DRONEOPTICON

Privacy Implications of Civilian Drones in the EU

By,

Girish Agarwal

TESI DOCTORAL UPF/2016-2020

Directors de la tesi

Dr Pablo Salvador Coderch (Departament de dret civil)

Dr Antoni Rubí Puig (Departament de dret civil)

Department of Law

Universitat Pompeu Fabra Barcelona

In dedication to Dr Gautam Agarwal without whose financial assistance this thesis would not have been possible.

Acknowledgements

I would like to thank my thesis Directors, Dr Pablo Salvador Coderch and Dr Antoni Rubí Puig, for investing their time, to go through my drafts, commenting on its accuracy, and giving invaluable feedbacks. Their patience will be remembered.

Ms. Luísa Garcia also deserves a thank, for being my administrative point of contact, always keeping me updated on seminars and courses. Without her, I would not know which classrooms to attend.

Abstract

Civilian drones are increasing in their use. One of the reasons for their rising popularity and increased use, is affordability. They are used for recreational photography, delivering medicines, dousing fire, spraying crops, and even surveillance of individuals.

As is the fate with all inventions, drones are also being regulated. Legislation is the most obvious armour against the negative social impacts of technology, in this case, visual privacy. But there are other negative social impacts, for example, property trespass, which may in combination with others, change the arithmetic of the legal liability.

Therefore, this study investigates the impact on visual privacy of individuals, by the increasing use of civilian drones, and the nature of liability. This study also investigates the adequacy of the existing solutions to fight the violations of visual privacy by drones and their remote pilots.

Resumen

El uso de drones civiles está aumentando. Una de las razones de su creciente popularidad y de su mayor uso es su asequibilidad. Los drones civiles se utilizan para, entre otras finalidades, fotografía recreativa, entrega de medicamentos, extinción de incendios, fumigación de cultivos e incluso vigilancia de personas.

Como ocurre con el destino de todas las invenciones, los drones también están siendo regulados. La legislación es la herramienta más obvia contra los impactos sociales negativos de esta tecnología,

en este caso, sobre la privacidad visual. Más allá de estos, existen otros impactos sociales negativos de los drones civiles, por ejemplo, las invasiones físicas en propiedades ajenas, que, en combinación con otros, pueden cambiar la aritmética de la responsabilidad civil.

Este estudio investiga el impacto que tiene el uso creciente de drones civiles en la privacidad visual de las personas, así como la naturaleza de la responsabilidad legal que se deriva de ello. Este estudio también investiga la adecuación de las soluciones existentes para combatir las intromisiones en la privacidad visual por parte de los drones y sus pilotos remotos.

Resum

L'ús de drons civils està augmentant. Una de les raons de la seva creixent popularitat i del seu major ús és la seva assequibilitat. Els drons civils s'utilitzen per a, entre d'altres finalitats, fotografia recreativa, lliurament de medicaments, extinció d'incendis, fumigació de cultius i fins i tot vigilància de persones.

Com passa amb el destí de totes les invencions, els drons també estan sent regulats. La legislació és l'eina més òbvia contra els impactes socials negatius d'aquesta tecnologia, en aquest cas, sobre la privacitat visual. Més enllà d'aquests, hi ha altres impactes socials negatius dels drons civils, per exemple, les invasions físiques en propietats alienes, que en combinació amb altres, poden canviar l'aritmètica de la responsabilitat civil.

Aquest estudi investiga l'impacte que té l'ús creixent de drons civils en la privacitat visual de les persones, així com la naturalesa de la

responsabilitat legal que se'n deriva. Aquest estudi també investiga l'adequació de les solucions existents per a combatre les intromissions en la privacitat visual per part dels drons i els seus pilots remots.

Table of Contents

List of Abbreviations

AI	Artificial Intelligence
BVLOS	Beyond the Visual Line of Sight
BRLOS	Beyond the Radio Line of Sight
CTOL	Conventional Take-off and Landing
CFREU	Charter of Fundamental Rights of the European Union
CCTV	Closed Circuit Television
CJEU	Court of Justice of the European Union
DARPA	Defence Advanced Research Projects Agency
DPD	Data Protection Directive
DPIA	Data Protection Impact Assessment
EU	European Union
EASA	European Aviation Safety Agency
ERSG	European Remotely Piloted Aerial System Steering Group
E-VLOS	Extended Visual Line of Sight
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
FP	Framework Programme
GDPR	General Data Protection Regulation
HALE	High Altitude Long Endurance
ICAO	International Civil Aviation Organisation
INOUI	Innovative Operational UAS Integration
ILS	Instrument Landing Systems

IOT	Internet of Things
LASE	Low Altitude Short Endurance
LALE	Low Altitude Long Endurance
MALE	Medium Altitude Long Endurance
MTOW	Maximum Take-off Weight
NPA	Notice of Proposed Amendment
NCAAs	National Civil Aviation Authorities
PITs	Privacy Invasive Technologies
PET	Privacy Enhancing Technology
RPA	Remotely Piloted Aircraft
RPAS	Remotely Piloted Aircraft Systems
RLOS	Radio Line of Sight
STAR21	Strategic Aerospace Review for the 21st Century
SESAR	Single European Sky Air Traffic Management Research
US	United States of America
UA	Unmanned Aircraft
UAS	Unmanned Aircraft Systems
VLOS	Visual Line of Sight
VTOL	Vertical Take-Off and Landing

List of Figures

1. INTRODUCTION

Drones have been around for some time now, although only lately have they become popular. This thesis is about the visual privacy impact of civilian drones. Civilian, according to the Oxford English dictionary ‘is a person not in the armed services or the police force’. Therefore, this thesis refers to drones being used by private individuals (natural persons) or corporations. The use of drones for law enforcement purposes as such is left out of this study. To what use the drones are put to, in the civilian sphere, will solely depend on the intention and discretion of the entities using them.

On the one hand drones can be used for benign purposes, such as for recreation by private individuals, and on the other hand, if the intention is malicious, they can be used to malign individuals by gathering and disseminating sensitive visual data about them to the public. It can be used for commercial gain by corporate entities like flying clubs, or civilian surveillance.

Restrictions or limitations on the use of civilian drones, however, may result out of factors like, law, technology, social norms, morality etc. These several layers will shape the level of protection of privacy in every setting and which will ultimately influence how drones are finally being used in the private sphere.

One of the major concerns in allowing the civilian use of drones is the impact on visual privacy of individuals. This concern arises because of the attached cameras used for the navigation of the

drone. Image capturing, processing, and dissemination technologies have improved exponentially. Due to this and the aerial capability of drones, they can take continuous high-quality images from extraordinary vantage points, in residential as well as public areas, not possible otherwise without many restrictions. This thereby compromises the visual privacy of others in proximity to the drone. All this raises the question of, to what extent there should be legal control of civilian drone use.

The need for visual privacy, to a lesser or greater extent, is felt by everyone for certain activities. It helps is developing bonding and intimacy, personality, reputation, but at the same time, a certain level of visual exposure to the outside world is inevitable. An individual, usually and depending on cultural influences, does not cover his face while walking on a public street, for pragmatic reasons. So, the goal should be to hit the right balance between the civilian use of drones and safeguarding of an individual's visual privacy, which may be lost without his consent or knowledge.

As drones are tangible objects, incidents of trespassing into private properties may also arise from their use. However, there is an issue. As they are also flying aerial objects, it becomes a little difficult to determine a trespass.

Moreover, there is also the question of how these two violations (trespass and visual privacy violation), interact with each other. By such interaction, does it modify the nature of violation or determine the legality of the violation, needs to be analysed.

There are quite a few legislations in place to deal with such violations and so the question of, how do the different layers of solutions interact with each other, also arise. It also needs to be also analysed whether the existing solutions are sufficient to deal with visual privacy violations resulting out of civilian drone use.

1.1 Problem statement

Firstly, as past literatures on the topic identified the invasion of privacy as the main adverse social impact,[1] the goal of this study is to be more precise and elaborative about the kind of privacy at jeopardy in the use of civilian drones. In this regard, the concept of visual privacy is examined as well as the different variables that impact their social and legal understanding.

Secondly, as the subject of trespass had rarely been discussed in combination with visual privacy, it is also the goal of the study to see how this would, from a legal standpoint, influence visual privacy from the use of civilian drones. Apart from privacy, the study also briefly investigates other areas of impact on the human self, like, autonomy, control, behaviour, and psychology.

[1] See for example, John Villasenor, 'Observations from above: unmanned aircraft systems and privacy' (2013) 36 Harvard Journal of Law and Public Policy 457; M. Ryan Calo, The Drone as Privacy Catalyst' (2011) 64 Stanford Law Review Online 29; Timothy T. Takahashi, 'Drones and Privacy' (2012) XIV Columbia Science and Technology Law Review 72; Margot E. Kaminski, 'Drone Federalism: Civilian Drones and the Things They Carry' (2013) 4 California Law Review Circuit 57; Robert Molko, The Drones are Coming! Will the Fourth Amendment Stop their Threat to Our Privacy? (2013) 78 Brooklyn Law Review 1279; Jennifer Bentley, 'Policing the Police: Balancing the Right to Privacy Against the Beneficial Use of Drone Technology' (2018) 70 Hastings Law Journal 249.

Thirdly, the adequacy of the Charter of Fundamental Rights of the European Union (CFREU)[2] and the European Convention on Human Rights (ECHR)[3] as direct forms of remedies for the adverse impact on the right to visual privacy from the use of civilian drones is also investigated. Additionally, the adequacy of the General Data Protection Regulation (GDPR)[4] is thoroughly analysed as part of the solution for the unlawful processing of visual data by civilian drones.

Some of the sub-topics or sub-questions that are dealt with in this study are:

a. Is mere observation an invasion of visual privacy?
b. What is the status of transitional images (non-recorded visual information) processed by civilian drones?
c. How do the different layers of regulations interact with each other?

1.2 Methodology

A multidisciplinary approach is taken in this research. This kind of methodology was well suited to study the problem at hand. Observational method (observing a camera drone) was used, as well

[2] Charter of Fundamental Rights of the European Union (Charter, CFREU) [2012] OJ C326/391.
[3] Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights (ECHR), as amended).
[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

as referring to jurisdictions outside the European Union (EU), for guidance and illustration. A theoretical approach can also be seen where previous research on the topic has been given new wings. Therefore, this study uses a mix of methodology and disciplines. This helped to fill the gaps if simply the legal doctrinal method had been adopted.

Not only legal literature but also literature from other disciplines of study, like, sociology, anthropology, architecture, culture, and technology, were referred. There were two fundamental pillars, camera drones and society, upon which rested the investigative slab of privacy. Therefore, it would not have been possible to get the whole picture if a multidisciplinary approach had not been taken. References to other disciplines were particularly helpful in coming up with the factors that determine visual privacy.

The infringement of privacy was the focal point of previous studies on civilian drones and so this research was constructed upon those studies which helped in conceptualising the right kind of privacy that was at stake. A lengthy description and discussion added substance to the advanced theory. Observational study and references to other disciplines of study enormously assisted the theoretical construction.

Substantial time was spent on desk research on the topic of historical development of drone technology. A thorough legal study was done considering primary and secondary legal sources in the EU. Attendance at international conferences were undertaken to

know about the latest developments in drone technology and its regulation.

The focus of this study is limited to EU law and the ECHR and therefore, national jurisdictions within the EU, specifically, have not been discussed. For the sake of example or illustration only, some national cases, and legal developments from the jurisdiction of EU member States as well as some developments from the common law jurisdictions, have been considered. However, this is not a comparative law thesis.

1.3 Organisation

The study begins with chapter two on the brief history of drones. This chapter gives a historical account of the development of drones. In here, how the definition has evolved over the century and the classification of drones are discussed. Rules applicable to drones in the EU are discussed as well as the beneficial applications of drone technology in the civilian sphere.

Chapter three discusses the role of drones in the infringement of visual privacy of individuals. In this chapter, drones and visual privacy are fused together with the aim of providing us an account of the elements of violations. The violations are categorised into visual violation and physical violation. Visual violation is broken down into three sub elements and then weighed against the physical violation. This chapter concludes with the impact of the violations on individuals.

Chapter four gives us an account of what is visual privacy and describes its determinant factors. Then it goes on to classify visual information and the kinds of relationships that generate visual information. In the end, a discussion on the notion of reasonable expectation of privacy is undertaken, carefully adapting it to the problem of violation of the right to visual privacy from the use of civilian drones.

In chapter five, the fundamental dimensions of visual privacy are discussed, in other words, visual privacy within the fundamental rights framework in the EU. In here, the difficulty associated with the indirect application of fundamental rights and the system of multi-level protection are discussed.

Chapter six discusses the available solutions to address the problems of visual privacy infringements by drones. In this chapter, legislation, technology, and self-regulation are discussed as means to address violations. Under legislation, the GDPR is discussed in relation to visual data processing by drones. The limitations of the GDPR are also discussed alongside the solutions. Under technology, means available to protect visual privacy either after the processing of images or prior to the image processing is discussed.

Finally, chapter seven concludes the study with the findings on the issues that impact the protection of visual privacy from the use of civilian drones. Additionally, theoretical implications and the way forward are discussed.

2. BRIEF HISTORY OF DRONES

2.1. The evolution of drone technology

Mostly, technological developments have its origins within the military. That is the case of the internet which began within the military and scientific industrial complex 'Defence Advanced Research Projects Agency' (DARPA),[5] and so is the case with drones. It is much later that these inventions tend to find commercial use because of the exorbitant price and the risk in the failures in developing these technologies, which can initially be borne only by national governments.

During the many conflicts, even before the two world wars, there was an interest in weapons which could be unleashed from a distance without human intervention, for the trajectory of the flight. This culminated in experiments with missiles or rudimentary aircrafts stuffed with explosives. To call them aircrafts will be a misnomer as they were literally aerial bombs. One stark difference between a bomb and an aircraft is that while the latter is reusable the former is not. These explosives stuffed aircrafts were not reusable and were meant to crash. Missiles and bombs explode on impact while 'drones' function as reusable aircrafts. Drones used in the military may be equipped and capable of launching missiles, but they are not missiles or bombs in themselves. Nevertheless, this

[5] Barry M. Leiner and others, Brief History of the Internet, (Internet Society, 1997) < https://www.internetsociety.org/wp-content/uploads/2017/09/ISOC-History-of-the-Internet_1997.pdf> accessed 12 August 2020.

distinction between a drone and a missile/bomb, although pertinent, will have to be ignored for the initial stages in the historical development of drones.

There are many events in the past that have contributed to the present drone technology. Isolating one event from the rest and giving it the whole credibility cannot be justified. To truly understand its modern development, we must look at a length in time. Early humans hunted keeping in mind the size of the kill. To take down bigger predators they had to keep some distance, for, if they got too close it would have jeopardised their life. To overcome this difficulty, they had to modernise the way they used their stone tools. As is evidenced in hunting woolly mammoths, they used projectiles.[6] The sharp stone tools were fastened to a piece of wood and thrown from a distance. Like spears, arrows, and boomerangs, early modern pilotless flights were intended to release an explosive payload over a distance. Broadly, the timeline of the development of drones can be divided into the pre 1900 and the post 1900 era (both the time periods referring to the current era).

2.1.1. Evolution prior to 1900

An early evidence of pilotless flight was the attack on Venice by Austria in the year 1849.[7] The Austrians used balloons which were filled with explosives and were guided by the wind. The explosives

[6] W. Karl Hutchings, 'Finding the Paleoindian Spear Thrower: Quantitative Evidence for Mechanically-Assisted Propulsion of Lithic Armatures during the North American Paleoindian Period' (2015) 55 Journal of Archaeological Science 34.

[7] 'More about Balloons' (1849) Volume 4, Number 26 Scientific American, 205. < https://www.jstor.org/stable/26128900> accessed 12 August 2020

in the balloons were ignited by electromagnetism from a distance.[8] Prior to this, a balloon was used by the French against the Austrians, as a reconnaissance aircraft in the year 1794.[9] The French balloon 'L'Entreprenant' was, however, tethered and controlled by men on the ground.[10] This reduced the distance it could travel as it had to be within the Visual Line of Sight (VLOS) of the operators. However, the French Montgolfier brothers were the first to experiment with balloons in the year 1783.[11] Once in vogue, they were a familiar arsenal used in wars, like in the American civil wars.[12] Balloons, however, are not in the true sense an aircraft because they lack aerodynamics. Then, they even lacked the true capability of being remotely controlled, an integral feature of a drone. But the remote-control technology quickly came into existence.

Nikola Tesla's idea of 'Automaton' was a great step forward in controlling vehicles from a distance. It has been described in his autobiography 'My Inventions'. He started working on his wireless investigations in the year 1893, although, the idea was hatched

[8] ibid.
[9] John Hughes Wilson, On Intelligence: The History of Espionage and the Secret World (Constable 2016) chapter 18.
[10] 'L'Entreprenant, Reconnaissance Aircraft, 1794' (Science Photo Library) <www.sciencephoto.com/media/775991/view> accessed 9 July 2017.
[11] 'Joseph-Michel and Jacques-Étienne Montgolfier | French Aviators' (Encyclopaedia Britannica) <https://www.britannica.com/biography/Montgolfier-brothers> accessed 15 July 2017.
[12] Tom Crouch, 'On This Spot...' (National Air and Space Museum 2009) <https://airandspace.si.edu/stories/editorial/spot> accessed 15 July 2017.

earlier.[13]

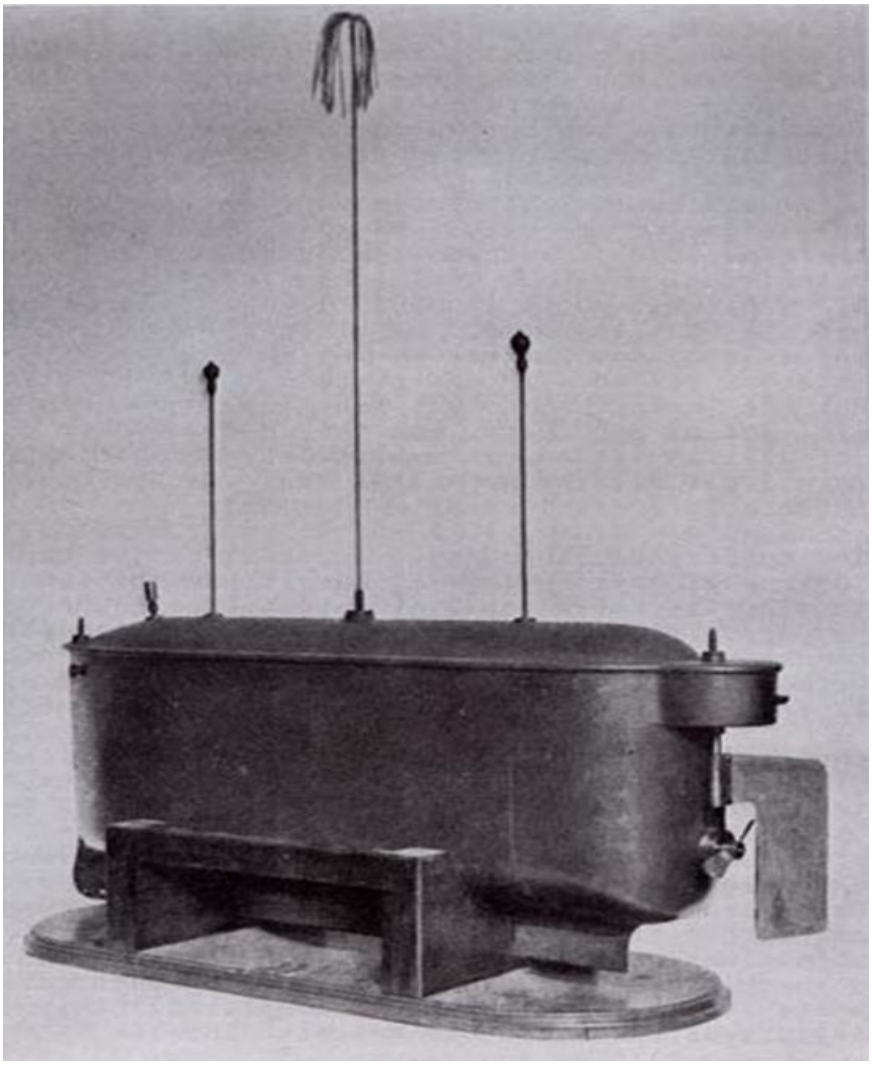

Figure1. Automatic boat by Nikola Tesla, Wikipedia.

He constructed several automatic mechanisms to be controlled from a distance. In 1896 he designed a machine capable of multitude of operations and in November 1898 a basic United States of America

[13] Nikola Tesla, My Inventions: The Autobiography of Nikola Tesla, Chapter 6, The Art of Telautomatics, <http://www.teslasautobiography.com/> accessed 10 July 2017.

