Technology in Society 71 (2022) 102079

Contents lists available at ScienceDirect

Technology in Society

journal homepage: www.elsevier.com/locate/techsoc

Safety and privacy regulations for unmanned aerial vehicles: A multiple comparative analysis

Dasom Lee [a], David J. Hess [b,*], Michiel A. Heldeweg [a]

[a] Department of Governance and Technology for Sustainability University of Twente Drienerlolaan 5, 7522 NB, Enschede, Netherlands
[b] Department of Sociology, Vanderbilt University PMB 351811, Nashville, TN, 37235-1811, USA

ARTICLE INFO

Keywords:
Unmanned aerial vehicles
Comparative analysis
Regulations
Privacy
Safety

ABSTRACT

With the growth of commercial and recreational use of unmanned aerial vehicles (UAVs, or drones), there is increasing attention to the need for regulation. A systematic review is conducted using a multiple comparative perspective: across three political jurisdictions (the United States, the European Union, and Japan) and across two areas of societal implication and policy (i.e., privacy and safety), with additional comparisons drawn from regulations for related cyber-physical systems. The multiple comparative analysis conducted in this paper shows that safety is a much more salient concern than privacy. Moreover, safety is focused on technical features of the UAVs, registration and certification, and differentiation by use case. Privacy regulations tend to follow broader digital privacy guidelines. Although there are some privacy rules that are UAV-specific, many of them do not yet directly address privacy challenges that are specific for UAVs. Additional comparisons with safety and privacy policies for automated vehicles and the smart grid reveal areas of potential development for harmonization and policy guidance. The study concludes with ten recommendations for future policy development.

1. Introduction

In countries across Africa, governments have teamed up with a drone company to allow a fleet of drones to deliver medical supplies to hospitals [1], and in the Netherlands, drones are being flown around greenhouses for lilies and tulips to detect diseased plants or to find weeds [2]. In the U.S, the first commercial drone delivery took place in Virginia in 2019 [3], and IT experts expect drones to change the landscape of the commercial delivery industry [4]. With the arrival of commercial use of unmanned aerial vehicles (UAVs) or unmanned aircraft systems (UASs) throughout the world, there is increasing recognition of the need for policy guidance that addresses societal implications and widely shared values such as safety and privacy.

Regulations and policy guidance for UAVs tend to vary widely across political jurisdictions, but the technologies and companies are already international. In order to improve manufacturing efficiency, to accommodate transboundary/border use, and to avoid undesirable regulatory competition, we argue that there is a need to consider both emerging differences in regulatory approaches and the potential for international harmonization. Harmonization can be beneficial by integrating best practices from different jurisdictions, and it can also reduce trade barriers.

This study provides a review of policy issues and potential next steps based on current developments in the three largest industrial economies among democratic countries: the United States (U.S.), the European Union (E.U.) area, and Japan. Furthermore, to identify gaps in safety and privacy within UAV regulations and to develop recommendations about next steps, we also draw on related policy developments for two other emerging cyber-physical systems: automated vehicles and the smart energy grid. We focus on automated vehicles because safety issues are prominent for this system, partly because of a prior history of governmental attention to vehicular transportation safety and partly because safety guidelines have already been established for on-road testing of automated vehicles [5–8]. Furthermore, we focus on the smart energy grid because there is also a prior history of governmental regulation of privacy for electricity data consumption and because the surveillance potential of real-time pricing systems has led to important innovations for this system with respect to privacy [9–13].

Based on a systematic review method, we build on a multiple comparative perspective that is emerging in the responsible innovation literature [14]: across different policy domains (safety and privacy), political jurisdictions (the E.U, Japan, and the U.S.), and other

* Corresponding author.
E-mail addresses: d.lee@utwente.nl (D. Lee), david.j.hess@vanderbilt.edu (D.J. Hess), m.a.heldeweg@utwente.nl (M.A. Heldeweg).

https://doi.org/10.1016/j.techsoc.2022.102079
Received 30 July 2021; Received in revised form 3 August 2022; Accepted 5 August 2022
Available online 13 August 2022

cyber-physical systems (comparisons with Connected and Automated Vehicles (CAVs) and smart grid systems). This perspective enables us to identify the potential for harmonization, gaps in existing policies, and next steps in policy development that can help to guide innovation in ways that address potential societal implications and challenges.

2. Literature review

2.1. Definitions

As aerial vehicles that carry no human operator on board, UAVs can often be piloted remotely, but increasingly the flight patterns and responses to the environment are automated. UAVs have been playing an integral role for military purposes (DeGarmo 2004), but they have many other applications, among them emergency response, search and rescue, border patrol, forest fire monitoring, traffic monitoring, humanitarian aid, crop monitoring, commercial security, and land use mapping (for more examples of UAV use, refer to DeGarmo [15]). Although drones can be classified by use case, there are other approaches, and an underlying issue for policy guidance is the challenge of classifying UAVs [16,17]. The United States Department of Defense has published classifications based on weight, normal operating altitude, and speed [18]. This study focuses on small UAVs (sUAVs), which are widely used for commercial and recreational purposes, and it excludes UAVs that are built for military purposes, which are not subjected to the same regulations.

There are many possible societal challenges and corresponding policy issues for UAVs, among them their effects on environmental sustainability, societal equity, civil liability, personal and public security, and also the broader issues of governance such as private UAV certification and regulation of airspace management. A full discussion of all societal implications of UAVs is beyond the scope of this study. We focus on privacy and safety because they are widely discussed and salient in the emerging policy developments and associated research [19–24]. Furthermore, safety and privacy also have become prominent policy issues in the comparison of cyber-physical systems. We follow the European Commission's definition of safety: a state of absence or reduced "occurrence or risk of injury, loss and danger to persons, property or the environment" [25]. With respect to privacy, we use the United Nations definition: "the presumption that individuals should have an area of autonomous development, interaction and liberty, a 'private sphere' with or without interaction with others, free from state intervention and excessive unsolicited intervention by other uninvited individuals. The right to privacy is also the ability of individuals to determine who holds information about them and how that information is used" ([26], p. 15).

2.2. Theoretical framework

The sociotechnical perspective has been widely discussed in the literature [27–31]. This approach to technological systems includes not only the design of hardware and software but also the connections with and among users, organizations, rules, and cultural dimensions. With respect to UAVs, the sociotechnical perspective has already been used with success. For example, Flores, Tan, and Crompvoets [27] drew attention to the role of governance and the support of local actors in understanding UAVs in Kenya. Similarly, Vujičić et al. [28] argued that attention to the social dimensions can define new ways to use drones (i.e., creating videos and using drones on vacations), which leads to new markets and opportunities.

The sociotechnical perspective is also foundational for much work in responsible innovation (RI) theory. RI reflects the ethical significance of a technical systems through the development of governance of innovation [32], and includes attempts to increase public participation through processes such as constructive technology assessment, participatory technology assessment, and upstream public engagement [33,34]. The framework of RI has become increasingly multidisciplinary [35] through the exploration of national culture, practicality and implementation, innovation actors, and utility [36,37]. RI is particularly interesting for new and emerging technological systems because it allows an in-depth analysis of new social challenges that the systems face, and it draws attention to policy-related and citizen-oriented solutions. For example, Buhman and Fieseler [38] showed how RI can be used to understand and improve the societal impacts of artificial intelligence research focusing on the issues of human autonomy, agency, fairness, and justice.

Within this broad terrain of sociotechnical and RI perspectives, we develop a comparative, sociotechnical design approach [14]. This approach focuses not only on the sociotechnical complexity of UAV systems but also on the choices involved in the design of hardware, software, user interfaces, organizations, standards, and policies. The approach provides a way of identifying the complex societal and regulatory challenges of new and emerging technologies. In addition, the approach promotes the comparative method as a way to develop new ideas and to reveal unexpected outcomes or unrealized assumptions about a new technology [14]. Furthermore, comparison can result in more effective regulatory frameworks by adopting best practices in design principles, which can be adopted across different types of technologies. In order to produce the most robust comparative analysis of new technologies, Hess and colleagues [14] suggested three comparative dimensions: (1) across technological systems, (2) across societal concerns and values, and (3) across political jurisdictions.

This review adopts the sociotechnical design perspective and uses its multi-dimensional comparative method. More specifically, it makes three comparisons (1) drones, automated vehicles, and smart grids/meters (across technological systems), (2) safety and privacy (across societal concerns and values), and (3) U.S, Germany, Netherlands, and Japan (across political jurisdictions).

2.3. Safety, privacy, and research questions

Despite the usefulness of UAVs, they raise a number of societal challenges and concerns, including effects on social equity, sustainability, security, and human rights [39]. In this study, we focus on safety and privacy because these two areas have received a high level of attention and some systematic policy guidance. With respect to safety, UAVs fly without a human operator in the aircraft, and the connection between the aircraft and the remote controller can be intermittent or not secure. The result can be a crash landing, interference with commercial aircraft, and other accidents. Rao et al. noted, "The primary criticism with the flying of commercial drones over public space is that small mistakes could result in crashes that threaten the health, well-being, and property of the public" [24, p. 86]. Micro or small UAVs also tend to have lower standards of hardware and software quality, which can increase the likelihood of accidents [40]. Furthermore, UAVs tend to be operated for a prolonged period of time, which can lead to interruptions in the attention given by operators [40]. (For a list of UAV related accidents and incidents, refer to Dedrone [41].)

