policy by design would naturally involve limiting certain capacities of drones in operation at the time of data collection. This includes limiting functionality. For example, some drones have advanced sensors on board (electromagnetic spectrum - visible light, infrared, ultraviolet), others have aerial sensors for sound, or data collection from sensors within the environment (such as other cameras, recorders or tracking devices) [87]. A privacy by design approach would seek to minimise or eliminate whichever function is unnecessary for the operation of a drone in a particular commercial context. Some questions could be asked at this stage of the process: Does a drone camera need the granularity necessary to capture licence plate IDs? If collision avoidance is the aim, is there a role for edge computing "on board only," or immediate and automatic deletion routes? [88] If cameras are needed, is a full 360 degree picture really necessary or is it possible to limit the field of view to a particular object or building to avoid capturing unnecessary data? Is heat sensing a necessary feature, if it might unintentionally capture bystanders? These and other questions can help guide the planning phase of a UAV system to ensure privacy of all stakeholders prior to deployment.

A range of suggested solutions have been made in the literature to ensure privacy by design [90]. One is to adopt a data management model that is based on the informed consent of the user [91], to effectively enforce the GDPR as part of the product itself [90]. The user would be able to say whether they consent or not for their data to be used. Others suggest performing a Data Protection Impact Assessment (DPIA), even when it is not required by the law, as it can serve as an effective self-assessment tool to see whether a product adheres to data protection principles [90]. Another solution is called "sticky policies," where users define a set of rules by which service providers must handle their data [92]. Whichever policy is adopted, the aim is to avoid a situation where users are faced with a "take it or leave it" system, where access to the system is limited by a demand for a large amount of data with no customisation on the part of the user [90]. In general terms, service providers should also strive to minimise the data collected, specifically identifying necessary data for the service, and other data that can be voluntarily shared [90]. Having an updated privacy policy and transparent terms for users is generally considered good practice in this regard [90].

Privacy by design is an evolving field and strives to include the steps, both technical, social, and legal and ethical dimensions of privacy into products and services, that need to be taken for a particular use-case, which are subject to change over time in response to technological innovation and the broader social context [89]. One way of managing this change is to adopt Nissenbaum's decision heuristic model [93]. This model allows service providers to run through a set of queries for a new technological implementation [93]. The steps include: describing the new practice "in terms of information flows," identifying the subjects, sender and receivers of information, specifying transmission principles, finding established information norms and where this new technology might change them, presuming that any deviation from established norms is a breach of privacy, and evaluating the moral, political, values and goals in the context of this breach, and then acting accordingly [93]. There has been some active discussion on the latter aspects of this heuristic, regarding the moral, political or indeed social implication of data privacy [93, 94]. Shilton suggests an anti-surveillance framework, for example, where product design is seen from the lens of decreasing surveillance and forms of privacy infringement [94]. In a participatory study, Shilton found that some technologists framed privacy as a "technical challenge," and this helped them move it away from a dry view of ethics as a moral imperative [94]. The same was found in data visualisations, where a creative, visual-language approach to data helped technologists understand the flaws of a particular dataset regarding privacy [94].

In terms of the use of drones, a survey found that drone operators self-reported a lack of understanding of European privacy law and data protection law [96]. Although ignorance is not a defence in the law, a general lack of knowledge of the rules will practically result in a lack of compliance [96]. Privacy by design principles can assist here in creating certain tools, frameworks or standards that operators can use in drone operations. There has been research for example, on how to ensure drones are private by design in compliance with the GDPR rules [95] Bassi et al., (2019) developed a tool to manage risks associated with data privacy "through the design of flight maps" [95]. The tool can help operators pick an air corridor for their drones that minimises the risk of privacy infringement in the community [95]. It can thereby be used in the planning stage of a project, in line with local authorities [95]. A well-chosen flight path, with a specifically targeted field of view, could allow drones to operate in areas that typically face higher regulatory burdens, such as parts of urban centres. Beck et al. use a different framework to allow for the operation of drones across different air spaces with different regulatory standards for privacy; allowing “guest” delivery drones to operate according to rules of a “host” recipient in a particular zone [96].

Finally, there is a growing body of literature on the concept of differential privacy. Differential privacy (DP) refers to the making of small, minor changes to a dataset to assist in de-personalizing irrelevant data, whilst keeping in place the data needed to make a particular decision or output. DP is therefore a mathematical privacy framework that can help create an output with less personal data being used [98]. The benefits of this technique is that it can reduce the risk of data breaches or data disclosure in the decision-making process [98]. At the same time, some of the drawbacks of DP is that it might move conversation away from discussions of the quality of data itself, and pose challenges for “data self-governance,” when users no longer have control over their anonymised data in a system [98]. For the use of drones, differential privacy can help ensure safety compliance of drone operators while de-identifying the operators concerned or maintain the privacy of workers on-site [99]. Laws in the US require the disclosure of a drone’s location to ensure that it can be prevented from causing harm, and DP can ensure that a drone’s location is shared without impinging upon the privacy of the operator [99]. Although no equivalent law currently exists in the UK, it is worth considering this as a potential future requirement that legislators might impose on UK operators.

