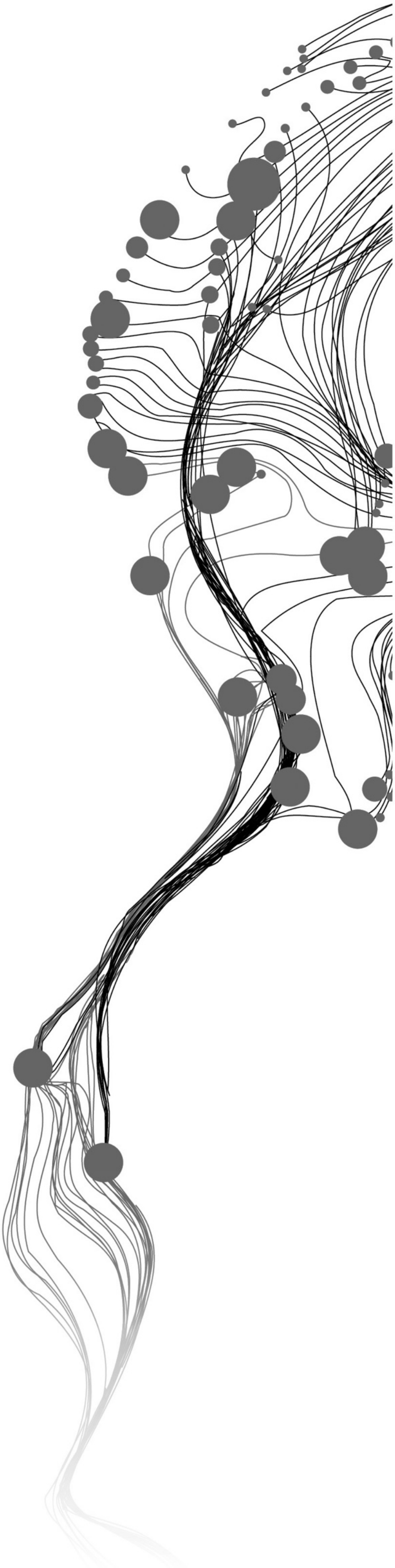
EVALUATE CURRENT REGULATORY FRAMEWORKS FOR UAVS IN TERMS OF PRIVACY

ZHIWEI MA
March, 2018

SUPERVISORS:
Dr. M. N. Koeva
Prof.dr.ir. J. A. Zevenbergen
Dr. F.C. Nex

ADVISOR:
MSc. E. C. Stöcker



EVALUATE CURRENT REGULATORY FRAMEWORKS FOR UAVS IN TERMS OF PRIVACY

ZHIWEI MA
Enschede, The Netherlands, March, 2018

Thesis submitted to the Faculty of Geo-Information Science and Earth Observation of the University of Twente in partial fulfilment of the requirements for the degree of Master of Science in Geo-information Science and Earth Observation.
Specialization: Land Administration

SUPERVISORS:
Dr. M. N. Koeva
Prof. dr. ir. J. A. Zevenbergen
Dr. F. C. Nex

ADVISOR:
MSc. E. C. Stöcker

THESIS ASSESSMENT BOARD:
Prof. dr. P.Y. Georgiadou (Chair)
Dr. M. N. Koeva
Prof. dr. Ir. J. A. Zevenbergen
Dr. F. C. Nex
Dr. ir. B. van Loenen (External Examiner, TU Delft)

DISCLAIMER

This document describes work undertaken as part of a programme of study at the Faculty of Geo-Information Science and Earth Observation of the University of Twente. All views and opinions expressed therein remain the sole responsibility of the author and do not necessarily represent those of the Faculty.

ABSTRACT

As a fitting technology for providing spatial and temporal scale data with low cost, unmanned aerial vehicles (UAVs) have raised increasing privacy concerns. To address the significant problem of privacy invasion in general, many international, as well as national authorities, have compiled and published UAV regulatory frameworks. However, as these regulations and guidelines are highly generalised, privacy violation concerns remain controversial. This study thereof conducted an evaluation of 14 UAV regulatory frameworks encompassing countries in different continents, with various legal systems, at diverse economic development levels. The results revealed that there is severe lack of privacy concerns in UAV regulations at the global level and some UAV operations prohibited under other legal frameworks are not clearly referred to current UAV regulatory frameworks.

With the rapid growth of similar image and video-based applications, Google Street View, Closed-circuit Television Cameras and visual lifelogging have already launched their solutions to address privacy concerns. This research identified the privacy threats of UAV applications by analysing current literature on UAV privacy concerns and referring to existing privacy threats distilled from Visual Lifelogging privacy studies. Based on the identified privacy threats, the technical applicability of possible solutions from other image and video-based applications have been analysed. The results indicated that feature-blurring solution of Google Street View, data uploading and data collection requirements of UK CCTV Code of Practice could be technically applied in UAV cases. However, solutions from Lifelogging are not applicable because of relatively complicated technical requirements.

This study ascertained the deficiency of current UAV regulations at the global level and proposed technically applicable solutions for mitigating UAV privacy concerns. Moreover, results of the research provided directions for future studies, such as to investigate how technically applicable solutions can be implemented under the influence of other factors (e.g. legal, cultural, economic aspects).

Keywords: UAV, Regulatory Framework, Privacy, UAV Regulations, Image-based Acquisition Techniques

ACKNOWLEDGEMENTS

Praise be to God, Lord of the Worlds.

My deepest gratitude goes to my supervisors Dr. Mila N. Koeva, Prof. Dr. Ir. Jaap A. Zevenbergen, Dr. Francesco C. Nex and M.Sc. Claudia Stöcker for the patient and immense support extended to me through their expert advice, continuous guidance, and constructive contribution. I am also grateful to Pr. Dr. P.Y Georgiadou for her comments during my mid-term presentation which opened my mind and helped me to improve my work.

I would like to express my sincere gratitude to my dear friends: Abubakri Zaid, Hedi Abdullah, Muhammad Arshad, Ahmed Buregya, Ahmed Ibrahim, Dr. Yousif Hussin, Zhihong Ji, Nuhu Mujeeb, Sadadi Ojoatre, Aslihan Kol, Jiawei Zhang, Janvier Muhimpundu, Sheilla Ramadhani, Dr. Norhakim Yosuf, Ali Abri, Dr. Islam Fadel, Mahmood Abdelkader, Dennis Vermeulen, Ahmed Sicey, Abdulrahman Showaiter, Samer Karam, Faried Rhmany, Abdullah Hijris, Ali Issa, and Musa Osman for their encouragement, support and love.

I also thank all the staff of ITC particularly Land Administration domain, my fellow course mates, the staff of the Student Affairs and the ITC International Hotel, for your knowledge, support and hospitality given to me during my study.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS

ACHR	The American Convention on Human Rights
APEC	Asia Pacific Economic Cooperation
AUVSI	Association for Unmanned Vehicle Systems International
CDHRI	Cairo Declaration of Human Rights in Islam
CFREU	European Union Charter of Fundamental Rights
COA	Certificate of Authorization (US)
COP	CCTV Code of Practice (UK)
DPA	Data Protection Act (UK)
ECHR	European Convention on Human Rights
FAA	Federal Aviation Administration (US)
FMRA	FAA Modernization and Reform Act (US)
GDPR	General Data Protection Regulation (EU)
HDI	Human Development Index
ICAO	International Civil Aviation Organization
IPTS	Institute for Prospective Technological Studies
OAIC	Office of the Australian Information Commissioner
RPAS	Remotely Piloted Aircraft System
UAS	Unmanned Aircraft System
UAV	Unmanned Aerial Vehicle
UDHR	Universal Declaration of Human Right
UNDP	United Nations Development Programme

1. GENERAL INTRODUCTION

1.1. Introduction

Unmanned aerial vehicles (UAVs) are rising as a fitting technology for providing spatial and temporal scale data with low cost. However, increasing concerns about UAVs privacy become ubiquitous nowadays. In order to approach this significant problem of privacy among other issues (e.g. safety), many international and national authorities have launched regulatory frameworks. This study aims at evaluating current regulatory frameworks in terms of privacy. Meanwhile, to analyse similar privacy issue in other domains. Consequently, to propose possible recommendations to enhance current UAV regulatory frameworks.

1.2. Background and Justification

Unmanned aerial vehicles (UAVs) - also known as Remotely Piloted Aircraft System (RPAS) or Unmanned Aerial System (UAS) - are aircrafts and associated elements intended to be operated without a pilot on board (ICAO, 2009). In particular context, a UAV refers to an aircraft being operated with no pilot, while a UAS encapsulates to the aircraft or UAV with other components including ground-based controllers and communication system. According to ICAO Standard, RPAS is a form of UAS in which the aircraft is expressly subject to a licensed 'remote pilot control' at all stages of flight (Koeva et al., 2016).

The first UAV was applied for military purpose by the US Army in WWI (McBride, 2009). Recently, besides its military origin (Nex & Remondino, 2014), UAVs are now being utilised in multi-purpose civilian applications encompassing environment monitoring (Scholtz et al., 2011), agriculture (Efron, 2015), mapping (Remondino et al., 2011), documentation of cultural heritages and archaeological sites (Rinaudo et al., 2012), energy efficiency (Matsuoka et al., 2012), and cadastral surveying (Manyoky et al., 2012).

The appearance of unmanned aircraft systems (UAS) or remotely piloted aircraft systems (RPAS) in civilian applications has been narrated as momentous as the introduction of the jet engine (Walker, 2008). Hence, the rising of UAVs industry can be engaged in promoting entrepreneurship, raising industrial competitiveness and generating new businesses in order to boost economic growth (European RPAS Steering Group, 2013). According to the recent market research report, the global UAVs market was worth 13.22 Billion in 2016 and estimated to be USD 28.27 Billion by 2022 (Markets and Markets, 2016).

UAVs market is now fast-growing. However, more and more concern about privacy has been aroused recently (Schaub & Knierim, 2016). Due to the fact that UAVs usually fly silently and quickly while carrying imaging equipment and sensors (Rao et al., 2016), it is difficult to be recognised in visual line of sight. Accordingly, it intensifies concerns about privacy invasion (Schlag, 2013).

Regarding the significant problem of privacy invasion in general, many international, as well as national authorities, have compiled and published regulatory frameworks. For example, Europe has enacted Article 7 (Respect for private life) and Article 8 (Data protection) of the European Union Charter of Fundamental Rights, 2000/C 364/01(CFREU), in favour of respecting private life mentioned in Article 8 European Convention on Human Rights (2014). In the United States, on January 23, 2012, under the Fourth Amendment, the US Supreme Court unanimously held the vehicle-monitoring GPS installation (Nackenoff, 2012). In Africa, aiming to address cybersecurity harmonisation and combat privacy invasion, the African Union Convention on Cybersecurity and Personal Data Protection was ratified by African Union (AU) in 2014 (Makulilo, 2015). The Asia Pacific Economic Cooperation (APEC), which consists of twenty-one member states from Asian, Oceania, North America and South America, have adopted APEC privacy framework in 2005 (Asia Pacific Economic Cooperation, 2005). Moreover, many countries have also published regulations specific to UAV operations (see Figure 1). Therefore, the UAV regulations are established by most countries in different continents. Although UAVs for commercial and civil purposes might be constrained by versatile regulations, there have been limited studies about the UAV privacy implications (Cho, 2013).

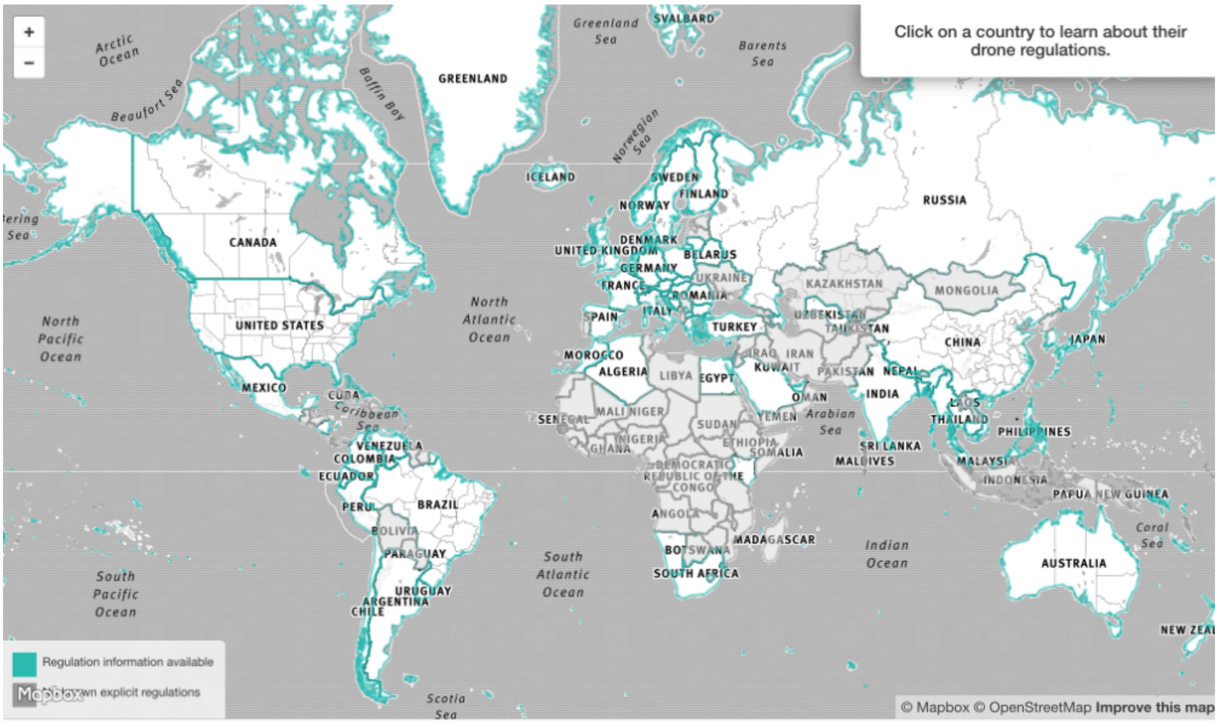


Figure 1: Worldwide UAV regulations overview[1]

In recent years, with rapid growth of systematically-gathered images, many image acquisition techniques are used to acquire high-resolution images such as Google Street View, Closed Circuit Television (CCTV), and Visual Lifelogging.

The most prominent example of image acquisition techniques is Google Street View. Google Street View was first launched as part of Google Maps in May 2007. Until June 2012, Google has proclaimed that 20 petabytes Street View data has been taken, which covered over 3,000 cities from 39 countries, consisting of images captured along 5 million miles of roads. Combining scale and accurate location, users could successfully locate interesting places. Simultaneously, these high-resolution street view images also make it possible to wander in a variety of sight scenes practically. Henceforth, Google Street View is broadly applied in travel planning, real estate search, virtual tourism, and business (Frome et al., 2009). As street-level imagery products develop, a prevalent dispute manifests itself as this kind of service may invade individual privacy. Personally identifiable features such as a person's face or license plate became significant concerns. Nevertheless, with face-blurring and car-plate-blurring solutions, the privacy-related problems can be partly solved (Frome et al., 2009).

1.3. Problem Statement

Privacy, data protection, and ethical concerns have been raised significantly since UAVs are being applied in multi-purpose civil applications. Correspondingly, aiming at decreasing the risk of UAV triggered

[1] World of Drones - Flights and Regulations. (August 20, 2017). Retrieved from http://drones.newamerica.org/#flights

incidents or accidents, miscellaneous international and national authorities have publicised regulations and guidelines for UAVs (Stöcker et al., 2017). However, as these regulations and guidelines are highly generalised, privacy violation concerns remain controversial, notably when UAVs are utilised for collecting images or video clips of particular targets without consent (Park & Lee, 2017).
Finn and Wright (2012) discussed contemporary UAS-related legislation in the EU, US and UK addressing privacy concerns. However, it was discovered that current regulatory frameworks fail to adequately grapple privacy concerns because UASs combine a variety of technologies and capacities. Schlag (2013) has also pointed out that protection of individual privacy should be guaranteed under the US Constitution Fourth Amendment, and privacy concerns should be prioritised rather than UAVs performance. Furthermore, Finn et al., (2014) said that in Europe some researchers assert that current regulatory frameworks regarding privacy are adequate. However, others held an opposite stand that specific regulations for UAVs are required.