In addition to safety, UAVs pose significant privacy concerns, particularly with camera attachment, which has become increasingly common [15,21,42,43]. UAVs can capture and record people or objects often without being seen, and they have the ability to easily cross terrestrial boundaries between private and public spheres [44]. Although we focus on privacy, the issue is frequently interconnected with security because the personal data and personally identifiable information collected by UAVs can also pose challenges to private and governmental security. Despite the significant challenges associated with data collection, storage, and use, there is a significant lack of national and international regulations addressing these concerns [24] and a need for more proactive regulation rather than reactive [45].

With this background in mind, the review that follows is based on two guiding research questions:

1. What are the current existing UAV regulations and policy guidelines on safety and privacy in the United States, the E.U. (countries specified below), and Japan?
2. What regulatory lessons can be learned from other new and emerging technologies regarding UAV safety and privacy?

After answering the two research questions, the review will then assess the potential for policy harmonization and for next steps in policy development.

3. Method

3.1. Political jurisdictions

The focus on the U.S, E.U, and Japan is based on the economic and political importance of the three economies. We use the phrase "political jurisdiction" rather than "countries" when referring to the comparison at this level because we include the E.U. in our analysis. The study does not include China, which also comprises one of the largest economies in the world, because of data accessibility problems. Focusing on large economies is important in analyzing relevant regulation of UAVs because they are likely to have the biggest commercial and civilian markets for UAV development, ownership, and use.

Because the E.U. is a supranational organization that is not comparable to a nation-state, the comparative unit of analysis needs further specification. The E.U. was included in the analysis because it often publishes guidelines and regulations for safety and privacy of new and emerging technologies. Most guidelines have a binding character, either by being immediately binding to E.U. citizens or by requiring member state implementation.

Member states have some room to develop their own regulatory framework, such as identifying no flying areas. Therefore, in order to address the differences among E.U. countries, and to ensure an even country-level comparison, we focus on two countries in Europe: Germany and the Netherlands. Germany is included because it has the largest economy in the E.U. and because it has advanced UAV regulations that are considered exemplary to other E.U. states. The Netherlands is also included because the country has a multidimensional approach (E.U. and national levels) that could contribute to a global development for the framework of UAV regulation.

3.2. Data selection and analysis

Adopting the descriptive methodology widely used in meta-analysis and comparative studies, data selection of this study is based on the Preferred Reporting Items for Systematic reviews and Meta-Analysis (PRISMA) [11,46,47]. Searches were conducted in both the Web of Science and Google Scholar. Because UAVs are referred to by different names, search terms included "Drones Regulation," "Drones Privacy," and "Drones Safety" with the country or region (i.e., E.U.) attached. Then we replaced the word "Drones" with "Unmanned Aerial Vehicles." In searching Unmanned Aerial Vehicles, we did not use quotation marks because the search would also include varying names of UAVs such as unmanned aerial systems, unmanned aircrafts, or unmanned aircraft systems. The country names were in quotation marks. The country/region names searched included the U.S, the E.U, Germany, Netherlands, and Japan.

Fig. 1 shows the selection process of research sources. In Phase 1, there were 871 records from Web of Science and 85 records from Google Scholar. In addition to the academic articles, we also used bills and other legal documents in the analysis, which led to additional 49 number of records. Once 281 duplicates were removed, we were left with 724 records. In Phase 2, the relevance of each article to the objectives of this study was determined based on a review of the abstracts. Here, articles were excluded if they focused on the engineering side of UAVs and applications of UAVs (e.g., water management, agriculture, natural disaster management/research). Because our primary interest is in commercial and recreational use of UAVs, we excluded articles on defense or military related usage of UAVs. The application of the inclusion criteria resulted in a further removal of 526 articles. In Phase 3, full text articles were assessed, which resulted in the exclusion of 11 additional articles from the analysis for lack of social science or policy relevance and 4 articles for irrelevance. As a result, 183 articles are included in this review.

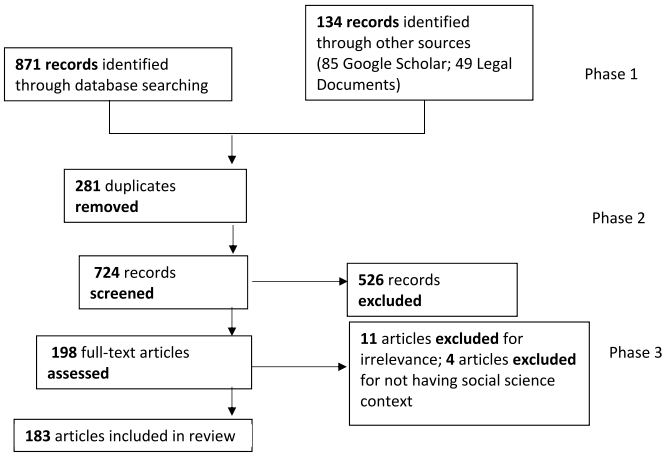

Fig. 1. Selection process for research sources.

The PRISMA method was used to collect UAV data only. For other cyber-physical systems discussed in this study, namely automated vehicles and smart grids/meters, we used existing studies that were based on reviews of regulations.

4. Findings

4.1. Current regulations on UAVs

4.1.1. United States

The development of regulations regarding commercial and recreational UAVs is relatively new in the U.S. at a federal government level. In 2014, the government courts developed a legal precedent that defined UAVs as "aircraft" (FAA v. Pirker case). In 2015, the Federal Aviation Administration (FAA) announced that businesses were allowed to gain approval to operate UAVs, and the agency mentioned that they expected over 7,000 businesses to have access to drones within three years [48]. In 2015, commercial drones with the maximum speed of 100 miles per hour, maximum weight of 0.55 pounds (250 g), and maximum altitude of 500 feet were allowed to fly during daylight only. Operators were required to be at least 17 years of age, have passed tests, and have a certificate to operate drones. Notably, the rules stated that drones could not be used for deliveries and that they must be directly visible by operator [49,50]. Later in the same year, the Federal Aviation Administration [51] announced that drones that weigh more than 0.55 pounds on takeoff, including everything that is attached to the aircraft, must be registered. In December 2020, the Federal Aviation Administration [52] announced the Final Rule on Operation of Small Unmanned Aircraft Systems Over People, which established four new categories of UAVs based on weight and severity of injury that can be caused, and it also permitted nocturnal flight with recurrent online training.

These new developments were particularly important from the perspective of safety. One notable change was the introduction of remote identification (Remote ID), which allows UAVs to provide "identification, location, and performance information that people on the ground and other airspace users can receive" ([53], pp. 6–7). If a UAV does not have the Remote ID technology, it must be operated within sight, which also improves safety. Most of the other regulations

on recreational and commercial drones in the U.S. also addressed safety issues (e.g., for recreational users, a drone must be under 0.55 pounds and must never fly near other aircraft; for commercial users, a drone must be less than 0.55 pounds including payload and must yield right of way to manned aircraft). Furthermore, recreational users are required to register their vehicles and take the recreational UAS safety tests, and commercial operators are required to be certified [54].

In contrast, there are no federal level privacy regulations that directly address the privacy challenges that UAVs pose. In the Final Rule, the FAA stated that "privacy issues are outside the focus and scope of the rule" [53]. Drone users are subjected to other privacy laws and regulations, and privacy is being addressed in some of the state governments. For example, in 2019, California amended the Assembly Bill No. 1129 to state that it is a misdemeanor to use UAV to invade a person's privacy [55], and Tennessee (a state with a significant music and concert industry) also prohibited using UAVs to take pictures and videos of individuals or events where more than 100 people are gathered unless otherwise consented [56].

4.1.2. The E.U

The E.U. has two bodies that are particularly involved in UAVs: the European Commission and the European Aviation Safety Agency. The discussion of UAV regulation first emerged in 2008 in "Regulation NO 216/2009 on Common Rules in the Field of Civil Aviation and Establishing a European Aviation Safety Agency" [57]. However, more in-depth discussion of regulation did not occur until the mid-2010s. In 2014, the European Commission published a communication that highlighted safety inspections, privacy, and data security of UAVs [58]. In 2015, the E.U. Aviation Strategy [54,59] acknowledged the need to develop a risk-based framework for regulating drones and addressed privacy, data protection, security, liability and insurance, and environment.

The European Aviation Safety Agency also has addressed UAV policy. In February 2019, the agency published an opinion document, which stated that the objective was "to increase the cost-effectiveness for drone operators, manufacturers and competent authorities, and to improve the harmonization of drone operations throughout Europe" [60]. This new UAV regulation does not make a distinction between commercial and recreational drones except for mandatory insurance. Operators of commercial drones, which are considered as air carriers and aircraft operators, are required to carry insurance [61].