In Diagram 1 below, we have identified the various steps to be considered for privacy by design in the flight planning phase and the data processing phase of drone deployment, as drawn from the literature discussed above:

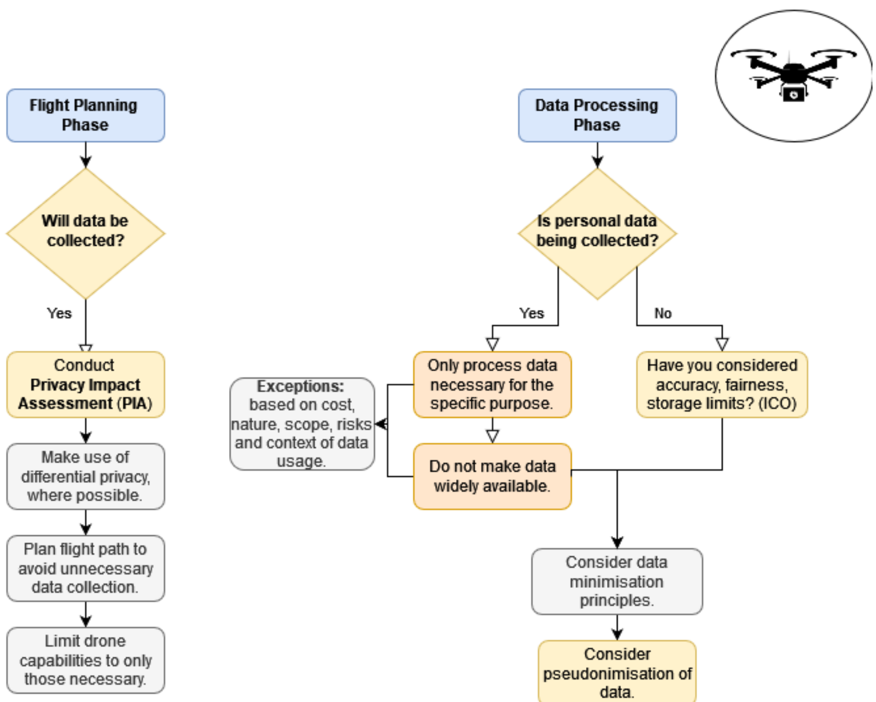

Diagram 1: Privacy by Design - Drones in Construction. [83, 85, 87, 90, 95, 98, 99]

4.6 Health and Safety Regulations

Our literature synthesis has so far considered the impact of drones in a diverse range of use-cases. However, there are also many regulations that apply specifically to private workplaces, of which construction sites are one. The Workplace (Health, Safety and Welfare) Regulations 1992, for example, defines a workplace as: "any premises or part of premises which are not domestic premises and are made available to any person as a place of work" [44]. The Construction, Design and Management Regulations 2015, in similar language, defines a construction site as "any place where construction work is being carried out or to which the workers have access" [45]. Construction sites must therefore abide by the relevant workplace regulations with regards to the use and deployment of various technologies [44, 45].

One of the most important workplace regulations in the UK is The Health and Safety at Work, etc. Act 1974 (HSWA) [44].[3] HSWA sets out general duties on workplaces, in particular, the duty to reduce risks to "as low as reasonably practicable" (ALARP). The onus is on the organisation (i.e. construction company) to prove that they have overcome ALARP in any consequent prosecution on the grounds of safety [46]. This is a very high hurdle to prove, and in most cases, the expectation is that all reasonable safety mitigations have to be put in place unless grossly disproportionate to the risk involved [46]. The courts have specified that:

> *"A computation must be made by the owner in which the quantum of risk is placed on one scale and the sacrifice involved in the measures necessary for averting the risk (whether in money, time or trouble) is placed in the other, and that, if it be shown that there is a gross disproportion between them – the risk being insignificant in relation to the sacrifice – the defendants discharge the onus on them" [46].*

"Reasonably practicable" is defined more narrowly than "physically possible," meaning that not all physically possible safety measures need to necessarily be pursued in all circumstances [46]. Overall ALARP must be judged on a case-by-case basis. Any new risk or novel technology proposed, will need to overcome the ALARP hurdle [46]. This applies to drones as to any other new technology. Aerial drones for construction pose an array of risks (outlined above) that would have to be considered under an ALARP framework. According to the Health and Safety Executive, a risk under ALARP is defined as "the likelihood that a hazard will actually cause its adverse effects" [47]. The likelihood can be measured by way of probability, frequency, or qualitatively, while the adverse effect can be described as causing illness, injuries, and so on [47].

Making decisions about risks and effects under ALARP is a very complicated process and, when the consideration is a new technology (such as drones), there is no standard "good practice" to follow [47]. A "first principles" analysis can be used, applying common sense, expertise or professional experience to the situation, but a more rigorous assessment may be necessary [47]. In this case, due to the complexity of using drones on construction (particularly, in the future, autonomously), a more rigorous assessment would be required, including a comprehensive cost-benefit analysis (CBA) [47].

Any CBA must consider all appropriate costs, such as the cost of installation and operation, training, lost production (but only the 'interest' of lost production, if it is merely delayed), and other costs necessary for implementing risk reduction measures [48]. In terms of benefits, the CBA must consider all benefits, including all *reductions* in risk to "members of the public, workers and to the wider community" [48]. For drones, the costs would include installation and operation, training and potential lost production while drones are being implemented to replace workers on certain tasks. These costs would differ according to the type of drone used, and the type of task imagined. The benefits would include those listed above, such as increased safety, reduced injuries and fatalities (where relevant), and increased safety compliance. But again, this depends on the way the drones are proposed to be used. It's possible that ALARP here sets up a "chicken and egg" scenario, where the true costs and benefits cannot be entirely known before implementation, specifically of a new technology [49]. The HSE has published a guide to assist in the CBA analysis, but even in the guide, they note "a CBA

[3] The Workplace (Health, Safety and Welfare) Regulations 1992, for example, define workplace as: "any premises or part of premises which are not domestic premises and are made available to any person as a place of work, and includes (a) any place within the premises to which such person has access while at work". The Construction, Design and Management Regulations 2015 (CDM) likewise define a construction site as "'construction site' includes any place where construction work is being carried out or to which the workers have access".

cannot form the sole argument of an ALARP decision, nor can it be used to undermine existing standards and good practice" [50]. At the same time, HSE recognizes that ALARP does not mean that there will be no risk at all [50].