After analysing 18 UAV regulations of countries ranging from different continents, with various legal systems, and at diverse economic development levels, it has been found that only twelve cases referred to privacy, but most of those 'only' advocate to 'respect personal privacy' (Stöcker et al., 2017). Therefore, there is a significant gap between current UAV regulatory frameworks and UAV privacy concerns in practice. Hence, this study is to make contribution to exploring privacy concerns of UAVs at regulatory framework level at a global scale, besides, to conducting an investigation of applicable solutions from current image-based acquisition applications such as Google Maps, closed-circuit television cameras (CCTV) and lifelogging.

This study provides information on weaknesses of current UAV regulatory frameworks. Accordingly, it can help international organisations and national authorities to understand a deficiency of current UAV regulations. This research can also help to enhance current regulatory frameworks by proposing possible solutions from image-based acquisition techniques which have already been successfully launched. Furthermore, this study can provide a baseline for future research in UAV related privacy, data protection, and regulatory framework directions.

1.4. Research Objectives

1.4.1. General Objective

To analyse UAV regulatory frameworks in terms of privacy at the global scale. To propose solutions from high-resolution image data privacy concerns in other domains and analyse if their solutions could be used in UAV regulations as well.

1.4.2. Specific Objectives

1. To review how privacy is conceived related to UAVs.
2. To evaluate current UAV regulatory frameworks in privacy aspect.
3. To propose solutions from other image-based acquisition techniques (e.g. Google Street View) and to analyse if they are applicable.

1.4.3. Research Questions

1. To review how privacy is perceived related to UAVs.
   1.1 How is privacy conceived related to UAVs in various regulations?
   1.2 How do current UAV regulations address privacy concern?

2. To evaluate the current regulatory frameworks in terms of privacy.
   2.1 What are weaknesses of current privacy terms?

2.2 What are the possible recommendations to improve current regulatory frameworks?

3. To propose solutions from other image-based acquisition techniques (e.g. Google Street View) and to analyse if they are applicable.
   3.1 What are similar applications in different domains?
   3.2 How do they deal with privacy concern?
   3.3 Can their experiences be applied in UAV regulatory frameworks?

1.5. Hypothesis

There is significant lack of privacy terms in the current UAV regulatory frameworks. Solutions for high-resolution image privacy concern in other domains could contribute to improving current UAV regulatory frameworks.

1.6. Conceptual Framework

The conceptual framework includes three parts (see Figure 2). The UAV regulations give guidance the UAV applications by setting different rules, constraints and restrictions. For example, in some countries and regions (Clarke & Moses, 2014), a UAV license on pilots is required for any UAV-based activity (Federal Aviation Administration, 2016). Meanwhile, privacy invasion cases are aroused by UAVs (Carr, 2016; Kaminski, 2013; Rao et al., 2016). Thus, UAV applications directly affect privacy concerns. However, it is not clear to which extent the existing UAV regulations have addressed the various aspects of privacy. Therefore, this research is going to explore the gap between UAV regulations and UAVs related privacy concerns and how proposed solutions can be effectively incorporated into UAV regulations in order to address the privacy concerns.

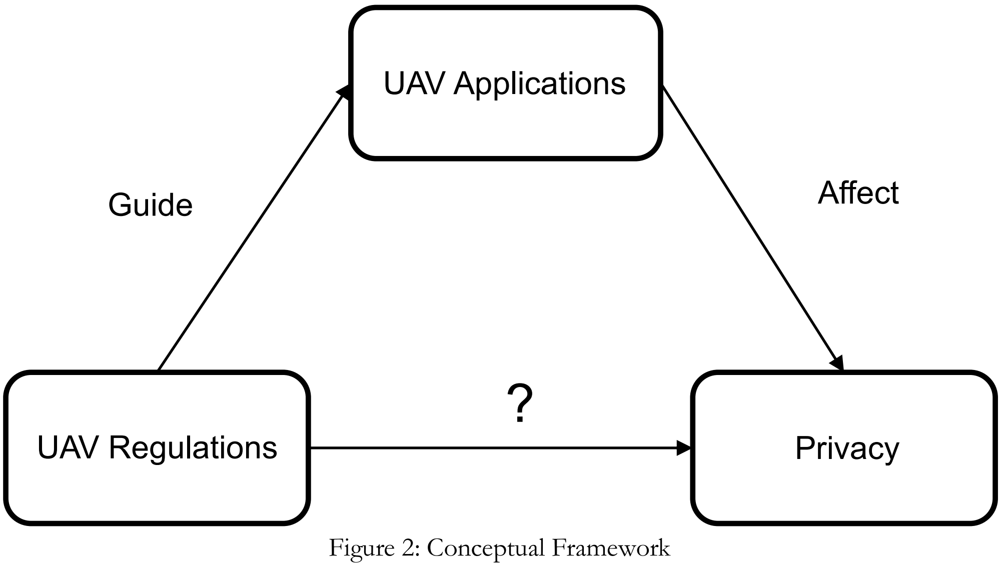


Figure 2: Conceptual Framework

1.7. Thesis Structure

The provisional thesis structure consists of:

Chapter 1: Introduction - includes the background and justification, research problem, research questions, hypothesis and conceptual framework.

Chapter 2: Literature Review - This chapter presents related literature and expounds research directions. It provides an overview of current regulatory frameworks and privacy acknowledgement.

Chapter 3: Study Area and Methodology – this chapter presents how the study will be conducted to operationalise research objectives and answer the research questions outlined in General Introduction section, which includes a description of methodology, selection of study area, the source of data and how to conduct data analyses.

Chapter 4: UAV Regulations Evaluation – This chapter focuses on selected UAV regulatory frameworks collected via official UAV regulatory bodies' websites and evaluating them based on variables and indicators developed in chapter 3.

Chapter 5: Similar Applications – includes the list of image-based acquisition techniques from other applications. Moreover, possible solutions for privacy will be discussed.

Chapter 6: Discussion – This chapter discusses the findings of this research presented in chapter 4 and chapter 5 viz-a-viz contemporary scientific literature.

Chapter 7: Conclusions and Recommendation – This chapter provides answers to research questions which feed into the main objective and the sub-objectives of this study, furthermore, the recommendations for further study.

1.8. Research Matrix

The Research Matrix (see Table 1) presents an overarching view of Specific Objectives, Research Questions, Methodology, Data Collection Source and Anticipated Results.

Specific objectives	**Research Questions**	**Methodology**	**Data Collection Source**	**Anticipated Results**
1. To review how privacy is conceived related to UAVs.	a. How is privacy conceived related to UAVs in various regulations? b. How do current UAV regulations address privacy concern?	Literature Review	Existing Literature Existing latest international and national regulations	Concept of privacy in regards to UAVs The extent to which privacy concerns are addressed and encompassed in current UAV regulations
2. To evaluate current UAV regulatory frameworks in privacy aspect.	a. What are weaknesses of current privacy terms? b. What are the possible recommendations to improve current regulatory frameworks?	Comparative research, Literature Review	Existing literature and latest regulations	Results of reviewing current regulations about weakness existing in current UAV regulations. Recommendations
3. To propose solutions from other image-based acquisition techniques (e.g. Google Street View) and to analyse if they are applicable.	a. What are similar applications? b. How do they deal with privacy concern? c. Can their experience be applied in UAV regulatory frameworks?	Literature view, comparative research	Existing Literature	List of similar applications Possible solutions from similar applications Results from analysis if possible solutions could be applied in current regulatory frameworks

Table 1: Research Matrix

2. LITERATURE REVIEW

2.1. Introduction

This chapter presents regulatory frameworks and privacy concerns related literature and expounds research directions. It provides an overview of various concepts of regulatory frameworks. Then, related privacy concerns and respective literature about privacy acknowledgement will be reviewed.

2.2. Regulatory Frameworks

Regulations, in context of this paper, are the delegated legislation used to implement government policies as a way to enforce legal restrictions, contractual obligations, and social regulations. Meanwhile, it is always referred to in the form of rules, principles, or laws. The word framework is interpreted as the fundamental and essential method to implement and enact regulations (Marty, 2013). Accordingly, regulatory frameworks could be defined as the advent of the necessary structure which implements delegated legislations in the form of rules, principles, or laws.

Having an effect on activities relating to UAVs which may invade privacy, public safety and personal data, general civil and criminal laws could decree penalties on UAV operations inducing detriment to people or property. If a party encounters privacy, public safety or personal data invasion, in some cases, compensation could be obtained. The possibility of penalty or liability could act as a kind of deterrent. Nonetheless, in order to be in accordance with particular criteria, for instance, privacy protection regulations, the deterrent is too general and the uncertainty encountered is too considerable (Clarke & Moses, 2014). Therefore more specific regulatory frameworks are required.

To address UAV related concerns, various regulations have already been published (see figure 1). For example, so far the International Civil Aviation Organization (ICAO) has publicised the Circular 328 on UAS which is the first formal ICAO document on UAV concerns (Colomina & Molina, 2014) and revised Annexes 2, 7 and 13 to the Chicago Convention. In Europe, a proposal for the revision of EASA Basic Regulation NO. 216/2008 was selected by European Commission in 2015, which narrates the requirements for advancing European UAV safety rules. The Basic Regulation aims at boosting progress in a single EU market for UAVs and cross-border UAV operations. The latest amendment was published on 12 May 2017. In accordance with Basic Regulation NO. 216/2008 Notice of Proposed Amendment 2017-05 (B) is mainly to harmonise maximum take-off mass (MTOM) in member states (EASA, 2018). In the United States, The Federal Aviation Administration (FAA) is administering most of the aircraft-associated operations. On February 14, 2012, President Obama authorised FAA Modernization and Reform Act of 2012 (FMRA) which allowed UAVs into national space. It is the first congressional legislation for UAVs. In order to be in line with policies publicised before the enactment of FMRA, a Certificate of Authorization (COA) was required for public aircraft operations which defined how and where UAVs can be used. A 'special airworthiness certificate' was necessary for civil UAV operations (Villasenor, 2013). Although the fact has been changed in 2014 that the certificates are not compulsory, since December 2015, all UAVs weighing over 250 grams are compulsory to be registered.

Clark and Moses (2014) identified UAV regulatory frameworks in four forms which encompass formal regulation, co-regulation, self-regulation and organisational self-regulation.

Accompanied by different authorities incorporating civil lawsuits and government agencies, formal regulations consist of statutes and legislation, moreover, in some countries, common law provisions. And the role of these authorities and government agencies may not be to establish rules but only to enforce and be responsible for protecting various parties' interests. (Kaminski, 2013).

A co-regulation refers to a set of requirements with significant input from industry, meanwhile, involving explicit legislative backing from the government. The outcome is within a statutory context which ensures interests of all stakeholders (Hepburn, 2006). However, the inadequate participation of stakeholders and transparency could lead result in a failure to fulfil the desire reflecting stakeholder interests. For example, according to Hayes et al. (2014), neither European Aviation Safety Agency (2012) nor European Commission (2013) had adequate engagement with stakeholders, especially those who are outside the industry, although Europe is often known for applying inclusive processes. In summary, it would be sensible to apply co-regulation to manage various aspects of civil UAV applications, which could satisfy all shareholders, especially for non-commercial micro-UAV applications by individuals. However, it may be precluded by industry associations and military interests (Clarke & Moses, 2014).

Industry self-regulation is defined as an industry Code of Conduct which imposes restrictions on all corporations in an industry, or at least most of its members (Singer & Lin, 2012). The Association for Unmanned Vehicle Systems International (AUVSI) is directly relevant in the UAVs industry, which claims that it has been granting membership to 'more than 7,500 members from government organizations, industry and academia'[2]. It has published the Unmanned Aircraft System Operations Industry Code of Conduct (AUVSI, 2012). Although the Code of Conduct is concise, there is no evidence to prove that it has neither created any enforceable obligations nor become an operation acquiesced by member corporations. For example, hundreds of standard documents could be accessed via the website of ICAO[3], but it has been found that none of them is related to UAVs after a search. Clarke and Moses (2014) concluded from their research that there is no sufficient evidence demonstrating that industry self-regulation could constrain disobedience of civil UAV applications. Nevertheless, with 'industry value chain' associations exercising their power to avoid efficiently being regulated, self-regulation could lack the motivation to preserve individual interests.

Being under the influence of professional criterion, organisational self-regulation exerts as self-restraint. Some organisations regard individual rights as moral rights although there is no specific legal basis (Kaminski, 2013). Other organisations involved in civil UAV applications might restrict themselves because they concede it as their responsibility. Whether or not an organisation dedicates itself to self-restraint, it is apparent that their publications may consist of an internal Code of Conduct or a Customer Charter (Clarke, 2014b). However, most such organisational customer charters are set out in highly generalised and vague terms. Scrutinising official websites of major UAV manufacturers, it finds that organisational self-regulations hardly play a vital role in their portfolios. For example, the leading UAV provider, the Chinese DJI company's website, offered no indication of any measure through which they encourage that their clients should prevent any possible privacy invasion[4]. Moreover, the French Parrot Drone, which claims by itself 'the largest volume of consumer-level micro UAVs', displays on its website the only amount of marketing expressions such 'Fly high. Fly fast. Far away from the ground', 'Trying your most daring tricks will not even challenge this cutting edge design'[5]. Hence, no evidence was found in UAV industry of privacy restrictions being applied by related organisations. Due to the absence of apparent evidence of accountability of UAV related organisations in relation to possible privacy invasion, it is inappropriate to regard the organisational self-regulation as a deterrent which restricts UAV civil applications regarding privacy concerns.

Although there is a wide range of studies on UAV regulatory frameworks, the discussion on privacy concerns is either limited, narrowly scoped (e.g. in few countries (Finn & Wright, 2012)), or only focus on technology improvement (e.g. clear criteria for drone equipped cameras (Park & Lee, 2017)).

[2] AUVSI – Who is AUVSI. (September 20, 2017). Retrieved from https:// www.auvsi.org/who-auvsi

[3] ICAO – Publications. (September 20, 2017). Retrieved from https://www.icao.int/publications/Pages/default.aspx

[4] DJI – The Future Of Possible. (September 20, 2017). Retrieved from https://www.dji.com

[5] Drones – Parrot Official. (September 20, 2017). Retrieved from https://www.parrot.com/eu/drones#

Many countries have processed to tailor their regulations to focus on technical and safety concerns. Nevertheless, those engagements fail to cover the most crucial problem: privacy invasion and inappropriate surveillance (Rao et al., 2016). Besides the fact that there is lack of appropriate privacy regulations, some address that current UAV regulatory frameworks have shortcomings, however, one of the challenges is, rather than compiling and publicising new regulations, how to interpret and understand current legislations (Vacca et al., 2017). Apart from maintaining baseline laws, by adding appropriate legislations, national governments could protect individual rights which is also a reasonable way to ensure expectation of privacy protection (Schlag, 2013).