The most important action taken by the EASA is the development of the new E.U. drone regulation, which came into effect from December 31, 2020, titled "Regulation (EU) 2019/947 of May 24, 2019 on the Rules and Procedures for the Operation of Unmanned Aircraft" [60]. UAVs are grouped into three categories: open (flights with low risk), specific (medium risk), and certified (high risk, larger size or dangerous cargo). The categories are defined based on the weight, size, and type of good that is being carried (i.e., dangerous goods such as explosives, gases, flammable liquids or solids etc.). There are subcategories, which further break down the open and specific categories into groups depending on weight and size [62].

The regulation has a specific section on safety. The most notable rule is the flight range. For the open category, UAVs must fly lower than 120 m; for the specific category, UAVs may fly higher than 120 m; and for the certified category, a special permit is required. All three categories require operators to have received some training whether it is an official certification or self-practicum unless they weigh less than 250 g. Additionally, in order to protect privacy, if the UAV has sensors that can breach privacy, it must be registered. The regulation also requires that member states establish registration systems to manage UAVs and to keep a record of UAV operators as well as manufacturers [62].

Regarding privacy, again there are no specific rules or guidance documents for privacy and UAVs. Instead, the General Data Protection Regulation (GDPR) has become a mandatory regulatory approach within the E.U. since 2015 [63]. Although the regulation does not directly discuss UAVs, it does provide an overarching regulatory framework for managing privacy in the process of digitalization, and it places a strong emphasis on the rights of the data subject and transfers of personal data to third parties. For the GDPR, member states are left to their own devices to develop their own strategies and regulatory frameworks that are consistent with the GDPR, yet appropriate to the national context.

Furthermore, another E.U. regulation also discuss the significance of privacy for UAVs. The EU Regulation 2018/1139 Section VII is dedicated to unmanned aircraft, in which it acknowledges the importance of "public security or protection of privacy and personal data" [64].

4.1.3. Germany

As a member of the E.U, Germany is required to follow the new rules introduced by the European Aviation Safety Administration (EU 2019/947). In addition, the federal government has introduced a few more rules that are specific to the country. Germany introduced two terms for UAVs: unmanned aviation systems (unbemannten Luftfahrtsystemen), which are UAVs used for commercial purposes, and flight models (model aircraft; Flugmodellen), which refer to recreationally used drones [65,66]. The Luftverkehrsgesetz (Aviation Act; LuftVG) has been in force since April 2017, and the government document regarding UAV regulations in 2022 indicates a gradual transition towards the EU2019/947. Until December 2022, a national exemption enabled drone operators to use drones in the open category [67].

Germany has several specific regulations regarding safety. With respect to identification and certification, all UAVs that weigh more than 0.25 kg must be marked with a sticker with the owner's name and address. For UAVs that weigh more than 2 kg, a certificate of knowledge is required. For UAVs weighing more than 5 kg or for nocturnal operations, permission must be granted by the Federal Supervisory Authority for Air Navigation Services (BAF). One aspect that is particularly notable in Germany is the acknowledgement that UAVs can have significant impact on various aspects of society, including nature conservation and aircraft noise [68]. Germany has also introduced a geospatial interactive map for drones to show where drones can be flown. Furthermore, by the end of 2022, the country aims to include additional safety measures such as online applications, route planner, and weather data or drone users [69]. In addition to safety, the rules also mention the issues of privacy regarding UAV operation. UAVs are banned over residential property if they weigh more than 0.25 kg or can receive, transmit, or record optical, acoustic, or radio signals [70].

4.1.4. Netherlands

In the Netherlands, rules were established by the Aviation Act 1992 (Wet Luchtvaart) and the Model Flying Scheme 2005 (Regeling Modelvliegen), which was specifically designed for model airplanes [71]. The Netherlands has successfully adopted the EU's drone classification in EU 2019/947. It uses the EU regulation as the basis for classification, registration, and licensing and supervision, and it maintains the nation-specific rules on flying drones (e.g., no flying at night). The country-specific rules regarding safety are introduced in two main regulations, "Regeling op afstand bestuurde luchtvaartuigen" (Remotely Piloted Aircraft Regulation, last amended in December 2020) and "Regeling onbemande luchtvaartuigen" (Regulation on unmanned aircraft, last amended April 2021) [72,73]. These rules include not being allowed to fly UAVs in the dark and a requirement for UAVs to yield to other aircraft, which means they must land immediately if there are any types of aircraft approaching, such as airplanes, helicopters, and gliders. Furthermore, specified areas where UAVs are partly or entirely off-limits can be checked using the safety map available online, or users can submit and receive digital clearance operations [74]. These areas may be restricted due to their national and political importance, such as the Royal Palace in Amsterdam or large national events [75]. Moreover, UAV operators are quired to report aviation accidents and incidents and must be safety aware.

The Netherlands also has an advanced commercial UAV regulation. Here, commercial is defined as making money from using UAVs. To fly a drone commercially, all rules that recreational users follow also apply. In addition, companies are required to register with the Human Environment and Transport Inspectorate (Inspectie Leefomgeving en Transport; ILT) directly, and operators should hold a pilot's license in addition to all the rules that apply to recreational drones [76].

4.1.5. Japan

In Japan, the Ministry of Land, Infrastructure, Transport and Tourism regulates UAVs. In 2015, an amendment to the Aeronautical Act required anyone who operates UAVs to obtain permission. It also prohibited UAV operation around airports, airspace at or above 150 m, and around densely inhabited areas. Furthermore, prohibited uses included flight at night, flight outside the line of sight, the transport of hazardous materials, and dropping of objects. In September 2019, some additional rules were introduced, which included prohibitions on use while under the influence of alcohol and drugs, flight paths that could cause collisions, and operation of UAVs in careless or reckless manner [77]. A new rule was enacted in June 2022, which changed the minimum weight limit to 100 g from 200 g and, it also required that any drone weighing more than 100 g will have to be registered [78].

If a person is found to have flown a UAV in a no-fly zone or in a densely populated area, a fine of 500,000 yen (approximately $4500 USD) can be charged. If a UAV operator is found to have operated UAVs under the influence of alcohol or drugs or not to have taken any preflight actions, the operator is liable for imprisonment up to one year or a fine up to 300,000 yen (approximately $2700 USD) [79].

Like the U.S, but unlike Germany and the Netherlands, there is little discussion of privacy in relation to UAVs. The Civil Aviation Bureau, which belongs to the Ministry of Land, Infrastructure, Transportation and Tourism, is in charge of establishing rules and public communication regarding UAV operation, but privacy is not discussed at all (see also Nakamura and Kajikawa [80]).

4.1.6. Summary of current UAV regulations

The currently existing UAV-specific regulations place high emphasis on the safety of UAVs and UAV operations. However, the discourse around safety tends to be focused on technical aspects (e.g., the weight or the height of flight), registration of the vehicles, and certification of the users. In general, as a matter of UAV-specific regulation, privacy is secondary, but there are some exceptions at the member state/country level in the E.U, and the GDPR provides an overarching framework on privacy regarding data collection and processing (See Table 1 for a summary.).

Table 1
Summary of UAV regulations.

	Safety	Privacy
United States	Weight and size regulation, remote ID	Acknowledged; generally state-specific rather than federal
E.U	Weight and size regulation, not allowed to transport dangerous goods, lateral distance regulation	General Data Protection Regulation (not specific to UAVs)
Germany	Follows the E.U. regulation	No recording or transmitting optical, acoustic, or radio signals for larger drones, adheres to the EU level regulations on privacy
Netherlands	Follows the E.U. regulation, no flying in the dark, UAVs not allowed in some areas, reporting of accidents	Unspecified, adheres to the EU level regulations on privacy
Japan	Weight and size regulation, lateral distance regulation, UAVs not allowed in some areas	No discussion of privacy

4.2. Cyber-physical systems comparisons

In this section, we draw on existing reviews to compare and contrast UAV regulations with two cyber-physical systems that have well established safety and privacy regulatory frameworks. For automated vehicles, there are unique regulations and guidelines for safety, which is one of the most essential goals of vehicle driving. Moreover, for the smart grid, privacy is a key challenge that many energy companies and consumers encounter. In analyzing the similarities and differences between these three cyber-physical systems, the goal of this paper is to open space for discussion on UAV regulatory improvements and harmonization.

4.2.1. Automated vehicles and safety

The understanding of safety in the automated vehicles regulatory framework focuses on four main issues: 1) rules for the safety driver to be present inside the vehicle or rules that guide remote control of the vehicle, 2) requirements for safety management plans or their equivalent, 3) requirements for data and reporting are required, and 4) rules for liability in case of accidents and collisions [5]. The U.S. does not have any regulations specific to automated vehicles at the federal level, but the federal government does provide guidelines for on-road testing [81, 82]. Therefore, this study uses California, which is the largest state (in population and aggregate gross economic product) and a leading site for automated vehicle testing, as an example of the United States. In addition, we also include the same political jurisdictions that are discussed above: the E.U, Germany, Netherlands, and Japan.