A classic problem with ALARP is that what is "reasonably practicable" is always changing and so assessments of risks and mitigations must be continuous by dutyholders. It may be grossly disproportionate to use a piece of work equipment today – but in a year's time that might change, if the costs and benefits change. Regarding drones, their availability has increased, and so their costs, in purchase and operation, have decreased dramatically over time [51]. The benefit of cost savings has, in turn, increased. E Construction Ltd, a Canadian paving contractor, has estimated that using drones has saved them between $50,000 to $60,000 a year, "because the surveying process has been reduced from nearly two weeks to 30 minutes" [52]. To put this into context, we may not be far away from a situation where a duty holder may be prosecuted for *not* using a drone where they could have, for making a task more unsafe than it needed to be. This transition is evident, for example, in Network Rail's Taskforce Final Report, after the fatal derailment in Carmont, where Lord Mair explained that drones should be used more often to monitor and survey earthworks [53].

Under ALARP, duty holders may face unlimited fines or even imprisonment, for failing to comply with health and safety requirements [54]. Imprisonment is also possible under separate corporate manslaughter legislation if fatalities were involved. This is why H&S legislation has to be a core consideration with the implementation of any new technologies, such as drones.

4.7 Lifting, Work and Safety Regulations

The literature review identified a number of lifting, work and safety regulations that apply generally to any new technology used to lift materials on site, with some specific new provisions regarding the use of drones or UAVs. We identified two core lifting regulations: the Lifting Operations and Lifting Equipment Regulations (1998 'LOLER' and 1999, Northern Ireland), and the Provision and Use of Work Equipment Regulations (1998 'PUWER' and 1999, Northern Ireland). In the construction sector, lifting, work and safety regulations have been put in place to attempt to ensure that construction workers operate in a safe working environment. LOLER stipulates that lifting equipment requires thorough examination by a competent person at periodicities defined by the regulation and the state of the equipment (installation, deterioration, repair, and utilisation) (r. 9) [55]. PUWER stipulates that work equipment be inspected by a competent person at various stages of work equipment service life (r. 30) [56]. Similar requirements for lifting equipment are evident in the Safety, Health and Welfare at Work (General Application) Regulations 2007 [57].

Drones operating on construction sites could, now and in the future, be used as lifting equipment, carrying materials on-site and replacing cranes in some tasks. But aerial drones raise new challenges, due to their remote nature, speed and mobility, that may not be catered for by existing regulation on lifting devices. We did not identify any substantial body of literature on lifting, work and safety regulations in regards to drones specifically used on construction sites. This calls for new research, which has resulted in this manuscript. Consequently, in order to address the lack of these regulations, we must turn our attention to **existing** lifting, work and safety regulations that currently serve the construction sector and apply those standards to the use of drones on construction sites, while also questioning their validity. This question is motivated by an ongoing debate about the nature of existing regulations and whether they are applicable to drones.

Remote-controlled self-propelled work equipment (which would include aerial drones that fit this description) face some restrictions under PUWER. Regulation 29 stipulates that "every employer shall ensure that where remote-controlled self-propelled work equipment involves risk to safety while in motion; it stops automatically once it leaves its control range and, where there is a risk of crushing or impact, it incorporates features to guard against such risks unless other appropriate devices are able to do so" [56]. Arguably, this regulation does not work with aerial drones in mind, given that a drone suddenly stopping mid-air would fall, potentially causing injury. Although depending on the interpretation, this could be seen as going outside of its "control range" [56].

Further regulations apply to work equipment of specific types, including electrical equipment and dangerous substances. The Electricity at Work Regulations 1989, r. 4, require the inspection of electrical systems and equipment, working on or near these, and electrical safety. Inspection scope and periodicity varies according to the complexity and risk profile of the electrical system [58]. The Control of Substances Hazardous to Health Regulations 2002 (COSHH) r. 9 requires periodic thorough examination of equipment that is subject to deterioration where that deterioration could lead to employees being subjected to high levels of hazardous substances [59]. This could include, for example, chemicals in battery components, although more research is needed on the scale of this risk in the context of construction.

4.8 Levels of Automation

Due to the lack of UK regulation on commercial drones, the use of autonomous drones on construction sites is unlikely now and for the foreseeable future. For instance, the Air Navigation Order specifies that an "unmanned aircraft" must always have a remote human pilot operating the aircraft at all times [28]. The Air Navigation Order also indicates that the unmanned aircraft should stay within the operator's line of sight [28]. Line of sight requirements prevent drones from operating independently in difficult-to-see locations, such as underground, underwater or in ventilation shafts. To use lifting drones in this capacity, commercial operators may have to apply for an exemption from the UK's Civil Aviation Authority (CAA) to use First-Person-View (FPV), where operators pilot the drone via its cameras, rather than line of sight [61]. However, FPV is currently limited to drones of less than 3.5kg, which would have decreased lifting capacity than the state-of-the-art 200kg lifters [61]. FPV also requires a "competent observer" who maintains line of sight [61]. A range of observers could maintain this requirement, but this would limit drones from operating in dangerous environments without any human presence (which is one of their major use-cases as autonomous machines).