2.3. Concept of Privacy

Privacy 'is the interest that individuals have in sustaining a 'personal space', free from interference by other people and organisations' (Clarke, 1999). Institute for Prospective Technological Studies (IPTS) defined privacy as 'freedom of self-determination 'for individuals', their right to be different and their autonomy to engage in relationships, their freedom of choice, their autonomy as regards - for example - their sexuality, health, personality building, social appearance and behaviour, and so on. It guarantees each persons' uniqueness, including alternative behaviour and the resistance to power at a time when it clashes with other interests or with the public interest. ' (IPTS, 2001). However, 'privacy' has disparate meanings in different conditions. Due to the involvement of different perspectives, such as social norms, political views and legal interpretations, and their highly volatile dynamic nature, it is being harder to cast light on a one-size-fits-all definition of privacy. Consequently, based on various perceptions, the concept of privacy has different definitions. The relationships between privacy and cognate concepts such as secrecy, deception, anonymity, are debatable. The main reason is that the boundaries of these concepts are unclear and highly depend on specific circumstances (Margulis, 2003). For example, Van Loenen et al. (2008) discussed how individuals and groups control or regulate access to themselves using a widely accepted research method called limited access approach, reflecting the individualist cultural model prevailing in western societies such as the US and Europe. Under this circumstance, privacy rights can be divided into four types by controlling or regulating access to oneself which are privacy of the body, privacy of the mind or psychological privacy, territorial privacy and behavioural privacy. Furthermore, behavioural privacy can be categorised as physical privacy, informational privacy, privacy of communications.

In Europe, privacy related to processing personal data is referred as 'Data Protection', while out of Europe it is described as 'data privacy' or 'information privacy' (Bygrave, 2010). Article 3 of the European Union General Data Protection Regulation (GDPR), which has been adopted in April 2016 and will be implemented in May 2018, defines the scope to the processing of personal data as " i*n the context of the activities of an establishment of a controller or a processor in the Union* ' and ' *to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to (a) the offering of goods or services to such data subjects in the Union; or (b) the monitoring of their behaviour* " (The European Parliament & The European Council, 2016). However, the scope of personal data could be slightly different among different EU countries (De Jong et al., 2016).

Nevertheless, the concept of privacy is underdeveloped in most African and Asian countries (Cannataci, 2009). It could be explained by the fact that in African and Asian cultures, loyalty to a group is more important at the expense of individuals (Bygrave, 2004).

The United Nations (UN) published Universal Declaration of Human Right (UDHR) (UN, 2015) which recognises privacy in the article: 'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.'

The Europe Convention for the Protection of Human Rights and Fundamental Freedom comprise the heart of European legislation (Van Loenen et al., 2007). In article 8 of European Convention on Human Rights (ECHR), the concept of privacy is addressed:

1. *Everyone has the right to respect for his private and family life, his home and his correspondence.*
2. *There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

The American Convention on Human Rights (ACHR) (Organization of American States, 1969) recognises privacy in Article 11 as:

1. *Everyone has the right to have his honour respected and his dignity recognized.*
2. *No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honour or reputation.*
3. *Everyone has the right to the protection of the law against such interference or attacks*

The Cairo Declaration of Human Rights in Islam (CDHRI) (Al-Mawdudi, 1980) addresses privacy in Article 18 as:

1. *Everyone shall have the right to live in security for himself, his religion, his dependents, his honour and his property.*
2. *Everyone shall have the right to privacy in the conduct of his private affairs, in his home, among his family, with regard to his property and his relationships. It is not permitted to spy on him, to place him under surveillance or to besmirch his good name. The State shall protect him from arbitrary interference.*
3. *A private residence is inviolable in all cases. It will not be entered without permission from its inhabitants or in any unlawful manner, nor shall it be demolished or confiscated and its dwellers evicted.*

It states The Fourth Amendment of the U.S. Constitution that '*the right of the people to be secure in their persons, houses, papers, and effects of unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.*' It addresses that people's privacy cannot be violated for any reason unless a warrant with an issued appropriate cause (Carr, 2016).

Being a predominant concept, many new technologies are criticised over privacy concern, especially surveillance technologies (Lyon, 2003). In the context of UAV applications, because they are equivalently invisible and relatively quiet, UAVs cause privacy invasion without being perceived. Several researchers define privacy in different dimensions related to UAV applications.

Clarke (1999) defines privacy in 5 dimensions: ' privacy of personal data, privacy of the person, privacy of personal communications, privacy of personal behaviour, and privacy of experience'. By those five dimensions, he found that '*UAVs greatly increase not only the scope for visual surveillance to be undertaken but also the degree of invasiveness of observation, transmission, recording, publication, location, tracking and the likelihood of interventions into the individual's behaviour by others*' (Clarke, 2014b). Therefore, a regulatory regime is required to protects behavioural privacy.

R. L. Finn, D. Wright, and M. Friedwald (2013) define seven types of privacy: ' Privacy of the person, Privacy of communication, Privacy of action and behaviour, privacy of data and image, privacy of thoughts and feelings, privacy of location and space and privacy of association'. He found that anyone could be monitored under the use of UAVs; accordingly, in all probability, actions are tracked and recorded. Private images of individuals could infringe privacy of data and image. Privacy of location can be invaded either by tracking or eroding scope of personal space. Negative impact could also be applied on privacy of association through UAVs covertly monitoring (Gutwirth et al., 2013).

In the context of UAV civil applications in public space in EU, being used for simple monitoring activities which means without recording, UAV activities have no interference with Article 8 of European Convention on Human Rights (ECHR) related to privacy. Conversely, if UAV activities get involved in following purposes in public place may cause a breach of Article 8 of ECHR (Finn et al., 2014):

1. *When UAV operators monitor and record data in a systematic and permanent way, regardless of whether the surveillance is covert or overt;*
2. *When UAV operators disclose images of someone previously collected;*
3. *When UAV operators do not record images but monitor a public space through 'sophisticated' means.*

Nonetheless, if the interference is for 'a legitimate and foreseeable purpose', such as public security, and if it meets the requirements in Article 8(2).13 of ECHR, the interference may be justified. Furthermore, in a case with 'non-sophisticated means', where the government-operated civil UAVs directly monitor in a surveillance context, they do not interfere with Article 8(1), similar as through the means of an ordinary camera.

EU (2014) categorised risks aroused from UAVs privacy invasion in seven dimensions: 'dehumanisation of surveilled, a chilling effect, function creep, privacy of location and space, transparency and visibility, and privacy of association'. According to these seven dimensions, the main risk to privacy should be privacy of association. Meanwhile, they found that restrictions on image details could notably decrease the risks, which may require higher altitude for UAVs flying so that less focused data is collected.

After analysing existing literature, it is clear that the definition of the concept of privacy is highly contentious. In this regards, considering the speciality of the UAV cases, this study provides its dimensions of the concept of privacy for evaluation in the next chapter.

2.4. Summary

Existing literature on the fundamental concepts has been reviewed in this chapter. Literature from researchers provided multi-disciplinary perspectives on regulatory framework and privacy. According to the literature, various UAV regulations have been published across different countries, and there are four types of UAV regulations including formal regulation, co-regulation, self-regulation and organisational self-regulation. The concept of privacy has been discussed broadly. Some researchers and originations published their own opinions, for instance, Clarke(1999) defined privacy as ' *the interest that individuals have in sustaining a 'personal space', free from interference by other people and organisations*'. IPTS (2001) defined privacy as freedom of self-determination ' for individuals', their right to be different and their autonomy to engage in relationships, their freedom of choice, their autonomy as regards - for example - their sexuality, health, personality building, social appearance and behaviour, and so on. Besides that, in different continents, the concept privacy has been published in the Declaration of Human Right, such as Universal Declaration of Human Right (UDHR) (UN, 2015), the American Convention on Human Rights (ACHR) (Organization of American States, 1969), and the Cairo Declaration of Human Rights in Islam (CDHRI). In addition, the concept of privacy in the context of UAV applications has been explored. According to the definition of the researchers, R. L. Finn, D. Wright, and M. Friedwald (2013) define 7 types of privacy : ' Privacy of the person, Privacy of communication, Privacy of action and behaviour, privacy of data and image, privacy of thoughts and feelings, privacy of location and space and privacy of association'. Moreover, Clarke (1999) defines privacy in five dimensions: 'privacy of personal data, privacy of the person, privacy of personal communications, privacy of personal behaviour, and privacy of experience'.

3. STUDY SCOPE AND METHODOLOGY

3.1. Introduction

In the previous chapter, various literature regarding regulatory framework and privacy has been explored. This chapter presents how the study will be conducted to operationalise research objectives and answer the research questions outlined in General Introduction section. This chapter includes a description of methodology, selection of study area, the source of data and how to conduct data analyses.

3.2. Selected Countries

In order to have an objective overview at the global level, considering most common factors which influence legislative making (Davis et al., 2010), a set of regulatory frameworks which encompasses countries in different continents, with various legal systems, and at diverse economic development levels intend to be selected. 14 countries are chosen: Azerbaijan, China, India, Kenya, Namibia, Rwanda, Tanzania, Canada, United States, Brazil, Colombia, Italy, United Kingdom, Australia. Those countries cover six continents (see Table 2), four different levels of Human Development Index (see in table 3), and three primary legal systems (see Table 4).

For measuring the economic development level, the Human Development Index (HDI) is chosen, which was introduced in 1990 as a part of the United Nations Development Programme (UNDP). HDI is used to measure the economic development level in three aspects: health, education and per capita income (United Nations Development Programme, 2016). Tracking changes in development level of countries over time, UNDP produces a development report. Compared with the other prevalent index Gross Domestic Product (GDP), HDI is an advantageous means of comparing the development level of countries. As an indicator of economic development, GDP per capita is apparently too narrow to illustrate other dimensions of development, for instance, school enrollment and longevity. Therefore, HDI is a more encompassing indicator than GDP, despite GDP still accounts for one-third of the index.

Continent	Country
Asia	Azerbaijan, China, India
Africa	Kenya, Namibia, Rwanda, Tanzania
North America	Canada, United States
South America	Brazil, Colombia
Europe	Italy, United Kingdom
Oceania	Australia

Table 2: Continents of Selected Countries

Human Development Index (HDI)	Country
Very high development	Canada, United States, Italy, United Kingdom, Australia
High development	Brazil , Azerbaijan, China, Colombia
Medium development	Kenya, Namibia, India
Low development	Rwanda, Tanzania

Table 3: HDI of Selected Countries

Legal System	Country
Civil law systems	Brazil, Colombia, Italy, Azerbaijan
Common law systems	Canada, United States, United Kingdom, Australia
Mixed law systems	Kenya, Rwanda, Namibia, Tanzania, China, India

Table 4: Legal System of Selected Countries

3.3. Research Methodology and Data Analysis

This research combines both comparative method and literature review as research methods. Comparative analysis is an essential method measuring variables 'on nominal, ordinal and cardinal scales' (Lor, 2011). Three main approaches are existing within comparative analysis: the statistical method, the comparative method and the experimental method, all of which convert most of the variables into indicators in order to isolate the effects of the remaining variables (Porta, 2008). In a cross-national analysis, with a small number of cases which are usually conducted between two and twenty, comparative method is more applicable rather than superficial statistical analysis (Lijphart, 1971).

Being a variable-oriented research, the lower the number of cases is, the fewer variables should be explanatory (Porta, 2008). Therefore, as a variable-oriented rather than cases-oriented study, this evaluation will choose few variables to measure privacy (see Table 5), which are: privacy of location, privacy of personal data and image, and privacy of personal behaviour, covering most of the dimensions or perspectives of current literature.

Variables used in this study are based on most common privacy invasion cases and distilled by a literature review:

Finn et al. (2014) categorised UAVs privacy concern into 'a chilling effect, body privacy, dehumanisation of the surveilled, privacy of location and space, transparency and visibility and privacy of association.'

Clarke (1999) defines privacy in 5 dimensions: ' privacy of personal data, privacy of the person, privacy of personal communications, privacy of personal behaviour, and privacy of experience.', which are applied for analysing UAV privacy invasion cases (Clarke, 2014a).

Volovelsy (2014) classified privacy risks entailed by UAVs in following groups: 'the psychological perspective, the technological perspective, the economic perspective and the legislative perspective. '

Variables	Indicators
Privacy of location and space	· Private location and space information
Privacy of personal data and images	· Collection of personal data and images; · Accuracy and duration of personal data retention; · Use of personal data and images; · Access to personal data and images
Privacy of personal behaviour	· Social preferences(e.g. relationships/ friendships/ preferences) · Sexual preferences and habits; · Political activities; · Religious practices.

Table 5: Variables and Indicators

After that, by reviewing relevant academic articles, this study assesses the possibility of applying solutions from another imagine acquisition domain in the case of UAV regulations. Applicability of Solutions are analysed according to how much they can mitigate privacy threats.

A threat is a weakness or fragile parts of a system, from which an adversary can attack a system or invade the privacy of the system users (Myagmar et al., 2005). Therefore, it is necessary to identify all the possible threats during the process of UAV applications. According to Clarke (Clarke & Moses, 2014) possible threats are identified as below:

- *Retention, storage, use and disclosure of data*
- *Collection of personal data in very large volumes*
- *Data misinterpretations from original context*
- *Interception of data-flows, e.g. of surveillance video transmissions*
- *Unauthorised stored data access*

3.4. Data Collection

The UAV regulations for analysing will be from official national websites through Global Drone Database (https://www.droneregulations.info), which provides accesses to the latest UAV regulations. Through Global Drone Database, regulations from different countries are collected (see Table 6). Data for the literature review is collected from relevant academic journals, books, reports published by various international organisations, research institutions and academic conferences.

No.	Country	Data	Year
1	Canada	Aeronautics Act	2017
2	United States	Operation and Certification of Small Unmanned Aircraft Systems	2016
3	Brazil	Requisitos Gerais Para Aeronaves Não Tripuladas de Uso Civil	2017
4	Colombia	Requisitos Generales de Aeronavegabllidad y Operaciones Para Rpas (numeral 4.25.8.2)	2015
5	Kenya	The Civil Aviation (Remotely Piloted Aircraft Systems) Regulations	2017
6	Rwanda	Civil Aviation (Unmanned Aircraft System) Regulations	2016
7	Namibia	Directorate of Civil Aviation	2015
8	Italy	Remotely Piloted Aerial Vehicles Regulations	2016
9	United Kingdom	Unmanned Aircraft System Operations in UK Airspace – Guidance	2015
10	Tanzania	Aeronautical Information Circular (AIC)	2017
11	Azerbaijan	Unmanned Aircraft Operations	2015
12	China	Flight Standards Division of Civil Aviation Administration	2015
13	India	Guidelines for obtaining Unique Identification Number (UIN) & Operation of Civil Unmanned Aircraft System (UAS)	2016
14	Australia	Flying drones/remotely piloted aircraft in Australia	2017

Table 6: UAV regulations

3.5. Summary

This research selected 14 countries covering six continents, four levels of Human Development Index and mainstream legal systems. The methodology outlined in this chapter presented the research methods. For UAV regulation evaluation, the comparative method was selected. The research data for evaluation was collected from accessible regulations via official websites. The variables and indicators were chosen after distilling existing literature. For similar applications and proposed solutions, existing privacy threats are identified from literature.

4. SELECTED UAV REGULATIONS EVALUATION

4.1. Introduction

This chapter focuses on selected UAV regulatory frameworks collected via official UAV regulatory bodies' website. These regulatory frameworks are valuated based on variables and indicators developed in chapter 3. This chapter begins by showing evaluation result, then focus is placed on three identified dimensions of UAVs related privacy variables – privacy of location and space, privacy of personal data and images and privacy of personal behaviour. Weaknesses of current UAV regulatory frameworks will be discussed.

4.2. Evaluation Results

After comparing current UAV regulations with distilled indicators and variables (see Table 5), the evaluation result shows as below (see Table 7 and Table 8). In Table 7 and Table 8, if one indicator is covered in any UAV regulations, it is marked with 'Yes'; if the indicator is not covered, it is marked with 'No'; besides, if the indicator is not covered in the UAV regulations but other regulations, the name of related regulations are mentioned.