In the U.S, the federal government recognizes the importance of safety for automated vehicles, particularly after the fatal accident in Arizona in 2018 [83]. For example, proposed federal legislation attempted to allow derogation from existing safety regulations for automated vehicles. The proposed SELF DRIVE Act would not have allowed states to ban automated vehicles and also would have granted exemptions to existing safety standards for a car manufacturing company's first 100,000 vehicles. In general, the states took a cautious approach and adopted many safety regulations for automated vehicles [84]. Although California is one of the few places in the world that as of 2021 did not require the presence of safety driver inside the vehicle if the right permit was obtained [85], the state did require functional safety plans for automated vehicles that identify and assess hazardous situations that can occur during automated vehicle testing. California also has an automated vehicle recording regulation [86]. In cases of disengagements, where the automated driving system automatically disengages due to unexpected occurrence (e.g., fast lane changes, illegible road signs etc.), the testing body is required to file a disengagement report. In addition, in case of collision, the California Department of Motor Vehicles requires that an event data recorder records at least 30 s before the collision [87].

The E.U. regulations for this area are somewhat behind those of California [88]. The transportation regulation that automated vehicles are required to follow at the E.U. level is the 1968 Vienna Convention on Road Traffic. Nevertheless, the E.U. has been publishing guidelines and communications on how to build infrastructures such as data networks and social platforms for planned future use of automated vehicles [89, 90]. As a global leader in automobile manufacturing, Germany has developed some regulations for automated vehicles. Currently only Verband des Automobilindustrie (VDA) level 3 testing is allowed, which refers to vehicles that have automated features but require drivers to take over on request. Unlike California, safety drivers must be present, but the driver is not required to pay full attention at all times. Additionally, for data reporting, Germany requires a black box inside the vehicle to record any road testing [91]. In the Netherlands, a safety driver's presence is not required under the Dutch Road Traffic Act [92]. Nevertheless, the remote driver is required to monitor the vehicle from a distance, and the location of the remote driver must always be clear [93].

Japan is somewhat late to the regulatory development in this area.

The country allowed SAE level 3 automation in April 2020 through the Road Transportation Vehicle Act and the Road Traffic Act. SAE level 3 requires a safety driver inside the vehicle, and the Road Traffic Act states that a driver can use a mobile phone or other screen device inside level 3 automated vehicles as long as drivers can immediately respond to any emergencies. Furthermore, the law states that the testing vehicle must have a recording device [94,95].

CAVs and UAVs tend to share similar safety challenges because either they are remotely operated (UAVs), or remote control is the ultimate goal (CAVs). In this sense, the reliability of the technology, relevant data collection, and operators' understanding of safety are all salient.

4.2.2. Comparing automated vehicles and UAVs' safety issues

Because of the similarities of the safety challenges that automated vehicles and UAVs face, in this section, we compare the safety regulatory frameworks of the two cyber-physical systems. As it is evident from the discussion above, automated vehicles have more resources invested in detecting safety challenges compared to UAVs. There are more stringent regulations for automated vehicles (e.g., limiting the level of automation on public roads) because the consequences of safety risks are more severe for automated vehicles compared to UAVs. Therefore, in order to develop and nurture a safety-oriented environment for UAVs, some safety lessons can be learned from automated vehicles.

One striking gap that emerges from the cross-technology comparison is that operators of UAVs are not required to submit any collision or accident reports except in the Netherlands. This type of practice is prevalent for automated vehicles, where disengagement reports and recordings of accidents are all submitted to various authorities.

Furthermore, some regulatory action regarding the level of users could minimize safety risks. For example, in order to ensure safety of automated vehicles, the drivers are required to have a driver's license, which ensures that they have met the minimum amount of required training [5]. For UAVs, similar user certification would be beneficial. For example, a different level of regulation could be applied to new UAV users compared to seasoned users.

Many countries are now adopting registration for UAVs, which is similar to the registration practices for automated vehicles. All four countries discussed in this study (US, Germany, Netherlands, and Japan) require UAV registration. When UAV users register, they should receive extensive training on UAV use cases and associated safety risks. Such practice is already in place in the US, Germany, and Netherlands (and other EU countries that adhere to EU 2019/947), but it is not yet in place in Japan. For the time being, this would be the most practical way to approach UAV users regarding training.

Regarding automated vehicles, there are extensive fines and penalties in not meeting safety regulations and rules. However, for UAVs, such penalties are not yet in place except in Japan.

4.2.3. Smart energy grid/meter's privacy regulations

With respect to advanced metering infrastructure and smart meters, privacy is a more salient topic than safety, and policy guidance is also more developed than for the case of automated vehicles. One central privacy issue is that fine-grained energy consumption data associated with real-time pricing or short-term reporting of a household's consumption can reveal personal and personally identifying information, such as a household's socioeconomic status and appliances usage [9]. Energy consumption data can indicate when a home is empty, which can lead to security risks [12]. Consequently, the regulations for data associated with smart meters have focused on addressing privacy issues and broader concerns regarding data management.

In the United States, a few federal level guidelines have been developed to address the privacy issues associated with smart grids/meters. The Guidelines for Smart Meters Grid Cybersecurity, which was developed by the National Institute of Standards and Technology [96], recommended privacy impact assessments and privacy practices risk assessment in addition to employee training, audits, and data retention. Another document addressing privacy issues is the Framework and Roadmap for Smart Grid Interoperability Standards 3.0 [97], which discussed the customers' right to access their own data, the ongoing review standards for privacy, and a need for further research on privacy issues on cyber-physical systems. At the state level, California has one of the most advanced privacy regulations in the United States, and in 2018, it passed the Consumer Privacy Act, Assembly Bill 375 [98], which came into effect in January 2020. This Act establishes the four fundamental privacy rights for consumers. More specifically for smart meters, a regulatory rule [99] allows customers to opt out of smart meter data collection with a fee.

Again, the member states of the E.U. refer to the General Data Protection Regulation (GDPR) for privacy, but some also have their own privacy regulations. Similar to the U.S, the European Commission [100] also recommended data protection impact assessment for the smart grid to evaluate personal data protection risks for individuals and to examine the nature and severity of such privacy risks. In 2016, Germany's Metering Point Operation Law (Messstellenbetriebsgesetz, MsbG) laid the groundwork for smart meter deployment and required that for consumers under 10,000 kwh, data will be retained at home, and only those with data sharing tariffs will transmit more frequent energy consumption data to energy grid operators and suppliers [101]. Furthermore, the Act stated that all consumers will receive a data sheet with an explanation of what data traffic is, and they will be able to access their energy consumption data at all times. In the Netherlands, the Law for the Protection of Personal Information (Wet bescherming persoonsgegevens, Wbp) is not specific to smart meters, but it gives customers their right to know what is happening to their data, to view their data, and to object to the uses and processing of personal data [102]. Regarding smart energy meters, the country requires data to be read once a month for monthly statements and then once a year for annual energy bill (meters can be read more often with consumer consent). The country also established the Dutch Data Protection Authority, which reviews, applies, and enforces privacy regulations for data associated with smart energy meters.

Japan has a somewhat different approach to the countries mentioned above. Although the Japanese government is cautious about using personal energy consumption data, it is planning to use such data to shape and change industries, regulatory institutions, and infrastructures [103]. Japan has a general privacy regulation, "Referring to the Protection Regulation in 2021 (Revision of Individual Information Protection Systems) for the Structuring of Digital Societies" (令和３年 改正個人情報保護法について（官民を通じた個人情報保護制度の見直し） デジタル社会の形成を図るための関係法律の整備に関する法律). The Regulation covers all privacy breaches, was amended in 2021 to address digital privacy issues [104], and has been effective since May 2022. This law harmonizes all privacy rules that existed separately under different ministries (i.e., individual privacy, administrative privacy, independent administrative privacy), addresses privacy regulations regarding medical and academic research, and redefines the concept of personal information. However, compared to other countries' privacy regulations on smart meters, this law does not address some of the key aspects that are specific to smart energy meters, such as frequency of energy data sampling and smart meter opt out.

4.2.4. Comparing smart grids/meters and UAVs' privacy issues

Privacy regulations for the smart grid focus on having privacy impact assessments, monitoring, opt-out options, frequency of sampling, and consumer consent. It is difficult to directly apply these regulations to UAVs because privacy challenges for UAVs tend to be different. Smart meters are immobile, whereas UAVs tend to move around, which makes them much more vulnerable to various privacy breaches. Nevertheless, we argue that key privacy principles are transferrable from one cyber-physical system to another. From the perspective of smart energy meters, there are several potential innovations that could be translated into privacy policy for UAVs.

First, opt-out rules that appear in some U.S. states for smart meters could be used for UAVs to allow people to opt-out of recording of images or audio from UAVs without permission (such as filming or audio recording of people in residences or businesses). Here, "opt out" is considered favorable compared to "opt in" rules because of the potential social and environmental benefits of UAVs and practical issues of receiving consents from all population. In other words, the assumption is that unless specified otherwise, consent is given for recording images and audio from UAVs. In this sense, governments should develop platforms for the general public to opt out of audio and video recording of UAVs.

Second, Germany's disclosure rules (i.e., 10,000 kwh data retention rule, offering data sharing tariffs, receiving a data sheet, and being able to access their energy consumption data) could be extended to UAVs to require companies or individuals that engage in recording to disclose what information they collect and the data management practices. A website or platform could be developed in which companies or individuals disclose the recordings collected by UAVs. The information collected should not be considered to be owned by UAV owner but a collection that belongs to the public and should be used for public good.