Lifting drones would also have to comply with inspection requirements under LOLER and PUWER. They would need to be inspected periodically and maintained to comply with safety requirements. PUWER stipulates, for example, that a remote-controlled device must stop "automatically once it leaves its control range and, where there is a risk of crushing or impact, it incorporates features to guard against such risk unless other appropriate devices are able to do so" (r. 29) [56]. These requirements would need to be included in drones. In the future, the CAA may permit certain uses of autonomous drones, or the use of non-autonomous drones for lifting materials. However, any commercial use would be subject to CAA safety analysis, including visual line of sight limits [34].

As a result, existing regulations appear to only consider use-cases for semi-autonomous drones with humans remaining in-the-loop and within line of sight. While the current rules make sense for drones operating in busy commercial or urban centres, there is some doubt about their suitability for remote or offshore drone use. There has been some research on the use of drones to maintain offshore wind farms or to monitor coastal regions, for example, where the use of drones was shown to decrease costs and safety risks to workers [77, 78]. While these studies relied on humans-in-the-loop [77, 78], it is foreseeable that as technology improves, autonomous drones could operate in remote areas without posing harm to human bystanders, as there would be few nearby. The risks to noise and privacy likewise may be decreased in remote offshore or very remote regional locations, with low population density.

5. DISCUSSION

This paper is an important contribution in the field of drone law in the UK. In mapping out the complexity of using and deploying drones in the UK within the construction sector, we bring together a disparate range of literature on the topic from across disciplines. Such literature includes insights from law, computer science, engineering, maritime, transport and construction, which helped us thematically reveal the opportunities and risks of drone use on construction sites, along with the regulatory context in the UK.

The literature review that we present has aimed to explore and qualitatively describe social, legal and regulatory research on the use of drones on construction sites. We sought to answer three research questions relating to the state of UK legislation with regards to trustworthy drones in construction, the policy landscape and the degree that these questions vary depending on levels of automation. To do this, we carried out a literature synthesis for publications in the ACM Digital Library, Google Scholar, GOV.UK, and websites such as the UK Civil Aviation Authority databases. We compiled 90 articles on the subject, published between 1988 and 2023. As a consequence, we identified four main themes in answer to our research questions. These included: (1) opportunities, (2) safety risks, (3) privacy risks, and (4) the regulatory context (Table 2).

We identified 21 sub-themes, which illuminated more specific opportunities, harms and regulatory initiatives commonly discussed in the literature.

The literature suggests that drones have the potential to provide a range of opportunities for the construction industry. For example, drones provide the opportunity to increase the quality and scope of monitoring of construction sites, safety inspection, and even the lifting and carrying of goods, with some drones capable of lifting over 20kg. Drones also provide opportunities to: reduce labour costs, operate in hard-to-reach locations, and operate in environments that are too hazardous or remote for human workers, including offshore. In locations with few bystanders, such as rural or offshore construction sites, drones can operate relatively safely and potentially autonomously. However, UK legislation prohibits fully autonomous drones and mandates that a human remains in the loop and within line of sight, which effectively means that fully autonomous drones are not possible, unless rare exemptions are provided by the CAA.

In terms of risks to humans, the literature suggests that drones pose a variety of risks to safety, privacy and security of workers and bystanders, particularly if used incorrectly or maliciously targeted by hackers or third parties. In terms of safety, they may cause accidents, interfere with a worker's concentration, cause psychological harm, or drop goods on site they are carrying. In terms of privacy, they may infringe on the privacy rights of bystanders, neighbours and workers on-site by capturing footage or audio recordings that include personal data. Some of these risks may be mitigated with the adoption of privacy by design principles, including data management plans, privacy frameworks and differential privacy (discussed above). They may also be mitigated with data minimisation strategies, including limiting the drone's sensor and recording capabilities to only those necessary for a particular work task.

There was a total absence of consideration for the welfare of wildlife in the literature. Consequently, future research is needed on the impact of drone use on wildlife, such as birds and ecosystems. By the same token, drones operating at sea are likely to disturb marine life, and so a greater focus should be placed on harm mitigation strategies, or at least an observation of potential risks in this area. Although construction is primarily a human domain, it is important that the impact of construction on the environment feature more prominently in future research.

Laws in the UK regarding the use of drones for commercial purposes are in their infancy, with a bottleneck system of approvals through the CAA. Some of the laws can be described as contradictory or chaotic in nature, with overlapping jurisdictions and at times competing legal principles. Specifically, the general laws for lifting regulations, worker health and safety, and other areas have historically been developed with different kinds of equipment in mind, rather than specifically targeted towards drones. A patchwork of amendments has attempted to resolve this, but the law still appears to have particular gaps in operation. Drone laws that have been written are typically focused on civilian use, rather than commercial deployment, and as such they reflect a particular kind of user who may or may not mirror the average commercial operator.