(US) patent was granted to him.[14] He showed how his boats were controlled through the joint actions of several circuits without any interference.[15] The discharges from his high tension transmitter ionised the air so that even a small aerial would draw electricity from the air.[16] He demonstrated the ability to remotely control a vehicle through radio waves which are still used in modern drones.[17]

Another innovator in wireless control was Bradley Allen Fiske who with the help of Western Electric Company, submitted two applications for a patent. The first was entitled 'Apparatus for Controlling Mechanism of Moving Vessels and Vehicles' in September 1898 and the second in April 1900, entitled, 'Method of Controlling Mechanism of Moving Vessels and Vehicles'.[18] In October 1900 he was granted two US patents generally covering the wireless control of mechanisms.[19] Fiske's application was very similar to Tesla's in material and time.[20] Fiske applied two months after Tesla but two months before Tesla was granted a patent.[21]

[14] ibid.
[15] ibid.
[16] ibid.
[17] 'The Emergence of Commercial Drones' (IFLY Infographics) <www.purefunds.com/learn-about-purefunds-etfs/infographics/ifly/> accessed 10 July 2017.
[18] H.R. Everett, Unmanned Systems of World Wars I and II (MIT Press 2015) 191-193.
[19] ibid.
[20] ibid.
[21] ibid.

2.1.2. Evolution post 1900

Post 1900, the opportunity to continue developments in drones came in the form of the two world wars. Elmer Ambrose Sperry designed a small gyro stabilizer for an airplane.[22] In 1913, he advanced on the concept when he devised a gyro unit where electrical contacts from this unit worked the clutches of servo motors, which in turn worked the ailerons and elevators of the airplane, as would be done by a human pilot.[23] In 1914, a test flight of the automatic plane was piloted by his son Lawrence Sperry.[24] During the first world war, Charles Kettering with the help of Sperry's gyroscope developed the Kettering Aerial Torpedo, used by the US army and which eventually developed into the Kettering Bug, having a successful test flight in the year 1918.[25] Around the same time the British were experimenting with a radio controlled pilotless airplane called the Ruston Procter Aerial Target in 1916.[26] They were used against the German Zeppelins.[27]

---

[22] J.C. Hunsaker, Biographical Memoir of Elmer Ambrose Sperry, 1860-1930 (National Academy of Sciences 1954) 233.
[23] ibid 235-236.
[24] ibid.
[25] 'Remote Piloted Aerial Vehicles: The Aerial Target and Aerial Torpedo in the USA' (Ctie.monash.edu, 2003) <http://www.ctie.monash.edu/hargrave/rpav_usa.html> accessed 11 July 2017; also see Anthony Finn and Steve Scheding, Developments and Challenges for Autonomous Unmanned Vehicles (Springer 2010) 8-9.
[26] ibid.
[27] Nikola Budanovic, 'The Early Days of Drones - Unmanned Aircraft from World War One and World War Two' (War History Online 2017) <www.warhistoryonline.com/military-vehicle-news/short-history-drones-part-1.html> accessed 11 July 2017.

After the first world war, while the US was laying the ground work for drones, the British Royal Navy conducted tests of aerial torpedo designs, such as the RAE Larynx, in 1927.[28] In 1935, radio controlled pilotless aircrafts used as target practise by the British was the DH.82B Queen Bee.[29] It was derived from the De Havilland Tiger Moth biplane trainer which was adapted to new radio technology.[30] The predecessor to the Queen Bee was the simple radio controlled aircraft known as the Fairey Queen.[31] It is suggested that the term drone as referring to pilotless aircrafts was derived from the name Queen Bee, as a drone in the bee kingdom refers to a male bee.[32] At the outbreak of the second world war, Reginald Denny's Radioplane Company, offered target drones to the US military.[33] His first model was the Radio Plane-1 (RP-1) while his most famous and the first mass produced model was called the OQ-2 which later evolved into the OQ-19.[34] During the late 1930's the US navy developed the Curtis N2C-2 target drone.[35]

---

[28] ibid Finn and Scheding 9.

[29] Robin Braithwaite, 'The Queen of Bees' (Lightaircraftassociation.co.uk 2012) <www.lightaircraftassociation.co.uk/2012/Magazine/June/QueenBee.pdf> accessed 15 July 2017; also see 'History of Unmanned Aerial Vehicles' (En.wikipedia.org) <https://en.wikipedia.org/wiki/History_of_unmanned_aerial_vehicles> accessed 15 July 2017.

[30] ibid.

[31] ibid.

[32] ibid.

[33] Laurence R. Newcome, Unmanned Aviation: A Brief History of Unmanned Aerial Vehicles (American Institute of Aeronautics and Astronautics Inc. 2004) 57.

[34] 'Radioplane OQ-2' (En.wikipedia.org) <https://en.wikipedia.org/wiki/Radioplane_OQ-2> accessed 17 July 2017; also see Newcome 58.

[35] Richard K. Barnhart and others, Introduction to Unmanned Aircraft Systems (CRC Press 2012) 5.

With the experience in developing the N2C-2, the US Navy directed its efforts in 1940 towards the development of the TDN-1 assault drone.[36] With the development of the pulsejet engines, the German's produced the V-1 flying bomb, a cruise missile type unmanned aircraft, which represented the height of guided missile technology during its time.[37]

Figure 2. A Radioplane OQ-3 and its launcher, Wikipedia.

[36] ibid 7.
[37] ibid 8-9.

The true inventor, however, of a radio-controlled unmanned aircraft that could fly Beyond the Visual Line of Sight (BVLOS) of the operator was Edward M. Sorensen.[38] His invention was the first to let an individual know from a ground terminal what the airplane was doing, such as, climbing, altitude, direction, RPM, and other instrumentation.[39] Radio controlled aircrafts prior to this were very limited in their operation.[40]

Thus, the most significant innovations which assisted in the development of modern civilian drones were gyro stabilisation, radio control, and automation.

2.1.2.1. Evolution post the two world wars

Post the two world wars, the interest in developing drones continued as there were many events that justified such a course. Straight after the second world war, there was the cold war. There was also the Vietnam war, the war in Iraq, the Afghanistan war, and the war against terrorism in which drones played a major role in reconnaissance activities. In this phase one noticeable observation is that the US was always a party to the various conflicts. So, the cold war was between the US and the USSR, the US was at war in Vietnam, the US was the main opponent in the Iraq war as well as the war in Afghanistan and the war on terrorism was fought by the US with other countries as allies.

[38] Ron Bartsch and others, Drones in Society: Exploring the Strange New World of Unmanned Aircraft (Routledge 2017) 26.
[39] ibid.
[40] ibid.

Due to the role played by the US after the second world war, which was supposedly that of maintaining peace and security, most of the developments and innovations in drone technology came from that part of the world. It is only later that the interest and development in drones proliferated to other parts of the world, like Israel, continental Europe, Russia, and China which is the leader in consumer drones today.

Reginald Denny's Radioplane company survived the second world war and its RP-4 model evolved into the RP-71.[41] It had a camera, was controlled by an operator on the ground and could even fly BVLOS.[42] Some of the major developments in drone technology post world war two happened in the areas of sensors, datalinks, photo transmission systems, power source and onboard electronics.[43] Mini and micro drones were developed and their take-off and landing styles were experimented with, like the vertical take-off and landing (VTOL) systems for the US navy.[44]

A few of the popular drones in this period are the Lightning Bug used during the Vietnam war, the Predator and Global Hawk drones used during the Afghanistan war, the Pioneer and Hunter drones used during the Iraq war, and the small hand launched Raven drones also used during the Iraq war.[45] It is to be noted that all of the developments and innovations that took place were within the

[41] John David Blom, Unmanned Aerial Systems: A Historical Perspective (CSI Press 2010) 50.
[42] ibid.
[43] ibid 71.
[44] ibid.
[45] ibid.

military sphere and it is only recently that commercial and civilian applications of drone technology came into vogue.

Figure 3. A Global Hawk drone (used by the military as well as the scientific community), Wikipedia.

2.1.3. The era of civilian drones and its role in privacy violations

The civilian drone technology initially came from the military. But as consumer demands for drones increased, civilian drone research became independent of research for defence and military purposes.

In fact, recent consumer drones owe little to military systems.[46] They owe their existence to the early radio-controlled aircrafts used for recreational purposes and smartphones.[47] Consumer drone is a piece of electronic gadget, like any other. It is not intimidating like an 'unmanned combat aerial vehicle' that drops bombs. Consumer drones are powered by lithium polymer batteries, the ones used in smartphones and laptops.[48] This makes them very quiet while buzzing around. They have electrical motors, micro controller chips and can even be manoeuvred by an app in a smartphone connected through wireless fidelity (WIFI).[49] Micro controllers and the quick pace at which it is getting better has allowed for a new style of drones, that of the multirotor systems, like a quadcopter.[50]

Figure 4. A DJI Phantom drone, Wikipedia.

[46] 'Taking Flight: Civilian Drones' Technology Quarterly (The Economist 2017) < https://shop.economist.com/products/technology-quarterly-civilian-drones> accessed 25 August 2020.
[47] ibid.
[48] ibid.
[49] ibid.
[50] ibid.

The year 2010 can be regarded as the beginning of the civilian drone era with the launch of the 'Parrot AR' drone by the French company Parrot.[51] It had a quadcopter design and controlled by a smartphone.[52] This was a revolutionary moment for the civilian drone industry which attracted new players during this time. There were vast opportunities which remained largely untapped. In 2013 DJI, a Chinese company launched its first camera drone 'Phantom'.[53] The popularity of the Phantom drones cemented DJI's dominance in the consumer drone industry. Towards the end of 2013, Amazon made known its plans to use drones for parcel delivery.[54] In July 2020 NASA launched a helicopter design drone to Mars.[55] With fierce competition in the consumer drone market, drones are getting cheaper, smaller, better, and more reliable.

Drone as a technology without its paraphernalia (camera and other sensory equipment), is a thing of amusement. It has no connections with privacy whatsoever. This reasoning is in line with Article 29 Working Party's opinion on privacy issues relating to the utilisation of drones.[56] This is because visual and other sensors mounted on a drone are Privacy Invasive Technologies (PITs) that have a negative

[51] David Pierce, The Wired Guide to Drones, 2018, <https://www.wired.com/story/guide-drones/> accessed 4 August 2020.
[52] ibid.
[53] ibid.
[54] David Pierce, Delivery Drones are Coming, 2013, <https://www.theverge.com/2013/12/1/5164340/delivery-drones-are-coming-jeff-bezos-previews-half-hour-shipping> accessed 4 August 2020.
[55] Information available at <https://mars.nasa.gov/technology/helicopter/> accessed 4 August 2020.
[56] Article 29 Data Protection Working Party, 'Opinion 01/2015 on Privacy and Data Protection issues relating to the Utilisation of Drones' 01673/15/EN, WP 231 (2015).

impact on privacy. A drone is neither a PIT nor a Privacy Enhancing Technology (PET). It is a passive technology when it comes to privacy infringements. But it does aid the PITs significantly, almost altering their nature. However, we will refer to the PITs (visual sensors) and drones as a single technology and not as separate PITs.

2.2. Evolution of the definition

According to the International Civil Aviation Organisation (ICAO),[57] Circular 328-AN/190 of 2011, Unmanned Aircraft (UA) is defined as 'an aircraft which is intended to operate with no pilot on board.' This definition is reflected in Annex 7 to the Convention on International Civil Aviation.[58] Again, according to the ICAO Circular 328-AN/190, together with its associated elements UA is termed as Unmanned Aircraft Systems (UAS). It is an umbrella term which encompasses Autonomous Aircrafts (AA) and Remotely Piloted Aircrafts (RPA).

According to the ICAO 'Manual on Remotely Piloted Aircraft Systems',[59] an RPA is defined as 'an unmanned aircraft which is piloted from a remote pilot station' and 'together with its remote pilot station(s), the required command and control links and any

[57] The ICAO is a United Nation specialized agency, established by States in 1944 to manage the administration and governance of the Convention on International Civil Aviation (Chicago Convention).
[58] Convention on International Civil Aviation, as amended (signed 7 December 1944 at Chicago, entered into force 4 April 1947).
[59] ICAO Doc 10019-AN/507 of 2015.

other components as specified in the type design, it is termed as Remotely Piloted Aircraft Systems (RPAS).'[60] On the other hand, according to the same manual, an AA is defined as 'an unmanned aircraft that does not allow pilot intervention in the management of the flight.'[61] This definition of an AA, however, has no official status within the ICAO, meaning that it is not a standardised definition.[62] Thus, the difference between an AA and an RPA is the intervention of a remote pilot.

In the European Union (EU), initially, the official terminology in use was an RPA and RPAS for civilian drones and its control systems, respectively.[63] But now, there is a shift in terminology from RPA and RPAS towards UA and UAS in the new EU legislations[64] governing drones. This is because UA and UAS is a broader terminology when compared to that of an RPA and RPAS. Autonomous drones will not fit within the RPAS terminology as they do not mean remotely piloted but will fit within the UAS

[60] ibid.
[61] ibid.
[62] ibid.
[63] ERSG, 'Roadmap for the integration of Civil Remotely-Piloted Aircraft Systems into the European Aviation System: Final report from the European RPAS Steering Group' June 2013.
[64] Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 [2018] OJ L212/1 (Basic Regulation); Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems [2019] OJ L152/1; and Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft [2019] OJ L152/45.

terminology. According to Article 3 (30) of Regulation (EU) 2018/1139 on common rules in the field of civil aviation (new basic law), UA ‘means any aircraft operating autonomously or piloted remotely without a pilot on board.’

These definitions have come a long way since unmanned aircrafts roamed the skies. They have been known by so many names over the decades that one will be perplexed. They have been known as Aerial Torpedoes, Pilotless Airplanes, Automatic Airplanes, Radio Controlled Aerial Targets, Remotely Piloted Vehicles, Unmanned Aircrafts, Automatically Piloted Vehicles, Unmanned Aerial Vehicles, Remotely Operated Aircrafts, Autonomous Aircrafts, Micro UAVs, Model Aircrafts, Unmanned Combat Aerial Vehicles, but somehow the name ‘DRONE’ lingers on.

It is this term that has caught the imagination of the public and to do justice to the popularity of the term it has been used in the entirety of this text. There may be instances where other terms for drones have been used, like an RPA, but that is only for accuracy purposes while referring to a legislation or terminology in a region or setting. Where a specific terminology is not the essence, the generic term drone has been used, meaning here, a civilian drone. Used as a Noun, the Oxford English dictionary defines a drone as ‘a remote-controlled pilotless aircraft or missile.’ However, we will not be referring to drones as missiles. The Cambridge English dictionary, more in line with popular thinking and to which definition we will adhere to, defines it as ‘a type of aircraft that does not have a pilot but is controlled by someone on the ground.’

An analysis of the definitions by the two leading English dictionaries reveals that they are not relevant today. This is because now we know that drones are not missiles and that it need not be controlled by someone on the ground. Drones can function near autonomously. There is also a broader meaning of the term drone, and it includes any kind of a vehicle that can function remotely, it need not necessarily be something that flies. So, there can be an underwater drone and even drones operating on land, but they are outside the realm of this paper.

2.3. Civilian drone classification

According to ICAO Circular 328-AN/190, UA is an 'aircraft' and so like other aircrafts drones can be classified into several categories and subcategories.

2.3.1. According to the wing type

To begin with, drones can either be fixed winged, rotary winged or hybrid. Fixed winged drones resemble an airplane while rotary winged drones resemble a helicopter. A rotary winged drone can have a multitude of rotors and blades and the number of rotors determines its name. If it has two rotors it is called a duo-copter, a tri-copter has three rotors, a quadcopter has four rotors, a hexa-copter has six rotors, and an octocopter has eight rotors and so on.

Both fixed winged and rotary winged drones have their own advantages and disadvantages. While fixed winged drones can

cover more distances, rotary winged drones can hover. This makes the rotary winged drone ideal for photography. Consumer drones are mostly rotary winged.

Figure 5. A drone with a hexa-copter design at the Amsterdam Drone Week (ADW) 2019.

A hybrid drone is neither fixed winged nor rotary winged. They are less common and fly by mimicking the motions of birds and insects. Their size corresponds to the birds or insects they mimic. They are called ornithopters. Their evolutionary history is different from the history of development of pilotless aircrafts and coincides with Leonardo da Vinci's drawings of a devise mimicking that of bird

flight.[65] There were earlier attempts around the 10th century A.D. to jump off towers strapped to a pair of wings made from feathers.[66] But where drones were pilotless, early ornithopters were manned. However, unmanned ornithopters evolutionary branch has now merged with that of modern drones. According to the ICAO definition, an ornithopter is 'a heavier than air aircraft supported in flight chiefly by the reactions of the air on planes to which a flapping motion is imparted'.[67]

2.3.2. According to the take-off and landing style

Drones can take off and land vertically or conventionally. VTOL mimics a helicopter and conventional take-off and landing (CTOL) mimics an airplane. VTOL is the norm with rotary winged drones and CTOL is the norm with fixed winged drones. The take-off and landing could either be human controlled or autonomous. Rotary winged drones are more suitable for autonomous take-off and landing when compared to fixed winged drones because they can take-off and land from the same point. Manned aircrafts use Instrument Landing Systems (ILS), but they are expensive to be used on a drone. Therefore, drones rely on sensor technologies which could be radar based or laser based.

[65] Benjamin J. Goodheart, 'Tracing the History of the Ornithopter: Past, Present and Future' (2011) 21 Journal of Aviation/Aerospace Education & Research, 31.
[66] ibid.
[67] See annex 7 to the Convention on International Civil Aviation.

Figure 6. A drone with a helicopter design at the ADW 2019.

2.3.3. According to endurance capabilities

Based on endurance capabilities, drones can be classified into Low Altitude Short Endurance (LASE), Low Altitude Long Endurance (LALE), Medium Altitude Long Endurance (MALE) and High-Altitude Long Endurance (HALE).[68] LASE and LALE drones are usually small sized and are optimised for launch by catapult systems or by hand.[69] MALE drones have strategic roles in the military but are also increasingly being used for civilian purposes by the

[68] Adam C. Watts, Vincent G. Ambrosia and Everett A. Hinkley, Unmanned Aircraft Systems in Remote Sensing and Scientific Research: Classification and Considerations of Use (2012) 4 MDPI Journal Remote Sensing 1671.
[69] ibid, see Raven drones used by the US military.

scientific community to assess environmental conditions and other scientific observations.[70]

Figure 7. A fixed wing drone at the ADW 2019.

They fly at altitudes common to manned aircrafts.[71] HALE drones are the largest and they are also used by the scientific community for large scientific studies.[72] The origins of this endurance-based classification can be traced back to the US military when drones

[70] ibid.
[71] ibid.
[72] ibid.

were developed based on the requirements of the different wings of the army, that is, the infantry, the navy, and the air force.[73]

2.3.4. According to the degree of autonomy

According to autonomy in flight, drones can be divided into autonomous and remotely piloted. Due to the advancements in artificial intelligence and other technologies, like hardware, software and microchip, drones are slowly getting rid of human intervention.

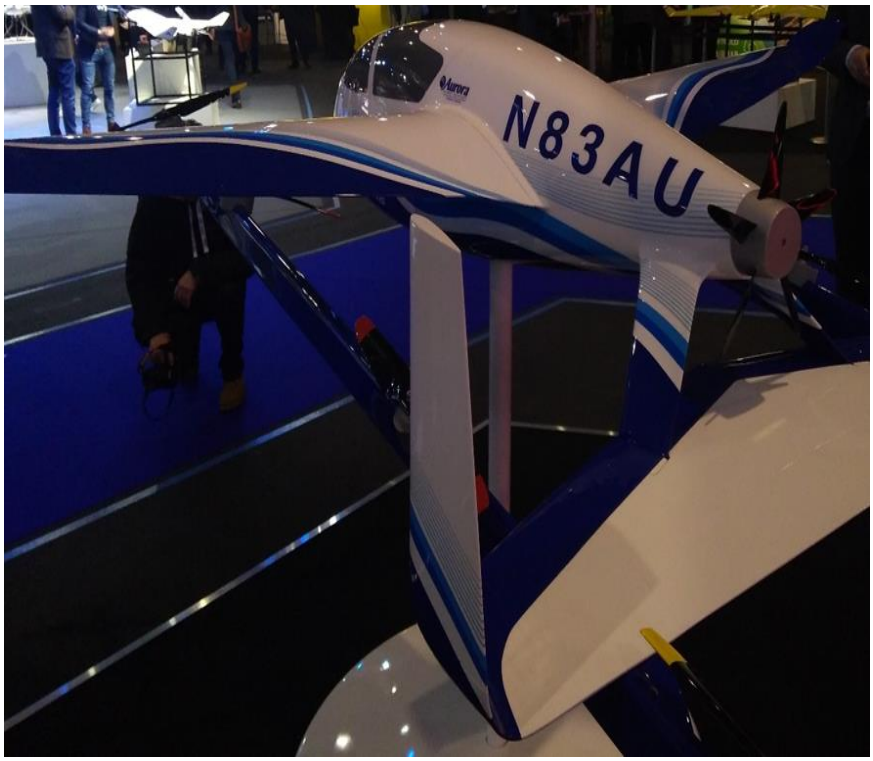

Figure 8. A drone by Aurora Flight Sciences which specialises in autonomous systems at the ADW 2019.