From the evaluation, for the most part, UAV regulations in selected 14 countries mainly focus upon four key concerns: 1) providing safety and operational standards for UAV operations; 2) setting limitations for the use of UAVs to be complied with in the national airspace; and 3) defining procedures in air navigation and airspace. 4) regulating general UAV related concerns such as pilot licenses application, insurance, penalties, data protection and privacy.

Although UAVs related privacy invasion, as well as data protection concerns, are increasingly raising attention (Cho, 2013; Finn & Wright, 2016; Rao et al., 2016), according to the result of this study, these concerns are scarcely addressed and even encompassed in current UAV regulations: only 4 out of 14 selected UAV regulations incorporated privacy concerns in UAV regulations, even only advocating to 'respect' personal privacy. 8 UAV regulations do not mention anything about privacy or data protection, nevertheless, 5 out of these 8 countries, data protection/ privacy regulations have been adopted for all forms of privacy invasion cases. Other 2 regulations referred to the Data Protection Act/ Privacy Code/ Privacy Act to be followed in regards to UAVs caused privacy concern.

Regulating the fairs related to Small Unmanned Aircraft Systems operation and certification, US Federal Aviation Administration explains that they acknowledge the privacy concerns raised by UAVs and they intend to participate in multi-stakeholder engagement in safeguarding privacy, civil rights, and civil liberties (Federal Aviation Administration, 2016). However, the opinion that how privacy should be addressed as well as to which extent UAVs posed potential risks for privacy intrusions is not in accord. Therefore, Federal Aviation Administration only provides regulations for air safety and efficiency without regulating privacy.

Although in some regulations the UAV privacy concerns are not even mentioned, there are national laws and regulations addressing UAV related privacy concerns. For example, the Office of the Australian Information Commissioner (OAIC) has published correspondence with the Attorney-General from 2012 to 2013 relating to the application of current privacy laws in using UAVs (OAIC, 2013). Furthermore, in Canada, Transport Canada, the government department, which is responsible for transportation safety and transportation operating permits and certifications, declared that UAV operators must 'follow the rules in all acts and regulations—including the Criminal Code, as well as all municipal, provincial, and territorial laws regarding trespassing and privacy.' (Transport Canada, 2017).

		Canada	US	Brazil	Colombia	Kenya	Rwanda	Namibia
Privacy of location and space	Private location and space information	Yes	No	No	Yes	Yes	Yes	No
Privacy of personal data and images	Collection of personal data and images;	Data Protection Act	Privacy or Data Security Laws	No	Data Protection Decree	Yes	Yes	No
	Accuracy and duration of personal data retention;	Data Protection Act	Privacy or Data Security Laws	No	Data Protection Decree	No	No	No
	Use of personal data and images;	Data Protection Act	Privacy or Data Security Laws	No	Data Protection Decree	Yes	Yes	No
	Access to personal data and images	Data Protection Act	Privacy or Data Security Laws	No	Data Protection Decree	No	No	No
Privacy of personal behaviour	Social preferences(e.g. relationships/ friendships/ preferences)	Data Protection Act	Privacy or Data Security Laws	No	Data Protection Decree	Yes	Yes	No
	Sexual preferences and habits	Data Protection Act	Privacy or Data Security Laws	No	Data Protection Decree	Yes	Yes	No
	Political activities;	Data Protection Act	Privacy or Data Security Laws	No	Data Protection Decree	Yes	Yes	No
	Religious practices.	Data Protection Act	Privacy or Data Security Laws	No	Data Protection Decree	Yes	Yes	No

Table 7: Evaluation Result 1

		Italy	UK	Tanzania	Azerbaijan	China	India	Australia
Privacy of location and space	Private location and space information	No	No	No	No	No	Yes	No
Privacy of personal data and images	Collection of personal data and images;	Yes	Data Protection Act	No	Data Protection Regulation	No	Privacy Rules	Privacy Act
	Accuracy and duration of personal data retention;	Privacy Code	Data Protection Act	No	Data Protection Regulation	No	Privacy Rules	Privacy Act
	Use of personal data and images;	Privacy Code	Data Protection Act	No	Data Protection Regulation	No	Privacy Rules	Privacy Act
	Access to personal data and images	Privacy Code	Data Protection Act	No	Data Protection Regulation	No	Privacy Rules	Privacy Act
Privacy of personal behaviour	Social preferences(e.g. relationships/ friendships/ preferences)	Privacy Code	Data Protection Act	No	Data Protection Regulation	No	No	Privacy Act
	Sexual preferences and habits	Privacy Code	Data Protection Act	No	Data Protection Regulation	No	No	Privacy Act
	Political activities;	Privacy Code	Data Protection Act	No	Data Protection Regulation	No	No	Privacy Act
	Religious practices.	Privacy Code	Data Protection Act	No	Data Protection Regulation	No	No	Privacy Act

Table 8: Evaluation Result 2

4.3. Privacy of Location and Space

Privacy of location and space, which includes private location and space information, concerns the limitations on the intrusion of private places rather than public places. With technologies and applications, UAVs can easily cross windows and fences into private places (such as house, balconies or garden) and observe details. In this sense, UAV operations may reveal identifiable personal information, human interactions and even group behaviour patterns, which would raise increasing concerns about private life (Van Loenen & Zevenbergen, 2007). With geospatial data collected by UAVs, not only individual privacy but also commercial confidentiality and national security may be violated (Abdulharis, Van Loenen, & Zevenbergen, 2005).

Most of the selected countries do not address privacy of location and space in UAV regulations. Only India, Canada, Colombia, Kenya and Rwanda mentioned this concept. In Colombia UAVs regulation (Aeronavegabllidad y Operaciones Para Rpas), it sets a precise distance (50 meters) within which UAVs cannot approach people or properties. Meanwhile, private properties or belongings are not allowed to be overflown without permission of the owner or inhabitant. On the contrast, the India UAVs regulation, Guidelines for obtaining Unique Identification Number (UIN) & Operation of Civil Unmanned Aircraft System (UAS), only regulates that privacy of per or property shall be given due importance, which is too general to implement. Regulations from Rwanda (Civil Aviation (Unmanned Aircraft System) Regulations) and Kenya (The Civil Aviation (Remotely Piloted Aircraft Systems) Regulations) specify consent rather than distance in privacy of location and space regard. Both of the regulations require that consent of a person or owner is a prerequisite for any UAV operations which may approach or recover any private property. In UAVs regulation of Canada (Aeronautics Act), it only requires that the UAV should return to the permitted operator as soon as possible once it has served its purpose, which seems to mitigate the possible invasion of privacy of location and space. However, it is difficult to implement in reality.

4.4. Privacy of Personal Data and Images

Privacy of personal data and images are data or images which contain personal information such as personally identifiable information in photos, videos or audio recordings. Because the sizes of particular UAVs (e.g. under 2kg) are small, they can quickly collect personal data while transferring to done operators who can be hundred meters or even kilometres away without being detected. Moreover, the data collected by UAV operators can be processed and even shared with third parties.

The comparative analysis result of privacy of personal data and images can be divided into three categories: 1). Countries which have relevant terms in their UAV regulations; 2). Countries which have some terms in this aspect but also refer to other regulations (e.g. data protection regulations); 3). Countries which neither have related rulings in their UAV regulations nor refer to other regulations.

Countries which have relevant content in their UAV regulations are Rwanda, Kenya, and Italy. The UAV regulations of Rwanda and Kenya both regulate that for the purpose of publishing or disseminating, photographs or video clips should have the individual's consent. They also specify that infrared or other similar thermal imaging technology equipment carried by UAVs shall be applied for the particular purposes such as scientific investigation, scientific research and agricultural purposes and so forth. Besides the fact that the terms in privacy of personal data and images in both regulations of Kenya and Rwanda are very similar, neither of them provide any restriction on accuracy and duration of retention of personal data or access to personal data and images.

UAVs regulation of Italy (Remotely Piloted Aerial Vehicles Regulations) has related content but also refers to the data protection regulations. Here, if UAV operations have the necessity of processing personal data, this fact shall be referred to in the documentation which ought to be submitted to the UAVs permission application authorisation. However, for personal data processing concern, it should be pursuant to the Italian Data Protection Code.

The remaining countries neither have relevant content nor refer to related regulations. However, there are some other laws/regulations/codes/acts which are ruling cases related to privacy of personal data and imagine invasion. For example, in the United Kingdom, images and videos recorded by UAVs, especially those include people but without their consent, could potentially breach the CCTV Code of Practice and Data Protection Act. Those two acts address the concern for UAVs collecting individual information. Likewise, in Azerbaijan, India, Australia, Colombia, Canada, and United States, related regulations can be found.

For countries which do not have specific regulations, such concerns are being regulated on some other general laws or even constitutions. For example, in China, provisions found in laws such as the General Principles of Civil Law and the Tort Liability Law are mostly interpreted as privacy/ data protection cases(Piper DLA, 2017b). In Brazil, privacy of personal data and image is under regulation of Federal Constitution, which administers general principles and provisions related to data protection and privacy (Piper DLA, 2017a).

4.5. Privacy of Personal Behaviour

Privacy of personal behaviour is about behaviour in private places, such as social preferences (e.g. relationships/ friendships/ preferences), sexual preferences and habits, political activities and religious practices. All of these behaviours could be interfered by UAVs observation and recording (e.g. sound and images), even sometimes with significant 'chilling effect' (Clarke, 2014a).

Only three countries regulate privacy of personal behaviour in current UAV regulations. In The Civil Aviation (Remotely Piloted Aircraft Systems) Regulations of Kenya, it regulates that UAVs shall not be operated to infringe of individuals; anyone conducting UAV operations with cameras should respect the privacy of others. In Civil Aviation (Unmanned Aircraft System) Regulations of Rwanda, it only mentions that UAV operators should respect the privacy of others. Terms in both regulations could be interpreted as protection of privacy of personal behaviour.

Canada, United States, United Kingdom, Colombia, Italy, Azerbaijan and Australia have privacy code, data protection act, privacy laws and privacy act to regulate privacy of personal behaviour. Brazil, China, Namibia, Tanzania, India do not have specific privacy or data protection laws/ regulations/ acts, but privacy of personal behaviour concerns are being regulated by general laws or constitutions.

4.6. Summary

In this chapter, based on the variables and indicators, the UAV regulations from 14 selected countries were evaluated. It is found that there is severe lack of privacy concerns in UAV regulations at the global level. All privacy related aspects (include but not limited to privacy of location and space, privacy of personal data and images and personal behaviour) need to be further addressed. A clear and complete regulatory framework could solve all concerns raised by UAVs application including safety, security, privacy, and data protection (Marzocchi, 2015).

It is found that current terms related to privacy are too general, some of the regulations only mentioned that UAVs with cameras should 'respect' individuals. UAV regulations should clarify safety, privacy and data protection requirements and obligations among all stakeholders such as users, manufacturers and controllers. None of these regulations addressed the role of manufacturers.

It is also discovered that UAV operations which may lead to surveillance are not mentioned in UAVs regulation but prohibited under constitution, environmental law, or data protection law, etc. The attention should be drawn to the fact that although there could be some gaps in UAV regulations, such privacy intrusions are still forbidden under other specific laws.

5. SIMILAR APPLICATIONS AND PROPOSED SOLUTIONS

5.1. Introduction

In this chapter, similar image and video-based applications will be discussed. This chapter focus on how privacy concerns are raised by Google Street View, Closed-circuit Television Cameras and visual lifelogging and solutions which are currently applied by these similar applications. After that, whether these proposed solutions could be implemented in UAV privacy invasion cases will be explored.

5.2. Privacy Concerns Raised by Image and video-based Acquisition Techniques

5.2.1. Google Street View

Google Street View (see Figure 3), which provides 360° horizontal and 290° vertical panoramic street level views, was launched in the United States in May 2007 (Sloot & Borgesius, 2012). This high-resolution image based technique enables users to see the natural wonders and even step inside places such as museums, restaurants and arenas through the eyes of the virtual person Pegman (Google Maps Help, 2017). Any user could also click one direction on the road so that the Pegman would move some steps forward. By using multiple particular built-in GPS equipped cameras, Google creates photographs which match to a specific location. Google acquires images by mounting the cameras assembly to a vehicle driving around neighbourhoods whose model varies on which country the car is working. After firstly being launched in cities such as New York, Las Vegas and San Francisco, Google Street has been expanded covering the United States and around the world.

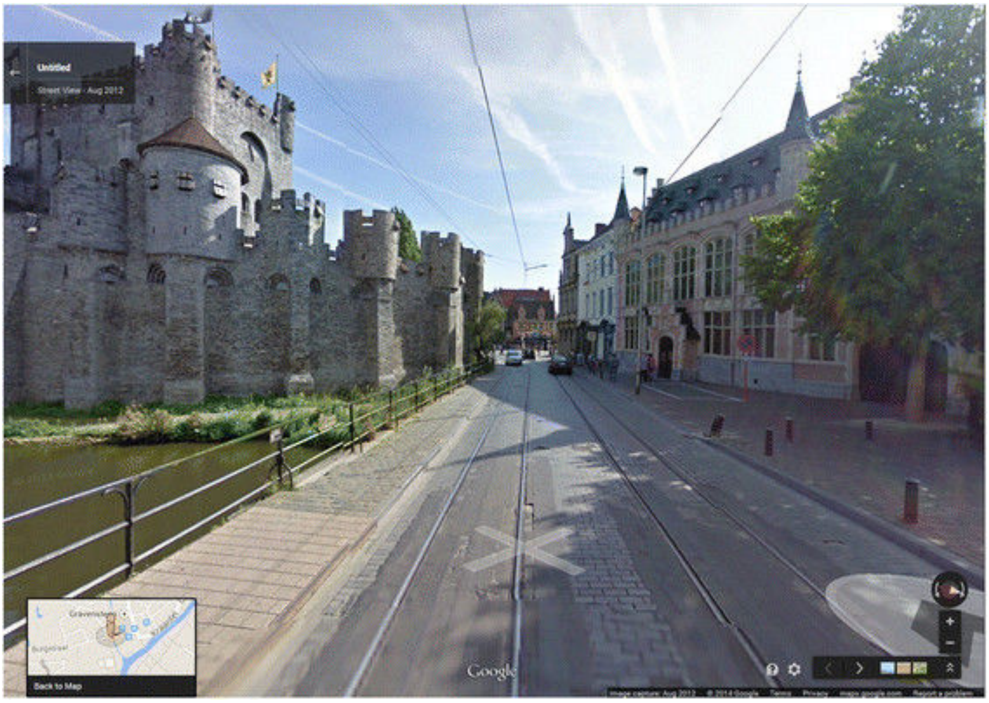


Figure 3: Example of Google Street View (Vandeviver, 2014)

Most of the images captured by Google Street View nowadays are considered high-definition. Till September 2010 the images were low resolution. Users can create immersive 360° views called 'photo spheres' by uploading the available imagery themselves (Rapoport, 2013). Being uploaded and connected, the spheres can be navigated by users. From April 2014, it is possible for users to explore historical imagery from past Street View collections dating back to 2007 (Shet, 2014). Google Street View is broadly applied, mainly as a convenient tool to reduce costs and expertise. Such as in Biology, researchers use Street View imagery to assess the habitat of certain animal species (Olea & Mateo-Tomás, 2013). In public health studies, Street View is being operated as a tool to collect data on the built environment (Badland et al., 2010). More than one billion users use Google Maps and related service like Google Street View monthly (Vandeviver, 2014).