In addition to our thematic analysis of the literature, we identified a variety of gaps in UK law which emerged from our analysis of theme 4: 'regulatory context'. As a consequence, we have created an extra column to present this observation in which we have titled 'Gaps in the Law (UK)'. We present these 'gaps in the law', along with a summary of our findings, below in Table 3:

Table 3: Results of the Literature Synthesis - Themes and Potential Use Cases

Themes	**Opportunities**	**Privacy and Safety Risks**	**Regulatory context**
Potential use cases			**Gaps in the Law (UK)**
Monitoring of Construction Sites	- Safety monitoring - Building progress monitoring - Monitoring large areas of land - Offshore / remote	- Privacy of workers - Privacy of the public	Privacy is well covered in UK law as a general principle and in tort. A gap exists in technical specifications for drones to

	monitoring		be “private by design”. The law could more closely reflect privacy by design principles found in the GDPR, but applied specifically to commercial drone use.
Lifting heavy goods and materials	- Capacity to outperform human workers - Reduced risk of injury to human workers	- Safety risk of falling materials - Distractions - Noise - Hacking or interference	Cybersecurity standards for drones could prevent hacking/interference and allow for the carrying of heavy materials on-site. In line with other lifting equipment standards.
Operating in hazardous environments	- Safety gains (Reducing risks, safety inspections, operating in hazardous environments, working from heights).	- Safety risks (Accidents, distraction of human operators).	The law is unclear on which environments drones are most suited for in operation. Our review identifies remote or offshore locations as ideal environments.
Intruder detection	- Prevention of theft or property damage	- Privacy risks	Privacy is generally well covered in UK law.
Drone swarms operating in concert	- Capacity to complete complicated operations in synthesis	- Noise	Lack of regulations on drone noise profile for how quiet they should be to reduce distractions.
Using drones for commercial construction	- Economic benefits - Cost and time savings	- Privacy - Safety - Noise - Adverse weather - Hacking / interference	Without commercial drone regulations, any economic benefit is subject to the business uncertainty of the CAA’s bottleneck approval system. This hinders the cost and time savings by requiring approval prior to deployment. A commercial drone regulation would allow companies to plan ahead and pre-plan savings.

5. CONCLUSION

We have revealed a variety of opportunities, risks and regulatory processes through which drones must go through to be used on construction sites in the UK context. Opportunities ranged from the potential for drones to replace human labourers in hazardous environments to the reduction of lifting injuries, whereas risks ranged from hacking to noise and distraction of workers. In addition to the regulatory context, analysis revealed numerous gaps in the law, specifically regarding UK drone regulations. In the absence of regulation by the UK government, various companies have stepped in to try and create rules and norms for the safety of drones. Moreover, determining how to regulate the more 'semi-autonomous' or 'autonomous' drones will likely bring further complexity to the regulatory environment. In addition, the bottleneck of the CAA approval system makes it difficult for regulators to openly develop new rules. Given systematic gaps in UK drone regulation, we suggest the use of drones in offshore and remote locations remains their best current application in order to avoid busy urban areas and the related drone flight restrictions.

Future drone regulations in the UK should seek to address the various uncertainties in the law identified. In particular, a new drone law for commercial use could specify technical requirements, safety features, privacy requirements, and cybersecurity requirements to prevent interference. A few tentative steps can be suggested here, along with calls for future research. First, standardised guidelines for commercial drones could be developed based on different use-cases and construction environments. For example, a future study on the difference in risk factors between autonomous, semi-autonomous and remote-controlled drones could be designed as a means of risk governance. A second type of future research could be based on a research design which investigates how CAA approval can be streamlined. Without national regulation on commercial drone use however, construction companies must still go through a bottleneck system, while also managing conflicting rules across different jurisdictions, such as the UK and Ireland, and considering the new rules implemented in the EU. Future policy could consider an outcomes-based approach, drawing on insights from the public, companies, stakeholders, and regulators to create a new commercial drone regulation. Commercial drone regulation may provide business certainty to the construction sector to explore use-cases of UAVs that provide the greatest benefit whilst mitigating potential risks.

REFERENCES

[1] Department for Business, Energy and Industrial Strategy. 2019. Policy Paper: Construction Sector Deal. <https://www.gov.uk/government/publications/construction-sector-deal/construction-sector-deal>.

[2] IBM. 2022. What is Industry 4.0? <https://www.ibm.com/uk-en/topics/industry-4-0>.

[3] UK Civil Aviation Authority. 2023. Future Flight Challenge: Information regarding the future flight challenge <https://www.caa.co.uk/our-work/innovation/future-flight-challenge/>.

[4] Department for Transport. 2017. Unlocking the UK's High Tech Economy: Consultation on the Safe Use of Drones in the UK: Government Response.

[5] Ed Camilleri, Jennifer Gisborne, Michelle Mackie, Reema Patel, and Matt Reynolds. 2022. Future Flight Challenge – Mini Public Dialogue: A Sciencewise report prepared for the Future Flight Challenge and UK Research and Innovation.

[6] Scott McLahlan, Kudakwashe Dube, Burkhard Schafer, Anthony Gillespie and Norman Fenton. 2022. The Chaotic State of UK Drone Regulation. Pre-Print, ResearchGate.

[7] Drones | Can regulators ever catch up with drone technology? 2022. Clyde & Co Podcast.

[8] Christopher J. Turner, John Oyekan, Lampros Stergioulas and David Griffin. 2021. Utilizing Industry 4.0 on the Construction Site: Challenges and Opportunities. IEEE Transactions on Industrial Informatics 17(2); UK Government, Construction 2025. (2013). Accessed: May 27, 2020. [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/210099/bis-13-955-construction-2025-industrial-strategy.pdf

[9] Zbynek Skoda and Jakub Holcman. 2021. Applications of UAV Technology Within the Construction Industry. Business & IT. 27.