[73] John David Blom, Unmanned Aerial Systems: A Historical Perspective (CSI Press 2010).

This reflects in the ICAO definition for autonomous drones, which is, a drone that does not allow pilot intervention in the management of the flight.[74] But they still need human intervention to at least pre-programme their flight path. The degree of autonomy, therefore, has not reached a level where they could be called fully autonomous. Autonomous signifies full independence, free from total human control including pre-programming the flight path. Therefore, the correct term for these drones should be automated drones or semi-autonomous drones. The US Department of Defence is experimenting with 'Perdix' drone which has a high degree of autonomy but not total autonomy.[75] If a drone indeed achieved total autonomy, in other words learnt how to think for itself, it should be a matter of concern.

2.3.5. According to the risk-based approach

As per this concept drones are grouped under three categories, open, specific, and certified.[76] The open category is for very low risk drone operation, the specific category is for medium risk drone operation and the certified category is for high-risk drone operation.[77] The purpose of this classification is to have a uniform regulation across all weight class of drones irrespective of the EU member State of operation. This classification was long in the

[74] ICAO 'Manual on Remotely Piloted Aircraft Systems'.
[75] U.S. Department of Defence press release (Release No: NR-008-17) of 2017, <www.defense.gov/News/News-Releases/News-Release-View/Article/1044811/department-of-defense-announces-successful-micro-drone-demonstration/> accessed 30 October 2017.
[76] See Regulation (EU) 2018/1139; Commission Delegated Regulation (EU) 2019/945 and Commission Implementing Regulation (EU) 2019/947.
[77] ibid.

pipeline and had been confirmed in the European Aviation Safety Agency (EASA) Notice of Proposed Amendment (NPA) 2017-05.[78] The arbitrary 150 KG weight limit and mass-based classification of drones, where drones less than 150 KG were governed at the national level and drones equal to or heavier than 150 KG were governed at the EU level according to the now repealed Regulation (EC) 216/2008,[79] has been done away with. Now all drones, irrespective of their weight, are governed at the EU level, depending on the degree of risk of their operation.

2.3.6. According to the type of use

Drones can also be classified into UA used for professional purposes, Model Aircraft and Toy. Model Aircraft is defined as a non-human carrying aircraft capable of sustained flight in the atmosphere and exclusively used for recreational, sport or competition activity (regardless of mass, authorised operations, and on-board sensors).[80] The difference between a Model Aircraft and an RPA according to EASA NPA 2014-09, is its use.[81] RPA are

[78] NPA 2017-05, 'Introduction of a regulatory framework for the operation of drones — unmanned aircraft system operations in the open and specific category'<www.easa.europa.eu/document-library/notices-of-proposed-amendment/npa-2017-05> accessed on 24 July 2017.
[79] See annex ll to Regulation (EC) No 216/2008 of the European Parliament and of the Council of 20 February 2008 on common rules in the field of civil aviation and establishing a European Aviation Safety Agency and repealing Council Directive 91/670/EEC, Regulation (EC) No 1592/2002 and Directive 2004/36/EC [2008] OJ L79/1.
[80] ERSG Roadmap of June 2013; also see recital 34 of Regulation (EU) 2018/1139.
[81] NPA 2014-09, 'Transposition of Amendment 43 to Annex 2 to the Chicago Convention on remotely piloted aircraft systems (RPAS) into common rules of the air' <https://www.easa.europa.eu/sites/default/files/dfu/NPA%202014-09.pdf> accessed 22 November 2020.

those that are used for professional purposes (commercial, non-commercial, corporate, aerial work) unlike model aircrafts. Toys are governed by Directive 2009/48/EC,[82] but now also by the Commission Delegated Regulation governing drones.[83]

Figure 9. A delivery drone by Antwork Robotics at the ADW 2019.

For the purposes of classification according to the type of use, it is important to bear in mind, that the new EU Regulations governing drones, make no differentiation between a drone used for private

[82] Directive 2009/48/EC of the European Parliament and of the Council of 18 June 2009 on the Safety of Toys [2009] OJ L170/1.
[83] Commission Delegated Regulation (EU) 2019/945.

purposes or commercial purposes.[84] But the terminology 'model aircraft' has been retained in reference to model aircraft clubs,[85] despite no differentiation being made between private and commercial use.

2.3.7. According to the flight profiles

According to the flight profiles of drones, it can be categorised as low altitude operations that is to say at an altitude of below 150 metres or 500 feet from the ground and high altitude operations above 150 metres or 500 feet from the ground.[86] In low altitude operations three scenarios are mentioned, where the drone is within the VLOS of the operator, where the drone is within the Extended VLOS (E-VLOS) of the operator (in a situation when the operator is supported by an observer/s) and BVLOS operation where the drone is supported by additional technology.[87] In operations at an altitude above 150 metres or 500 feet from the ground two scenarios are mentioned, where the drone is within the Radio Line of Sight (RLOS) of the operator and where the drone is Beyond the Radio Line of Sight (BRLOS) of the operator (in a situation when it is supported via satellites).[88]

The new Commission Delegated Regulation and the Commission Implementing Regulation, governing drones, has reduced the

[84] Regulation (EU) 2018/1139; Commission Delegated Regulation (EU) 2019/945; Commission Implementing Regulation (EU) 2019/947.
[85] ibid.
[86] ERSG Roadmap of June 2013.
[87] ibid.
[88] ibid.

threshold from 150 metres to 120 metres for low-risk drone operations.[89]

Figure 10. A Boeing hexa-copter at the ADW 2019.

For high-risk drone operations, the height will depend on individual authorisations.[90]

[89] Commission Delegated Regulation (EU) 2019/945; Commission Implementing Regulation (EU) 2019/947.
[90] ibid.

2.3.8. According to the weight

Before the new basic law, at the national level of the EU member States, drones were grouped into different weight categories, a legacy of the now repealed Regulation (EC) 216/2008 (generally 20-25 KG being the threshold), and the type of activity. For example, France had three classified activity; the first activity was for leisure and competition purposes, the second activity was for experimental and testing purposes and the third was for particular activity that does not fit into the first and second activity.[91] Furthermore, drones in France were subdivided into two categories; Category 1 envisaged drones which weighed no more than 25 KG and any drone which did not fall within Category 1 fell under Category 2.[92] Additionally, there was a category of not more than 2 KG for model aircrafts used for leisure and competition purposes if it was used within a maximum horizontal distance of 200 metres from the remote pilot and flying at a maximum height of 50 metres.[93] In Spain, drones were categorised as follows, the first with a Maximum Take-off Weight (MTOW) of more than 25KG, the second with a MTOW of less than 25KG and third with a MTOW of less than or equal to 2 KG.[94] These classifications and

[91] Arrêté du 17 décembre 2015 relatif à la conception des aéronefs civils qui circulent sans personne à bord, aux conditions de leur emploi et aux capacités requises des personnes qui les utilisent.
[92] ibid.
[93] ibid.
[94] Real Decreto 1036/2017, de 15 de diciembre, por el que se regula la utilización civil de las aeronaves pilotadas por control remoto, y se modifican el Real Decreto 552/2014, de 27 de junio, por el que se desarrolla el Reglamento del aire y disposiciones operativas comunes para los servicios y procedimientos de

categorisations, although differing from one member State of the EU to another, helped in regulating the authorisation to fly drones. Lighter drones needed fewer authorisations than heavier drones.

But now, the member States of the EU abide by Regulation (EU) 2019/947 on the rules and procedures governing drones, which applied from the 1st of July 2020. From then, the new EU rules have replaced the individual national rules.

2.4. The European Union and drones

There is tremendous backing by the EU of the civilian drone industry which can be gauged from their emergent drone policy. There have been so many roadmaps and projects to integrate drones in the civilian airspace, under the 'Framework Programmes' (FP), that it is hard to follow every detail of it. However, an effort has been made here to chalk out chronologically, some important ones.

2.4.1. Former norms

Drones emerged in the EU policy dialogue in the year 2002 with the 'Strategic Aerospace Review for the 21st Century (STAR 21)'.[95] In the published document it is expected that Europe should become competitive in developing drones and its critical infrastructures for

navegación aérea y el Real Decreto 57/2002, de 18 de enero, por el que se aprueba el Reglamento de Circulación Aérea.

[95] Strategic Aerospace Review for the 21st century (STAR21): Creating a coherent market and policy framework for a vital European industry (European Commission Enterprise Publications 2002) <http://cordis.europa.eu/pub/era/docs/report_star21_en.pdf> assessed 3 August 2017.

defence purposes lest it be left behind and dominated by the US.[96] The document also sought to establish a masterplan for a Single European Sky[97] (which was later launched in the year 2004 as the Single European Sky Air Traffic Management Research (SESAR))[98] and a fully empowered European Aviation Safety Agency (EASA) to replace the Joint Aviation Authorities (consisting of National Civil Aviation Authorities (NCAAs) of the member States of the EU).[99]

There have been many individual research projects undertaken by the EU on drones and its infrastructures from the 5th FP onwards and continuing under the current 8th FP (Horizon 2020). While some relate to security and safety, others relate to border control. During the 5th FP (1998-2002), a few of the projects undertaken to advance the utilisation of drones in the civilian sphere were, 'UAV-NET' which established a thematic network on drones and 'CAPECON' which studied the economic effectiveness of potential configuration solutions relating to High and Medium Altitude Long Endurance missions and Rotary drones.[100]

---

[96] ibid STAR21, 30.
[97] ibid STAR 21, 25.
[98] 'SESAR Joint Undertaking | History' (Sesarju.eu) <http://www.sesarju.eu/discover-sesar/history> accessed 3 August 2017.
[99] ibid STAR21, 26.
[100] 'Civilian UAV Thematic Network: Technologies, Applications, Certification' | Projects | FP5-GROWTH | CORDIS | European Commission' (CORDIS | European Commission) <https://cordis.europa.eu/project/rcn/61170_en.html>; and 'Civil UAV Application and Economic Effectiveness of Potential Configuration Solutions' | Projects | FP5-GROWTH | CORDIS | European Commission' (CORDIS | European Commission) <https://cordis.europa.eu/project/rcn/63495_en.html> accessed 3 August 2017.

In 2005, 'European Civil Unmanned Air Vehicle Road Map' under the title '25 Nations for an Aerospace Breakthrough' was launched. The roadmap consisted of an overview, an action plan and a strategic research agenda and was led by Israel Aerospace Industries.[101] In 2007 a 'Study Analysing the Current Activities in the Field of UAV' was undertaken by Frost & Sullivan and funded by the European Commission Enterprise and Industry Directorate General.[102]

A 'Regulatory Roadmap for UAS Integration in the Air Traffic Management' was undertaken under the 6th FP (2002-2006). It was called 'Innovative Operational UAS Integration' (INOUI) and meant to supplement the SESAR programme.[103] In 2008, Regulation (EC) No 216/2008, on common rules in the field of civil aviation, brought drones heavier than 150 kgs, within the ambit of EU governance.[104] At the time, this was the basic law governing

[101] '25 Nations for an Aerospace Breakthrough: European Civil Unmanned Air Vehicle Roadmap' (2005) <https://www.uvsr.org/Documentatie%20UVS/Publicatii-internationale/EuropeanCivilUnmannedAirVehicleRoadmap1.pdf> assessed 3 August 2017.

[102] Frost and Sullivan for the European Commission, 'Study Analysing the Current Activities in the Field of UAV' ENTR/2007/065 (2007) <https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/security/pdf/uav_study_element_2_en.pdf> accessed 3 August 2017.

[103] 'Innovative Operational UAS Integration' (Transport-research.info) <http://www.transport-research.info/sites/default/files/project/documents/20130111_100721_43303_INOUI_Booklet.pdf> assessed 3 August 2017; also refer to the website <www.inoui.isdefe.es/INOUI/>.

[104] Regulation (EC) No 216/2008 of the European Parliament and of the Council of 20 February 2008 on common rules in the field of civil aviation and establishing a European Aviation Safety Agency and repealing Council Directive

drones in the EU. The governance of drones, equal to or lighter than 150 kgs were left to individual member States which resulted in disharmonious legislations across the EU landscape. Regulation 216/2008 also established the EASA.

During the period of the 7th FP (2007-2013) in September 2012, a formal Commission Communication, 'Towards a European Strategy for the Development of Civil Applications of RPAS' was published.[105] This led to the establishment of the 'European Remotely Piloted Aerial Systems Steering Group (ERSG)' which published its own Roadmap entitled 'Roadmap for the Integration of Civil Remotely Piloted Aircraft Systems into the European Aviation System' in June 2013.[106]

The June 2013 complete Roadmap consists of three Annexes including an Annex dealing with societal issues wherein it identified that invasion of privacy was a serious concern in allowing the civilian use of drones. Annex 3, which dealt with societal issues, took into consideration aerial surveillance by drones, however, most of the rhetoric focussed on data protection and failed to directly address visual privacy. The 2013 regulatory roadmap foresees till the year 2028 for the full integration of drones into the civilian airspace. Under the 7th FP in the year 2012, a master plan relative to

91/670/EEC, Regulation (EC) No 1592/2002 and Directive 2004/36/EC [2008] OJ L79/1 (repealed).

[105] Commission, 'Towards a European strategy for the development of civil applications of Remotely Piloted Aircraft Systems (RPAS)', SWD (2012) 259 final, 4 September 2012.

[106] ERSG Roadmap of June 2013.

the insertion of UAS in European airspace with a strong focus on small RPAS was launched and was called ULTRA.[107]

In 2015, the Riga declaration on drones was published, wherein, it was highlighted that drones need to be treated as a new type of aircraft with rules based on the risk of their operation and that EU wide rules needed to be developed.[108] Following the Riga declaration, the EASA was requested by the European Commission (EC) to develop a regulatory framework for drones in the EU.[109] EASA responded to the request by publishing a technical opinion entitled 'Introduction of a regulatory framework for the operation of unmanned aircraft' in December of 2015.[110] Also in December of 2015, a Commission Communication, 'An Aviation Strategy for Europe' was published.[111] In it the EC proposed a basic legal framework for drone operations in the EU in replacement of the

[107] 'Unmanned Aerial Systems in European Airspace | Projects | FP7-TRANSPORT | CORDIS | European Commission' (CORDIS | European Commission) <https://cordis.europa.eu/project/rcn/103989_en.html> accessed 4 August 2017.
[108] Claudia Stöcker and others, 'Review of the Current State of UAV Regulations' (2017) MDPI Journal 2017.
[109] Miguel Rosa and others, Spain–UK–Belgium Comparative Legal Framework: Civil Drones for Professional and Commercial Purposes. In: de Miguel Molina M., Santamarina Campos V. (eds) Ethics and Civil Drones, (Springer Briefs in Law 2018).
[110] EASA's Technical Opinion, Introduction of a regulatory framework for the operation of unmanned aircraft (2015) < https://www.easa.europa.eu/document-library/opinions/opinion-technical-nature> accessed 8 August 2020.
[111] Commission, 'An Aviation Strategy for Europe', SWD (2015) 261 final, 7 December 2015.

earlier Regulation (EC) No 216/2008 (on common rules in the field of civil aviation).[112]

The Riga declaration was followed by the Warsaw declaration in November 2016, wherein, the tremendous potential of the drone services market was recognised. This was followed by the EASA NPA 2017-05,[113] and finally the new basic law.

2.4.2. The current legal framework

Regulation (EU) 2018/1139 has replaced Regulation (EC) No 216/2008 as the new basic law governing drones. One of the major changes is that the weight-based classification of drones has been replaced by the risk-based approach. Recital 26 of the new basic law reflects the just previous statement:

> 'Since unmanned aircraft also operate within the airspace alongside manned aircraft, this Regulation should cover unmanned aircraft, regardless of their operating mass. Technologies for unmanned aircraft now make possible a wide range of operations and those operations should be subject to rules that are proportionate to the risk of the particular operation or type of operations.'

A degree of flexibility has however been provided to the EU member States to adjust the risk-based approach according to their local circumstances and based on the principle of proportionality.

[112] ibid.

[113] NPA 2017-05, 'Introduction of a regulatory framework for the operation of drones — unmanned aircraft system operations in the open and specific category'<www.easa.europa.eu/document-library/notices-of-proposed-amendment/npa-2017-05>

Another major change is that it is explicitly stated that compliance with the fundamental right to privacy and data protection is an aim of the new rules governing drones. In this regard, Recital 28 states that:

> ‘The rules regarding unmanned aircraft should contribute to achieving compliance with relevant rights guaranteed under Union law, and in particular the right to respect for private and family life, set out in Article 7 of the Charter of Fundamental Rights of the European Union, and with the right to protection of personal data, set out in Article 8 of that Charter…’

An explicit statement does increase the importance given to the right to privacy and data protection in the use of civilian drones. It should help in the overall adherence to the right to privacy because of the requirement that the remote pilot be well versed with the rules governing civilian drones.

Article 56 (7) of the new basic law, with regards to registration requirements, states:

> ‘Member States shall ensure that information about registration of unmanned aircraft and of operators of unmanned aircraft that are subject to a registration requirement […] is stored in digital, harmonised, interoperable national registration systems […].’

Thus, one of the measures to be adopted to safeguard privacy is the registration requirements for the UA and the operator of the UA.[114] Registration requirements will, supposedly, help in the identification of a drone with the remote pilot in case of violations of the right to privacy and other rights as well. But simply registration requirements will not be enough because a drone will need to be identifiable to the victim of a privacy violation, at the time of actual violation, for any utility of the registration requirements.

Article 56 (8) of the new basic law, with regards to flexibility to make rules, states:

> 'This Section shall be without prejudice to the possibility for Member States to lay down national rules to make subject to certain conditions the operations of unmanned aircraft for reasons falling outside the scope of this Regulation, including public security or protection of privacy and personal data in accordance with the Union law.'

Thus, EU member States, with regards to privacy and data protection, have the flexibility to make rules and take measures outside the scope of the new basic law governing drones.[115] Although this will be helpful in strengthening the protection of the right to privacy, as local differences present in the EU member States will be taken into consideration, like the density of the population, it will have its own drawbacks. The major drawback

[114] See also Recital 31 of Regulation (EU) 2018/1139.
[115] See also Recital 33 of Regulation (EU) 2018/1139.

will be the differences in the degree of protection of the right to privacy and data protection in the use of civilian drones. This will result in a multilevel protection system like the multilevel system of protection of fundamental rights in the EU member States, which may compromise harmonisation at the EU level.

The new basic law governing drones, the successor to Regulation (EC) No 216/2008, is an empowering legislation that lays down the broad policy of uniform aviation safety, certification, and operation requirements.[116] It prescribes the common rules for civil aviation in the EU. It empowers the EC to enact more detailed requirements for the use of civilian drones in the form of delegated and implementing regulations. The main provisions applicable to drones are contained in Article 55 to 58 of the new basic law. The essential requirements that need to be fulfilled with respect to the design, manufacture, maintenance, and the remote pilots of UAS are listed in Annex IX of the new basic law. Privacy by design and default, airworthiness, product integrity, knowledgeable and skilled remote pilots, are some of the essential requirements mentioned in Annex IX. Certification requirements for the UAS and the remote pilots and their registration in interoperable national registration systems, are outlined in Article 56.

Commission Delegated Regulation (EU) 2019/945 and the Commission Implementing Regulation (EU) 2019/947 have been adopted based on the new basic law in the field of civil aviation in

[116] Blanca Torrubia Chalmeta, 'Aeronaves civiles no tripuladas. Contexto y regulación', in Agustí Cerrillo and Miquel Peguera (eds.), Retos Jurídicos de la Inteligencia Artificial, (Thomson Reuters-Aranzadi, 2020) 255-268.

the EU. They contain the detailed rules applicable to the use of civilian drones. While the delegated regulation contains requirements for the design and manufacture of UAS, the implementing regulation lays down the rules for their operation.

Commission Delegated Regulation (EU) 2019/945:

The delegated regulation is mainly aimed at the open category of UAS operation. There are five classes in the open category (C0, C1, C2, C3 and C4) and all have varying requirements relating to the weight, power source, voltage, sound power level, geo awareness systems etc. The maximum height in the open category has been capped at 120 m. User manuals provided by the manufacturer and information notice published by the EASA is mandatory for each class of UAS. Toys are covered, as mentioned in Recital 5 of the delegated regulation, however, at the same time, UAS to be exclusively operated indoors are not covered according to Article 2 paragraph 4 of the delegated regulation. This can be confusing as toys, in most circumstances, will be the ones being used mainly indoors. The printing of CE and the class markings on the drones have been made mandatory. Manufacturers, importers, and distributors have an obligation to ensure that the drones comply with the EU rules and that the mark of the manufacturer or the importer and their contact details are printed on the drone or provided as a separate leaflet.