Third, a significant part of smart meter privacy policy involves rules about data aggregation and data sharing with third-parties, and these rules could be extended to UAVs. Data sharing with third parties should be controlled and restricted, and data storage and deletion should have a limited time period. These privacy challenges are discussed and regulated by the GDPR, but they are not applicable in non-European countries.

Fourth, US, Germany, and Netherlands have privacy management government authorities that investigate privacy complaints. These privacy management institutions are important because they allow the public to communicate their concerns with government authorities. Once regulatory frameworks around UAV privacy become more developed and the public awareness increases, privacy management institutions will also become gradually more important in addressing UAV privacy challenges.

5. Discussion

5.1. Sociotechnical design perspective and harmonization efforts

This review uses the comparative sociotechnical design perspective to theoretically ground the technological, societal issues, and political jurisdiction dimensions of an emerging technological system. Because of multidimensional comparisons, the perspective is especially useful for harmonization efforts. It allows the identification of best practices across different technologies and across societal issues. Furthermore, because the similarities and differences are identified across various political jurisdictions, the approach can facilitate the harmonization of regulatory frameworks and the integration of best practices across multiple jurisdictions.

Regulatory harmonization for cyber-physical systems is important because it allows the standardization of technologies, leads to cost minimization and transparency, and facilitates smoother cross border interaction. Furthermore, harmonization can help developing countries to more address societal challenges that come with adopting new cyber-physical systems. In this sense, although international regulatory harmonization itself is a controversial topic [105], for new and emerging cyber-physical systems, regulatory harmonization is a useful tool.

Several efforts have been made regarding UAV regulatory harmonization. For example, the International Civil Aviation Organization (ICAO) with 193 member states [106] has produced a number of international standards, recommended practices and policies regarding aviation safety, infrastructure, operational risk, and global priorities [107]. One of the examples include global safety target of zero fatalities by 2030 [108]. Regarding UAVs, ICAO is specifically concerned about the safety related to the integration of UAVs into the existing airspace. Consequently, several proposals and workshops are being held to discuss operations of UAVs and standards related to altitude [109].

Another notable organization for international harmonization for UAVs is the Joint Authorities for Rulemaking on Unmanned Systems (JARUS), which includes a group of UAV experts from national and regional aviation authorities. One of the main contributions that JARUS has made is the introduction of Specific Operations Risk Assessment (SORA), which is a risk mitigation assessment method that is now widely used in Europe [110,111]. SORA has been essential in understanding and developing "safe creation, evaluation, and conduction of UAS operations" [112, p. 2]. It identifies operational safety objectives, which specifies and lists potential UAV related safety issues related to technical challenges, deterioration of external systems, human error, and other adverse operating conditions for UAV users to check before their fly their drones [112].

Although ICAO and JARUS have built the foundations for harmonization efforts, their efforts can be improved with the multiple comparative perspective developed here. For example, JARUS's SORA is mainly adopted only in Europe. Building on these existing efforts, this review makes UAV regulatory recommendations that would be applicable to a wider range of countries that are currently using UAVs. It also draws on comparisons across technological systems to assess the extent to which rules or guidelines developed for other systems can be useful for UAV-related policy.

5.2. Safety and privacy regulatory recommendations

Based on the existing UAV regulations and societal challenges discussed in the automated vehicles and smart meters literatures, we develop several recommendations as next steps in policy development. Some of the recommendations are in practice in some of the political jurisdictions discussed above, whereas others are not implemented at all. Our assumption is that government policy guidance or regulation is necessary, but in some cases private governance options may also be pursued.

1. Safety and privacy training for UAV users as part of their licensing or certification, with different levels required depending on the user type and use case.
2. Mandatory data reporting of collision and accidents, with recorded information where available.
3. Unique identifiers for all UAVs similar to vehicle registration.
4. Detailed differentiation of safety, privacy, and certification rules based on specific use cases.
5. Where UAVs conduct electronic recording, opt-out rights for residences or companies whose premises or activities are recorded.
6. Required disclosure by UAV users of data management practices (collection, storage, sharing, and deletion).
7. Specified limitations on third-party sharing of data collected by UAVs.
8. Penalties in cases of safety or privacy violations.
9. Government agencies or independent third-party monitoring and certification of privacy practices and complaints; an agency that collects, stores, and manages data collected by UAVs.
10. Efforts to harmonize or standardize UAV classifications, registration, certification, and use cases.

6. Conclusion

As UAVs become more widely adopted, providing a solid regulatory framework that is specific to the technology will become increasingly important. This study conducted a multiple comparative analysis based on a sociotechnical design perspective. The systematic review and comparative exercise provided the basis for the development of a list of

policy recommendations that could improve how companies, governments, and nongovernmental organizations are thinking about the issue. Although we focus on privacy and safety, we recognize other important societal implications, and it is possible that the methodology developed here could be extended to these other areas of implication and policy in future research.

Comparing regulations and developing foundations of regulatory frameworks is important not only for policy makers, but also for engineers, computer scientists, and civil society organizations. Through social scientific analysis and development of regulations, technical researchers and engineers can identify the important social challenges and attempt to address them in their technology design. Furthermore, civil society organizations have been addressing important social concerns by raising public awareness of new and emerging technologies (e.g., JARUS), and their role will become increasingly important in the future.

In order for a technological system to gain public acceptance, it is important for it to be deployed under clear conditions that ensure that widespread societal values and potential negative implications are addressed. Although we have restricted the analysis to two societal values, a similar analysis could be extended to other, less developed areas of policy (e.g., equity, democracy-surveillance, and sustainability implications). With respect to safety and privacy, no one wants a UAV to fall on their head while they are walking down the road or to have their (recognizable) pictures taken from afar without their knowledge. UAVs have been deployed and widely accessible for some time, which left many members of the public vulnerable to these issues. With the adoption of UAVs widening through commercial channels and with cheaper UAVs readily available through various easily accessible websites, issues such as safety and privacy will likely become increasingly salient. The policy recommendations that we provide above showcase some important insights into potential solutions to the use of UAVs that aligns with the public interest and that would improve public acceptance and confidence.

Author statement

Lee: Literature review, methods, empirical research, writing, revisions. **Hess**: Conceptual framework, editing, revisions, project administration. **Heldeweg**: European law, reviewing.

Funding

This project was partially supported by the U.S. National Science Foundation, OISE-1743772, Partnerships for International Science and Engineering (PIRE) Program: "Science of Design for Societal-Scale Cyber-Physical Systems." Any opinions, findings, conclusions, or recommendations expressed here do not necessarily reflect the views of the National Science Foundation.

Declaration of competing interest

The authors have no financial interest in the organizations or technologies described.

Data availability

As a review essay, data are cited. Additional information is available on request.

Acknowledgements

This study was also presented at the NSF-PIRE Workshop: Assured CPS Autonomy for 3D Urban Transportation: Drones, Flying Cars and Beyond in June 2021.