[10] Tariq Umar. 2020. Applications of drones for safety inspection in the Gulf Cooperation Council construction. Engineering, Construction and Architectural Management 28(9).

[11] A.O. Onososen, I. Musonda D. Onatayo, M.M. Tjebane, A.B. Saka, R.K. Fagbenro. 2023. Impediments to Construction Site Digitalisation Using Unmanned Aerial Vehicles (UAVs). Drones. https:// doi.org/10.3390/drones7010045.

[12] Health and Safety Executive (HSE). 2022. Construction Statistics in Great Britain 2022.

[13] Mohammad Z. Shanti, Chung-Suk Cho, Borja Garcia de Soto, Young-Ji Byon, Chan Yeob Yeun, Tae Yeon Kim. 2002. Real-time monitoring of work-at-height safety hazards in construction sites using drones and deep learning. Journal of Safety Research.

[14] Des Butler. 2019. Drones and Invasions of Privacy: An International Comparison of Legal Responses. 42(3) University of New South Wales Law Journal.

[15] R. Finn and A. Donovan. 2016. Big data, drone data: Privacy and ethical impacts of the intersection between big data and civil drone deployments in: B. Custers (ed.). The Future of Drone Use: Opportunities and Threats from Ethical and Legal Perspectives. Asser Press. pp. 47-70.

[16] Roger Clarke. 2014. The Regulation of civilian drones' impacts on behavriousal privacy. Computer Law & Security Review.

[17] Idris Jeelani and Masoud Gheisari. 2021. Safety challenges of UAV integration in construction: Conceptual analysis and future research roadmap. Safety Science 144.

[18] Alana Mitchelson. 2017. Peeping Tom Drones Prompt Calls for a Close Look at Privacy Law. The New Daily.

[19] Robbie Patterson. 2017. Sydney Couple Catch Drone Spying on Them from Fifth Floor Balcony. Daily Telegraph.

[20] Campbell v MGN [2004] 2 AC 457, 465 [14] (Lord Nicholls).

[21] Vidal-Hall v Google Inc [2016] QB 1003.

[22] Edward Snowden. 2014. Edward Snowden: 'If I end up in chains in Guantánamo I can live with that' - video interview. The Guardian.

[23] A. J. Kerns, D.P. Shepard, J.A. Bhatti, T.E. Humphreys. 2014. Unmanned aircraft capture and control via GPS spoofing. J. F. Robot. https://doi.org/10.1002/ rob.21513.

[24] Jhonattan G. Martinez, Masoud Gheisari and Luis F. Alarcon. 2020. UAV Integration in Current Construction Safety Planning and Monitoring Processes: Case Study of a High-Rise Building Construction Project in Chile. Journal of Management in Engineering.

[25] A. Vasic Billard. 2013. Safety issues in human-robot interactions, in: 2013 Ieee International Conference on Robotics and Automation. IEEE.

[26] Gwyn Topham, Matthew Weaver and Haroon Siddique. 2018. Runway Reopens after Days of Drone Disruption at Gatwick, The Guardian.

[27] Samira Shackle. 2020. The Mystery of the Gatwick Drone. The Guardian.

[28] The Civil Aviation (Air Navigation) Order 2016.

[29] Department for Transport. 2019. Taking Flight: The Future of Drones in the UK. UK Government Response Paper.

[30] Civil Aviation Authority. 2022. Single European Sky Interoperability Requirement. <https://www.caa.co.uk/commercial-industry/airspace/air-traffic-management-and-air-navigational-services/air-navigation-services/single-european-sky-interoperability-requirements/>

[31] Civil Aviation Authority. 2019. Air Navigation Order 2018 and 2019 Amendments Guidance for Small Unmanned Aircraft Users. CAA Publication No CAP 1763.

[32] Civil Aviation Authority. 2022. Drone and Model Aircraft Code (Updated July 2022).

[33] Ministry of Defence. 2017. Drones: how to fly them safely and legally.

[34] Paul Bryan. 2021. Using drones for inspection and survey. Context 168. Institute of Historic Building Conservation.

[35] Civil Aviation Authority. 2022. CAP 722A: Unmanned Aircraft System Operations in UK Airspace – Operating Safety Cases.

[36] European Convention on Human Rights. 1953.

[37] Human Rights Act 1988 (UK).

[38] Wainwright v Home Office [2004] 2 AC 406.

[39] Tugendhat J in *Goodwin v NGN Ltd* [2011] EWHC 1437 (QB).

[40] Protection from Harassment Act 1997.

[41] Data Protection Act 2018.

[42] General Data Protection Regulation (‘GDPR’) 2016 (EU).

[43] Rishi Sunak, as quoted in. 2023. Prepared to withdraw from European Convention on Human Rights. Independent.

[44] The Workplace (Health, Safety and Welfare) Regulations 1992.

[45] The Construction, Design and Management Regulations 2015.

[46] Edwards v. National Coal Board, [1949] 1 All ER 743.

[47] Health and Safety Executive. 2023. ‘ALARP ‘at a Glance’ Risk Management: Expert Guidance <https://www.hse.gov.uk/managing/theory/alarpglance.htm>.

[48] Health and Safety Executive. 2023. Cost Benefit Analysis (CBA) checklist.

[49] Reece A. Clothier, Brendan P. Williams, Neale L. Fulton and XunGao Lin. 2013. ALARP and the Risk Management of Civil Unmanned Aircraft Systems in Tony Cant (ed.). *Conferences in Research and Practice in Information Technology* (CRPIT) Vol. 151 (3).