Despite all this, Recital 1 states that drones which pose the lowest risk should not be subject to classic aeronautical compliance procedures. Model aircrafts should also not be subjected to

disproportionate technical requirements. Concerning drones in the specific and certified categories, their design, manufacture, and maintenance, shall be certified by the competent authority if the dimension of the drone is 3 m or more and operated over assemblies of people or it is designed for transporting people and dangerous goods.

Commission Implementing Regulation (EU) 2019/947:

The Implementing regulation allows 3 categories of operation, that is, open, specific, and certified. It also states that the rules and procedures to be applicable to drones should depend on the amount of risk they pose. Thus, drones that pose the lowest risk should have the least number of rules applicable to them. Registration of drones is mandatory if on impact it can transfer to a human kinetic energy above 80 Joules or it presents a risk to the privacy or safety of individuals. Therefore, all drones with a camera will need to be registered at the national level in interoperable national registration systems.

Drone operation in the open category does not require operational authorisation whereas drone operation in the specific category requires operational authorisation. For drones in the certified category, the UAS, the operator and the remote pilot need a certificate for operation by the competent authority. There is a possibility that a drone in the open category may need an operational authorisation and a drone in the specific category may need certification. This may happen when the intended use of the drone is covered under the specific or certified category

respectively, for example, drones meant for specific categories while carrying dangerous goods may need to be certified.

Under the open category of operations, there are 3 subcategories (A1, A2, and A3). This subcategorization is based on operational limitations, requirements for remote pilots and technical requirements for drones. Subcategory A1 includes C0 and C1 class of drones and privately built drones having a MTOM of less than 250 g. Subcategory A2 includes C2 class of drones, and subcategory A3 includes C2, C3 and C4 class of drones and privately built drones having a MTOM of less than 25 kg. Thus, the sub-categorisations in the implementing regulation corresponds to the classes of drones in the delegated regulation.

In the open category, the remote pilot needs to be within the VLOS of the drone. Flying over assemblies of people (crowds) is prohibited in the open category of operations. In subcategory A1, flying over uninvolved persons (people who are not in a crowd) is allowed but is to be avoided. In subcategory A2 flying over uninvolved persons is not allowed and a safe horizontal distance of 30 metres needs to be maintained from the uninvolved persons. In subcategory A3, the drone operation should be conducted in an area where the remote pilot reasonably expects that no uninvolved persons will be endangered and at a safe horizontal distance of 150 metres from residential, commercial, industrial, and recreational areas.

The requirements for drones in the specific and certified categories will depend on the extent of permission given by the competent

authority in the operational authorisation or the certificate of operation, respectively. BVLOS operations are allowed in the specific and certified categories.

2.5. Applications

Drones can have manifold applications. It is difficult to give an exhaustive list here because research into future drone applications is an ongoing process. So, for example, there is ongoing research into the beneficial applications of drones in the health care sector, the agricultural sector, the construction sector, the information technology sector, the real estate sector and even the energy sector.[117] Drones are being used to transport emergency medical supplies, like blood/test samples, medicines, and personal protective equipment in the midst of the Corona virus pandemic.[118] They are also being used to inspect bridges and other infrastructures for damages.[119] In the agricultural sector, they are preferred over the traditional way of doing things as they have cost advantages. For example, prior to the induction of drones in agriculture, crop spraying was either done by hiring a labourer on the ground or a piloted aircraft which sprayed from the air. For large pieces of land,

[117] See, for example, research being carried out at Syddansk Universitet on health and energy drones among a few < https://www.sdu.dk/en/forskning/sduuascenter> accessed 15 August 2020.
[118] Harry Kretchmer, How Drones are Helping to Battle Covid-19 in Africa and Beyond < https://www.weforum.org/agenda/2020/05/medical-delivery-drones-coronavirus-africa-us/> accessed 15 August 2020.
[119] Marianne Harbo Frederiksen and others, Drones for Inspection of Infrastructure: Barriers, Opportunities and Successful Uses, (SDU Centre for Integrative Innovation Management 2019)

the second method was preferred. Drones do the same spraying from the air but even more efficiently at a fraction of the cost of hiring a piloted aircraft.[120] Due to their cost advantage the uses to which they are put to have increased. They not only spray but even monitor crops and analyse the soil.[121] In dangerous areas, where one will presume that a human life would perish, they are the heroes that do the dirty work. This holds no truer than in search and rescue operations.[122]

Now, due to the increasing use of drones in different sectors, they are sometimes called, corresponding to the sector that they are utilised in, as health drones, inspection drones, energy drones or even humanitarian drones.

Despite drones having so many beneficial applications they do pose a danger to human autonomy. Newton said that every action has an equal and an opposite reaction. In the context of this work, for every technology that the society adopts or permits its use, there are two consequences in the adoption of such a technology. On the one hand are the positive aspects and on the other are the negative aspects. Nuclear power plant is one such technology. The good aspect is that it provides electricity to millions of homes without the carbon

[120] Crop Dusting Drones – Making Work Safer and Easier for Farmers, < https://www.dw.com/en/crop-dusting-drones-making-work-safer-and-easier-for-farmers/a-50128698> accessed 15 August 2020.
[121] Use of Drones in Agriculture < https://wingtra.com/drone-mapping-applications/use-of-drones-in-agriculture/> accessed 15 August 2020.
[122] Sonia Waharte and Niki Trigoni, Supporting Search and Rescue Operations with UAVs (University of Oxford Computing Laboratory 2010) < https://www.researchgate.net/publication/228954615_Supporting_Search_and_Rescue_Operations_with_UAVs> accessed 15 August 2020.

emissions of fossil fuels. The negative aspect is that it destroys millions of homes due to the radiation that is leaked from the plant, in the event it is damaged. Drone technology is no exception to the rule, but the damage in this regard will be the invasion of an individual's visual privacy.

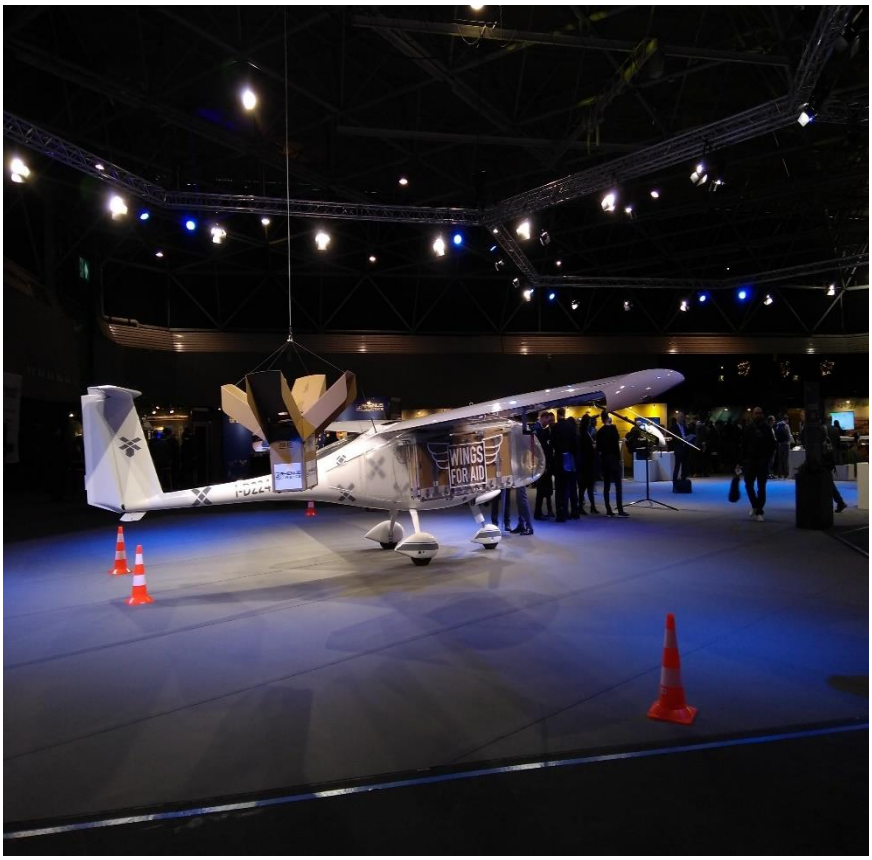

Figure 11. A Wings for Aid humanitarian drone at the ADW 2019.

There will be a few who will be cursing the utilisation of drones in the civilian commercial sector because drones will be taking away their jobs. Parcel delivery is one area where drones will make people redundant. The products that can be delivered by drones are

myriad, from food and medicines to documents. It is the perfect technology for companies like Amazon to increase the efficiency of their logistics services, meaning parcel delivery. Passenger drones are being experimented for releasing traffic congestions in the world's major cities.[123] How are we going to react to interactions that lack human emotions can only be determined in time. For instance, what will be the psychological impact on an individual who is being followed by a drone as opposed to a physical person. Will he be less anxious or more anxious being followed by a machine?

Thus, using drones for the above-mentioned applications has its own set of problems. The problems are not only restricted to privacy and psychological health but are broader in scope and includes lack of city planning for the use of civilian drones. Even if a viable city plan is outlined for the optimal utilisation of civilian drone technology, the cost to implement such a plan will be beyond the financial capacity of most state governments. Most commercial drone operations, however, will need to fly beyond the line of sight of the operator, which at present is mostly restricted, therefore, we still have time to put on our boots before there is an explosion of drones in our personal airspace.

Of all the negative outcomes of using civilian drones, privacy and data protection takes one of the prominent positions. There are other more dangerous outcomes, like drone accidents over crowds of

[123] Robin Kellermann, 'Drones for Parcel and Passenger Transportation: A Literature Review' (2020) 4 Transportation Research Interdisciplinary Perspectives (Elsevier).

people, which could result in an actual physical harm and not just psychological harm like a privacy invasion. Having said that, the focus of this paper is visual privacy invasion by civilian drones. The next chapter will discuss how drones invade our visual privacy and how does it impact us.

3. ELEMENTS OF PRIVACY INVASION

This chapter explores the topic of visual privacy invasion by civilian drones. Therefore, we take a visual approach to privacy. Here, the element of visual invasion is broken down into sub elements and analysed. The primary sub elements are observation, recording and publishing. In addition to visual invasion, this chapter also explores the topic of physical invasion by drones, wherein, the element of aerial trespass is analysed. Subsequently, the interplay between the two elements, that is, visual invasion and physical invasion, is analysed. Finally, this chapter ends with the impact of drone invasion on the human souls.

3.1. Scope of visual invasion

Drones are a channel for passing physical visual information to ground stations, from the airspace, for processing and distribution. What makes it even more interesting is the possibility of them being operated without anyone suspecting their presence. They are an extension of our human physical abilities, primarily an extension of the physical ability to see. The degree of extension is dependent on the on-board sensors and the endurance and size of the drone. For example, low quality visual sensors will get only hazy pictures, infrared sensors will get pictures in the dark, high endurance drones will increase the area that can be seen with greater heights and with

better battery capabilities drones can stay afloat observing for a longer period.

Whether in navigable airspace or private airspace, there are only three scenarios under which a visual invasion will fall. Either it is simply observing or simultaneously while observing there is a recording of the observation, and subsequently, the publication of the recording. However, visual invasion may also take place where a collection of pictures may be used for the purposes of inference, assessment and even decision making. But this latter type of visual invasion is only secondary to the primary invasion.

3.1.1. Observation

Observation is a necessary precondition to record. Not to forget, observation means more than an act of glance. Mere observation may seem to be a less serious interference than recording, nevertheless, it does reduce a person's autonomy. Observations can be of two kinds, where the person observed knows that he is being observed and where he does not know that he is being observed. For example, in the first case, where there is prior knowledge of the observation, a person will restrict himself from doing certain acts, like stealing. Even in the latter case, his autonomy is affected, although he has no knowledge about his observation. His secrecy is intruded upon and the one who knows his secrets will have the power to influence him, like in the case of online targeted advertisements.

But how would the European Court of Human Rights (ECtHR), decide a pure case of observation, that intrudes upon the right to

respect for private and family life without there being a record of the observation? *Pierre Herbecq and the Association Ligue des droits de l 'homme v Belgium*[124] is just such a case, where the European Commission on Human Rights examined, whether unrecorded video surveillance, where a person has no knowledge of the surveillance being carried out, amounts to an intrusion into a person's private life. The Commission noted that the information available to the person looking at the screen is the same if he were personally to go to the place and observe the visual information with the naked eye. The Commission found it not to be an intrusion into a person's private life, noting:

> 'In the present case the Commission notes that the photographic systems of which the applicant complains are likely to be used in public places or in premises lawfully occupied by the users of such systems in order to monitor those premises for security purposes. Given that nothing is recorded, it is difficult to see how the visual data obtained could be made available to the general public or used for purposes other than to keep a watch on places. The Commission also notes that the data available to a person looking at monitors is identical to that which he or she could have obtained by being on the spot in person (…) Therefore, all that can be observed is essentially, public behaviour. The applicant has also failed plausibly to demonstrate that

[124] Pierre Herbecq and the Association Ligue des droits de l 'homme v. Belgium, nos. 32200/96 and 32201/96, Commission decision of 14 January 1998 (on the admissibility of the joined applications).

private actions occurring in public could have been monitored in any way'.

The US courts have also held, where the property owner's premises were observed with the naked eye, from the air, for marijuana plantations, it did not infringe a person's right to privacy.[125]

The inference, if we are to follow the reasoning in the above case, is that surreptitious observation with the help of drones does not amount to an invasion of an individual's visual privacy as it is possible for the drone pilot to personally visit the spot where the drone is and observe with the naked eye what the drone observes. If the drone is in the airspace above the pilot's personal property or in the airspace above a public space, a right of action does not arise because it is not trespassing onto another's personal space. So, anything which is within the VLOS from one's private property or a public space is legally observable.

There are, however, certain conditions for an observation to be not actionable, according to the reasoning in the *Pierre Herbecq* case. The observation should not be recorded nor distributed to others to see. But there may be instances where the observation is recorded but not distributed and not recorded but distributed (a live broadcast).

Only for the purposes of furthering our discussion on the topic of 'observation', public events like a cricket match may be observed from outside of a stadium, atop a tall tree, which when climbed

[125] California v. Ciraolo, 476 US 207 (1986).

upon, lets an individual view the match. This sort of an action is an aberrant behaviour from a utilitarian perspective. The usual thing to do, if someone is interested in observing the match, will be to buy a ticket for a seat inside the stadium. If the interested individual does not have the money or all the tickets have been sold out, then she/he would resort to climbing a tree. It may go unnoticed if it is only a single person, but hypothetically, if everyone resorted to climbing a tree or other protruding objects of a similar length and observing the match from the outside of the stadium, then there will be consequences, as the stadium would be sparsely populated. That anomaly would be noticed easily as against a single person.

The organiser of the cricket match has property rights to the match. He decides who enters the stadium and who stays out, for example, in Spain, the right of admission to a premise is expressly regulated by law 'Real Decreto 2816/1982'.[126] So, for example, dress codes may be prescribed, and a person may be denied entry if he does not adhere to the dress code.

The intention of the organiser is to allow the observation of the match only from the inside of the stadium and not from anywhere else, not from the airspace above the stadium or from ground level observation from outside of the stadium. His intention is manifested by the wall that surrounds the stadium. But spectacle rights do not extend to say to the public, not to observe the match, if the public are observing it from a public space and if that event is observable

[126] Article 59. 1. e) of Real Decreto 2816/1982, de 27 de agosto, por el que se aprueba el Reglamento General de Policía de Espectáculos Públicos y Actividades Recreativas.

from that space. If the public are not trespassing onto the organiser's property, they are well protected to observe the match, whether by climbing a tree or using some other apparatus (binoculars) to observe, from a public space or their own private property.

While observing the match, if the information about whole of the match, for example, who are bowling, which are batting, the number of runs and other information relating to the match is conveyed to a crowd, which is standing below the observer, should be actionable, as it should amount to publication. However, in the EU, events of 'high interest to the public' can be used by broadcasters, from the exclusive broadcaster of the event, for short news reporting.[127]

Now, should the use of a technological devise, in the observation, change the equation from being not actionable to being actionable? The logical interpretation should be, it should not, if the observation is not being recorded or published, in consonance with the reasoning in the *Pierre Herbecq* case. But with the massive use of civilian drones even observation may turn problematic, for example, if only one person uses a drone to observe the match then that is not problematic but if hundreds of drones are used this becomes a major problem and legal intervention will be required.

Taking an example from the Australian jurisdiction, in the case of *Victoria Park Racing and Recreation Grounds Company Limited v*

[127] Asser Institute, Study on sports organisers' rights in the European Union (Publication office of the European Union, 2014); also see case C-283/11, Sky Österreich [2013] ECR I-nyr.

Taylor,[128] it was held that observing a race from an erected platform from outside the racecourse and relaying information about the race to a broadcasting company which in turn broadcasted it to the public, thereby, reducing the attendance at the racecourse, did not infringe any legal rights to the spectacle of the plaintiff.

The *Victoria Park Racing* case was decided when broadcasting technology was still in its nascent stage of development and if instead of a natural person observing the race from the erected platform, a video camera was mounted, it is uncertain how things would have unfolded. As McTiernan J. noted:

> 'It is not shown that the broadcasting interferes with the use and enjoyment of the land or the conduct of the race meetings or the comfort or enjoyment of any of the plaintiff's patrons. Indeed, it appears quite impossible that any such result would be caused by the action of Angles in standing on this platform aloof from the racecourse, observing the races and talking into a microphone or telephone. The principle upon which liability for acts in the nature of nuisance is founded is not to be restrained by the instances in which that liability has been found to exist. The list of acts which may give rise to an action on the case in the nature of nuisance is not closed against broadcasting. But to broadcast a lawful description of what is happening on premises cannot be an actionable nuisance at least unless

[128] Victoria Park Racing and Recreation Grounds Company Limited v Taylor, [1937] HCA 45.

it causes substantial interference with the use and enjoyment of the premises.'

In *Bathurst City Council v Saban,*[129] almost five decades after the *Victoria Park racing* case, it was held that recording an image and a video of a disorderly backyard of a homeowner's property, from a public street, did not amount to a nuisance because no trespass had been committed to the land or airspace above the property. The Australian legal system, which is based on the common law system, did not recognise a right to privacy so the outcome of the cases is not startling.

If we compare the *Pierre Herbecq* case with the *Victoria Park Racing* case, one obvious difference is the publication of the information (short news reporting and journalistic activities are exempt). In the former case, there was no publication, whereas, in the latter case, there was publication to the broadcasting company which in turn published it to the public. The Australian case was purely decided based on property rights while the European case was decided based on the fundamental right to privacy as contained in the ECHR. But the European case did consider the placement of the camera which was on the private premises of the observer. If the camera were installed on the property of the observed or a public space, then even in the European case, it would have amounted, in addition to a violation of the privacy right of the observed, a violation of property rights.

[129] Bathurst City Council v Saban, [1985] 2 NSWLR 704, 706.

In the case of, *Peck v The United Kingdom*,[130] the ECtHR, in para 59 of the judgement noted:

> 'The monitoring of the actions of an individual in a public place by the use of photographic equipment which does not record the visual data does not, as such, give rise to an interference with the individual's private life'

These cases, whether from the civil law jurisdiction or the common law jurisdiction, lead us in the direction, that observation, if it avoids trespassing onto another's private property, is harmless. But should the ambit of trespass be limited to physically stepping onto another's property or also include visual trespass, where the ingredient of physically stepping onto another's property is missing, is tricky.

Public spaces exist for a purpose. For example, highways are meant for passage, parks are meant for resting or leisure, public libraries are meant for reading etc. The public spaces need to be used for the purpose for which it is designed, although, there are instances of improper use, like when a couple have sex in a park. Using the public highway to land an aircraft amounts to use for other than its intended purpose. A little leeway may be granted, for instance a person may rest at the side of the highway or sketch things which are within his VLOS. In *Hickman v Maisey*[131], an English case, it was held that taking a sketch while observing from a highway

[130] Peck v. The United Kingdom, no. 44647/98, ECHR 2003.
[131] Hickman v Maisey, [1900] 1 QB 752.

would not amount to a trespass but if the highway is used for other than its intended use it would amount to a trespass.

How much deviation is allowed from the intended use? There can be no rigid answer to this question. Shooting a duck on someone else's private property from the highway, most definitely will not be covered under normal use of the public space. Installing cameras, around a private property, on a public space also will not fall under normal use of the public space. In the English case of *Harrison v Duke of Rutland,*[132] a highway ran across the defendant's land. The Plaintiff, while on the Highway, disrupted the grouse shoot on the defendant's land when he was removed by the defendant's men. The plaintiff sued the defendant on the grounds of false imprisonment and assault, while on the other hand, the defendant claimed that the plaintiff was a trespasser on the highway. It was held that the plaintiff indeed was a trespasser as the highway was merely an 'easement' for the public to pass and repass over the land and not to disrupt the grouse shoot. Therefore, the plaintiff's use was outside the use for which the highway was dedicated by the defendant. We can see that a private law and a restrictive approach has been applied in the case. So, any use which was not thought of by the dedicator fell outside lawful use.