References

[1] Zipline, Transform Health Access, 2022. https://flyzipline.com/global-healthcare/. (Accessed 14 July 2022).
[2] Rethink Work, Dutch Precision Farming with Digital Agriculture, 2020. https://www.konicaminolta.eu/eu-en/rethink-work/business/digital-agriculture-how-dutch-farmers-use-precision-farming-for-floriculture. (Accessed 14 July 2022).
[3] J. Fisher, First consumer drone delivery service takes off in Virginia, FleetOwner (Oct. 21, 2019). https://www.fleetowner.com/technology/article/21704392/first-consumer-drone-delivery-service-takes-off-in-virginia. (Accessed 14 July 2022).
[4] M. O'Brien, Girl Scout Cookies Take Flight in Virginia Drone Deliveries, AP NEWS, 2021. Apr. 28,, https://apnews.com/article/health-technology-lifestyle-business-coronavirus-fdb288e4c4dc285b9eefae46ebe67201. (Accessed 14 July 2022).
[5] D. Lee, D.J. Hess, Regulations for on-road testing of connected and automated vehicles: assessing the potential for global safety harmonization, Transp. Res. Part Policy Pract. 136 (2020) 85–98.
[6] A. Taeihagh, H.S.M. Lim, Governing autonomous vehicles: emerging responses for safety, liability, privacy, cybersecurity, and industry risks, Transp. Rev. 39 (1) (Jan. 2019) 103–128, https://doi.org/10.1080/01441647.2018.1494640.
[7] Y.-C. Lee, A. Momen, J. LaFreniere, Attributions of social interactions: driving among self-driving vs. conventional vehicles, Technol. Soc. 66 (Aug. 2021) 101631, https://doi.org/10.1016/j.techsoc.2021.101631.
[8] T. Jannusch, et al., Surveillance and privacy – beyond the panopticon. An exploration of 720-degree observation in level 3 and 4 vehicle automation, Technol. Soc. 66 (Aug. 2021) 101667, https://doi.org/10.1016/j.techsoc.2021.101667.
[9] C. Beckel, L. Sadamori, T. Staake, S. Santini, Revealing household characteristics from smart meter data, Energy 78 (Dec. 2014) 397–410, https://doi.org/10.1016/j.energy.2014.10.025.
[10] J. Kaatz, Resolving the conflict between new and old: a comparison of New York, California and other state DER proceedings, Electr. J. 30 (9) (Nov. 2017) 6–13, https://doi.org/10.1016/j.tej.2017.10.005.
[11] D. Lee, D.J. Hess, Data privacy and residential smart meters: comparative analysis and harmonization potential, Util. Pol. 70 (2021), 101188.
[12] P. McDaniel, S. McLaughlin, Security and privacy challenges in the smart grid, IEEE Secur. Priv. 7 (3) (May 2009) 75–77, https://doi.org/10.1109/MSP.2009.76.
[13] D.D. Furszyfer Del Rio, Smart but unfriendly: connected home products as enablers of conflict, Technol. Soc. 68 (Feb. 2022) 101808, https://doi.org/10.1016/j.techsoc.2021.101808.
[14] D.J. Hess, et al., A comparative, sociotechnical design perspective on Responsible Innovation: multidisciplinary research and education on digitized energy and Automated Vehicles, J. Responsible Innov. 8 (3) (Sep. 2021) 421–444, https://doi.org/10.1080/23299460.2021.1975377.
[15] M.T. DeGarmo, Issues concerning integration of unmanned aerial vehicles in civil airspace, Cent. Adv. Aviat. Syst. Dev. 98 (2004).
[16] E. Mitka, S. Mouroutsos, Classification of drones, Am. J. Eng. Res. 6 (Jul. 2017) 36–41.
[17] A.G. Korchenko, O.S. Illyash, The generalized classification of unmanned air vehicles, in: 2013 IEEE 2nd International Conference Actual Problems of Unmanned Air Vehicles Developments Proceedings (APUAVD), Oct. 2013, pp. 28–34, https://doi.org/10.1109/APUAVD.2013.6705275.
[18] Department of Defense, Unmanned aircraft system Airspace integration plan, Jan. 21, https://web.archive.org/web/20160121155841/http://www.acq.osd.mil/sts/docs/DoD_UAS_Airspace_Integ_Plan_v2_(signed).pdf/, 2016. (Accessed 14 July 2022).
[19] J. Antunes, Addressing Privacy and Safety Concerns about Drones, UAV News, 2018. https://www.commercialuavnews.com/infrastructure/addressing-privacy-safety-concerns-drones-percepto. (Accessed 14 July 2022).
[20] S.J. Fox, The 'risk' of disruptive technology today (A case study of aviation – enter the drone), Technol. Soc. 62 (Aug. 2020), 101304, https://doi.org/10.1016/j.techsoc.2020.101304.
[21] R. Luppicini, A. So, A technoethical review of commercial drone use in the context of governance, ethics, and privacy, Technol. Soc. 46 (Aug. 2016) 109–119, https://doi.org/10.1016/j.techsoc.2016.03.003.
[22] L. Novaro Mascarello, F. Quagliotti, The civil use of small unmanned aerial systems (sUASs): operational and safety challenges, Aircraft Eng. Aero. Technol. 89 (5) (Jan. 2017) 703–708, https://doi.org/10.1108/AEAT-01-2017-0014.
[23] J. Nelson, T. Gorichanaz, Trust as an ethical value in emerging technology governance: the case of drone regulation, Technol. Soc. 59 (Nov. 2019) 101131, https://doi.org/10.1016/j.techsoc.2019.04.007.
[24] B. Rao, A.G. Gopi, R. Maione, The societal impact of commercial drones, Technol. Soc. 45 (May 2016) 83–90, https://doi.org/10.1016/j.techsoc.2016.02.009.
[25] European Commission, Safety rule, https://www.eionet.europa.eu/gemet/en/concept/7366, 2022. (Accessed 14 July 2022).
[26] D. Kaye, U. Secretary-General, and U. H. R. C. S. R. On the P. and P. of the R. to F. of O. and Expression, "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Aug. 2017 [Online]. Available: https://digitallibrary.un.org/record/1304394. (Accessed 14 July 2022).
[27] C. Casiano Flores, E. Tan, J. Crompvoets, Governance assessment of UAV implementation in Kenyan land administration system, Technol. Soc. 66 (Aug. 2021), 101664, https://doi.org/10.1016/j.techsoc.2021.101664.
[28] M.D. Vujičić, J. Kennell, U. Stankov, U. Gretzel, Đ.A. Vasiljević, A.M. Morrison, Keeping up with the drones! Techno-social dimensions of tourist drone