[50] Health and Safety Executive. 2023. HSE principles for Cost Benefit Analysis (CBA) in support of ALARP decisions. Risk Management: Expert Guidance. <https://www.hse.gov.uk/managing/theory/alarpcba.htm>.

[51] Padraig Belton. 2015. Game of drones: As prices plummet drones are taking off. BBC News.

[52] Joy Powell. 2019. In roadbuilding and bridge inspections, drones cut time, costs and safety risks. Equipment World.

[53] Robert Mai. 2021. A Review of Earthworks Management. Network Rail.

[54] Lexis PSL. 2023. Sentencing health and safety offences. Health and Safety Offences Overview. <https://www.lexisnexis.com/uk/lexispsl/corporatecrime/document/391421/5J17-5R61-F188-N303-00000-00/Health_and_safety_offences_overview>.

[55] Lifting Operations and Lifting Equipment Regulations 1998 (LOLER).

[56] Provision and Use of Work Equipment Regulations 1998 (NI 1999).

[57] Safety, Health and Welfare at Work (General Application) Regulations 2007.

[58] Electricity at Work Regulations 1989.

[59] Control of Substances Hazardous to Health Regulations 2002 (COSHH).

[60] FlyingBasket, FB3 Cargo Drone <flyingbasket.com>.

[61] Civil Aviation Authority. 2019. Small Unmanned Aircraft First Person View (FPV) Flying (ORS4 No 1294).

[62] Ferdinand v MGN Ltd [2011] EWHC 2454 (QB).

[63] National Cyber Security Centre. 2022. CNI Hub.

[64] Beehive Drones. 2017. <https://beehivedrones.com/>.

[65] Tricco A, Khalil H, Holly C, Feyissa G, Godfrey C, Evans C, et al. 2022. Rapid reviews and the methodological rigor of evidence synthesis: a JBI position statement. JBI Evid Synth 2022 Apr;20(4):944-949. doi: 10.11124/JBIES-21-00371.

[66] Maria J. Grant and Andrew Booth. 2009. A typology of reviews: an analysis of 14 review types and associated methodologies. Health Info Libr J 2009 Jun. 26(2):91-108. doi: 10.1111/j.1471-1842.2009.00848.x.

[67] Denyer, D. and Tranfield, D. 2009 “Producing a systematic review”, in David A. and Bryman, Alan (Ed.), The Sage Handbook of Organizational Research Methods, Sage Publications Ltd, Thousand Oaks, CA, pp. 671-689.

[68] Christian Pohl and Gertrude Hirsch Hadorn. 2008. Methodological challenges of transdisciplinary research, *Natures Sciences Sociétés*, vol. 16, no. 2, pp. 111-121.

[69] Drone Industry Insights. 2022. Drone Regulation. Drone Readiness Index

[70] PWC. 2022. Skies Without Limits v2.0. A refreshed look at how drones could impact the UK’s economy, jobs, productivity and quality of life.

[71] Hullysses Sabino, Rodrigo V.S. Almeida, Lucas Baptista de Moraes, Walber Paschoal da Silva, Raphael Guerra, Carlos Malcher, Diego Passos, Fernanda G.O. Passos. 2022. A systematic literature review on the main factors for public acceptance of drones. *Technology in Society*. Volume 71.

[72] J. Kennedy, S. Garruccio, and K. Cussen. 2021. “Modelling and mitigation of drone noise,” *Vibroengineering PROCEDIA*, Vol. 37, pp. 60–65, https://doi.org/10.21595/vp.2021.21988

[73] Albeaino, Gilles, Patrick Brophy, Idris Jeelani, Masoud Gheisari, and Raja R. A. Issa. 2023. "Impact of Drone Presence on Construction Individuals Working at Heights." Journal of Construction Engineering and Management 149, no. 11: 04023119.

[74] Shi Zhou and Masoud Gheisari. 2018. Unmanned aerial system applications in construction: a systematic review. Construction Innovation.

[75] Justice Mann, Shobna Gulati and ors v MGN Limited [2015].

[76] Trade Unions Congress. 2022. Guide to Privacy and Monitoring. <https://www.tuc.org.uk/workplace-guidance/basic-rights-and-contracts/privacy-and-monitoring>.

[77] Sara Bernardini, Ferdian Jovan, Zhengyi Jiang, Simon Watson, Andrew Weightman, Peiman Moradi, Tom Richardson, Rasoul Sadeghian, and Sina Sareh. 2020. A Multi-Robot Platform for the Autonomous Operation and Maintenance of Offshore Wind Farms. In Proceedings of the 19th International Conference on Autonomous Agents and MultiAgent Systems (AAMAS '20). International Foundation for Autonomous Agents and Multiagent Systems, Richland, SC, 1696–1700.

[78] Yongcan Yu, Feifei Yu, Yajie Zhang, and Zhennan Chen. 2018. Application Of Unmanned Aerial Vehicle Network Control To Coastal Water Quality Monitoring. In Proceedings of the 2018 International Conference on Mechatronic Systems and Robots (ICMSR '18). Association for Computing Machinery, New York, NY, USA, 115–118. https://doi.org/10.1145/3230876.3230894

[79] Uchechi F. Ukaegbu, Lagouge K. Tartibu, Modestus O. Okwu, and Isaac O. Olayode. 2021. Integrating Unmanned Aerial Vehicle and Deep Learning Algorithm for Pipeline Monitoring and Inspection in the Oil and Gas Sector. In Proceedings of the International Conference on Artificial Intelligence and its Applications (icARTi '21). Association for Computing Machinery, New York, NY, USA, Article 1, 1–6. https://doi.org/10.1145/3487923.3487924

[80] C.T. Graham, I. O'Connor, L. Broderick, M. Broderick, O. Jensen, H.T. Lally, Drones can reliably, accurately and with high levels of precision, collect large volume water samples and physio-chemical data from lakes, Science of The Total Environment, Volume 824, 2022.