In the beginning, zooming in on specific objectives for any details was allowed, which inevitably raised concerns of privacy (identification the faces of a couple having intercourse on the highway, for instance (Mashable, 2017)). Since Google launched the Street View project, it encountered numerous concerns, especially across Western countries. In the United States, one couple, Aaron and Christine, had a complaint in the Western District Court of Pennsylvania in April of 2008 (Boring, 2010). They claimed that Google Street View service invaded their right of privacy, moreover, committed a trespass, conversion, and negligence. In the United Kingdom, many residents from different towns and cities have had a multitude of complaints about Google Street View because of infringing of privacy and lack of security (Whittaker, 2009). In Switzerland, in November 2009, the Federal Data Protection and Information Commissioner of Switzerland, Hanspeter Thür, urged the captured images should be removed from the internet because the faces and cars plates presenting online were not sufficiently blurred (Kirk, 2009). Besides the facts mentioned above, countries such as Germany, Denmark, Greece, Lithuania, Australia and so forth. All had privacy concerns.

5.2.2. Closed-circuit Television Cameras(CCTV)

Closed Circuit Television (CCTV) is a system of cameras, with or without a recording device (see Figure 4), undertaking retrieval and storage of video footages, object tracking, data classification, data mining and the prediction of events, which sends images or videos to a limited set of monitors rather than broadcast publically (Oram, 2011).

Figure 4: Closed-circuit Television Cameras (CCTV)[6]

[6] CCSL - CCTV Camera in Sri Lanka. (January 1, 2018). Retrieved from http://www.cctvcamerainsrilanka.com

Nowadays, instead of being limited to one single purpose, the functionalities of CCTV systems are well applied in the different industries ranging from identification of unwanted individuals and targeted criminals, detection of lawbreaker actions, through the prediction of traffic jams and prosecution of traffic wrongdoers, besides, the statistical analysis of consumer behaviour (Möllers & Hälterlein, 2013).

The spread of video surveillance technologies, CCTV, for instance, for the purpose of evidence gathering or crime prevention both in the public and the private sectors, has become a crucial component of surveillance policies (Coudert & Dumortier, 2008). From a legal standpoint, the development of surveillance technology demands legitimate definition (Agustina & Galdon, 2011). Having strong inclination, government authorities firmly require and extensively fund researches on surveillance technology because of global risks including organised crime and terrorism which is essential to be cracked by efficient means. However, simultaneously, surveillance technologies are being criticised by privacy advocates because of the threat posed by these technologies may invade individual liberty (Möllers & Hälterlein, 2013). Moreover, when transmitting images and videos captured from cameras, CCTV systems operate in a ‘closed loop’. It means only the people who operate the system have the privilege to the data access. It can undoubtedly lead to the fact that the live images are available only to people associated with the transmission system. Consequently, the images and videos in digital formats are at stake because they can be shared outside of the closed system by certain people (e.g. system operators) (Hartmus, 2014). Therefore, general regulations are required for legitimising the implementation of CCTV cameras in public spaces.

5.2.3. Visual Lifelogging

Lifelogging is an activity which utilises mobile devices or wearable technology (see Figure 5 and Figure 6) to capture and chronicle the first-person perspective of a user's life in a continuous and automatic fashion (Ferdous et al., 2017). Collecting and capturing personal interactions, lifelogging can capture activities away from the computer, out of the office in the daily life. Through the digital representation of recorded daily life experience stored in a storage medium, a user can retrieve, recollect, remember intentions and/or use the collected data for other purposes (Sellen & Whittaker, 2010). More importantly, the lifelogging technique does not only store consequential content but also crucial contextual details of the activities which can help access the content later.

Individuals can wear a Lifelogging device designed for recording daily affairs to sense the environment for some potential benefits or infer valuable knowledge about life activities. For instance, an individual can discover statistics about the ambulatory activities with the help of a Lifelogging camera using inbuilt accelerometers (Gurrin et al., 2014). Moreover, there are plenty of potential benefits: such as prescribe tailored healthcare applications, build better self-awareness which may contribute to longer and more active lifespans, invent advance studying methods, improve working productivity, design new patterns of online and offline social interactions and increase mobility or independence for patients suffering from various memory and cognitive impairments. Above all, Lifelogging would bring benefits from healthier and more productive perspectives (Daskala, 2011).

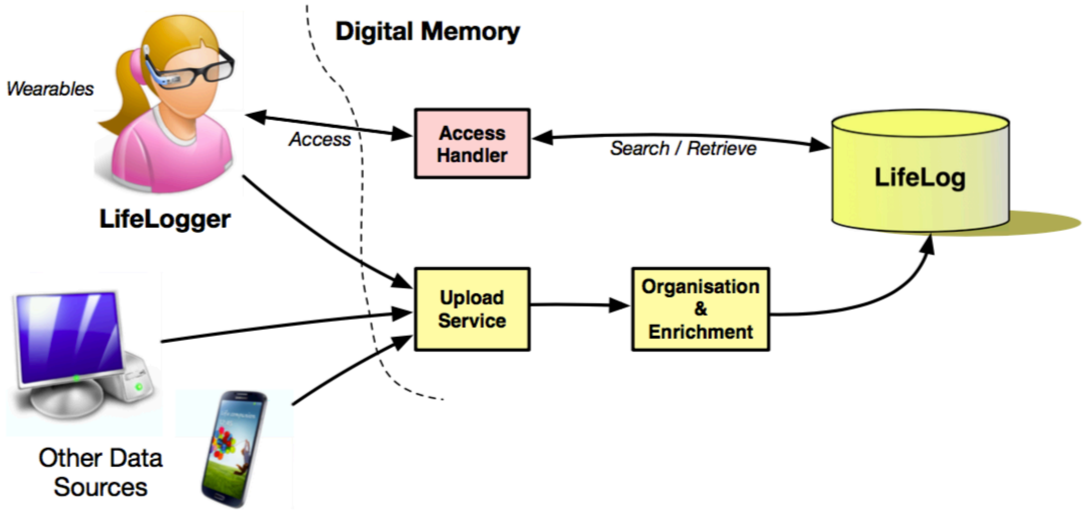


Figure 5: A basic lifelogging architecture (Gurrin et al., 2014)

Although there is an increase of interest, lifelogging is not a new technique. It can be traced to 1945, supporting the searching, archiving, and indexing of personal information revolving around documents (Bush, 1945). However, lifelogging today is not limited to store desktop objects, while it seeks to be all-encompassing and effortless in terms of data capture.

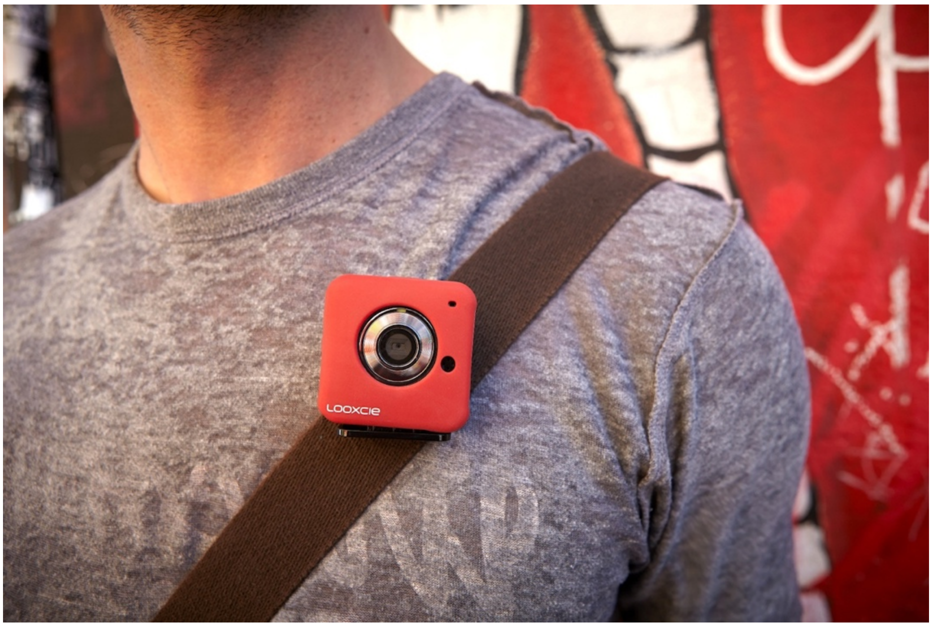


Figure 6: A Life Logging Device[7]

Generally speaking, in lifelogging, there are two types of privacy concerns: one is of the lifelogger, and another is of the people who interact with lifeloggers. For lifeloggers, their lifelogging data might contain sensitive personal information ranging from health data and bank card information (e.g. when taking cash from an ATM during lifelogging) to all social interactions with different people including intimate

[7] Kapital - 5 Subcultures and Trends that Affect the Business. (December 12, 2017). Retrieved from https://kapital.kz/business/58782/5-subkultur-i-techenij-kotorye-vliyayut-na-biznes.html

behaviour and embarrassing actions. Therefore, the privacy concerns on the lifelogger side focus on data protection and security. For the bystanders, who may be captured by a lifelogger without their consent or permission, the privacy concern should be that they cannot control their appearance in others' lifelogs. Anyone in the lifelogs can be identified under certain circumstances (e.g. specific time, places ect.), engaged in particular activities, and interacted with other people. Moreover, considering that a picture captured by a lifelogging device of another person and assuming that such a lifelog with GPS coordinates and timestamp embedded has been wrongfully exposed, there is a severe risk of the privacy breach in visual lifelogging. For example, the lifelogging devices are usually equipped with sensors which have embedded GPS coordinates, the attacker can combine relatively accurate face recognition techniques with image search algorithms to identify the person in a lifelog, even locate a person through the GPS. The concern of personal privacy invasion in different domains has already arisen because of the invasive and intrusive nature of lifelogging (Ferdous et al., 2016).

5.3. Solutions from Images and video-based Acquisition Techniques for Privacy Concerns

5.3.1. Google Street View

In order to solve the concern of privacy invasion, based on the fact that in most Data Protection Directive/ Privacy Act/ Privacy law of various countries, there are broad definitions of personal data. Google has ensured that the most direct and sensitive information, which may include but not limited to personal details, clothing and cars, whichever may directly or indirectly lead to personal identification, is blurred. Regarding car plates and faces: *"Cutting-edge face and registration plate blurring technology that is applied to all of Google's Street View images, which is designed to blur all identifiable faces and registration plates within Google-contributed imagery* (Google Street View, 2017)*"*.

To improve data transparency, in case users might be or have been photographed in residential or working places, instead of any disproportionate effort (e.g. a court claim) from individuals, Google admits the right of data subject including the erasure of personal data:

> *If a face or a registration plate that requires additional blurring or if you would like us to blur your entire house or car, submit a request using the Report a Problem tool. Please note, however, that once Google blurs an image the effect is permanent. If you submit a request to have your personal home blurred from Google Street View imagery, all historical and future images of your home will also be blurred. Note: we do not blur third-party contributions because this content is not owned by Google. If you find your identifiable image in third-party contributions, and you wish to have the image removed, use the report a problem feature on the image* (Google Street View, 2017).

Moreover, in Europe, Google gives warnings in advance to the residents of the locations where they intend to take photographs. While in the United States, individuals must know that they are being photographed and do not receive any notice beforehand (Segall, 2010).

5.3.2. Closed-circuit Television Cameras(CCTV)

CCTV systems are implemented in countries all over the world. However, The United Kingdom, which has influential legislation, practice and public perception concerning surveillance and privacy, is the leader in CCTV application (Hartmus, 2014). During the period from 1992 to 2002, the British Home Office has spent more than three-quarters of the total budget for crime prevention on CCTV, which is estimated more than 500 million GBP (Hempel & Töpfer, 2009). Therefore, in this section, the laws and regulations in the UK are going to be discussed.

UK legislation provides some guidance for the use and control of CCTV, meanwhile, undertaking some protection to the general public. Article 8 of the Human Rights Act (HRA) addresses the right to '*respect for* *private and family life*', which allows individuals to claim against public authorities in terms of privacy invasion (UK Government, 1998). In 1998 the UK introduced the Data Protection Act (DPA), which is to comply with the 1995 EU Data Protection Directive facilitating the freedom of movement of personal data in the European Union, dedicated to '. . . *processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information*' (Office of Public Sector Information, 1998). DPA is in charge of individual information held by organisations. Therefore, CCTV operators are bearing legal obligations from DPA, although the DPA was not specifically for CCTV (Sheldon, 2011). For the purpose of complying DPA and protecting individual privacy, the Information Commissioner's Office (ICO) issued the first 'CCTV code of practice' (COP) in 2000. This document was first updated in 2008. Then in 2013, the name of this regulation was revised to Surveillance Camera Code of Practice. Since 2017, this regulation is referred to as 'In the picture: A data protection code of practice for surveillance cameras and personal information' (Information Commissioner's Office, 2017). The CCTV Code of Practice provides guidance for operating within the law and sets good practice standards (Hartmus, 2014):

> *Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.*
>
> *The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.*
>
> *There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.*
>
> *There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.*
>
> *Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.*
>
> *No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.*
>
> *Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.*
>
> *Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.*
>
> *Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.*
>
> *There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.*

5.3.3. Visual Lifelogging

Regarding privacy concern of visual lifelogging, existing studies in this domain has proposed some solutions (Ferdous et al., 2017):

Jana et al. (2013) have presented a solution which provides an abstraction privacy layer between applications and sensor data which is called OS (operating system). Having an images/ videos analysis mechanism, the abstraction layer works with recognisers to identify sensitive objects and obscure them based on the standards ('Privacy Goggles') set by users. As parts of an image/ video being appropriately obscured, the OS delivers information to the requested app (see Figure 7).

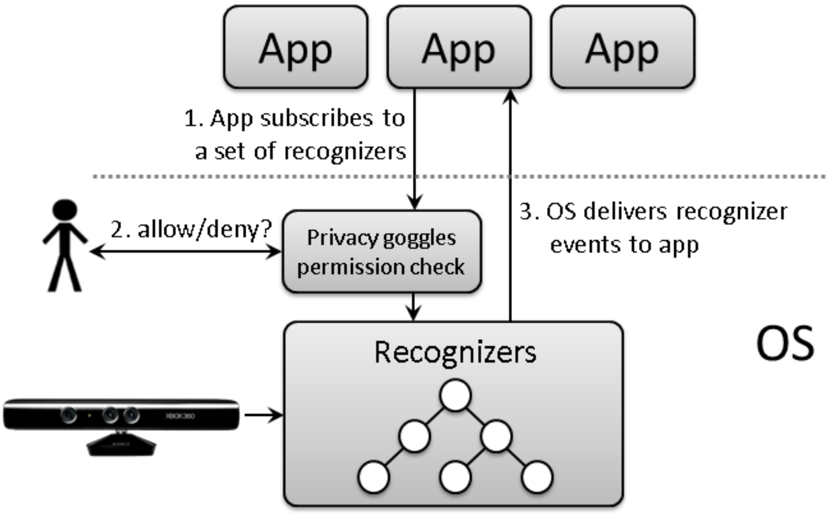

App
App
App
1. App subscribes to a set of recognizers
2. allow/deny?
Privacy goggles permission check
3. OS delivers recognizer events to app
Recognizers
OS

Figure 7: Abstraction layer of privacy solution (Jana et al., 2013)

Templeman et al. (2014) presented a solution called PlaceAvoider, which is used for blocking images taken from first-person perspective cameras in sensitive spaces (e.g. private places such as bathrooms and bedrooms). The system comprises a set of privacy rules and an image classifier. Being set by users, the privacy rules determine the places where taking photos is not allowed. While the image classifier acts as the privacy rules, enforcer managing captured images.

For setting privacy rules, the images, locations and videos of sensitive places should be captured beforehand. Then the image classifier implements a probabilistic algorithm to determine whether the captured images/videos are sensitive based on sensitive place settings (e.g. preset the bathroom as a sensitive place). Enforcing the preset rules, the image classifier can avoid taking photos or filming videos in sensitive places.