videography, Technol. Soc. 68 (Feb. 2022) 101838, https://doi.org/10.1016/j.techsoc.2021.101838.
[29] A.A. Nyaaba, M. Ayamga, Intricacies of medical drones in healthcare delivery: implications for Africa, Technol. Soc. 66 (Aug. 2021), 101624, https://doi.org/10.1016/j.techsoc.2021.101624.
[30] K. Haula, E. Agbozo, A systematic review on unmanned aerial vehicles in Sub-Saharan Africa: a socio-technical perspective, Technol. Soc. 63 (Nov. 2020), 101357, https://doi.org/10.1016/j.techsoc.2020.101357.
[31] A. Smith, J.E. Dickinson, G. Marsden, T. Cherrett, A. Oakey, M. Grote, Public acceptance of the use of drones for logistics: the state of play and moving towards more informed debate, Technol. Soc. 68 (Feb. 2022), 101883, https://doi.org/10.1016/j.techsoc.2022.101883.
[32] R. Von Schomberg, A vision of responsible research and innovation, Responsible Innov. Manag. Responsible Emergence Sci. Innov. Soc. (2013) 51, https://doi.org/10.1002/9781118551424.ch3. –74.
[33] A. Rip, Futures of Science and Technology in Society, 2018 [Online]. Available: https://link.springer.com/book/10.1007/978-3-658-21754-9. (Accessed 19 July 2022).
[34] A. Ely, P. Van Zwanenberg, A. Stirling, Broadening out and opening up technology assessment: approaches to enhance international development, co-ordination and democratisation, Res. Pol. 43 (3) (2014) 505–518, https://doi.org/10.1016/j.respol.2013.09.004.
[35] P.M. Loureiro, C.P. Conceição, Emerging patterns in the academic literature on responsible research and innovation, Technol. Soc. 58 (Aug. 2019), 101148, https://doi.org/10.1016/j.techsoc.2019.101148.
[36] A.D. Setiawan, The influence of national culture on responsible innovation: a case of CO2 utilisation in Indonesia, Technol. Soc. 62 (Aug. 2020), 101306, https://doi.org/10.1016/j.techsoc.2020.101306.
[37] M. Lukovics, S.M. Flipse, B. Udvari, E. Fisher, Responsible research and innovation in contrasting innovation environments: socio-Technical Integration Research in Hungary and The Netherlands, Technol. Soc. 51 (Nov. 2017) 172–182, https://doi.org/10.1016/j.techsoc.2017.09.003.
[38] A. Buhmann, C. Fieseler, Towards a deliberative framework for responsible innovation in artificial intelligence, Technol. Soc. 64 (Feb. 2021), 101475, https://doi.org/10.1016/j.techsoc.2020.101475.
[39] T. Wall, T. Monahan, Surveillance and violence from Afar: the politics of drones and liminal security-scapes, Theor. Criminol. 15 (3) (Aug. 2011) 239–254, https://doi.org/10.1177/1362480610396650.
[40] R. Clarke, L. Bennett Moses, The regulation of civilian drones' impacts on public safety, Comput. Law Secur. Rep. 30 (3) (Jun. 2014) 263–285, https://doi.org/10.1016/j.clsr.2014.03.007.
[41] Dedrone, Map of Global Drone Incidents by Dedrone Anti-drone/CUAS Solution, 2022. https://www.dedrone.com/resources/incidents/all. (Accessed 14 July 2022).
[42] A. Cavoukian, Privacy and Drones: Unmanned Aerial Vehicles, Information and Privacy Commissioner, 2012 [Online]. Available: https://www.publicsafety.gc.ca/lbrr/archives/cnmcs-plcng/cn29822-eng.pdf.
[43] U. Volovelsky, Civilian uses of unmanned aerial vehicles and the threat to the right to privacy – an Israeli case study, Comput. Law Secur. Rep. 30 (3) (Jun. 2014) 306–320, https://doi.org/10.1016/j.clsr.2014.03.008.
[44] J.R. Nelson, T.H. Grubesic, D. Wallace, A.W. Chamberlain, The view from above: a survey of the public's perception of unmanned aerial vehicles and privacy, J. Urban Technol. 26 (1) (Jan. 2019) 83–105, https://doi.org/10.1080/10630732.2018.1551106.
[45] J. Villasenor, Observations from above: unmanned aircraft systems and privacy, Harv. J. Law Publ. Pol. 36 (2013) 457.
[46] D. Moher, A. Liberati, J. Tetzlaff, D.G. Altman, PRISMA Group, Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement, Int. J. Surg. Lond. Engl. 8 (5) (2010) 336–341, https://doi.org/10.1016/j.ijsu.2010.02.007.
[47] A.C. Tricco, et al., PRISMA extension for scoping reviews (PRISMA-ScR): checklist and explanation, Ann. Intern. Med. 169 (7) (Oct. 2018) 467–473, https://doi.org/10.7326/M18-0850.
[48] United States Government Publishing Office, Full Committee Hearing on Oversight of the Small Business Administration and its Programs, 2009. https://www.govinfo.gov/content/pkg/CHRG-111hhrg48124/html/CHRG-111hhrg48124.htm. (Accessed 14 July 2022).
[49] Federal Aviation Administration, 14 CFR Part 107 – Small Unmanned Aircraft Systems, National Archives, 2021. https://www.ecfr.gov/current/title-14/chapter-I/subchapter-F/part-107. (Accessed 14 July 2022).
[50] Kurtis Lee, FAA Drone Rule Proposal: what They Allow, Who Benefits, Who Doesn't, Los Angeles Times, Feb. 16, 2015. https://www.latimes.com/nation/nationnow/la-na-nn-proposed-drone-rules-20150216-story.html. (Accessed 14 July 2022).
[51] Federal Aviation Administration, Code of Federal Regulations, 2020. https://www.govinfo.gov/content/pkg/CFR-2020-title14-vol1/xml/CFR-2020-title14-vol1-part48.xml. (Accessed 14 July 2022).
[52] Federal Aviation Administration, Operation of Small Unmanned Aircraft Systems over People, Federal Aviation Administration, 2021 [Online]. Available: https://www.faa.gov/news/media/attachments/OOP_Final%20Rule.pdf.
[53] Federal Aviation Administration, Remote Identification of Unmanned Aircraft, Federal Aviation Administration, 2020 [Online]. Available: https://www.faa.gov/news/media/attachments/RemoteID_Final_Rule.pdf.
[54] European Commission, Unmanned Aircraft, 2022. https://defence-industry-space.ec.europa.eu/eu-aeronautics-industry/unmanned-aircraft_en. (Accessed 14 July 2022).
[55] Assembly Bill 1129, "An Act to amend section 647 of the penal code, relating to privacy.," California Legislative Information. https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201920200AB1129 (accessed Jul. 14, 2022).
[56] State of Tennessee, Public Chapter No 40, Public Chapter No 40. An Act to Amend Tennessee Code Annotated Title 39, Chapter 13, relative to Unmanned Aircraft (2019) [Online]. Available: https://publications.tnsosfiles.com/acts/111/pub/pc0040.pdf.
[57] European Commission, Regulation (EC) No 216/2009 of the European Parliament and of the Council of 20 February 2009 on Common Rules in the Field of Civil Aviation and Establishing a European Aviation Safety Agency, 2008 [Online]. Available: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:079:0001:0049:EN:PDF.
[58] European Commission, Communication from the Commission to the European Parliament and the Council: A New Era for Aviation. Opening the Aviation Market to the Civil Use of Remotely Piloted Aircraft Systems in a Safe and Sustainable Manner, 2014 [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52014DC0207&from=EN/.
[59] European Commission, European Commission Presents an Aviation Strategy for Europe, 2019. https://transport.ec.europa.eu/news/european-commission-presents-aviation-strategy-europe-2019-06-27_en. (Accessed 14 July 2022).
[60] European Union Aviation Safety Administration, *Commission Implementing Regulation (EU) 2019/947 of 24 May 2019* on the Rules and Procedures for the Operation of Unmanned Aircraft (Text with EEA relevance.) vol. 152, 2019 [Online]. Available: http://data.europa.eu/eli/reg_impl/2019/947/oj/eng. (Accessed 14 July 2022).
[61] European Parliament, Regulation (EC) No 785/2004 of the European Parliament and of the Council of 21 April 2004 on Insurance Requirements for Air Carriers and Aircraft Operators, 2004 [Online]. Available: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:138:0001:0006:EN:PDF.
[62] European Union Aviation Safety Administration, EASA Publishes Opinion 'Standard Scenarios for UAS Operations in the "Specific" Category, '" *EASA*, 2019. https://www.easa.europa.eu/newsroom-and-events/news/easa-publishes-opinion-standard-scenarios-uas-operations-specific-category. (Accessed 14 July 2022).
[63] European Parliament and the Council of the European Union, Regulation (EU) 2016/679 of the European Parliament of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016. https://eur-lex-europa-eu.ezproxy2.utwente.nl/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN/. (Accessed 14 July 2022).
[64] European Parliament, Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on Common Rules in the Field of Civil Aviation and Establishing a European Union Aviation Safety Agency, and Amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and Repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91, 2018 [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32018R1139&from=EN#d1e3731-1-1.
[65] Bundesministerium der Justiz und fur Verbraucherschutz, Luftverkehrsgesetz (LuftVG), 2020. https://www.gesetze-im-internet.de/luftvg/. (Accessed 14 July 2022).
[66] Bundesministerium für Verkehr und digitale Infrastruktur, EU-Regelungen für Drohnen, 2021. https://www.bmvi.de/SharedDocs/DE/Artikel/LF/drohnen.html. (Accessed 14 July 2022).
[67] Bundesministerium für Digitales und Verkehr, "Betreff: Erlass des Bundesministeriums für Digitales und Verkehr zum gewerblichen Betrieb von unbemannten Luftfahrtsystemen in der offenen Kategorie, Unterkategorie A2, die nicht gemäß der Delegierten Verordnung (EU) 2019/945 klassifiziert sind. Gültigkeit: 01. Januar 2022 bis 31. August 2022." 2022. [Online]. Available: https://www.lba.de/SharedDocs/Downloads/DE/B/B5_UAS/Erlass_03.01.22_A2.pdf;jsessionid=F5AAC6D71DE2879D6EB86C999C352AAF.live21304?_blob=publicationFile&v=2.
[68] H. Eißfeldt, et al., The acceptance of civil drones in Germany, CEAS Aeronaut. J. 11 (3) (Sep. 2020) 665–676, https://doi.org/10.1007/s13272-020-00447-w.
[69] Federal Ministry for Digital and Transport, BMDV - Digital Platform for Unmanned Aviation Launched, 2022. https://www.bmvi.de/SharedDocs/EN/PressRelease/2022/004-wissing-digital-platform-unmannend-aviation.html. (Accessed 20 July 2022).
[70] Federal Ministry of Transport and Digital Infrastructure, Clear Rules for the Operation of Drones, 2021 [Online]. Available: https://www.bmvi.de/SharedDocs/EN/Articles/LF/clear-rules-for-the-operation-of-drones.html.
[71] Ministerie van Binnenlandse Zaken en, Regeling Modelvliegen, 2022. https://wetten.overheid.nl/BWBR0019147/2019-04-01. (Accessed 14 July 2022).
[72] Ministerie van Binnenlandse Zaken en, Regeling Op Afstand Bestuurde Luchtvaartuigen, 2020. https://wetten.overheid.nl/BWBR0036568/2020-12-31#Bijlage6. (Accessed 14 July 2022).
[73] Ministerie van Binnenlandse Zaken en, Regeling Onbemande Luchtvaartuigen, 2021. https://wetten.overheid.nl/BWBR0044598/2021-04-22#Hoofdstuk6. (Accessed 14 July 2022).
[74] GoDrone, Welcome to GoDrone, 2022. https://www.godrone.nl/. (Accessed 15 July 2022).