On the contrary, a more liberal approach was applied in the English case of *Lowdens v Keaveney,*[133] wherein, it was held that only excessive or unreasonable use of the highway was prohibited, thus in essence, expanding the notion of grounds of use as thought of by

[132] Harrison v Duke of Rutland, [1893] 1 QB 142.
[133] Lowdens v Keaveney, [1903] 2 IR 82.

the dedicator. So, activities on the highway are allowed if it does not obstruct the primary activity of passing and repassing. This liberal approach was applied in a more recent English case of *DPP v Jones.*[134] In this case the question to determine was whether a peaceful and non-obstructive demonstration on a grass verge nearby Stonehenge constituted a trespassory assembly. The House of Lords held, by a majority, that a peaceful non obstructive assembly could fall within the limits of the public's right of access to the highway endorsing the right to peaceful assembly on the highway.

The ECHR guarantees the freedom of assembly and association in Article 11. If the restrictive private law model is applied, then the right granted under Article 11 of the ECHR will be denied. However, no right is absolute, and actions taken to prevent wilful obstructions will be consistent with Article 11 of the ECHR.

Is the airspace, above a public area, also covered within the meaning of a public area? By referring to a public space or a public area we generally refer to spaces used by the public at the ground level. But that general reference is only because there are very few opportunities for the public to use the airspace above a public area. There is no qualification of intended purpose of the airspace above a public area, like it is there at the ground level. Therefore, the position of a drone observing from the airspace above a public area is clouded. No dedicator of a highway would have thought that the airspace above the highway will one day be used by drone enthusiasts.

[134] DPP v Jones, [1999] 2 All ER 257.

A dentist in 1904 asked for legal protection from a family in Balham which placed large mirrors on their property which assisted them to observe what the dentist was doing in his study and operating room.[135] The dentist did not find any relieve as the courts did not reason that any of his rights were infringed. The English law had always insisted that there is no right not to be observed.[136] The right to privacy simply did not exist in common law. On the contrary, in India, a right not to be observed has been followed, now to a limited extent, as in the case of a Pardanashin woman.[137]

Parks, beaches, shopping centres, markets, and streets are some public areas where one might spot a politician or a celebrity and just observing them is not an intrusion into their private life because it is an activity that is being performed in a public sphere. The public have the right to be there. Alpha numeric visual information may be invaded in a public sphere by snooping into another's computer screen. So, observation is not just limited to physical information but also extends to alpha numeric information. For instance, one may be sitting in a park and a person sitting next to him on a bench could be ingesting his private bank account details by snoopily observing his screen from a side angle, or one's colleagues in an open plan office might intrude upon company secrets displayed on the screen when one is out on a break.

[135] Courtney Stanhope Kenny, A Selection of Cases Illustrative of the English Law of Tort, Fifth Edition (Cambridge University Press 1928) 367.
[136] ibid.
[137] Gokal Prasad v. Radho, (1888) 10 Indian Law Reports Allahabad Series, 358-389.

Therefore, observation, simple, is not as innocent as one would think. It could be laced with malice. But the degree to which an individual has taken precautions to hide what he does not want others to observe will matter. So, if an individual does not want others to observe his diary, intentionally or unintentionally, locking it in a safe is a better solution than just leaving it on the desk. In the English case of *Fearn v Tate Gallery*,[138] residents of a newly constructed luxury apartment block sued the Tate Gallery in nuisance for privacy breach. In the case, opposite the luxury apartment block, was Tate Gallery's extended viewing platform. Visitors to the gallery were able to see inside the apartments from the viewing platform as the apartments had floor to ceiling glass windows. It was held that the residents of the luxury apartment blocks were unduly sensitive. The part of the flats visible from the viewing platform had been initially designed as winter gardens to function as quasi balconies without heating for occasional use. It was only later that developers put under floor heating because of which the residents were using the gardens, with floor to ceiling glass windows, as full-time living accommodation. Had they used it as a balcony there would have been nothing to complain. They also had the option to use sun blinds, which would prevent the intrusive eyes from the viewing platform, to peep inside the flats.

But it is not always that observation is negative. Observation by drones can have a positive impact. Often, during critical emergencies, like a car crash or a heart attack, patients lose their lives due to unprofessional attendance. Live coverage by drones of

[138] Fearn v Tate Gallery, [2019] EWHC 246 (Ch).

the condition of patients broadcasted to the hospital will get them professional and expert attendance at the crash sites.[139] The hospital staffs by knowing the condition of the patients can be better prepared to receive them. So, to take a stand that mere observation is detrimental to an individual is not true. It may take away a little bit of his visual privacy, but the legality of it, must be decided based on several factors, including public benefit.

Another dimension that observation can take, is that of false observation, meaning where people feel they are being observed but in fact no one is watching. A Spanish case dealt with observation by a dummy closed-circuit television (CCTV) camera.[140] The question before the Spanish Supreme Court was whether that amounted to an infringement of the right to privacy. The court concluded that, that can amount to an infringement of the right to privacy as an individual can feel that he is under constant surveillance, a chilling effect:

> '3rd) The plaintiff's right to be let alone in his private life also includes the right not to endure a permanent uncertainty about whether the camera facing his property is operational or not, since its external appearance prevents him from checking it and, on the other hand, the defendant would always have the possibility of replacing the non-operating camera with an operating one.

[139] Momont A, 'Ambulance Drone' (TU Delft) <www.tudelft.nl/en/ide/research/research-labs/applied-labs/ambulance-drone/>

[140] STS, Sala Primera, de lo Civil, Sentencia 600/2019 de 7 Nov. 2019, Rec. 5187/2017

> 4th) For the same reasons, the installation of the camera facing the plaintiff's garden cannot be considered an exercise of *ius usus inocui* in the area of nuisance law, since far from being innocuous, it objectively disturbed, and without necessity, the life of the plaintiff' (FJ 6th).

On the contrary, the Dutch data protection authority, on the question of whether dummy cameras in saunas amounts to violation of privacy, held that it did not.[141]

To conclude, one may ask, when is an observation lawful, or otherwise unlawful. There can be no simple answer to the query as other factors also come into play, like, whether it is a naked eye observation or through the lens of a camera, the length of the observation, whether the observation is continuous and targeted, the place from where the observation takes place, whether the observation is also recorded and published etc. For example, targeted observations may build patterns of behaviour which may amount to a privacy violation.

However, it will be safe to assume that most cases of observations will be harmless for the observer so long as the drone does not commit a trespass. Although in the *Pierre Herbecq* case the difference between naked eye observations and observations with the help of technology was non-existent, for the purposes of the GDPR, observations with the help of drones will amount to

[141] The Dutch Data Protection Authority, AP constateert geen misstanden met camera's in onderzochte sauna's <https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-constateert-geen-misstanden-met-cameras-onderzochte-saunas> assessed 26 November 2019.

processing of personal data within the meaning of Article 4 (2) of the GDPR, and as such, be liable to comply with the GDPR. This aspect has been analysed in more detail further below.

3.1.2. Recording

When the observation results in a recording, either a still photograph or a video of moving images, the imprint is permanent. The information is not just in the observer's visual cortex but on a medium that can be distributed to others to see. But without any publication, it should be equivalent to mere observation, although, there are higher risks of further distribution than when no recording is made.

A primary reason to record is the desire to publish, or else, one would just observe with the naked eye. But there can be reasons to record other than publishing. Observing the woman of one's fantasy naked, will only gratify the individual for the moment but with a still photograph of her that gratification becomes permanent. A police officer may take still photographs of criminals for purposes other than publication, for example, to feed it to a computer identification database, similarly, persons in positive relationships may take still photographs to remember their loved ones.

So, there is little difference, if at all, between mere observation and, recording strictly for personal use. Both lack publication and distribution which is a major element of privacy invasion. The only difference is the length in time. An observation will pass from memory but if recorded, the memory can be refreshed from the recording. So, a similar culpability, that is attached to mere

observation, should be attached to the unpublished recording, which is no culpability in most cases of observation.

However, in the case of *Reklos and Davourlis v. Greece*,[142] the ECtHR, clarified that a mere taking of a photograph without publication and dissemination may interfere with a person's right to private life. In this case, two photographs of a new-born baby, placed in the sterile unit of a private clinic immediately after birth, was taken face on by a professional photographer without the parents' consent. The parents complained to the management of the clinic about the photographer's intrusion into the sterile unit where only the clinic's staff should have had access and the likelihood of the baby being upset by the face on photograph. The ECtHR in para 42 noted:

> 'It is not insignificant that the photographer was able to keep the negatives of the offending photographs, in spite of the express request of the applicants, who exercised parental authority, that the negatives be delivered up to them. Admittedly, the photographs simply showed a face-on portrait of the baby and did not show the applicants' son in a state that could be regarded as degrading, or in general as capable of infringing his personality rights. However, the key issue in the present case is not the nature, harmless or otherwise, of the applicants' son's representation on the offending photographs, but the fact that the photographer kept them without the applicants' consent. The baby's image

[142] Reklos and Davourlis v. Greece, no. 1234/05, ECHR 2009, para 38-43.

was thus retained in the hands of the photographer in an identifiable form with the possibility of subsequent use against the wishes of the person concerned and/or his parents'.

In the same case the ECtHR in para 40 also noted:

> 'A person's image constitutes one of the chief attributes of his or her personality, as it reveals the person's unique characteristics and distinguishes the person from his or her peers. The right to the protection of one's image is thus one of the essential components of personal development and presupposes the right to control the use of that image. Whilst in most cases the right to control such use involves the possibility for an individual to refuse publication of his or her image, it also covers the individual's right to object to the recording, conservation and reproduction of the image by another person. As a person's image is one of the characteristics attached to his or her personality, its effective protection presupposes, […] obtaining the consent of the person concerned at the time the picture is taken and not simply if and when it is published. Otherwise, an essential attribute of personality would be retained in the hands of a third party and the person concerned would have no control over any subsequent use of the image.'

So basically, the court concluded that the act of recording itself violates the right to privacy even though the recording is not published. From the two immediately quoted paragraphs above, the

court's reasoning is clear that individuals have image rights and any recording or reproduction of their image by another person without the consent of the person whose image is recorded or reproduced, amounts to a violation of the right to privacy as enshrined in Article 8 of the ECHR.

But should all recordings be unlawful? Should not there be a difference between intentional and unintentional recordings? If all recordings are deemed to be unlawful then we all have been guilty of violating the right to privacy at some point in our lives. This is because however careful one might be, our personal photographs sometimes unintentionally do capture images of people without their consent, for example, taking a holiday snap in a crowded plaza may capture images of other people in the same personal photograph unintentionally. Are we to blame them for being in the wrong place at the wrong time or are we to blame ourselves for including them in the personal photographs, although unintentionally?

In the case of *P.G. and J.H. v. The United Kingdom*,[143] the ECtHR in para 57 noted:

> 'There are a number of elements relevant to a consideration of whether a person's private life is concerned by measures effected outside a person's home or private premises. Since there are occasions when people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner, a person's

[143] P.G. and J.H. v. The United Kingdom, no. 44787/98, ECHR 2001-IX.

> reasonable expectations as to privacy may be a significant, although not necessarily conclusive, factor. A person who walks down the street will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means of the same public scene (for example, a security guard viewing through closed-circuit television) is of a similar character. Private life considerations may arise, however, once any systematic or permanent record comes into existence of such material from the public domain.'

If an individual is a celebrity, the chances of him/her being recorded are more as compared to someone who is not a celebrity. So, the expectations of an individual can turn an unlawful act of recording into a lawful exercise. But what about expectations of people being recorded by drones? In this case, celebrity, and non-celebrity alike, share somewhat the same expectations, which is, they do not expect to be photographed by drones. In the case of drones, there is the ingredient of secrecy. Thus, a recording made in secret, by its nature, will be outside the ambit of the law till the time it is published. The consent requirement, which was an important element in the case of *Reklos and Davourlis,* the lack of which turned the act of recording unlawful, will be impossible to fulfil in the case of recordings by drones.

Taking an example of another case, in *Friedl v Austria*,[144] the Commission considered the question of whether the taking of photographs violates the right to privacy. In this case, Friedl

[144] Friedl v. Austria, no. 28/1994/475/556, Commission decision of 1994 (report); also see Friedl v. Austria, 31 January 1995, Series A, no. 305-B.

participated in a demonstration wherein the police took video recordings of the public demonstration. Friedl also alleged that he was personally photographed by the police authorities which infringed his right to privacy. In the case, which resulted in a friendly settlement, the European Commission on Human Rights opined that there had been no breach of Article 8 of the ECHR. In deciding that no violation of the right to privacy had occurred, the Commission also considered the question of whether the photographs related to private matters or public incidents and whether the recording was envisaged for limited use or was it likely to be made available to the public. Therefore, the opinion of the Commission was based on the reasoning that as the photographs were taken at a public demonstration for limited use by the police (to be kept in a file without the photographs being processed for identification purposes), it did not violate Article 8 of the ECHR.

Comparing the case of *Reklos* with *Friedl*, one major difference between the two cases was the place where the recording was made. In the case of *Reklos*, the recording was made in a more private setting than compared to in the case of *Friedl*. Then are we to say that anything recorded in a public place does not violate the right to privacy. This line of reasoning could not be further away from the truth as there is such a thing as a private moment in a public place. In both the cases, however, the recordings were not meant to be published and the recordings were taken without consent. In the case of *Reklos* the recordings were meant to be given to the parents of the child while in the case of *Friedl* the recordings were meant to be kept in the police file.

So, if a person takes himself to a public place where a film crew is shooting and an image of him/her is recorded, would not amount to a violation of the person's right to privacy because he made himself public, participated in a public exercise and that the depiction of his image in a film published to the world is anonymous. But in the case of accidental appearances in films mostly nobody is going to be crying that their right to privacy has been violated, to be honest.

The recordings can be either covert or overt, like observations which can be covert or overt. In the case of *López Ribalda and others v. Spain*,[145] which was a case about covert recordings including monitoring, the Grand Chamber (GC) of the ECtHR held that there was no violation of Article 8 of the ECHR. In the case, employees of a supermarket were kept under observation which was recorded. Due to discrepancies in sales and the cash register, the owner of the supermarket suspected the employees of theft. To catch who was committing the theft, the owner installed secret video cameras at the checkout area. As suspected, the employees were committing theft and those responsible were dismissed from service.

Subsequently, the dismissed employees filed a case with the Employment Tribunal for unlawful dismissal, on the grounds, that as the video cameras were installed without any prior information given to them, the recordings which were used in evidence for their dismissal were bad in law, as the secret monitoring and recordings infringed their right to privacy. The Employment Tribunal found the

[145] López Ribalda and others v. Spain, nos. 1874/13 and 8567/13, ECHR 2019 (GC).

monitoring to be proportionate as it was limited in space and time, and appropriate to the aim of finding whether the employees were committing theft. It also found the recordings to be necessary to provide evidence of the theft.

If the employees had been given prior information about the monitoring and recordings it would have defeated the whole purpose of the action. The employees then appealed to the High Court of Justice of Catalonia which upheld the judgements of the Employment Tribunal. Thereafter, the employees appealed to the Supreme Court and the Constitutional Court where, in both instances, their application was deemed inadmissible. The case was then heard by the Chamber of the ECtHR, which held in 2018, that as the video monitoring and recording equipment's were installed by a private party, the state failed in its positive obligation to properly balance the privacy rights of the employees with the rights of the employer to properly manage his business. The Chamber observed that although there was a reasonable suspicion of theft, which justified the use of video monitoring, the monitoring was broad in scope, affecting all employees and covering all working hours. It also breached the obligation under domestic law to give prior information to those persons affected by the monitoring. As such, the monitoring, and the consequent recording breached Article 8 of the ECHR.

The case was then referred by the Government, to the GC of the ECtHR, which found no violation of Article 8 of the ECHR in its judgement of 2019. In para 127 of the judgement, the GC noted:

> ‘As regards the consequences of the impugned monitoring for the applicants, the Court finds that they were significant because the employees concerned were dismissed on the basis of recordings obtained by that means. It nevertheless observes, as the domestic courts also noted, that the video-surveillance and recordings were not used by the employer for any purposes other than to trace those responsible for the recorded losses of goods and to take disciplinary measures against them.’

However, in an earlier case of *Perry v. The United Kingdom*,[146] the ECtHR held covert recordings to be in violation of Article 8 of the ECHR. In the case of *Perry*, the applicant was covertly videotaped at the custody area of a police station and the recordings were subsequently used in an identification parade to identify the applicant. The court’s reasoning was that, as the recordings and its use in an identification parade could not have been anticipated by the applicant, and obtained without the consent of the applicant, it violated the applicants right to privacy.

In summary, it can be said that an act of recording is a more serious interference with the right to privacy than plain observation. What will make a recording lawful or unlawful will depend, like observation, on factors, like, whether the recordings were in a public or a private sphere, the purpose for which the recordings were used, whether the recordings were published, and whether the

[146] Perry v. The United Kingdom, no. 63737/00, ECHR 2003; also see Vukota-Bojić v. Switzerland, no. 61838/10, ECHR 2016, wherein covert recordings by an insurance company (a state entity) violated Article 8 of the Convention.

recordings were taken with or without the consent of the individual concerned.

Comparing the two cases of *López Ribalda* and *Perry*, both of which involved covert recordings but having different outcomes, it is not immediately clear as to what caused the different outcomes. In both the cases the videotaping happened in a place that was public, of activities which were not private in nature, of individuals who had a reasonable expectation of privacy, without the consent of the individuals concerned, for a legitimate aim, based on prior suspicion and without prior information given of the videotaping to the concerned individuals as required by law. The only ground which differentiated the case from one another was that in the case of *López Ribalda* the ECtHR decided the case based on the positive obligation of the State to ensure the respect for the right to privacy between private individuals, whereas in the case of *Perry*, the State itself was accused of violating the fundamental right to privacy. There is the slightest of possibility, that due to this, the ECtHR may have taken a stricter stance in the case of Perry.

3.1.3. Publication and distribution

Once the recording is published it receives an audience. The audience changes the observation into a public spectacle. A major ingredient of the invasion, therefore, is the publication and distribution of the visual information. But publication, in some cases, is protected by Article 10 of the ECHR (the right to freedom of expression and of the press).

It is important to acknowledge the fact that publication and distribution has become a lot easier in the digital age. Photographs or video feeds posted online can amass millions of views in a day or two. Thus, it has become more difficult to prevent unauthorised publication and distribution. With regards to the role of drones in publishing, they are capable of instantaneous publication. Drone video feeds can be streamed instantaneously on Facebook.[147]

In *Peck v. The United Kingdom*,[148] the ECtHR observed that distribution generates far more publicity than would otherwise arise. In the *Peck* case, the applicant complained about the disclosure to the media by the Council, of images of himself, taken by CCTV cameras in a public place, which were widely broadcast and published. In the publication and distribution, by the media, the images of the applicant were not properly masked, as anyone who knew him, would have easily recognised the applicant from the distinctive hairstyle and moustache apparent in the images. The applicant only came to know about the publication after neighbours, friends, and family told him that they had seen him on television. The ECtHR held that the disclosure violated Article 8 of the ECHR. In para 42 of the judgement, the court noted:

> 'The present applicant was in a public street, but he was not there for the purposes of participating in any public event and he was not a public figure. It was late at night; he was

[147] DJI Broadcasts First Drone Video Over Facebook Live <https://www.dji.com/newsroom/news/dji-broadcasts-first-drone-video-over-facebook-live> accessed 1 September 2020.
[148] Peck v. The United Kingdom, no. 44647/98, ECHR 2003-I.

> deeply perturbed and in a state of some distress. While he was walking in public wielding a knife, he was not later charged with any offence. The actual suicide attempt was neither recorded nor therefore disclosed. However, footage of the immediate aftermath was recorded and disclosed by the Council directly to the public in its "CCTV News". In addition, the footage was disclosed to the media for further broadcast and publication purposes. Those media included the audio-visual media: Anglia Television broadcast locally to approximately 350,000 people and the BBC broadcast nationally and it is "commonly acknowledged that the audio-visual media have often a much more immediate and powerful effect than the print media." The "Yellow Advertiser" circulated in the applicant's locality to approximately 24,000 persons. The applicant's identity was not adequately, or in some cases not at all, masked in the photographs and footage so published and broadcast. He was recognised by certain members of his family and by his friends, neighbours, and colleagues. As a result, the relevant moment was viewed to an extent which far exceeded any exposure to a passer-by or to security observation and to a degree surpassing that which the applicant could possibly have foreseen.'