[81] Wang, Jingbo, Kaiwen Zhou, Wenbin Xing, Huanhuan Li, and Zaili Yang. 2023. "Applications, Evolutions, and Challenges of Drones in Maritime Transport" Journal of Marine Science and Engineering 11, no. 11: 2056. https://doi.org/10.3390/jmse11112056

[82] Stokes, H.J.; Mortimer, J.A.; Laloe, J.-O.; Hays, G.C.; Esteban, N. Synergistic Use of UAV Surveys, Satellite Tracking Data, and Mark-Recapture to Estimate Abundance of Elusive Species. Ecosphere **2023**, 14, e4444. [Google Scholar] [CrossRef]

[83] Cavoukian, A. Privacy by design: the definitive workshop. A foreword by Ann Cavoukian, Ph.D. *IDIS* **3**, 247–251 (2011). https://doi.org/10.1007/s12394-010-0062-y

[84] Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995)

[85] Information Commissioner's Office, 'A guide to the data protection principles' (2022) https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/

[86] Information Commissioner's Office (ICO), In the picture: A data protection code of practice for surveillance cameras and personal information, 2015.

[87] David Gallacher. 2016. Drones to manage the urban environment: Risks, rewards, alternatives. *Journal of Unmanned Vehicle Systems*. **4**(2): 115-124. https://doi.org/10.1139/juvs-2015-0040

[88] A. Carrio, J. Tordesillas, S. Vemprala, S. Saripalli, P. Campoy and J. P. How, "Onboard Detection and Localization of Drones Using Depth Maps," in *IEEE Access*, vol. 8, pp. 30480-30490, 2020, doi: 10.1109/ACCESS.2020.2971938.

[89] Cavoukian, A. (2013). *Privacy by Design*: Leadership, Methods, and Results. In: Gutwirth, S., Leenes, R., de Hert, P., Poullet, Y. (eds) European Data Protection: Coming of Age. Springer, Dordrecht. https://doi.org/10.1007/978-94-007-5170-5_8

[90] Saltarella, M., Desolda, G., Lanzilotti, R. (2021). Privacy Design Strategies and the GDPR: A Systematic Literature Review. In: Moallem, A. (eds) HCI for Cybersecurity, Privacy and Trust. HCII 2021. Lecture Notes in Computer Science(), vol 12788. Springer, Cham. https://doi.org/10.1007/978-3-030-77392-2_16

[91] Fatema, K., Hadziselimovic, E., Pandit, H., Debruyne, C., Lewis, D., O'Sullivan, D. 2017. Compliance through informed consent: Semantic based consent permission and data management model. In: CEUR Workshop Proceedings.

[92] Gol Mohammadi, N., Leicht, J., Ulfat-Bunyadi, N., Heisel, M.: Privacy policy specification framework for addressing end-users' privacy requirements. In: Gritzalis, S., Weippl, E. R., Katsikas, S. K., Anderst-Kotsis, G., Tjoa, A. M., Khalil, I. (eds.) TrustBus 2019. LNCS, vol. 11711, pp. 46–62. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-27813-7_4

[93] Grodzinsky, F. and H. Tavani. "Privacy in "The Cloud": Applying Nissenbaum's Theory of Contextual Integrity." ACM SIGCAS Computers and Society 41.1 (2011): 38-47.

[94] Shilton, Katie, Building Values into the Design of Pervasive Mobile Technologies (June 18, 2011). Available at SSRN: https://ssrn.com/abstract=1866783 or http://dx.doi.org/10.2139/ssrn.1866783

[95] Bassi, E., Bloise, N., Dirutigliano, J. *et al.* The Design of GDPR-Abiding Drones Through Flight Operation Maps: A Win–Win Approach to Data Protection, Aerospace Engineering, and Risk Management. *Minds & Machines* **29**, 579–601 (2019). https://doi.org/10.1007/s11023-019-09511-9

[96] Rakesh Rajan Beck, Abhishek Vijeev, and Vinod Ganapathy. 2020. Privaros: A Framework for Privacy-Compliant Delivery Drones. In Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security (CCS '20). ACM, New York, NY, USA, 181–194. https://doi.org/10.1145/3372297.3417858

[97] Riham Altawy and Amr M. Youssef. 2016. Security, Privacy, and Safety Aspects of Civilian Drones: A Survey. ACM Trans. Cyber-Phys. Syst. 1, 2, Article 7 (April 2017), 25 pages. https://doi.org/10.1145/3001836

[98] Jeremy Seeman and Daniel Susser. 2023. Between Privacy and Utility: On Differential Privacy in Theory and Practice. ACM J. Responsib. Computing. (October). https://doi.org/10.1145/3626494

[99] Winfield, Alan & Harper, Christopher & Nembrini, Julien. (2005). Towards Dependable Swarms and a New Discipline of Swarm Engineering. Lecture Notes in Computer Science. 3342. 126-142. 10.1007/978-3-540-30552-1_11.