[75] Ministerie van Infrastructuur en, Rules for the Recreational Use of Drones - Drones - Government.Nl, Jul. 21, 2016. https://www.government.nl/topics/drone/rules-pertaining-to-recreational-use-of-drones. (Accessed 14 July 2022).
[76] M. van I. en Waterstaat, Rules for the Commercial Use of Drones - Drones - Government.Nl, Jul. 21, 2016. https://www.government.nl/topics/drone/rules-pertaining-to-the-commercial-use-of-drones. (Accessed 17 July 2022).
[77] Ministry of Land, Infrastructure, Transport and Tourism, "Civil Aviation Bureau：Japan's Safety Rules on Unmanned Aircraft (UA)/Drones - MLIT Ministry of Land, Infrastructure, Transport and Tourism, 2022. https://www.mlit.go.jp/en/koku/uas.html. (Accessed 14 July 2022).
[78] Ministry of Land, Infrastructure, Transport and Tourism, 2022. Drone/UAS Information Platform System," *Drone/UAS Information Platform System*, https://www.dips-reg.mlit.go.jp/drs/manual_en.html. (Accessed 17 July 2022).
[79] Ministry of Land, Infrastructure, Transport and Tourism, "Rules on Flying Drones in Japan, 2021. https://dwl.gov-online.go.jp/video/cao/dl/public_html/gov/book/hlj/20191201/html5.html#page=23. (Accessed 14 July 2022).
[80] H. Nakamura, Y. Kajikawa, Regulation and innovation: how should small unmanned aerial vehicles be regulated? Technol. Forecast. Soc. Change 128 (Mar. 2018) 262–274, https://doi.org/10.1016/j.techfore.2017.06.015.
[81] U.S. Department of Transportation, Preparing for the future of transportation: automated vehicles 3.0, National Highway Traffic Safety Administration (2018) [Online]. Available: https://www.transportation.gov/av/3.
[82] U.S. Department, Of Transportation, "Automated Driving Systems 2.0: A Vision for Safety, National Highway Traffic Safety Administration, 2017 [Online]. Available: https://www.nhtsa.gov/sites/nhtsa.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf.
[83] National Transportation Safety Board, Preliminary Report Highway HWY18MH010 - Urbanism Next, 2018. https://www.urbanismnext.org/resources/preliminary-report-highway-hwy18mh010. (Accessed 14 July 2022).
[84] United States Congress, Summary of H.R. 3388 (115th): SELF DRIVE Act," *GovTrack.Us*, 2020. https://www.govtrack.us/congress/bills/115/hr3388/summary. (Accessed 14 July 2022).
[85] State of California Department of Motor Vehicles, Order to Adopt. Title 13, Division1, Chapter 1, Article 3.7 Testing of Autonomous Vehicles, State of California Department of Motor Vehicles, 2018 [Online]. Available: https://www.dmv.ca.gov/portal/uploads/2020/06/Adopted-Regulatory-Text-2019.pdf.
[86] State of California Department of Motor Vehicles, DMV Statement on Federal Automated Vehicle Policy, California DMV, 2016. https://www.dmv.ca.gov/portal/news-and-media/dmv-statement-on-federal-automated-vehicle-policy/. accessed Jul. 14, 2022.
[87] State of California Department of Motor Vehicles, Express Terms Title 13, Division 1, Chapter 1 Article 3.7 – Autonomous Vehicles. State of California Department of Motor Vehicles, 2015 [Online]. Available: https://www.tellusventure.com/downloads/transport/calif_dmv_express_terms_autonomous_vehicles_30sep2016.pdf.
[88] A. Medina, A. Maulana, D. Thomson, N. Shandilya, S. Almeida, Public Support Measures for Connected and Automated Driving: Final Report, 2017 [Online]. Available: file:///Users/dasomlee/Downloads/CAD%20-%20Final%20Report%202017.05.31.pdf.
[89] European Commission, Autonomous cars: a big opportunity for European industry. European commission, digital transformation monitor, Eur. Community (2017) [Online]. Available: https://ati.ec.europa.eu/sites/default/files/2020-07/Autonomous%20cars%20%28v1%29.pdf.
[90] European Commission, Communication from the Commission to the European Parliament, Council, the European Economic and Social Committee and the Committee of the Regions, 2017. https://ec-europa-eu.ezproxy2.utwente.nl/transparency/documents-register/detail?ref=COM(2017)9&lang=en. (Accessed 14 July 2022).
[91]]] Bundesministerium der Justiz und für Verbraucherschutz, Straßenverkehrsgesetz (StVG)., 2019. https://www.gesetze-im-internet.de/stvg/BJNR004370909.html. (Accessed 14 July 2022).
[92] Government of the Netherlands, Experimenteerwet Zelfrijdende Auto, 2019. https://www.internetconsultatie.nl/experimenteerwet_zelfrijdendeauto/berichten/. (Accessed 14 July 2022).
[93] N. Kieboom, Experimenteerwet Zelfrijdende Auto: Bestuurder Op Afstand Aansprakelijk (Self Driving Car Experimentation Law: Driver Remotely Liable), VerkeersNet, 2018. https://www.verkeersnet.nl/mobiliteitsbeleid/25758/experimenteerwet-zelfrijdende-auto-bestuurder-op-afstand-aansprakelijk/. (Accessed 14 July 2022).
[94] Ministry of Land, Infrastructure, Transport and Tourism, "Transport and Tourism, Road Traffic Act (道路交通法), 2020. https://elaws.e-gov.go.jp/document?lawid=335AC0000000105. (Accessed 14 July 2022).
[95]]] Ministry of Land, Infrastructure, Transport and Tourism, "Road Transportation Vehicle Act (道路運送車両法), 2020. https://elaws.e-gov.go.jp/document?lawid=326AC0000000185_20220401_504AC0000000004&keyword=%E9%81%93%E8%B7%AF%E9%81%8B%E9%80%81%E8%BB%8A%E4%B8%A1%E6%B3%95. (Accessed 14 July 2022).
[96] The Smart Grid Interoperability Panel–Smart Grid Cybersecurity Committee, Guidelines for Smart Grid Cybersecurity, National Institute of Standards and Technology, Sep. 2014, https://doi.org/10.6028/NIST.IR.7628r1. NIST IR 7628r1.
[97] C. Greer, et al., NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0, National Institute of Standards and Technology, NIST SP, Oct. 2014, https://doi.org/10.6028/NIST.SP.1108r3, 1108r3.
[98] Assembly Bill No. 375, Assembly Bill No. 375 Chapter 55, an Act to Add Title 1.81.5 (Commencing with Section 1798.100) to Part 4 of Division 3 of the Civil Code, 2018. Relating to Privacy, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375. (Accessed 14 July 2022).
[99] California Public Utilities Commission, Decision Regarding Smart Meter Opt-Out Provisions, 2014 [Online]. Available: https://docs.cpuc.ca.gov/PublishedDocs/Published/G000/M143/K904/143904205.PDF.
[100] European Data Protection Supervisor, Data Protection Impact Assessment (DPIA) | European Data Protection Supervisor, 2022 accessed Jul. 20, 2022), https://edps.europa.eu/data-protection/data-protection-impact-assessment-dpia_en.
[101] Bundeministerium für Wirtschaft und Energie, Gesetz über den Messstellenbetrieb und die Datenkommunikation in intelligenten Energienetzen (Messstellenbetriebsgesetz - MsbG), 2016 [Online]. Available: https://www.gesetze-im-internet.de/messbg/MsbG.pdf.
[102] Ministerie van Binnenlandse Zaken en, Wet Bescherming Persoonsgegevens, 2018. https://wetten-overheid-nl.ezproxy2.utwente.nl/BWBR0011468/2018-05-01#Hoofdstuk3. (Accessed 14 July 2022).
[103] SankeiBiz, スマート電力メーターの個人記録、情報銀行介して活用 経産省、制度変更へ - 産経ニュース, 2019. https://www.sankei.com/article/20191120-7WEWC2JDBVJ67HMZULH6RBMF3M/. (Accessed 14 July 2022).
[104] Personal Information Protection Commission Japan, 令和３年 改正個人情報保護法について（官民を通じた個人情報保護制度の見直し, 2021 [Online]. Available: https://www.ppc.go.jp/personalinfo/minaoshi.
[105] D.A. Singer, Capital rules: the domestic politics of international regulatory harmonization, Int. Organ. 58 (Jul. 2004), https://doi.org/10.1017/S0020818304583042, 03.
[106] International Civil Aviation Organization, Member States, 2022. https://www.icao.int/about-icao/Pages/member-states.aspx. (Accessed 18 July 2022).
[107] T. Gastineau, What can vaccines learn from aviation? Vaccine 38 (33) (2020) 5082–5084, Jul, https://doi.org/10.1016/j.vaccine.2020.06.027.
[108] International Civil Aviation Organization, Saf. Now. (2022). https://www.icao.int/safety/Pages/default.aspx. (Accessed 18 July 2022).
[109] International Civil Aviation Organization, ICAO Issues Call for Innovative Solutions for Drone Airspace Management, 2018. https://www.icao.int/Newsroom/Pages/ICAO-issues-call-for-innovative-solutions-for-drone-airspace-management.aspx. accessed Jul. 20, 2022.
[110] C. Capitán, J. Capitán, Á.R. Castaño, A. Ollero, Risk assessment based on SORA methodology for a UAS media production application, in: 2019 International Conference on Unmanned Aircraft Systems (ICUAS), Jun. 2019, pp. 451–459, https://doi.org/10.1109/ICUAS.2019.8798211.
[111] K.H. Terkildsen, K. Jensen, Towards a tool for assessing UAS compliance with the JARUS SORA guidelines, in: 2019 International Conference on Unmanned Aircraft Systems (ICUAS), Jun. 2019, pp. 460–466, https://doi.org/10.1109/ICUAS.2019.8798236.
[112] P. Janik, M. Zawistowski, R. Fellner, G. Zawistowski, Unmanned aircraft systems risk assessment based on SORA for first responders and disaster management, Appl. Sci. 11 (12) (Jan. 2021), https://doi.org/10.3390/app11125364. Art. no. 12.

Dasom Lee is an assistant professor in the Department of Governance and Technology for Sustainability at the University of Twente, Netherlands. She received her Ph.D. from Vanderbilt University in sociology and has a master's degree in economics from Kyoto University (www.dasomlee.com).

David J. Hess is the James Thornton Fant Chair in Sustainability Studies, Professor of Sociology at Vanderbilt University, and Director of the Program in Environmental and Sustainability Studies (www.davidjhess.net).

Michiel A. Heldeweg is a professor of Law, Governance, and Technology at the University of Twente, program director of the Master's in Environmental and Energy Managmenet (MEEM), chairman of the UT Committee of Scientific Integrity, and member of the BMS/UT Academic Advisory Board. He is a member of the Netherlands Institute of Governance (NIG), an associate senior member of the Ius Commune Research School (ICOS), a partner to the Netherlands Institute for Law and Governance (NILG), and leader of the European Sustainable Energy Innovation Alliance (Eseia) Working Group (1) on Energy Governance, Business Models and Legal Frameworks.