In the English case of *Douglas v. Hello*,[149] the right to publication of photographs were assigned to OK magazine, but Hello magazine

[149] Douglas v Hello, [2005] EWCA Civ 595, [2005] 4 All ER 128, [2005] 3 WLR 881, [2006] QB 125.

sneaked in camera/s and thereby photographed the event. Hello magazine published the photographs, surreptitiously acquired, before it could be published by OK magazine. The publication reduced the value of the rights acquired by OK magazine. If Hello magazine had withheld publication it would not have been culpable. Nobody would have known about the incident of the invasion of visual privacy, but for the publication.

In a Spanish case,[150] which involved model and actress Elsa Pataky, a paparazzo took pictures of her when she was participating in a shooting for the magazine Elle. The paparazzo used a very powerful camera and sold the pics to Spanish magazine 'Interviú'. Elle brought a lawsuit against the publisher of Interviú on unfair competition grounds (violation of an exclusive deal it had paid for). Elsa Pataky had promised not to grant image rights to other publications for a specific period. Elsa Pataky also brought a lawsuit against the publisher of Interviú. Here, the Supreme Court held that the dissemination of the secretly captured images during a professional photoshoot in an isolated part of the beach violated her image rights.

In *Campbell v. Mirror Group Newspapers Ltd*,[151] an English case, Naomi Campbell was observed leaving Narcotics Anonymous meeting, when she was photographed. It is most probable that other people saw her leave the meeting as well. But if someone did

[150] Judgement 518/2012 of the Spanish Supreme Court of 24 July 2012.
[151] Campbell v Mirror Group Newspapers Ltd, [2004] UKHL 22, [2004] 2 WLR 1232, [2004] 2 AC 457, [2004] UKHRR 648, [2004] EMLR 15, 16 BHRC 500, [2004] HRLR 24, [2004] 2 All ER 995.

simply observe her while she left, there is no culpability attached to the observation. It will be outlandish to tell people not to look at her while she left the building. If she was so concerned, about people seeing her leave the meeting, and inferring that she was a drug addict, she should not have attended the meeting and stayed in the comforts of her homely walls. If someone observed, and secretly took a photograph of her she would not know it until it was published. So, there is no culpability in the secret photograph either. The culpability arises only after the publication because people who did not see her leave would also know that she attended the meeting and infer that she is a drug addict.

In the case of *Sciacca v. Italy*,[152] the ECtHR held the publication of photographs as a violation of Article 8 of the ECHR. In the case, a criminal file was prepared on the applicant by the Revenue Police. The file also contained photographs of the applicant. During a press conference, the file of the applicant was released by the Revenue Police to the press which in turn published articles on the investigation along with the photograph of the applicant. In para 29 of the judgement, the Court noted:

> 'Regarding whether there has been an interference, the Court reiterates that the concept of private life includes elements relating to a person's right to their image and that the publication of a photograph falls within the scope of private life'

[152] Sciacca v Italy, no. 50774/99, ECHR 2005.

However, it might matter if an individual is a public figure. In the case of *Schüssel v Austria*,[153] the ECtHR did not find any violation of Article 8 of the ECHR in the publication of a picture of a politician. The Court in its judgement noted:

> 'the limits of acceptable criticism are wider with regard to a politician than as regards a private individual'

Publication often involves a conflict between the right of the publisher to publish matters of public interest (Article 10 of the ECHR), and the privacy rights of the individual whose image has been published. In the case of *Küchl v. Austria*,[154] the applicant, principal of the St Pölten seminary, alleged that the Austrian courts had failed to protect him against a violation of his right to respect for his private life on account of the publication of an article accompanying a photograph in a weekly newspaper. The article stated that the police had searched the seminary on suspicion of someone having downloaded child pornography from the internet and found photographs showing seminarians engaging in homosexual activities. The photograph showed the applicant with his left arm around one of the seminarians, holding the seminarian's wrist with his left hand and with his right hand on the man's crotch. With regards to the publishing of the photograph, the Austrian Supreme Court did grant an injunction to the applicant against the publishing of his photograph but did not grant any compensation. Although the ECtHR held that the publication of the photograph

[153] Schüssel v Austria, no. 42409/98, ECHR 2002.
[154] Küchl v Austria, no. 51151/06, ECHR 2012.

accompanying an article did not violate Article 8 of the ECHR, in para 90 of the judgement, the court noted:

> 'the photograph, […] showed an intimate detail of the applicant's private life. Taking into account, moreover, that his physical appearance was not known to the general public before publication of the article, the Court considers that the publication of his photograph amounted to more substantial interference than the written article'

But what amounts to publication? Is there a need for a certain number of individuals to whom it has been published or is it sufficient if the publication was only to a single individual? Even if the publication is only to a single individual what are the chances that it will not be further published. The question, to whom was it published is also pertinent. A nude photograph published to a stranger, will not be as demeaning as, the publication of the same photograph, to someone who knows the person well. In the latter, the person will be more uncomfortable with the fact of the publication than in the former.

In a nutshell, we can say that publication is the gravest element of the three because it is through this element that the public gain knowledge of something the concerned individual did not want to disclose. As with observation and recording, the legality of the publication will also depend on other factors, such as, whether the data subject has a celebrity status or not, how intimate were the disclosed visual information, whether the publication contributed to

a debate of general interest, whether the published materials were obtained covertly, and the consequences of the publication.

So, a celebrity has lesser protection with regards to publication than a non-celebrity, more intimate the matter published the greater the protection, the greater the public interest in the publication the lesser the protection, publishing of covertly obtained materials attract lesser protection than compared to materials obtained and published with consent, and if the publication results in consequences which a prudent man could not reasonably expect then the protection will be greater.

The aspect of publication has been discussed further below.

3.1.4. Links with the internet of things and artificial intelligence

Technology connected people, and now, it is connecting things. Internet of Things (IOT) is a term coined by Kevin Ashton in the year 1999.[155] According to Gartner, 'it is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment.'[156] It basically means physical things connected to the internet. It could be anything that has a sensor which can sense activity. For example, baby monitors contain audio and video sensors that can yield personal information about the users and their

[155] Kevin Ashton, 'That Internet of Things Thing' (Rfidjournal.com 2009) <www.rfidjournal.com/articles/view?4986> accessed 26 November 2017.
[156] 'Internet of Things Defined - Tech Definitions by Gartner' (Gartner IT Glossary) <www.gartner.com/it-glossary/internet-of-things/> accessed 26 November 2017.

surroundings. From toasting bread to refrigerating our food, information is collected by sensors in these things. In the case of refrigerators, it knows which foods we store in them and if they run low, they alert us to replenish them. They could even be capable of alerting the grocery stores in our neighbourhood who in turn could deliver the foods right at our doorsteps.

Drones are also physical objects which are connected to the internet. But drones gather visual information, whereas other physical things that we use, collect mostly alphanumeric information; and if all the physical objects are connected to a single Wi-Fi network, then all that a person needs, is a single hack. So, if Amazon is collecting visual information by drone parcel delivery and, at the same time, is an internet service provider, in addition to selling household physical objects which are connected to its internet service, the amount of information it has in its hands about a user is enormous.

The traditional data processing methods are incapable of handling such vast amounts of data. This is where big data comes in. Big data means, basically, the way in which this large dataset, which may or may not consist of personal data, is combined, and analysed to extract information.[157] Thus, with modern data analytics systems, intricate patterns of behaviour can be built of individuals. The big data could relate to the health care sector, the automobile sector, or any other sector where data is generated on an enormous scale.

[157] Guidelines on the protection of individuals with regard to the processing of personal data in a world of big data (Council of Europe 2017); The Impact of Big Data and Artificial Intelligence (AI) in the Insurance Sector (OECD 2020).

Multinational companies that have operations in different sectors can combine data for predictive analysis and making inferences on individuals.

Although limited in their capabilities, as of now, artificial intelligence (AI) is also a concern, when it comes to data intensive technologies, like big data. AI is difficult to define as there are variety of ways in which AI is approached, like neural networks.[158] However, for general understanding, it is the emulation of human cognitive abilities by machines, through machine learning with the help of algorithms.[159] Like big data, AI also could relate to the health care sector, automobile sector, or other sectors. The difference between big data and AI is that the latter uses big data to achieve the machine learning outcomes.[160]

As drones produce massive amounts of visual data, irrespective of the sectors that they are used in, the application of big data and AI technologies on the visual data processed by drones, will be a concern from a privacy and data protection point of view. Facial recognition, the morphing of images by applications like sex bots are just few of the concerns when it comes to visual data and the application of big data and AI technologies.

---

[158] Cédric Villani, 'For a meaningful artificial intelligence: Towards a French and European strategy' (Creative Commons 2018) < https://www.aiforhumanity.fr/pdfs/MissionVillani_Report_ENG-VF.pdf> accessed 3 December 2020.

[159] ibid.

[160] The Impact of Big Data and Artificial Intelligence (AI) in the Insurance Sector (OECD 2020).

Facial recognition technologies have been made possible because of the transition from film-based photography to digital photography, and the rise of the internet, where people post digital pictures of themselves online.[161] Websites like Facebook, Google, and Instagram where digital pictures of human faces are posted in astronomical numbers, provide the fuel for facial recognition algorithms. Even though facial recognition technologies have been said to supposedly assist law enforcement personnel in the identification of criminals (one of the beneficial applications of the technology), they are riddled with bias.[162] Biases get embedded in the algorithms which results in inaccurate detection of emotions, skin tone, gender differentiation, age inaccuracies, etc.[163] Biases result from the lack of, identification of discriminatory imbalances, by the data set builders and algorithm designers.[164]

For example, a facial recognition system which has been fed only white male faces, will be discriminatory towards non-white lighter skin tones and dark skin tones. Therefore, these technologies are as good as the data that has been fed into them.[165]

---

[161] David Leslie, Understanding bias in facial recognition technologies: an explainer (The Alan Turing Institute 2020).
[162] ibid, also see Joy Buolamwini and Timnit Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' (2018) Conference on fairness, accountability, and transparency.
[163] ibid.
[164] ibid.
[165] Clare Garvie, Garbage In, Garbage Out: Face Recognition on Flawed Data (The Center on Privacy & Technology at Georgetown Law 2019) < https://www.flawedfacedata.com/#acknowledgements> accessed 4 December 2020.

As data is at the heart of all these technologies, it is obvious that the principles of data protection apply. But the application of data protection principles is, now, mainly restricted to the input data and not the output. This is because these technologies are only beginning to be regulated. As the output is dependent on the input, restrictions on input data will result in the development of inaccuracies. So, to have the most accurate big data and AI applications, the restrictions on the input must be negligible.

Recently, the EU has proposed a Data Governance Act.[166] This has huge implications on data intensive technologies like big data and AI. What the Data Governance Act proposes is, to make public sector data available for reuse, the sharing of data among businesses, allowing personal data of individuals to be used with the help of data intermediaries, and allowing altruistic use of personal data.[167] With data being more freely available and with lesser restrictions, data intensive technologies like big data and AI can thrive. The proposed Data Governance Act, in Article 2, defines data as, 'any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audio-visual recording'. Thus, personal visual data is also within the ambit of the Data Governance Act and treated the same as alphanumeric data.

[166] Commission, 'Proposal for a Regulation of the European Parliament and of the Council on European data governance' COM (2020) 767 final, 25 November 2020.
[167] ibid.

The data collected on a mass scale of many individuals are not intended for the purposes of influencing interpersonal relationships but influencing the relationship of the corporations, who have access to those vast amounts of data, with the society at large. They determine the direction in which the society is moving and hence bear an unusually large burden of ensuring that, that direction is the correct one. But often these corporations are motivated by greed and profit, not denouncing their beneficial impact that corporations may have, and induce people into consumption of unnecessary products. The power that they exercise over society is not limited to selling their products, but it also permeates to the political system and the government machinery. They influence laws, innovations, and most of the functions of the government towards the society. They are the actual guards in terms of Bentham's penitentiary who dictate what we should eat, what we should wear, when should we sleep and how we should behave.

There is a marked difference between the visual information collected by drones on the one hand and information collected by things on the other. Visual information collected by drones can be termed as *macro information* as against the information collected by sensors attached to the physical things that we use, which can be termed as *micro information*. Micro information will consist of a person's heartbeat or the number of steps he/she have taken daily in numbers, the driving patterns like how much acceleration is normally uses, the time of the day when the home appliances are used, etc. We can instantly see how this information differs from pure visual information. A precise analogy will be the difference

between classical physics and quantum mechanics. They both study the universe but at very different levels. The micro information, which is mainly alphanumeric, however, is also visual information when it is depicted in the form of graphs or otherwise when displayed on the smartphone through an app. Individual pieces of micro information has very little value compared to individual pieces of macro information. It is only when sets of micro information are combined that it begins to reveal the behavioural patterns of individuals. Therefore, macro information is self-evident whereas micro information may not be self-evident. But micro information gathered overtime may reveal more minute details than macro information.

3.2. Scope of physical invasion

Although drones do not occupy the land, they do occupy the airspace above the land. Due to the notion of extension of property rights to the airspace above the land, it becomes important to determine whether that occupation of the airspace violates the property rights of the owner of the land. If it does violate the property rights, then in many jurisdictions, it is termed as a trespass.

3.2.1. Overview

Trespass and privacy may be related to one another. But not all trespass results in the violation of privacy rights and not all violation of privacy rights has an element of trespass. Trespass and violation of privacy rights can exist independently of one another or

both could co-exist together. Visual privacy for instance, can be violated by trespassing onto another's property, or, with the assistance of technology, it is possible to violate another's privacy rights even without trespassing. For example, with the help of a hearing aid, it will become possible to hear private conversations on the other side of the wall, which would not be possible otherwise than by trespassing.

Delineating a piece of land suggests that I am isolating that land from the rest. This may be done by building a wall, or running a fence, or simply by planting trees if it helps to distinguish it from the rest, on the delineating line. The main reason for distinguishing is an individual's desire to control or use the land to the exclusion of everyone else (Blackstone's 'Despotic Dominion'),[168] although, there may be other reasons to delineate, like cooperating with the neighbour or reducing information costs to potential buyers. It could also be a signal that the distinguished land is private and that entering that realm would be treated as a trespass. It is no more a public property. Therefore, ownership and property rights are important to determine trespass by drones.

However, in the European jurisdiction, there exists a right to roam but this right mainly applies to forest lands for camping and outdoor activities and it differs considerably across Europe.[169] In Switzerland, everyone can access freely, other people's forest and

[168] William Blackstone, Commentaries on the Laws of England, Volume 1 Book 2 (Sharswood G ed, JB Lippincott Company 1893) chapter 1.
[169] Brian Sawers, The Right to Exclude from Unimproved Land (2011) 83 Temple law review 665.

grazing land and may pluck berries and other small fruits, and use most paths and roads even on private lands.[170] In Germany, forest access (includes rough grasslands, marsh, unused meadows, and all paths and roads) is open to the entire country.[171] The right to roam, however, is balanced with the property owner's right to privacy.[172]

3.2.2. The position in the European legal system

Referring in passing, there are two legal systems in Europe, the civil law system which is prevalent in continental Europe and the common law system which is prevalent in England and Wales.[173] The former has its origins in Roman law while the latter has its origins in the Writs issued by the English Monarchy.[174] They are the major legal systems not only in Europe but also around the world, as passed down to the colonies. But undeniably, one cannot refute the influence of one system upon the other.[175] As still separate entities, they are slowly getting merged.

Under the European legal system, there are two major instruments that have a bearing on the relationship between privacy and trespass. They are, the ECHR and the CFREU. Article 8 of the ECHR and Article 7 of the CFREU (discussed in detail further below) contain the right to privacy. By illegally entering someone's home you not only commit a trespass by violating his personal

[170] ibid.
[171] ibid.
[172] ibid.
[173] Piyali Syam, 'What is the difference between common law and civil law?' < https://onlinelaw.wustl.edu/blog/common-law-vs-civil-law/> accessed 11 September 2020.
[174] ibid.
[175] ibid.

space, but also violate his privacy. The relationship between privacy and trespass came up for consideration, although not decided conclusively, by the ECtHR, in the case of *Cyprus v Turkey*.[176] In this case, one of the issues brought by Cyprus against Turkey was the alleged violation of the home and property rights of displaced Greek Cypriots in Northern Cyprus which amounted to a violation of Article 8 of the ECHR.

3.2.3 Origins of the law on trespass

The law on trespass has a historical origin as with all other common law principles because they are judge made laws passed down through centuries. Before the common law, the Saxon Dooms provides that if a man passed over a person's fence he was obliged to pay four shillings.[177] But trespass as we know it today is a product of the common law and is addressed in damages.[178] It was intended to provide a remedy for an injury to a person or to his property.[179] For example beating a person would constitute a trespass against his person or disposing a person of his property would constitute a trespass against his property. However, in the early days if a person was disposed of his property an action in assize of novel disseising lied, a kind of action for property

[176] Cyprus v. Turkey, no. 25781/94, ECHR 2001; also see Affaire Halabi v. France, no. 66554/14, ECHR 2019, wherein it was held that public officials who entered a home without the consent of the occupier or owner violated Article 8 of the Convention.
[177] George F. Deiser, 'The Development of Principle in Trespass' (1917) 27 Yale Law Journal 220, 222.
[178] ibid Deiser 221; also refer to J. B. Ames, 'The History of Trover' (1897) 11 Harvard Law Review 277, 282-289.
[179] ibid Deiser 221.

trespass.[180] Although some form of transgression was involved the remedy was usually monetary. It was a civil wrong where the defendant disturbed the King's peace.[181]

In the restricted sense trespass refers to an entry upon another man's land without lawful authority and causing damage.[182] Currently, Section 158, of the American Restatement (Second) of Torts (1979) establishes the elements for physical trespass to land. To sum up, for a claim to be successful, a plaintiff should show that the defendant: (1) entered the land without authorization, or 'cause[d] a thing or a third person to do so'; (2) 'remain[ed] on the land'; or (3) 'fail[ed] to remove from the land a thing which he [had] a duty to remove.' There is no need to cause harm.

Trespass needs to be differentiated here with the tort of nuisance due to its similarity. Nuisance can be of two types, private and public nuisance.[183] A private nuisance is an unreasonable interference with a person's right to use and enjoy his land whereas public nuisance refers to an unreasonable interference with a person's public right, like that of the right to the safe use of the highway.[184] A private nuisance is more similar to trespass than a public nuisance.[185] Thus, the basic difference is that trespass

[180] ibid Deiser 226.
[181] ibid Deiser 221.
[182] William Blackstone, Commentaries on the Laws of England, Volume2 Book 3 (Sharswood G ed, JB Lippincott Company 1893) chapter 12.
[183] Jesse Elvin, 'The law of Nuisance and the Human Rights Act' (2003) 62 Cambridge Law Journal 546.
[184] ibid.
[185] Osborne M. Reynolds, 'Distinguishing Trespass and Nuisance: A Journey through a Shifting Borderland' (1991) 44 Oklahoma Law Review 227.

involves the infringement of the right to exclusive possession of real property while private nuisance involves the infringement of the right to use and enjoyment of that real property.[186] For instance, if for the purpose of turning my car I have to enter my neighbour's driveway then it is a trespass if it is without authorisation, but if I am hearing loud music at night in my home which has the consequence of unreasonably disturbing my neighbour and prohibiting him from falling asleep then it is a nuisance. Thus, trespass is tangible while nuisance is intangible, damage is not an essential ingredient of trespass whereas it is essential in cases of nuisance.[187]

The Roman law made a direct prohibition necessary to constitute trespass,[188] meaning that if a person entered the property of another without prior prohibition of the owner, it did not constitute a trespass. Prior prohibition need not necessarily be spoken words not to enter but in the form of some action like a sign to stay out or a fence which signifies that the property is not meant to be enjoyed by the public. But the Common law takes it a step further and treats every entry upon the others land a trespass, whether previously prohibited or not.[189] It is not only a trespass if a person himself

[186] ibid.
[187] Thomas W. Merrill, 'Trespass, Nuisance, and the Costs of Determining Property Rights' (1985) 14 Journal of Legal Studies 13.
[188] William Blackstone, Commentaries on the Laws of England, Volume 2 Book 3 (Sharswood G ed, JB Lippincott Company 1893) chapter 12.
[189] ibid.

enters upon another's land but also if his cattle enter another's realm.[190] But how extensive are property rights?

3.2.3.1. Aerial trespass

Before anyone took to the air, which is before the first balloon flights of the Montgolfier brothers, the Latin maxim '*Cuius est solum, eius est usque ad coelum et ad inferos'* (ad coelum doctrine) was coined.[191] What it means is that property owners have rights not only to the plot of land itself, but also to the air above and the ground below, infinitum. Going by this logic, if a tree which is planted on my neighbour's land and has branches overhanging my property, it will constitute a trespass. Similarly, if my neighbour decides to dig an underground passage which passes through my property, although not visible from the surface, will constitute a trespass. But this could also constitute a nuisance. These actions of my neighbour restrict the enjoyment of my property. The overhanging branches may weaken and fall thereby destroying my fence or the underground passage may collapse and sink my house. To think it this way it is not an unreasonable doctrine.