Memon & Tanaka (2014) proposed a framework for privacy-preserving lifelogging through which the other parties can be notified by wearable devices in some places and particular period of time that they are not willing to be captured. By defining specific conditions, the rules set up in the system prescribe the time period and location constraints. The conditions could incorporate different aspects such as spatial, temporal, spatiotemporal and other users' preferences. For instance, defining locations, time and specific groups of other users of which a lifelogging user can capture lifelogging materials. Then, using techniques, such as Bluetooth, smartphones can be operated as lifelogging devices obeying different privacy rules. Moreover, assuming that each device has a distinctive ID number, every user involved is identified with the unique device according to this number. Meanwhile, equipped with infrared transceivers, smartphones can transmit ID number when devices are being in the sight of one another. Under this circumstance, if one device receives an ID number from another via the infrared channel, all privacy rules set in the devices will be evaluated. Then, according to the privacy rules evaluation result, qualified lifelogging materials will be acquired.

5.4. Possible Solutions Applicability for UAVs

5.4.1. Threats Identification in UAVs Applying Process

Whether potential solutions from other domains (e.g. faces and car plates blurring techniques from Google) are able to reduce threats are regarded as the indications of the solution applicability in this research. Considering the similarity and referring to the threats of visual lifelogging (Ferdous et al., 2017) and combining with the UAV privacy threats identified in Section 3.3., following threats in UAVs application process are proposed:

T-1: Unconsent capture. A UAV can be very small and quiet during flying. When a UAV takes a photo, there is high possibility that no consent is acquired. For instance, a UAV can take photos in sensitive places (e.g. out of the window of the bathroom) and intimate environments.
T-2: Unaware identification. UAV operators can identify a person using the images taken by UAV cameras via powerful image search engines. Identification of a person with images and/ or geographic locations can cause personal information leakage, even worse, criminals may use personal information from identified people to commit crimes (e.g. fraud).

T-3: Unauthorised disclosure. UAV images/ videos can be easily shared on the internet, especially on the social network. If there is sensitive information contained in the shareable content, it will not only cause the discontentment, but also expose sensitive content to people who could exploit it.

T-4: Storage concern. The system should take great care of UAV works for preventing inappropriate access and possible information leakage.

5.4.2. Indication of Solutions Applicability

	Google Street View Solutions	UK CCTV Code of Practice 2017	Lifelogging Solutions
T-1: Unconsent capture	–	✔	✔✻
T-2: Unaware identification	✔	–	✔✻
T-3: Unauthorised disclosure	✔	✔	–
T-4: Storage concern	–	✔	–

Table 9: Solutions for Threats

Solutions for privacy threats are analysed through Google Street View, CCTV cameras and Lifelogging (see Table 9). Applicable solutions are presented with a tick (✔), inapplicable solutions are presented with the symbol '–', and solutions which could only be applied theoretically but not practically are marked with the symbols a tick and a star (✔✻).

Google Street View Solution: Face blurring can reduce the threat of T-2 and T-3. Google requires to blur the faces or any other identifiable features (e.g. car plates), and it also allows users to request further blurring. With feature-blurring, a person can hardly be identifiable. Therefore, it solves the threat of unaware identification. Also, since people are not identifiable, the sensitivity of information in shareable content is decreased. And so forth, the threat of unauthorised disclosure is reduced.

UK CCTV Code of Practice 2017: The latest regulation published in 2017 reduced the threat of T-1, T-3 and T-4. Before doing any camera surveillance, this regulation requires users to carefully consider '*when surveillance camera systems should be used* (Information Commissioner's Office, 2017)', also to take into consideration of the possible effects cameras may have on other people. The regulation also suggests that 'after evaluation then continue using it'. Moreover, it even provides a document which is *Conducting privacy* *impact assessments code of practice (*see a part of this document in appendices). In this way, it helps to mitigate the threat of dissent capture.

In the section 5.2.2 of this regulation, it rules that disclosure of information should be aligned with the purpose for which the system is set up. It also declares that it is not suitable to upload information on the internet in most cases. By this means, this regulation prevents personal data from possible leakage. Thus, the threat of disclosure is reduced.

For storing collected information, the CCTV Code of Practice requires that all material should be stored in a way which not only keeps its integrity but also protects the individual rights. Furthermore, CCTV Code of Practice insist that all data should be in operations for the intended purposes. Encryption is encouraged for securely keeping the information. Consequently, by applying these terms in UK CCTV Code of Practice, the threat of storage concern can be reduced.

Lifelogging solutions: The solutions of developing a privacy layer, proposing a privacy framework and PlaceAvoider may solve the threat of T-1 and T-2 theoretically. Because according to their algorithms, users who have not given consent will not be taken into images/ videos. Accordingly, the threat of unaware identification is reduced. However, there is a concern about applying the solutions impractically. Because it is difficult to deploy these approaches in any dedicated UAV cameras on UAVs, neither is there any user interface to confirm any permission. Hence, this approach may be suitable only for smart devices used in lifelogging but not for UAVs.

5.5. Summary

There are three similar image and video-based applications discussed in this chapter, which are Google Street View, Closed-circuit Television Cameras and visual lifelogging.

Providing 360° horizontal and 290° vertical panoramic street level views and offering zooming options on specific objectives for any details, Google Street View raised concerns of privacy (identification of the faces of a couple having intercourse on the highway, for instance). To improve mitigate privacy concerns, Google’s Street View implements faces and car-plates blurring technology, designing for blurring all identifiable features, to all of images. Besides that, Google admits the right of data subject including the erasure of personal data. It means that once users have been photographed in residential or working places, they can make a claim to remove their data on Google Street View. Moreover, in Europe, Google gives warnings in advance to the residents of the locations where they intend to take photographs.

Closed Circuit Television (CCTV) is a system of cameras undertaking retrieval and storage of video footages, object tracking, data classification, data mining and the prediction of events. Because the functionalities of CCTV systems are well applied in the different industries ranging from identification of unwanted individuals and targeted criminals, to detection of lawbreaker actions ect., simultaneously, CCTV is being criticised by privacy advocates because of the threat posed by these technologies seems to invade individual liberty. The United Kingdom, which has influential legislation, practice and public perception concerning surveillance and privacy, is the leader in CCTV application. In order to comply with DPA and protect individual privacy, ICO issued the first ‘CCTV code of practice’ in 2000. This document was first updated in 2008. Then in 2013, the name of this regulation was changed into ‘Surveillance Camera Code of Practice’. Since 2017, this regulation is referred as ‘In the picture: A data protection code of practice for surveillance cameras and personal information’ (Information Commissioner’s Office, 2017). The CCTV Code of Practice provides guidance for operations within the law and sets good practice standards.

Lifelogging is an activity which utilises mobile devices or wearable technology to capture and chronicle the first-person perspective of a user's life in a continuous and automatic fashion. Lifelogging has two types of privacy concerns: one is of the lifelogger, and another is of the people who interact with lifeloggers. Regarding privacy concern of visual lifelogging, existing studies in this domain have proposed some solutions, such as adding abstraction privacy layer between applications and sensor data and blocking images taken from first-person perspective cameras in sensitive spaces.

Privacy threats of UAV applications are identified by analysing current literature about UAV privacy concerns and referring to existing privacy threats distilled from Visual Lifelogging privacy studies. Based on the identified privacy threats, the technical applicability of possible solutions from other image and video-based applications have been analysed. The results indicated that feature-blurring solution of Google Street View, data uploading and data collection requirements of UK CCTV Code of Practice can be technically applied in UAV cases. However, solutions from Lifelogging are not applicable because of relatively complicated technical requirements.

6. DISCUSSION

6.1. Introduction

This chapter discusses the findings of this research presented in chapter 4 and chapter 5 viz-a-viz contemporary scientific literature. The first part is about a discussion over UAV regulations evaluation and the second part presents a discussion in relation to similar applications from current image acquisition techniques and proposed solutions from these techniques which could be applied in UAV regulations. Then the limitations of this study will be explored.

6.2. UAV Regulations Evaluation

Privacy, data protection, and ethics issues have been raised significantly since UAVs have been applied in multi-purpose civil applications. Currently, many countries have processed tailored UAVs regulations to focus on technical and safety issues. Nevertheless, those engagements do not cover the most crucial problem: privacy invasion and inappropriate surveillance (Rao et al., 2016). Identification of privacy deficiency of UAVs regulations will facilitate the development of current regulations and improve the protection of individual privacy.

In this study, based on the analysis of privacy in Chapter 3, the variables including privacy of location, privacy of personal data and images and privacy of personal behaviour are selected to identify how privacy is addressed in UAV regulations. Through a combination of indicators developed from those variables, this study identified a severe lack of privacy in UAV regulations at the global level. Nevertheless, some countries address privacy issue in other regulations rather than in UAV regulations, and those related regulations are not well referred to the current UAV regulatory frameworks.

A previous study demonstrated that current UAV regulations acting as the deterrents for privacy invasion cases are too general and uncertainty embraced is too considerable (Clarke & Moses, 2014). This research result is consistent with one of the findings of this study. According to the result of this study, privacy concerns are scarcely addressed and even encompassed in current UAV regulations. It indicated that only 4 out of 14 selected UAV regulations incorporated privacy concerns in UAV regulations, even only to advocate 'respect' personal privacy. 8 UAV regulations do not mention anything about privacy or data protection. Besides, the rest two regulations referred Data Protection Act/ Privacy Code/ Privacy Act to be followed in regards to privacy concerns raised by the application of UAVs.

Although some researchers indicated that the concept of privacy is underdeveloped in most African and Asian countries (Cannataci, 2009), and the reason can be that in African and Asian cultures, loyalty to a group is more important than the expense of individuals (Bygrave, 2004). From the result of this study, the two selected African countries are Kenya and Rwanda, whose UAV regulations covered more aspects than the other selected countries. Despite in Africa, countries failed to mention privacy in the African Charter of Human and Peoples' Rights 1981, which is viewed s as proof of privacy culture on absence on the continent, with years of development, privacy protection in African have had remarkable progress. The desire to engage in global e-Commerce and the economy requires the concept of trust as a fundamental component, both of these two factors pushed the development of privacy law among developing countries. Economic development has been the most effective motivation for the development of privacy-related legislations in Africa (Makulilo, 2015).

Based on the evaluation results, this research suggests that UAV regulations should clarify safety, privacy and data protection requirements and obligations among all stakeholders including users, manufacturers and controllers. If any requirements and obligations of all stakeholders are mentioned in other regulations, these related content should be explicitly referred by UAVs regulations. This is aligned with the conclusion that by adding appropriate legislations, national governments could protect individual rights which is also a reasonable way to ensure expectation of privacy (Schlag, 2013).

6.3. Similar Applications and Proposed Solutions

The results from Chapter 5 provide analysis of similar applications with image acquisition techniques and possible solution generated from these applications. Considering these techniques have already been launched for years, with optimisations, they can offer some insights for UAV regulations improvements from technique perspectives.

This part of solution applicability mostly focuses on solving privacy threats from a technique aspect. Since the privacy threats, which have already been applied in the Visual Lifelogging privacy research (Ferdous et al., 2016) and identified in the process of UAV applications (Clarke & Moses, 2014), covered most aspects as UAVs privacy concerns identified in Section 3.2, the distilled privacy threats were selected (see Table 9).

The solution from Goole Street View is to blur the identifiable features such as faces and car plates. This solution can reduce the privacy to a large extent. However, the algorithm behind the Google face blurring policy is a cutting-edge innovation. With latest Deep Learning model, Google can intensely reduce the computational cost, at the same time, increase the accuracy (Ibarz, 2017). Although the algorithm is technically applicable to prevent UAVs related privacy invasion, it is still difficult to implement the same algorithm in reality because it is not open source. However, with the development of Deep learning, there are several different open-source objective blurring techniques available (Cao et al., 2014; Chen, Lu et al., 2013; Hu et al., 2017). Thus, the identifiable feature blurring could be a new requirement in the UAV regulations of the countries where the UAV producers are capable enough of implementing such algorithms.

The solutions from UK CCTV Code of Practice 2017 can contribute to the UAV regulations, especially at data access and storage aspects. Since according to the evaluation results, most of the regulations even do not mention these concerns at all, UK CCTV Code of Practice 2017 can show a proper direction to various UAV regulatory bodies. As for adding concrete terms in current term in current regulations, it should depend on the situation of the regions.

For the scope of applying proposed solutions. In many cases, considering personally identifiable information as information which can identify a particular person, data collected by UAVs may not contain any identifiable feature, not to mention apparently distinguishing people. Moreover, equipment allowing for collecting geo-location information during flying in the air may not be integrated into UAVs. Therefore, not all UAV applications are harmful or potentially harmful to privacy. However, in some private UAV applications, for instance, hobbyists (Serna, 2014) and paparazzi (Peter & Caroline, 2014), it is most likely to invade privacy. Based on these facts, generally speaking, the UAV regulations should not be so rigorous to all kinds of UAV civil applications.

6.4. Limitations

There are 2 limitations of this study for the sake of time constraint:

1. This study chose 14 countries from different continents. Although they can be the representatives of particular continents, among all the countries in each continents they could comparatively be individual cases. If more country cases are selected in the comparison, the outcome can have a broader overview.

2. Only the technical applicability of possible solutions was analysed. For implementation of a regulation/ policy, more aspects of applicability in a certain social context should be explored such as law environment, public opinion, costs, economic situations (Georgiadou & Reckien, 2018).

7. CONCLUSIONS AND RECOMMENDATIONS

7.1. Introduction

The previous chapters discussed the evaluation of current UAV regulatory frameworks at the international level and presented possible solutions according to contemporary literature on the similar image/video acquisition applications which include Google Street View, Closed-circuit Television Cameras (CCTV) and visual lifelogging. This chapter provides the answers to research questions which feed into the sub-objective and the main objectives of this study, furthermore, the recommendations.

7.1.1. Research Sub-objective One: To review how privacy is conceived related to UAVs

a) *How is privacy conceived related to UAVs in various UAV regulations?*

The concept of privacy is not well conceived in UAV regulations. Few countries only mention the term with bare restrictions, for the most part, UAV regulations in selected 14 countries mainly focus on four key concerns: 1) providing safety and operational standards for UAV operations; 2) setting limitations for the use of UAVs to be complied with in the national airspace; and 3) defining procedures in air navigation and airspace. 4) regulating general UAV related concerns such as pilot licenses application, insurance, penalties, data protection.

b) *How do current UAV regulations address privacy concern?*

According to the result of this study, privacy concerns are scarcely addressed and even barely encompassed in current UAV regulations. Only 4 out of 14 selected UAV regulations incorporated privacy concerns in UAV regulations, even only to advocate 'respect' to personal privacy. 8 UAV regulations do not mention anything about privacy or data protection, nevertheless, in 5 countries of which, data protection/ privacy regulations have been adopted for all means of privacy invasion cases. Besides, other 2 regulations referred to Data Protection Act/ Privacy Code/ Privacy Act to be followed in regards to UAVs caused privacy concern.

7.1.2. Research Sub-objective Two: To evaluate current UAV regulatory frameworks in privacy aspect.

a) *What are weaknesses of current privacy terms?*

In general, based on the evaluation of 14 selected countries, there is severe lack of privacy concerns in UAV regulations at the global level. All privacy related aspects (include but not limited to privacy of location and space, privacy of personal data and images and personal behaviour) need to be further addressed. None of these regulations addressed the role of manufacturers or other shareholders. Some UAV operations are not explicitly mentioned in UAVs regulation but prohibited under constitution, environmental law, or data protection law, and so forth.

b) *What are the possible recommendations to improve current regulatory frameworks?*

UAV regulations should clarify safety, privacy and data protection requirements and obligations among all stakeholders such as users, manufacturers and controllers. Rather than only paying attention and setting restrictions on the users, the duties of manufacturers (a UAV manufacturer should inform clients on its website, for instance), and the obligations of controllers (e.g. how to interfere the UAVs privacy invasion cases) should be apparently written on the regulations. However, the details of these terms for different requirements should depend on the circumstances of the specific countries.