The origin of this Latin Maxim, however, is clouded. The exact wordings do not have its origins in Roman law but rather is closer in meaning in Jewish law.[192] In Hebrew, the phrase depth and

[190] ibid.

[191] 'Cuius est solum, eius est usque ad coelum et ad inferos' (En.wikipedia.org) <https://en.wikipedia.org/wiki/Cuius_est_solum,_eius_est_usque_ad_coelum_et_ad_inferos> accessed 28 August 2017.

[192] Arnold McNair, The Law of the Air (Butterworth 1932) 13-16; also refer to Fredman Ashe Lincoln, The Legal Background to the Starrs (London, E.

height were used in conveyances to indicate the vertical limits of rights in property. The Mishna (Bava Batra IV, II) in the Babylonian Talmud[193] says, 'Title is not given to a well, or to the stone wall thereof (if this was not plainly mentioned in the bill of sale of the house), although there is mentioned that he sold him the depth and the height.'[194] Rabbi Dimi of Nahardea in the Gemara said 'If one sells a house with the intention of giving title to all its contents, although the bill of sale states from the bottom to the top, title is not acquired in wells, etc. (if such there were), unless he writes: "You shall acquire title from the depth of the earth to the height of the sky."'[195]

Roman law did treat land together with its associated space above as one and not as a flat structure.[196] Thus, landowners had the rights to reasonable enjoyment of their property including the airspace above. In case where an owner constructs a building on his land thereby blocking the rays of the sun from reaching the land of his neighbour commits no offence if the neighbour had no servitude.[197] But the height to which the owner has dominion has not been addressed directly in Roman law. Francisco Lardone, after independently examining the Roman sources concludes that Roman

---

Goldston1932) 63; and John Cobb Cooper, 'Roman Law and the Maxim Cujus est Solum in International Law' (1952) 1 McGill Law Journal 23, 50.

[193] The Mishnah is the collection of rabbinic traditions.

[194] 'Tractate Bava Batra: Chapter 4 Rules and regulations concerning unconditional and conditional sales…' (Jewishvirtuallibrary.org) <www.jewishvirtuallibrary.org/tractate-bava-batra-chapter-4> accessed 29 August 2017.

[195] ibid second last paragraph before Mishna II.

[196] ibid Cooper 26; also refer to Francesco Lardone, 'Airspace Rights in Roman Law' (1931) 2 Air Law Review 455.

[197] ibid Cooper34.

lawyers did not deal with high altitudes but only lower altitudes because the Romans thought anything existing at high altitudes to be impossible.[198] So they restricted their jurisprudence to natural heights of trees and buildings.

But they did not altogether disregard the airspace at high altitudes and their ownership, in accordance with the roman spirit of the law, lay with the owner of the property.[199] The sky was the limit.[200] One cannot say for certain that if they anticipated aircrafts flying at high altitudes, or thought that it was even possible, what would their reactions be to airspace rights?[201] Romans did conform to the idea that air was common to all and that it was not the subject of ownership.[202] But air has to be distinguished from airspace as they are not one and the same thing.[203] It is possible to empty out all the air and create a vacuum in the space that once held air. Even in the absence of air the space remains. Ulpian, the prominent Roman jurist, held that the flight of an arrow or other missile over lands not owned by the hunter did not constitute a trespass.[204] Therefore, transitional interference in the airspace above the landowner's property was not actionable if no damage had been caused.

[198] ibid Lardone.
[199] ibid.
[200] ibid Cooper 33.
[201] ibid Cooper and Lardone.
[202] ibid Cooper 36-38; and Lardone.
[203] ibid.
[204] ibid Cooper 39.

Gradually, this doctrine made its way into the common law and in *Bury v Pope*,[205] the first recorded case where the maxim was used, the owner of a land was entitled to erect a house blocking the sunlight of his neighbour.[206] Since then on, this maxim has been a part of the common law.[207]

This is all to do with private law but even in the domain of public law, it is generally agreed that the sovereignty of a State extended to the airspace above its territory. It is only because the State has sovereignty that it can pass on that sovereignty to its citizens in the form of property rights.[208] A person cannot transfer a better title than he has. The Convention relating to the Regulation of Aerial Navigation in Article 1 states, 'The High Contracting Parties recognise that every Power has complete and exclusive sovereignty over the air space above its territory.'[209] The limits or the altitude to which this sovereignty extends has not been specifically mentioned nor has any weight been put to differentiate between air and airspace. However, it is reasonable to think that this sovereignty is limited as other Contracting States have the right to cross the airspace of another member State, if they are only transiting without

[205] Bury v Pope, (1587) Croke Eliz 118, [1653] EngR 382, (1653) Croke Eliz 118, (1653) 78 ER 375 (B).
[206] ibid Cooper 48; also see Franklin Gevurtz, 'Obstruction of Sunlight as a Private Nuisance' (1977) 65 California Law Review 94.
[207] See cases where the maxim has been used, Fay v Prentice, [1845] EngR 79, (1845) 1 CB 828, (1845) 135 ER 769; The Electric Telegraph Co. v Overseers of Salford, [1855] EngR 552, (1855) 11 Exch 181, (1855) 156 ER 795; Ellis v Loftus Iron Company, (1874) LR 10 CP 10; Wandsworth Board of Works v United Telephone Company, (1884) 13 QBD 904.
[208] ibid Cooper 26, and Lardone.
[209] Convention relating to the Regulation of Aerial Navigation (signed 13 October 1919 in Paris).

landing, as agreed by the Contracting States for the purposes of air navigation.[210] But States are very reluctant to impose limits on their sovereignty over the airspace above their territory,[211] as evident from the Convention on International Civil Aviation, which restates the rule of States sovereignty, as stated in the Regulation of Aerial Navigation, over the airspace, in Article 1.[212]

The ad coelum doctrine has evolved a lot, since its inception, due to modern aerial navigation, as is evident from the US case of *United States v. Causby*.[213] In the case, the US Supreme Court held that the public's right of flight does not extend downward to the earth's surface and recognised that a claim of property ownership indefinitely upward 'has no place in the modern world.' It found:

> 'if the landowner is to have full enjoyment of the land, he must have exclusive control of the immediate reaches of the enveloping atmosphere. Otherwise, buildings could not be erected, trees could not be planted, and even fences could not be run'… 'The fact that he does not occupy [space] in a physical sense – by the erection of buildings and the like – is not material. As we have said, the flight of airplanes, which skim the surface but do not touch it, is as much an appropriation of the use of the land as a more conventional entry upon it.'

[210] ibid Article 15.
[211] F.B. Schick, 'Space Law and Space Politics' (1961) 10 International and Comparative Law Quarterly 681, 687.
[212] Convention on International Civil Aviation, as amended (signed 7 December 1944 at Chicago, entered into force 4 April 1947).
[213] United States v. Causby, 328 U.S. 256 (1946).

3.2.3.2. Deductions

From the above discussion the following points emerge, firstly, that private property rights gradually includes the airspace over the land, secondly, that the airspace rights are limited to an extent to reasonably enjoy the property,[214] thirdly, that the height to which the airspace rights extend is incapable of being ascertained, fourthly, that there can be an action on the grounds of trespass if the airspace has been invaded within the reasonable height necessary to enjoy the property, fifthly, that it is necessary to prove ownership or possession of the property where the trespass has occurred, sixthly, that it is not necessary to prove damages on an action of trespass and lastly, that the basic tenets in civil law and the common law are the same with minor variations.

The basic question is, to what height does property rights extend to the airspace above the land. If there was a universal answer, then it would be easier to pinpoint a trespass by drones into private properties of individuals. But as that is not coming, the whole issue revolving on trespass by drones is not clear. This is because as the airspace rights are limited to an extent to reasonably enjoy the property, what is reasonable will defer from person to person. For a rich person, the threshold of reasonableness will be higher when compared to someone with limited resources. Municipal corporations may have rules in place regarding the maximum height of residential buildings. There might be other bylaws or local laws governing the height of residential buildings, which restrict a

[214] Bernstein of Leigh v Skyview & General Ltd, [1977] EWHC QB 1, [1977] 3 WLR 136, [1977] 241 EG 917, [1977] 2 All ER 902, [1978] QB 479.

person's right to reasonably enjoy his property. An individual may have the resources to build additional four floors to his existing residential structure, but the local laws may allow only two floors. So, the whole answer to the question is not well-defined as it will differ from person to person and city to city.

3.2.4. Applicability to drones

But what significance do these rules and principles have on civilian drones? Drones occupy the air and not the land and if the Latin maxim were to be adhered strictly today, in a sense, they would be trespassers, irrespective of the height. But if we referred to what Ulpian said, regarding the flight of bullets, then the flight of drones over the airspace of a person's property would not amount to a trespass. But will it then amount to a nuisance? Both the common law torts of trespass and nuisance fit unevenly when applied to drones.[215] With trespass, there is no physical possession of the land although drone operations at near ground level will be treated as a trespass. However, no one operates a drone at near ground level, it will be unusual. With nuisance, there is no major restriction to the physical use and enjoyment of a property by a hovering drone, except the lack of privacy if detected.

Although, States still recognise complete sovereignty over the airspace up to the heavens, over their territories, the same does not hold true for private property owners. They have limited rights over

[215] Hillary B. Farber, Keep Out! The Efficacy of Trespass, Nuisance and Privacy Torts as Applied to Drones (2017) 33 Georgia State University Law Review 359, 380.

the airspace over their private property, compared to the sovereign from whom they derive those rights.

If that were not true, then a passing aircraft would be liable for repeated and multiple trespass actions by the landowners. If permission were to be sought, then it would render the flight highly impractical as the number of permissions needed would be countless, keeping in mind the flight path. A case in point is Pickering v Rudd.[216] But even if we agree that a drone is a trespasser at low heights, whether it interferes with the reasonable enjoyment of a person's private property, at heights where one would assume that property owners do not have proprietary rights, drones will still interfere with their reasonable use of their property. They would not be causing damage in the traditional sense per se, but they will be infringing a person's right to visual privacy. So even if a bullet just passing over one's land, without striking any tangible property,[217] causes no damage, it is not the same with drones.

The problem is even more exemplified with miniature drones. A few centuries ago, trespass was an action based entirely on land with a few lone standing aerial trespasses of overhanging branches, and more recently, electrical wires, even they were fastened to the ground, but now the law of trespass is burdened with low height

[216] Pickering v Rudd, [1815] EWHC KB J43, (1815) 4 Camp 219, (1815) 171 ER 70, (1815) 171 ER 400 (B); also refer to Lyttleton Fox 'The Law of Aerial Navigation' (1909) 190 The North American Review 101.
[217] Kenyon v Hart, (1865) 6 Best and Smith's Reports 249.

aerial invasion. These invasions are not only transitory, but some are continuous, like a hovering drone.

The arbitrary height benchmark of 400 feet does not help in solving the issue. Drone operations at low height which is below 400 feet from the ground no doubt should be treated as a trespass if it passes over private property, but operations above 400 feet will be difficult to detect. In low residential areas, where the average height of buildings is below 400 feet from the ground level, a drone passing above 400 feet will be unnoticeable, however, in high residential areas, where the average height of the building is above 400 feet from the ground, drones even if they operate at 400 feet or slightly above, will still be in the visual line of sight, although unnoticeable in low residential areas. The word ground can also be interpreted differently, keeping in mind, from where the drone takes off. For a drone taking off from the roof of a high-rise building, the roof will be its ground, whereas, for a drone taking off from the pavement of a building, the pavement will be its ground. So, the definition of low and high-altitude operations will be interpreted differently depending on from where the drone takes off.

In residential areas, which consist of mostly apartment buildings, it will be difficult to prove a trespass as there is no single owner to whom one can attribute the ownership of the land, to the depths below and the heavens above. The ownership is shared between many and if an action were to prevail on trespass it will have to be brought jointly by all the residents of the building.

Figure 12. Technische Universiteit Delft displaying a quad-copter style 'Drone Catcher' at the ADW 2019.

But as each own only a certain space within the building it will be difficult to say that it invaded the privacy of all. So, although the trespass is common to all, the damage is not. In this case only the person who has sustained the damage (privacy invasion) has a ground for an action. In public spaces the airspace above is not owned by anyone, presumably. So, drones flying in the airspace above the road or even in between the buildings commit no trespass as they do not fly over private property, even then they could invade

a person's privacy. But to invade a person's privacy that individual should expect privacy in the space that he is present.

In the case of a trespass on land the property owner has a right to evict the trespasser. The force used to evict must be proportionate and reasonable. It will be unreasonable, if unarmed persons who pose no danger or threat to life are evicted, by shooting at them. It will be unreasonable to cut down the whole tree if only a branch of it trespasses onto the property. But how much force is proportionate to evict a trespassing drone? If the operator of the drone is visible it will be proportionate if he is told that by flying the drone in low airspace, he is trespassing onto another's property. If he is not visible it will be proportionate if the drone can be brought down by throwing a net at a reasonable height and if it beyond the capability of netting, then striking it with an object will be an alternative.

However, a case in the Stanislaus small claims court in the US, in *City Drone v Country Shotgun*, where a Californian man decided to test out his hand built drone above his family's orchard and while testing his drone, his neighbour shot it down, the court found the act of shooting down the drone unreasonable, regardless of the fact whether it was over the neighbour's property or not, and ruled in favour of the man whose drone was shot down.[218] But there have been opposing cases, where the act of shooting a drone has been held as reasonable in the US.[219] In the European context there are

[218] Farivar C, 'Man shoots down neighbour's hexacopter in rural drone shotgun battle' (Ars Technica 2015) <http://arstechnica.com/tech-policy/2015/06/man-shoots-downs-neighbors-hexacopter-in-rural-drone-shotgun-battle/>.
[219] John David Boggs v. William H. Merideth [2016], In the United States District Court, Western District of Kentucky, Louisville Division, Case No. 3:16-cv-6-DJH.

no case laws to elucidate this point so we just have to infer from the US cases for now. However, to note, gun ownership in the US is more liberal than in the EU, so cases involving shooting a drone over private property will be rare in Europe. There is still confusion about the reasonableness of force to evict a trespassing drone. Now, it is riddled with uncertainty and only in time, as case laws develop,

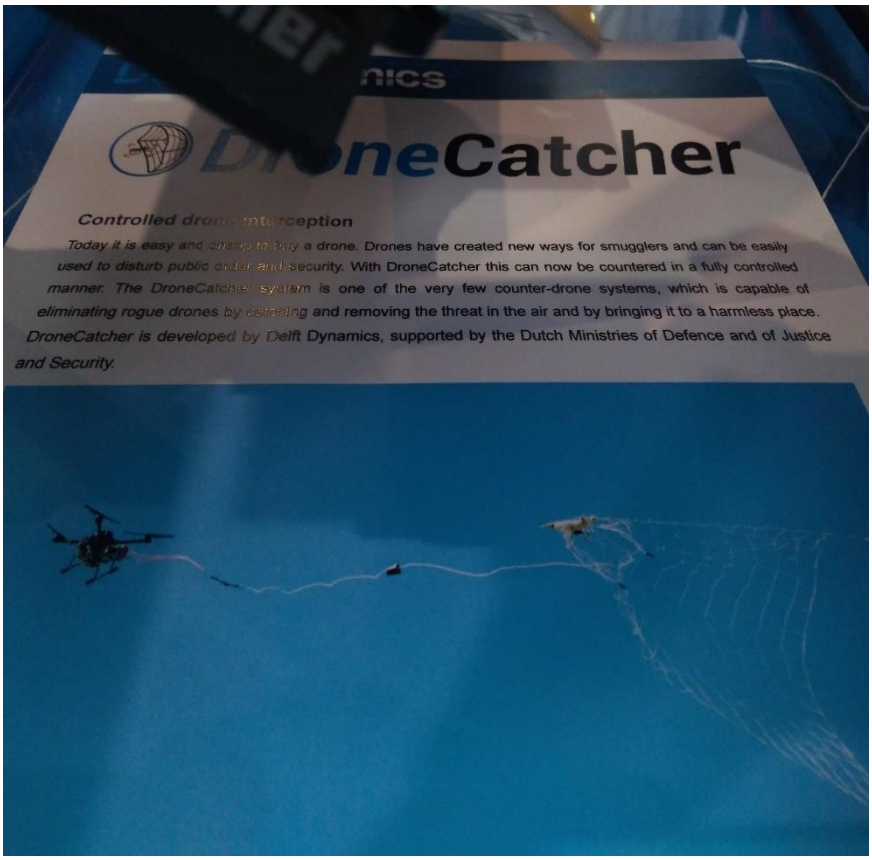

Figure 13. A picture showing how a drone catcher works by throwing a net, at the ADW 2019.

we will know with precision what the law holds.

A few scholars have taken the position that drones have a limited impact on privacy.[220] They base their arguments on the fact that drones are like any other imaging device and operate in few spaces to capture visual data not accessible to other imaging technologies.[221] One of the reasons why they operate in few spaces could be because they have been regulated by legislation early on in their existence, in the civilian sphere. The comparison to other imaging devices is to an extent true, but other imaging devices are not mobile, they are fixed. The mobility of drones (more than pocket mobility of a smartphone) greatly enhances their capability to violate visual privacy.

3.3. The variables

So far, having discussed, to fasten liability onto individual drone enthusiasts for visual privacy violations, there are many variables that come into play which exert a force upon each other. For there to be an actionable claim for visual privacy infringement by drones, according to the basics discussed above, the different variables will have to be aligned. For example, whether the violation consists of a single variable like observation or does it also include other variables like recording, publishing, consent, and trespass. Further, what are the consequences of two or more variables existing at the same time is analysed.

[220] For example, David Sella-Villa, 'Drones and Data: A Limited Impact on Privacy' (2020) 55 University of Richmond Law Review.
[221] ibid.

First, trespass or physical proximity of a drone to the observed subject matter is an important variable as in many cases an aerial trespass will need to be proved to hold a person accountable for the invasion of visual privacy. It will not be easy to prove an aerial trespass as the height to which a person has dominion over the airspace above his property is not well-defined, property owners will be hesitant to act in case their actions turn out to be against the law. Instead of protecting their property from hovering eyes, they might be in violation of damaging the moveable property of another. Even if there was a trespass, mere observation (in a case where the same thing could be observed from a public area) would be trivial (from the perspective of visual privacy infringement) if there is no recording. In such a case, a more likely claim would be that of trespass rather than visual privacy violation. But then we also need to factor in the rulings in the dummy camera cases.

Second, the degree of intimacy of the activity observed will also play a role. Some activities may qualify as intimate on a universal scale but watering the lawn or mowing the grass can hardly qualify as intimate even though performed within a private sphere. Still, as it is within a private sphere, no matter the degree of intimacy, an individual would want to protect the activity from prying eyes. He may be tolerant to a certain extent but when it comes to observation of female family members even a tolerant person would lose his patience.

Reasonable expectation of privacy is a slippery concept, like the concept of privacy itself.[222] Within the perimeter of one's own home there could exist differential degrees of reasonable expectation. Reasonable expectation of privacy also changes with the changing times. For drones, it is not even necessary to enter the column of airspace above the property as they can visually trespass even from a public space like a street.

Many public spaces, like streets and parks, are privately owned by corporations. Most Britons would have little access to open lands if it were not for the statutory right to roam (applies to other European countries as well) as, as much as 52 percent of the land is owned by 1 percent of the population.[223] This is not just true for the countryside, as it is evident in the cities as well.[224] As is the case with many public spaces that the public themselves have limited rights because they are actually on private property. Their rights to demonstrate and take pictures are curtailed.[225]

So, drones flown by private enthusiasts, even in a public space, technically and contrary to any previous statement in this regard, would be physically trespassing. In this case a private enthusiast would be trespassing onto a third person's property to invade the

[222] Serge Gutwirth, Ronald Leenes, Paul de Hert and Yves Poullet eds, European Data Protection: Coming of Age (Springer Netherlands 2013) 5.
[223] Richard Norton Taylor, Whose Land Is It Anyway? Agriculture, Planning and Land Use in the British Countryside (Turnstone Press 1982) 23.
[224] Dr Bradley L. Garrett, 'London's future...public space' (Museumoflondon.org.uk 2017) <www.museumoflondon.org.uk/discover/londons-future-space> accessed 4 November 2017.
[225] ibid.

visual privacy of another. On the other hand, corporations who own the public space could keep an eye on the public unhindered and clandestinely. They would incur no liability as the vertical airspace which would be used by drones belongs to them. As the public will be uninhibited in their behaviour, due to the surreptitious nature of drones, the corporations would have a field day in amassing not only visual information but also listening into the lives of anonymous people. The information gathered could be used in whatever way the corporations deemed fit.