UAV regulations should encourage UAV manufacturers to implement privacy protection by design (e.g. in cameras) or at least have a notice informing UAV users related laws and regulations, which could support and increase compliance.

Although there could be some gaps in UAV regulations, such privacy intrusions are still being forbidden under other specific laws and regulations. In order to enhance privacy protection, laws and regulations related to privacy invasion should be explicitly referred in current UAV regulations, and UAV applications which may lead to privacy invasion should be identified based on the local legal situation.

7.1.3. Research Sub-objective Three: To propose solutions from other image-based acquisition techniques (e.g. Google Street View) and to analyse if they are applicable

a) What are similar applications?

Google Street View, Closed Circuit Television (CCTV) and visual lifelogging are selected for this study. Google Street View provides panoramic street-level views. Closed Circuit Television (CCTV) is a system of cameras sends images or videos to a limited set of monitors undertaking retrieval and storage of video footages, object tracking, data classification, data mining and the prediction of events. Besides, Lifelogging activities utilise mobile devices or wearable technology to record and chronicle the first-person perspective of a user's life. All of these three techniques lead to concerns of privacy invasion.

b) How do they deal with privacy concern?

Google assures that sensitive information, which include but not limited to personal details, clothing, and other features leading to possible personal identification, is blurred. To improve data transparency, in case users might be or have been photographed in residential or working places, instead of any disproportionate effort (e.g. a court claim) from individuals, Google admits the right of data subject including the erasure of personal data. Moreover, in Europe, Google gives warnings in advance of the locations where they intend to take photographs.

For CCTV, UK legislation provides some guidance for the use and control of CCTV, meanwhile, undertaking some protection to the general. Data Protection Act (DPA) is the legislation being in charge of individual information held by organisations. CCTV operators are bearing legal obligations from DPA, although the DPA was not specifically for CCTV (Sheldon, 2011). Besides, in an effort to ensure organizations to comply DPA and protect individual privacy, the Information Commissioner's Office (ICO) issued the first 'CCTV code of practice' (COP) in 2000, which was updated in 2008 and 2013 (the name was revised as 'Surveillance Camera Code of Practice'), and in 2017 the name of this regulation was revised as 'In the picture: A data protection code of practice for surveillance cameras and personal information'. This CCTV COP provides guidance to CCTV operations within the law and implement proper practice standards (Hartmus, 2014).

Regarding privacy concern of visual lifelogging, existing works in this domain have proposed some solutions (Ferdous et al., 2017):

Jana et al. (2013) have presented a solution which provides an abstraction privacy layer between applications and sensor data which is called OS (operating system).
Templeman et al. (2014) presented a solution called PlaceAvoider, which is used for blocking images taken from first-person perspective cameras in sensitive spaces (e.g. private places such as bathrooms and bedrooms).

Memon & Tanaka (2014) proposed a framework for privacy-preserving lifelogging through which the other parties may be notified by wearable devices of places and times that they are not willing to be captured in the lifelogging images/ videos/ microphones.

c) *Can their experience be applied in UAV regulatory frameworks?*

Based on the privacy threats identified in section 5.4.1, Google Street View Solution, UK CCTV Code of Practice 2017 and Lifelogging solutions are analysed:

Google Street View Solution: Face blurring can reduce the threat of unaware identification and unauthorised disclosure as Google requires to blur the faces or any other identifiable features (e.g. car plates). Moreover, it is also acceptable when a user demands further blurring. With face blurring, a person can hardly be identifiable. Therefore, feature-blurring solution from Google solves the threat of unaware identification. Also, since people are not identifiable, it means the sensitivity of information in shareable content dramatically decreases, then the threat of unauthorised disclosure is reduced as well.

UK CCTV Code of Practice 2017: The latest COP was published in 2017 which can reduce the threat of dissent capture, unauthorised disclosure and storage concern.

This regulation requires users to carefully consider when the CCTV camera system should be applied and to take consideration of effect cameras may have on other people. Besides, this regulation also suggests that 'after evaluation then continue using it'. Moreover, it even provides a document which is *Conducting privacy impact assessments code of practice* (see a part of this document in appendices). In this way, it helps to mitigate the threat of dissent capture.

In the section 5.2.2 of this regulation, it rules that disclosure of information should be aligned with the purpose for which the system is set up. Additionally, it is not suitable to upload information on the internet in most cases in order to prevent personal data from leakage. In this way, the threat of disclosure is reduced.

For storing collected information, the CCTV Code of Practice requires that all material should be stored in a way which not only keeps its integrity but also protects the individual rights. Furthermore, CCTV Code of Practice insists that all data should be in operations for the intended purposes. Encryption is encouraged for securely keeping the information. Consequently, by applying these terms in UK CCTV Code of Practice, the threat of storage concern can be reduced.

Lifelogging solutions: The solutions of developing a privacy layer, proposing a privacy framework ad PlaceAvoider could solve the threat of dissent capture and unaware identification theoretically. Because according to their algorithms, users who do not consent will not be taken into images/ videos. Accordingly, the threat of unaware identification is reduced. However, in practice, it is difficult to deploy these approaches in any dedicated UAV cameras equipped on UAVs, neither is there any user interface to confirm any permission. Hence, this approach may be suitable only for smart devices used in lifelogging but not for UAVs.

7.2. General Conclusion on Main Research Objective

The main objective of the research is to analyse UAV regulatory frameworks in terms of privacy at the global scale and propose solutions from high-resolution image data privacy concern in other domains. Besides, to analyse if proposed solutions could be applied in UAV regulations.

According to the evaluation of currently selected UAV regulations, severe lack of privacy concern is identified at the global level. Form the proposed solutions, it can be found that faces and any other identifiable features blurring technique applied by Google Street View can be implemented to reduce the threat of unaware identification and unauthorised disclosure. As stated by UK CCTV Code of Practice 2017, evaluation privacy impact confirming to *Conducting privacy impact assessments code of practice* can mitigate the threat of dissent capture. Disclosure of information should match the purpose for which the system is set up, either, not to upload information on the internet in most cases. By these means, the threat of disclosure can be decreased. In regards of data storage, requiring that all material should be stored in the way which can not only keep its integrity but also protect the individual rights. Additionally, ensuring all the data can be used in the intended purposes can be applied in UAV regulations, for the purpose of reducing the concern of threat of storage. Solutions from lifelogging are not feasible to apply on UAV regulations at this moment.

7.3. Recommendations

Based on the cross-country UAV regulation evaluation and solutions application analyses from Google Street View, Closed-circuit Television Cameras(CCTV) and Life Logging, three recommendations are proposed for UAVs related privacy invasion cases and future research:

First, UAV regulations should be compiled to encompass aspects including safety, privacy and data protection and obligations among all stakeholders including users, manufacturers and controllers. All the requirements should be based on the local situation. Countries which have already published UAV regulations but not complete, could learn from relatively complete regulations, for instance, EU data protection regulations. In implementation, terms in relatively complete regulations (e.g. GDPR) should be transposed according to domestic requirements. For countries with relatively complete laws and regulations systems, such as EU countries and US, if there are existing laws/regulations (e.g. Data Protection Law) especially working on specific aspects (e.g. data protection) besides the UAV regulations, UAV regulations should explicitly refer to external terms which may have impacts on the current UAV privacy invasion cases.

Second, the solution from Google Street view which is to blur identifiable features including faces and car plates can be technically applied in UAV regulations. Once all images and videos have removed identifiable features, the threat to personal privacy can be severely reduced. For countries which have independent UAV regulatory bodies, the identifiable feature blurring process should be compulsorily implemented under the supervision of UAV regulatory bodies. This procedure should be better started from the manufacture by design, or at least, the producers should inform users not only to 'respect' privacy but also to blur identifiable features in data transmission. For countries which don't even have an UAVs regulatory agency, the first step should be to establish an independent regulatory body bearing the responsibility for all UAVs related actions such as safety, privacy and data protection.

Third, the solutions from UK CCTV practice code are meaningful with the supervision of UAVs regulatory bodies. UAV regulations or UAV regulatory bodies can inform UAVs users in advance to take consideration that the cameras may affect people. This procedure could slightly mitigate the privacy threat. Conducting a privacy assessment beforehand can also be applied on civil UAV applications, but the requirements and conditions should be based on the local situation. In this regards, if UAVs applications can be aligned with privacy assessment result (the result decides whether to allow UAV applications) and the most probable privacy invasion cases can be reduced at the beginning. For data storage, the CCTV code of practice can show a good example to UAV cases. Because the CCTV Code of Practice requires that all material should be stored in the way which not only keeps its integrity but also protects the individual rights. Furthermore, CCTV Code of Practice ensures all data can be in operations for the intended purposes. Compared with the current UAVs data storage means which have barely restrictions (e.g. in data storage,), the way CCTV Code of Practice requires to store data can reduce privacy concerns caused by data leakage.

This research provides baselines for future studies. Apart from the technical applicability of possible solutions from Google Street View and UK CCTV Code of Practice, more dimensions such as legal and economic applicability or requirements of possible solutions implementation can be explored in future research.

LIST OF REFERENCES

Abdulharis, R., van Loenen, B., & Zevenbergen, J. (2005). Legal aspects of access to geo-information within Indonesian spatial data infrastructure. *ISPRS Workshop on Service and Application of Spatial Data Infrastructure, XXXVI (4/W6)*. Retrieved from http://www.bastiaanvanloenen.nl/pubs/Abdulharis_2005_ISPRS.pdf

Agustina, J. R., & Galdon, C. G. (2011). The impact of CCTV on fundamental rights and crime prevention strategies: The case of the Control commission of video surveillance devices. *Computer Law and Security Review*, *27*(2), 168–174.

Al-Mawdudi, A. A. Cairo Declaration on Human Rights, Ham § (1980).

Asia Pacific Economic Cooperation. (2005). *APEC privacy framework. Framework*. Retrieved from http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx

AUVSI. Unmanned Aircraft System Operations Industry " Code of Conduct " (2012).

Badland, H. M., Opit, S., Witten, K., Kearns, R. A., & Mavoa, S. (2010). Can virtual streetscape audits reliably replace physical streetscape audits? *Journal of Urban Health*, *87*(6), 1007–1016.

Boring. Boring v. Google, Inc. (2010). Retrieved from https://www.wsgr.com/attorneys/BIOS/PDFs/boring_v_google.pdf

Bush, V. (1945). As We May Think. *The Atlantic*, *176*(1), 101–108. Retrieved from http://www.theatlantic.com/magazine/archive/1969/12/as-we-may-think/3881/

Bygrave, L. A. (2004). Privacy Protection in a Global Context – A Comparative Overview. *Scandinavian Studies in Law*, *47*, 319–348.

Bygrave, L. A. (2010). Privacy and Data Protection in an International Perspective. *Scandinavian Studies in Law*, *56*, 165–200.

Cannataci, J. A. (2009). Privacy, Technology Law and Religions across Cultures. *JILT-Journal of Information Law & Technology*, *1*(1), 22. Retrieved from http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2009_1/cannataci/#endnotes

Cao, Z., Wei, Z., & Zhang, G. (2014). A No-reference Sharpness Metric Based on the Notion of Relative Blur for Gaussian Blurred Image. *Journal of Visual Communication and Image Representation*, *25*(7), 1763–1773.

Carr, E. B. (2016). Unmanned Aerial Vehicles: Examining the Safety, Security, Privacy and Regulatory Issues of Integration into U.S. Airspace. *National Center for Policy Analysis Report*. Retrieved from http://www.ncpa.org/pdfs/sp-Drones-long-paper.pdf

Chen, Y. H., Lu, E. J. L., & Wang, C. F. (2013). Privacy Image Protection Using Fine-grained Mosaic Technique. In *2013 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference, APSIPA 2013* (Vol. 1, pp. 0–3).

Cho, G. (2013). Unmanned aerial vehicles: Emerging policy and regulatory issues. *Journal of Law, Information and Science*, *22*(2), 201.

Clarke, R. (1999). Introduction to Dataveillance and Information Privacy, and Definitions of Terms. Retrieved November 11, 2017, from http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html%0AThis

Clarke, R. (2014a). Managing Drones' Privacy and Civil Liberties Impacts. Retrieved November 1, 2017, from http://www.rogerclarke.com/SOS/Drones-PCLI.html

Clarke, R. (2014b). The regulation of civilian drones' impacts on behavioural privacy. *Computer Law and Security Review*, *30*(3), 286–305.

Clarke, R., & Moses, L. B. (2014). The regulation of civilian drones' impacts on public safety. *Computer Law and Security Review*, *30*(3), 286–305.

Colomina, I., & Molina, P. (2014). Unmanned aerial systems for photogrammetry and remote sensing: A review. *ISPRS Journal of Photogrammetry and Remote Sensing*, *92*, 79–97.

Coudert, F., & Dumortier, J. (2008). Intelligent video surveillance networks: Data protection challenges. In *ARES 2008 - 3rd International Conference on Availability, Security, and Reliability, Proceedings* (pp. 975–981).

Daskala, B. (2011). *TO LOG OR NOT TO LOG ? Risks and benefits of emerging life-logging applications. Information Security.*

Davis, K., Jain, S., Wattam, D., McMurtry, J., & Johnson, M. (2010). Factors of influence on legislative decision making: A descriptive study - Updated August 2009. *Journal of Legal, Ethical, and Regulatory Issues*, *13*(2), 55–69.

De Jong, A. J., Van Loenen, B., & Zevenbergen, J. A. (2016). Geographic Data As Personal Data in Four EU Member States. *ISPRS Annals of Photogrammetry, Remote Sensing and Spatial Information Sciences*, *III-2*(July), 151–157. Retrieved from http://www.isprs-ann-photogramm-remote-sens-spatial-inf-sci.net/III-2/151/2016/isprs-annals-III-2-151-2016.pdf

EASA. Notice of Proposed Amendment (NPA) 2012-11 (2012).

EASA. Notice of Proposed Amendment 2017-05 (A), 5 (2018).

Efron, S. (2015). *The Use of Unmanned Aerial Systems for Agriculture in Africa*. Retrieved from y:%5C21098.pdf

European RPAS Steering Group. (2013). *Roadmap for the integration of civil Remotely - Piloted Aircraft Systems into the European Aviation System.*

Federal Aviation Administration. Operation and Certification of Small Unmanned Aircraft Systems, 81 § (2016). Retrieved from https://federalregister.gov/a/2016-15079

Ferdous, M. S., Chowdhury, S., & Jose, J. M. (2016). Privacy threat model in lifelogging. *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing Adjunct - UbiComp '16*, 576–581.

Ferdous, M. S., Chowdhury, S., & Jose, J. M. (2017). Analysing privacy in visual lifelogging. *Pervasive and Mobile Computing*, *40*, 430–449.

Finn, R. L., & Wright, D. (2012). Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications. *Computer Law and Security Review*, *28*(2), 184–194.

Finn, R. L., & Wright, D. (2016). Privacy, data protection and ethics for civil drone practice: A survey of industry, regulators and civil society organisations. *Computer Law and Security Review*, *32*(4), 577–586.

Finn, R. L., Wright, D., Jacques, L., De Hert, P., & Union, E. (2014). *Study on Privacy, Data Protection and*

Ethical Risks in Civil Remotely Piloted Aircraft Systems Operations. Summary for Industry.

Frome, A., Cheung, G., Abdulkader, A., Zennaro, M., Wu, B., Bissacco, A., … Vincent, L. (2009). Large-scale privacy protection in Google Street View. *Proceedings of the IEEE International Conference on Computer Vision*, (Iccv), 2373–2380.

Georgiadou, Y., & Reckien, D. (2018). Geo-Information Tools, Governance, and Wicked Policy Problems. *ISPRS International Journal of Geo-Information*, *7*(1), 21. Retrieved from http://www.mdpi.com/2220-9964/7/1/21

Google Maps Help. (2017). Use Street View in Google Maps. Retrieved December 12, 2017, from https://support.google.com/maps/answer/3093484?co=GENIE.Platform%3DDesktop&hl=en

Google Street View. (2017). Image Acceptance & Privacy Policies. Retrieved December 15, 2017, from https://www.google.com/streetview/privacy/

Gurrin, C., Albatal, R., Joho, H., & Ishii, K. (2014). A privacy by design approach to lifelogging. *Digital Enlightenment Yearbook 2014*, (January 1878), 49–73. Retrieved from http://doras.dcu.ie/20505/1/Gurrin.pdf

Gutwirth, S., Leenes, R., De Hert, P., & Poullet, Y. (2013). Seven Types of Privacy. *European Data Protection: Coming of Age*, 1–440.

Hartmus, D. M. (2014). Government Guidelines for CCTV: A Comparison of Four Countries. *International Journal of Public Administration*, *37*(6), 329–338.

Hayes, B., Jones, C., & Töpfer, E. (2014). *EURODRONES Inc. A report by Ben Hayes, Chris Jones & Eric Töpfer.* Retrieved from http://www.statewatch.org/news/2014/feb/sw-tni-eurodrones-inc-feb-2014.pdf

Hempel, L., & Töpfer, E. (2009). The Surveillance Consensus: Reviewing the politics of CCTV in three European countries. *European Journal of Criminology*, *6*(2), 157–177.

Hepburn, G. (2006). Alternatives to Traditional Regulation. *Oecd*, 1–65.

Hu, X., Peng, S., Wang, L., Yang, Z., & Li, Z. (2017). Surveillance video face recognition with single sample per person based on 3D modeling and blurring. *Neurocomputing*, *235*(September 2015), 46–58.

Ibarz, J. (2017). Updating Google Maps with Deep Learning and Street View. Retrieved February 1, 2018, from https://research.googleblog.com/2017/05/updating-google-maps-with-deep-learning.html

ICAO. (2009). *Unmanned Aircraft Systems. Cir 328 AN/190* (Vol. 23).

Information Commissioner's Office. Surveillance Camera Code of Practice (2013). Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/282774/SurveillanceCameraCodePractice.pdf

Information Commissioner's Office. Conducting privacy impact assessments code of practice, Ico.Org.Uk § (2014). Retrieved from https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf%0Ahttps://ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Practical_application/pia-code-of-practice-final-draft.pdf

Information Commissioner's Office. In the picture : A data protection code of practice for surveillance cameras and personal information (2017).

IPTS. (2001). *Security and Privacy for the Citizen in the Post September 11 Digital Age : A Prospective Overview.*

Jana, S., Molnar, D., Moshchuk, A., Dunn, A., Livshits, B., Wang, H. J., & Ofek, E. (2013). Enabling Fine-Grained Permissions for Augmented Reality Applications with Recognizers. *Presented as Part of the 22nd USENIX Security Symposium (USENIX Security 13)*, 415–430. Retrieved from https://www.usenix.org/conference/usenixsecurity13/technical-sessions/presentation/jana

Kaminski, M. E. (2013). Drone Federalism: Civilian Drones and the Things They Carry. *California Law Review Circuit*, *4*(May 2013), 57–74.

Kirk, J. (2009). Swiss Contend Google Doesn't Blur Street View Enough. Retrieved September 12, 2017, from https://www.pcworld.com/article/182150/article.html

Koeva, M., Muneza, M., Gevaert, C., Gerke, M., & Nex, F. (2016). Using UAVs for map creation and updating. A case study in Rwanda. *Survey Review*, 1–14. Retrieved from https://www.tandfonline.com/doi/full/10.1080/00396265.2016.1268756

Lijphart, A. (1971). Comparative Politics and Commparative Method. *The American Political Science Review*, *Vol.65*(No.3), 682–693.

Lor, P. (2011). Methodology in comparative studies. *International and Comparative Librarianship*, 1–21. Retrieved from https://pjlor.files.wordpress.com/2010/06/chapter-4-draft-2011-04-20.pdf

Lyon, D. (2003). *Surveillance after September 11. Polity Press.*

Makulilo, A. B. (2015). Myth and reality of harmonisation of data privacy policies in Africa. *Computer Law and Security Review*, *31*(1), 78–89.

Manyoky, M., Theiler, P., Steudler, D., & Eisenbeiss, H. (2012). Unmanned Aerial Vehicle in Cadastral Applications. *ISPRS - International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*, *XXXVIII-1/*(September), 57–62.

Margulis, S. T. (2003). On the Status and Contribution of Westin's and Altman's Theories of Privacy. *Journal of Social Issues*, *59*(2), 411–429.

MarketsandMarkets. (2016). Unmanned Aerial Vehicle (UAV) Market Global Forecast to 2022. Retrieved July 31, 2017, from http://www.marketsandmarkets.com/Market-Reports/unmanned-aerial-vehicles-uav-market-662.html

Marty, I. J. (2013). *Final Report. Alain Rabeau, Intersol Consulting Associates Limited.*

Marzocchi, O. Privacy and Data Protection Implications of the Civil Use of Drones, European Parliament § (2015). Retrieved from http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/519221/IPOL_IDA(2015)519221_EN.pdf

Mashable. (2017). 36 Embrassing Google Street View Sightings. Retrieved September 9, 2017, from https://mashable.com/2013/06/10/google-street-view-embarrassing/#vmKNPYxd_Sqr

Matsuoka, R., Nagusa, I., Yasuhara, H., Mori, M., Katayama, T., Yachi, N., … Atagi, T. (2012). Measurement of Large-Scale Solar Power Plant By Using Images Acquired By Non-Metric Digital Camera on Board UAV. *ISPRS - International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*, *XXXIX-B1*(September), 435–440.

McBride, P. (2009). Beyond Orwell: The Applicatino of Unmanned Aircraft Systems in Domestic

Surveillance Operations. *The Jouarnal of Air Law and Commerde2*, *74*, 627–662.

Memon, M. A., & Tanaka, J. (2014). Ensuring Privacy during Pervasive Logging by a Passerby. *Journal of Information Processing*, *22*(2), 334–343. Retrieved from http://jlc.jst.go.jp/DN/JST.JSTAGE/ipsjjip/22.334?lang=en&from=CrossRef&type=abstract

Möllers, N., & Hälterlein, J. (2013). Privacy issues in public discourse: The case of "smart" CCTV in Germany. *Innovation*, *26*(1–2), 57–70.

Myagmar, S., Lee, A. J., & Yurcik, W. (2005). Threat Modeling as a Basis for Security Requirements. *Symposium on Requirements Engineering for Information Security (SREIS)*, 1–8.

Nackenoff, C. October Term, 2011, Supereme Court of the United States § (2012). Retrieved from http://www.supremecourt.gov/opinions/11pdf/10-1259.pdf

Nex, F., & Remondino, F. (2014). UAV for 3D mapping applications: A review. *Applied Geomatics*, *6*(1), 1–15.

OAIC. (2013). Regulation of drone technology — Letter from Attorney-General to Privacy Commissioner. Retrieved September 4, 2017, from https://www.oaic.gov.au/media-and-speeches/statements/regulation-of-drone-technology

Office of Public Sector Information. Data Protection Act 1998, The Stationery Office of UK § (1998).

Olea, P., & Mateo-Tomás, P. (2013). Assessing Species Habitat Using Google Street View: A Case Study of Cliff-Nesting Vultures. *PLoS ONE*, *8*(1), 1–8.

Oram, J. (2011). Balancing surveillance between needs of privacy and security: CCTV in Japan and England. *CALE Discussion Pappers*, (6), August. Retrieved from http://ir.nul.nagoya-u.ac.jp/jspui/handle/2237/20102

Organization of American States. American Convention on Human Rights (1969).

Park, S. H., & Lee, K. H. (2017). Developing Criteria for Invasion of Privacy by Personal Drone. *2017 International Conference on Platform Technology and Service, PlatCon 2017 - Proceedings*, 1–7.

Peter, S., & Caroline, G. (2014). Attack of the drones: Hollywood celebrities are besieged by paparazzi spies in the sky. Worried? You should be... because they'll soon be a regular fixture over YOUR home. Retrieved February 11, 2018, from http://www.dailymail.co.uk/news/article-2746231/Attack-drones-Hollywood-celebrities-besieged-paparazzi-spies-sky-Worried-You-ll-soon-regular-fixture-YOUR-home.html

Piper DLA. (2017a). Data Protection Laws of the World - Brazil. Retrieved October 1, 2017, from https://www.dlapiperdataprotection.com/index.html?t=law&c=BR

Piper DLA. (2017b). Data Protection Laws of the World - China. Retrieved October 1, 2017, from https://www.dlapiperdataprotection.com/index.html?c=CN&c2=&t=law

Porta, D. (2008). Comparative analysis: case-oriented versus variable-oriented research. *Approaches and Methodologies in the Social Sciences. A Pluralist Perspective*, 198–122.

Rao, B., Gopi, A. G., & Maione, R. (2016). The societal impact of commercial drones. *Technology in Society*, *45*, 83–90.

Rapoport, E. (2013). Create your own Street View. Retrieved January 31, 2018, from https://maps.googleblog.com/2013/12/create-your-own-street-view.htmlvvv

Remondino, F., Barazzetti, L., Nex, F., Scaioni, M., & Sarazzi, D. (2011). UAV photogrammetry for mapping and 3d modeling–current status and future perspectives. *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*, *38–1/C22*(September), 25–31.

Rinaudo, F., Chiabrando, F., Lingua, A., & Spanò, A. (2012). Archaeological Site Monitoring: UAV Photogrammetry Can Be an Answer. *ISPRS - International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*, *XXXIX-B5*(September), 583–588.

Schaub, F., & Knierim, P. (2016). Drone-based Privacy Interfaces: Opportunities and Challenges. *SOUP 2016 - Twelfth Symposium on Usable Privacy and Security*. Retrieved from https://www.usenix.org/system/files/conference/soups2016/wfpn16-paper_schaub.pdf

Schlag, C. (2013). The New Privacy Battle: How the Expanding Use of Drones Continues to Erode Our Concept of Privacy and Privacy Rights. *Pittsburgh Journal of Technology Law and Policy*, *13*(2), 1–22.

Scholtz, A., Kaschwich, C., Krüger, A., Kufieta, K., Schnetter, P., Wilkens, C.-S., … Vörsmann, P. (2011). Development of a new Multi-Purpose UAS for ScientificApplication. *Proceedings of the International Conference on Unmanned Aerial Vehicle in Geomatics (UAV-G), XXXVIII-1/*(September), 1682–1777.

Segall, J. (2010). Google Street View: Walking the line of privacy-intrusion upon seclusion and publicity given to private facts in the digital age. *Pittsburgh Journal of Technology Law and Policy*, *X*(May).

Sellen, A. J., & Whittaker, S. (2010). Beyond total capture. *Communications of the ACM*, *53*(5), 70.

Serna, J. (2014). As hobby drone use increases, so do concerns about privacy, security. Retrieved February 11, 2018, from http://www.latimes.com/local/la-me-drone-hobbyist-20140622-story.html

Sheldon, B. (2011). Camera surveillance within the UK: Enhancing public safety or a social threat? *International Review of Law, Computers and Technology*, *25*(3), 193–203.

Shet, V. (2014). Official Google Blog: Go back in time with Street View. Retrieved January 30, 2018, from https://googleblog.blogspot.nl/2014/04/go-back-in-time-with-street-view.html

Singer, P. W., & Lin, J. (2012). Baby Steps: The Drone Industry's Code of Conduct Skips Over Key Questions.

Sloot, B. Van Der, & Borgesius, F. Z. (2012). Google and Personal Data Protection. *Google and the Law*, *2012*, 75–111.

Stöcker, C., Bennett, R., Nex, F., Gerke, M., & Zevenbergen, J. (2017). Review of the current state of UAV regulations. *Remote Sens. FOR PEER REVIEW*, *9*, 1–26.

Templeman, R., Korayem, M., Crandall, D., & Apu, K. (2014). PlaceAvoider: Steering First-Person Cameras away from Sensitive Spaces. *Proceedings of The 21st Annual Network and Distributed System Security Symposium (NDSS)*, (February), 23–26. Retrieved from https://www.cs.indiana.edu/~kapadia/papers/placeavoider-ndss14.pdf

The European Parliament, & The European Council. General Data Protection Regulation, Official Journal of the European Union § (2016).

Transport Canada. (2017). Proposed rules for drones in Canada. Retrieved December 12, 2017, from http://www.tc.gc.ca/eng/civilaviation/opssvs/proposed-rules-drones-canada.html

UK Government. United Kingdom: Human Rights Act 1998 (1998). Retrieved from http://www.legislation.gov.uk/ukpga/1998/42/contents

UN. Universal Declaraiton of Human Rights (2015). Retrieved from http://www.un.org/en/udhrbook/pdf/udhr_booklet_en_web.pdf

United Nations Development Programme. (2016). *Human Development Report 2016. United Nations Development Programme*. Retrieved from http://hdr.undp.org/sites/default/files/2016_human_development_report.pdf

Vacca, A., Onishi, H., & Cuccu, F. (2017). Drones: Military weapons, surveillance or mapping tools for environmental monitoring? Advantages and challenges. A legal framework is required. *Transportation Research Procedia*, *25*, 51–62.

Van Loenen, B., De Jong, A., & Zevenbergen, J. (2008). *Locating mobile devices - Balancing privacy and national security.*

Van Loenen, B., Groetelaers, D., Zevenbergen, J., & De Jong, J. (2007). Privacy versus national security: The impact of privacy law on the use of location technology for national security purposes. *Lecture Notes in Geoinformation and Cartography*, 135–152. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-84879666651&partnerID=tZOtx3y1

Van Loenen, B., & Zevenbergen, J. (2007). Privacy (regimes) do not threaten location technology development. In *Proceedings - IEEE International Conference on Mobile Data Management* (pp. 238–242).

Vandeviver, C. (2014). Applying Google Maps and Google Street View in criminological research. *Crime Science*, *3*(1), 13. Retrieved from http://www.crimesciencejournal.com/content/3/1/13

Villasenor, J. (2013). Observations from above: Unmanned aircraft systems and privacy. *Harvard Journal of Law and Public Policy*, *36*(2), 457–517.

Volovelsky, U. (2014). Civilian uses of unmanned aerial vehicles and the threat to the right to privacy - An Israeli case study. *Computer Law and Security Review*, *30*(3), 306–320.

Walker, N. (2008). Pilot-less Aircraft: the Horse-less Carriage of the 21st Century? *Journal of Risk Research*, *11*(8), 999–1023. Retrieved from http://www.ingentaconnect.com/content/adis/smd/2010/00000040/00000004/art00001

Whittaker, F. (2009). Staunton Man Dubs Google Streetview "An Invasion of Privacy:" Has Google Street View Arrived in Gloucestershire? Retrieved December 16, 2017, from https://web2.westlaw.com/Find/default.wl?cite=2009+WLNR+9255534&rs=LAWS2.0&vr=1.0.

APPENDICES

Data Protection Act

- Conducting privacy impact assessments code of practice (UK)

Privacy impact assessment screening questions

These questions are intended to help organisations decide whether a PIA is necessary. Answering 'yes' to any of these questions is an indication that a PIA would be a useful exercise. You can expand on your answers as the project develops if you need to.

You can adapt these questions to develop a screening method which fits more closely with the types of project you are likely to assess.

Will the project involve the collection of new information about individuals?

Will the project compel individuals to provide information about themselves?

Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?

Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?

Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.

Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?

Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private.

Will the project require you to contact individuals in ways which they may find intrusive?