So, the variable of public private divide is more of an oasis which exists when seen from a distance but vanishes in thin air when approached closely. But moments captured on camera in a public space may still be protected.[226] But then again if the image has been blurred or anonymised that protection may be taken away.[227]

Third, consent is another variable which legitimises actions which would otherwise be held in violation of the law. Entering a private property with the consent of the owner, taking a still photograph of a person with his consent, borrowing a car with the owner's consent, having intercourse with the consent of one's partner, are some of the activities, if lacking in consent, would be tantamount to an unlawful act. If consent were lacking when entering a private property if would amount to a trespass, if consent were lacking taking a still photograph of a person it would amount to an invasion

[226] See Murray v Express Newspapers plc, [2008] EWCA Civ 446.
[227] Pablo Salvador Coderch, Antoni Rubi Puig and Pablo Ramírez Silva, 'Imágenes Veladas: Libertad de Información, Derecho a la Propia Imagen y Autocensura de los Medios (2011) Vol.1 InDret, available at SSRN: <https://ssrn.com/abstract=1762790>

of his privacy, if consent were lacking when taking a car, it would amount to a theft and if consent were lacking when having intercourse, it would amount to a rape.

But sometimes even when there is consent a person may be liable. In the case of *Laskey, Jaggard and Brown v the United Kingdom,* consensual acts were unlawful as it was against public interest.[228] Matthew J is quoted from an earlier judgement as stating, 'There is however abundant authority for saying that no consent can render that innocent which is in fact dangerous.'[229] The case of *Laskey* involved sadomasochistic acts (including maltreatment of the genitalia with wax and the likes of fish hooks and needles, ritualistic beatings with spiked belts, and branding) between consenting homosexual men. Even though there was consent they were punished because the acts that they indulged in were against morals, public interest, and public health.

In the context of drones, an individual may consent, to his neighbour, to fly a drone in the other's airspace but can that consent also be used to secretly film an individual's home? Maybe the individual consented only to the use of his private airspace without consenting to the filming of his home. It can also be the case where the individual when consenting knew about the existence of the camera on the drone, and thus, an inference can be drawn that his consent also included the consent to film his home. However, we cannot apply the *Laskey* case to visual privacy infringements by

[228] Laskey, Jaggard and Brown v. the United Kingdom, 19 February 1997, Reports 1997-I.
[229] ibid para 21.

drones because in the latter, consent is always good. But this is not without exceptions as minors and persons of unsound mind are not capable of giving consent.

Whether it is mere observance of physical visual information or involves the recording and publishing of the information as well, the liability will have to be determined on a case-to-case basis. The discussions in this chapter, with regards to elements of visual privacy infringements by drones, have been represented diagrammatically in *Figure 14* below. The Figure assumes that drones always have a camera and does not factor in the GDPR because it is discussed in detail further below. The Figure is limited in nature as it does not include all the variables but enough variables so that the reader can determine, descriptively, the rough extent of liability for using camera drones in the EU.

Mere observation without a property trespass will attract no liability, recording of the physical information in a public or a private space may attract liability and recording with publication will in most cases attract liability, irrespective of whether there was a property trespass or whether the moment was captured in a private or a public space. The variables that could nullify the illegality would be consent or the freedom of expression. But then that expression should be necessary in the general-public interest.

Gender, age, culture, religion, architecture, affluence, and technology can all be variables. But these variables do not determine the legality but affect only the subjective tolerance towards an invasion.

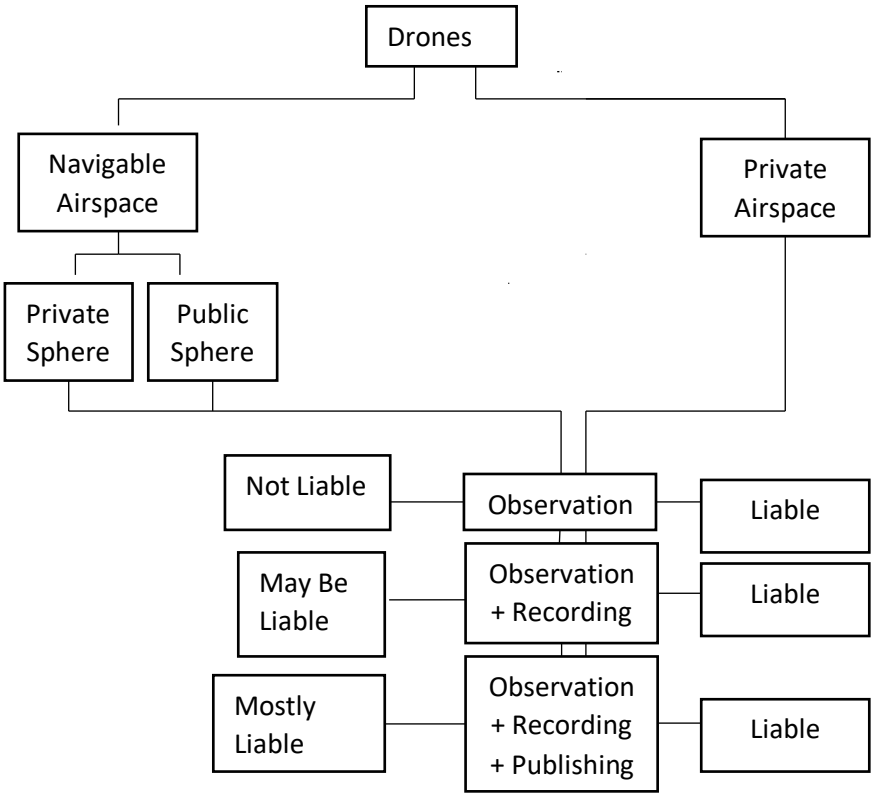

Figure 14. The variables that determine liability.

They may influence each other or simply act alone. A playful adolescent will be more tolerant than a grown man with a gun. Covered roof homes will allow little opportunity for observation when compared to open architecture styles from other cultures. An affluent person will have his property more guarded than a person living in a slum. Islamic culture will be more sensitive than western cultures to prying technologies and an ignorant will be more tolerant than a person who knows the technology.

3.4. The impact

A drone is not the first technology that invades visual privacy and certainly it is not going to be the last. Thus, adding another layer to the list of visually PITs (like smartphone with cameras and fixed street surveillance cameras) should not make a difference. But it has some characteristics that set it apart from the others. Firstly, it is associated with mainly collecting physical visual information and, secondly, that it is airborne. The convergence of these two aspects distinguish it from the other PITs.

3.4.1. Risk of the panoptic effect

The etymology of the word panoptic can be traced to the Greek word 'Pan' meaning 'all' and 'Optikos' meaning 'of or for sight'. The word gained popularity after Jeremy Bentham introduced his designs for a panopticon prison system in the late 18th century. It was a system where with a single guard all the inmates of a prison were to be kept watched.[230] The idea being, the location of the guard was to be such that all the cells were to be within the VLOS of the guard.[231] Even though it would not have been possible to keep a watch on all the inmates at one time, the feeling by the inmates that they are being watched would keep them behaved.[232]

Drones are a perfect analogy to the panopticon prison. With greater height, the angle of visibility increases in relation to the ground.

[230] Janet Semple, Bentham's Prison: A Study of the Panopticon Penitentiary (Clarendon Press 1993).
[231] ibid.
[232] ibid.

Then satellites should have the greatest angle of visibility and anything further in space will beat even the satellites. This is true, but the distance must match the sensors. If the distance is more than what the sensors can focus, then it is as good as being invisible as the pictures will be blurry. If the distance is less than what the sensors can focus, the pictures will be sharp but the angle of visibility decreases. So, to get the best results, one needs to maintain an optimum distance in relation to the capacity of the sensors.

Modern satellites have impressive visual sensors which can pierce through the atmosphere and see with detail. However, they are expensive to operate and are mainly used by governments, scientists, or corporations like Google. The sensors on board civilian drones are going to be no match for the sensors on satellites but drones fly in the troposphere. As the distance to the ground is less, even a 4k resolution camera is enough. CCTV cameras are fixed to the ground and as such they have a limited angle of visibility. It lacks the feel of a panopticon. Moreover, drones can follow a target once they are locked. Together with facial recognition technologies and x-ray sensors it is the perfect instrument for surreptitious watching. This kind of technology with the power to observe others was mostly out of reach of normal people. It was the preserve of governments and big corporations. Now anyone with a few thousand Euros can become Panoptes,[233] the all-seeing.

[233] A giant in Greek mythology who had many eyes (See Encyclopaedia Britannica for Argus Panoptes).

The disadvantage, of private individuals having this kind of ability, is the invasion of visual privacy on a grand scale. Social control in the hands of private individuals, at the scale of neighbourhoods, is something new. In such an environment, the one keeping an eye will have somebody keeping an eye on him, as the technology is within the reach of many. It is unlike the situation in Bentham's panopticon prison where observation was a one-way affair, the guard keeping an eye on the prisoners and not vice versa.

Prior knowledge gives a person an upper hand and the primary sense through which it is gained is sight. But knowledge can also be gained by other means, such as, hearing and touching. It is sometimes also said that the eyes can be mistaken. But a person will still trust his eyes, more than any other senses. It is the most reliable medium of knowing the truth. But if it is combined with the other senses the reliability increases. The need for knowing the truth arises because of our innate desire and the curiosity to know. If it is public or known, then there is no need to know.

So basically, private individuals can discover the truth and by knowing the truth they can exert control over others. But this is not always the case because if it is a positive truth the knowledge will have little deterrence effect. Only when it is a negative truth that others will be controlled. But in-between control and the inability to control is the sphere of influence. So, by gaining prior knowledge, a person will, at the least, be able to exert an influence on others.

A person's physical image is public. He is willingly exposing himself. One can determine the colour, gender, age, height, but that

does not say much without more outside information. Even for the purposes of making inferences, irrespective of whether those inferences are correct or false, more outside information is needed. One cannot determine what he is thinking by looking at him nor can one determine the person he is, like his character. Thus, one must observe a chain of events, that pieced together, makes up his life, and that chain of events is capable of being seen. The chain of events consists of activities or actions that have been performed by him over a period. It might be the case that some activities are hidden and so requires a research, the knowledge of which can be gained by other means, like going through his public alphanumeric information.

For example, by simply looking at a person, one does not know whether he is a murderer, he might be out on parole or may have served his sentence or he might be the nice guy. Once one knows his basic alphanumeric information, like his name and address, the research can start. What the search will reveal cannot be guessed. So, it is the aggregation of what he looks like and his alphanumeric information that paints a whole picture. Knowing only the name, without knowing what he looks like, is of little value, because one may come across a murderer who is known by name and not recognise him because the knowledge of his image is lacking. But if one knew a murderer by his image other information becomes irrelevant.

Thus, continuous observation builds an individual’s knowledge about another person through his activities. The house that he lives

in, the car that he drives, the clothes that he wears, the friends that he keeps, all add to his identity. But the identity which he himself makes known may be different from what his identity is as a private person. He may have borrowed money from the bank to portray himself as rich to scam people in his neighbourhood. So, extending the observation to include his friends may add more value in deciphering his identity.[234] Further still if the conversations he had could be overheard would complete the picture.

So, visual information itself has immense value, but it gains more importance if outside information complements it. It is like watching a silent Charlie Chaplin movie. It is still laughable even though nothing funny has been said. What is seen is a person with a funny behaviour. It is enough to understand the setting as it is simple. But if a movie with a more complex setting were to be seen and not heard, it will be difficult to understand the whole picture. An individual will know when a person is shot but not know why he is shot. The knowledge gathered, therefore, by simply seeing without any outside information, is not complete. But it is still enough to influence.

Influence is so pervasive that it is all around us. It is not possible to find a person who has not been influenced in some way or another. It starts moulding a person right after he is born, therefore, the first sphere of influence is the home. A child is influenced by his parents and when he is old enough to go to school, he gets a new source of

[234] Solon Barocas and Karen Levy, 'Privacy Dependencies' (2020) 95 Washington Law Review 555 (in this the authors describe a tie-based dependency where an observer learns about a person through his relationships with others).

influence. He is bombarded with new sources of influence all throughout his life, from the corporations influencing people through the medium of television or the internet to being influenced at the workplace. But the common denominator is that they have power over us. If they did not have power, they would not be able to influence us. Parents have power over their children, teachers have power over their students and even among students some students can exert more influence on others. But what cannot be determined is whether influence comes first or the power. In other words, whether a person must be influenced first to have power over him or must have power over him in order to influence him. A similar conundrum arises when answering the question whether the chicken came first or the egg. Therefore, the personality of a person is the sum of the influences that has shaped him.

3.4.1.1. On autonomy

Drones also have an impact on individual autonomy. This is because they can have facial recognition cameras and can fly almost without being detected, depending on their size and the height to which it can fly. Autonomy, although a vague concept like privacy,[235] basically denotes that an individual is free to govern himself, in other words, able to choose one alternative over the other and make independent decisions free of any influence.

[235] Evan Selinger and Woodrow Hartzog, 'The Inconsentability of Facial Surveillance' (2019) 66 Loyola Law Review, 101.

Acquiring consent of everyone, who may be photographed or videoed by a drone, is almost impossible.[236] Lack of consent together with facial recognition cameras onboard the drones, impact the autonomy of individuals.[237] This is because the once obscure individual, is revealed.[238] This revelation allows corporations and private individuals to track activities and behaviours of others.[239] Once a sufficient amount of knowledge is gained, an individual loses his ability to choose freely and make independent decisions as he can be influenced.

But from another perspective one can say, that despite all the influences, an individual still has the right of self-determination and autonomy. He is free to choose one influence over the other. But this statement is a paradox because how can a person be free to choose when his choice itself is influenced. If there is influence means he is not free. Then a man is never free because even if all the man-made influence is lacking, he is still influenced by nature.

But the degree of influence exerted at an individual scale is nothing compared to what is exerted on a grander scale, by corporations and governments. It is because they have more resources. Thus, at an individual scale, only interpersonal relationships are capable of being influenced. The amount of influence being based on the extent of knowledge derived from the visual information.

---

[236] Nancy S. Kim, Consentability: consent and its limits (Cambridge University Press 2019)
[237] ibid Selinger and Hartzog.
[238] ibid.
[239] Benjamin Hale, 'Identity Crisis: Face Recognition Technology and Freedom of the Will' (2005) 8 Ethics Place and Environment, 141.

Compared to the prisoners in Bentham's panopticon, there is no denying the fact that a free person has more autonomy. There are more sources of influence outside of the prison than inside, despite this he has more autonomy. It is because at the same time a person outside has more choice between the sources of influence. This gives a false sense of being free. Inside the prison, there is strong direct influence which is spread among a few prisoners in a confined space. Outside of the prison, the influences are spread among a greater number of people, so the force of any single influence is less. Therefore, by limiting the number of influences, a person's autonomy is limited because of his limited choices.

For example, a person is free to decide when he wants to sleep. In a prison, assuming, there is a routine that all the prisoners should go to bed by eight in the night. But it is not necessary that everyone is going to sleep by eight. Some may just lie in their cell looking at the walls and decide to sleep by nine. So, the prisoners still have autonomy to decide when they want to sleep but as there is no television or other activities to influence the prisoners to stay awake, in most probability, they will try and sleep by eight.

A free person on the other hand also has autonomy to decide when he will sleep. Nobody dictates the time when he is to go to bed, like in a prison, and he may have a television, or other sources of influence, to keep him awake at night in his home. Even then he will have an approximate time when he goes to bed. Not as strict as a prison nevertheless he has. That probability is dependent on what time he must go to work in the morning.

So, there is not much difference between the two groups of people. In spite there being more things to influence a free person from going to bed, he feels freer than a prisoner. Therefore, by influencing a person through knowledge gained from visual information, he is given more choices and hence increasing his degree of freedom. He may act upon the influence or ignore it; the choice is his.

If he is given more freedom to choose then what is the issue? The issue is the inequality between the influencer and the influenced. But that inequality is necessary to exert an influence. If an individual knows what the corporations know about him then there would be no influence. We are influenced by nature because there is inequality. The only way to beat this inequality is by making rational choices. Sometimes we are so overwhelmed by the influence which leads to irrational choices being made.

3.4.1.2. On behaviour

Behavioural monitoring is another area that will have an impact. Not for the simple reason that knowledge can be gained from the visual information but because processing, and analytics of visual information has become sophisticated. Machine learning and predictive analysis will have dangerous consequences for an individual.[240] Therefore, a more in-depth knowledge is gained compared to a plain looking. For example, if it can be deduced whether an individual is gay or straight from a photograph, we can

[240] Sandra Wachter and Brent Mittelstadt, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' (2019) Issue 2 Columbia Business Law Review.

conclude that visual analysis is truly advanced. Apart from the few, like object recognition, who knows what else we could infer from visual information that a normal person would not guess. And true behaviour analysis can only be made without disturbing the subject, which is in the DNA of drones.

Pervasive surveillance by drones will also have a chilling effect on individuals.[241] Chilling effects are basically behavioural changes when one knows that he is being watched, and which effects the overall autonomy of an individual.[242] The chilling effect is not only limited to individuals but also extends to the society collectively.[243] The chill from visual surveillance by drones, can also be used as a tool for social control.[244]

3.4.1.3. On Psychology

Due to the panoptic affect, the psychological impact of drone use cannot be belittled. There have been a few experiments in this field which explains the impact of a watchful eye.[245] One such experiment was undertaken at Newcastle University's campus.[246] The high incidence of bicycle theft was the subject of the study. Images of eyes were placed at three locations with the highest

[241] For a more exploratory reading on chilling effects see, Jonathon Penney, 'Chilling Effects and Transatlantic Privacy' (2019) 25 European Law Journal 122.
[242] ibid.
[243] ibid.
[244] Daniel J. Solove, 'A Taxonomy of Privacy' (2006) 154 University of Pennsylvania Law Review 477.
[245] See for example, Arthur L. Beaman and Others, 'Self-Awareness and Transgression in Children: Two Field Studies' (1979) 37 Journal of Personality and Social Psychology 1835.
[246] Daniel Nettle and Others, 'Cycle Thieves, We Are Watching You: Impact of a Simple Signage Intervention against Bicycle Theft' (2012) 7 PLoS ONE.

number of theft while other locations remained as control locations. It was found that by just placing the sign with images of eyes reduced the number of bicycle thefts in the three locations. However, it was also found that there were increases in the number of thefts in the control or other locations. What this means is that the crime shifted to other locations where there were no images. Therefore, it is no secret that under observation people tend to behave. They tend to be less socially aberrant. Drones will affect the psychology of people in a similar manner. But how far will drones curb the normal behaviour of people cannot be determined with certainty. We can only estimate by how it has been affected using other PITs.

Therefore, actual observation is not even necessary to change behaviour. Going by the logic of the experiment at Newcastle University, to influence psychology, a dummy drone would be enough. A dummy drone would be a drone without a camera or other imaging sensors. Dummy drones may make persons feel psychologically, that visual privacy is being or has been invaded, but in fact, it has not.

3.4.2. Impact due to the inherent nature of visual information

How is visual information's impact different from other information? Micro information can monitor behaviour, affect a person's autonomy, and influence choice as well. However, visual information is more expressive and capable of influencing to a greater extent. Telling someone that his/her spouse is having an

affair will have less of an impact than a photograph depicting them having an affair. If it is coloured, as against a black and white photograph, its impact on the human senses is even more conspicuous. Therefore, while it may take time to deduce the behaviour of an individual from micro information, it is instantaneous from visual information. Due to this, people are more reserved when it comes to the invasion of visual privacy, than invasion of privacy by other means.

But people are also voluntarily sharing more visual information than ever before. From that it cannot be fully inferred that people are not concerned about their visual privacy. The only way to make sense of these contradictory statements is to assume that the umbra within which people cherished visual privacy has reduced thereby increasing the penumbra. This reduction is due to many reasons like a change in cultural patterns. By far the most important being technology which assists in collection and dissemination of visual information. The more sharing of visual information may also be to a defined set of people.

Aside from the influence that a person can assert, visual information itself has value, more so in this technology fuelled age. In the past, identification was necessary in addition to the facial identity. People have passports to aid in the identity of their person. If a stranger joyfully walked up and said that he was Jack, then he may be Jack. But together with his introduction if he showed his passport mentioning that his first name is Jack then it is certain he is Jack. But we are gradually moving away from this alpha numeric

assistance in aiding identity. The face and its features have become the sole criteria in identifying a person. It is the key to unlocking electronic devices and passing identity checks. Therefore, the value in pure visual information has increased. This increase in value means that it needs to be safeguarded more than ever before. Identity theft was the most breached data according to 2016 global internet report of the internet society.[247]

3.4.3. Impact on information storage

It is a known fact that storage capacities have increased. To store recorded visual information (an image or a video file) requires more space as compared to alphanumeric information (a word file). There was a time when floppy disks were in use. They had limited storage capacities and were used to store alphanumeric information. It would be meaningless to generate so much of visual information if there was not enough space to store them. The human journey through the field of storage technology has taken us from magnetised tapes, compact discs, digital video discs, hard drives, solid state drives to electronic memories.

We generate so much of visual information nowadays that we have moved to the cloud. This has also allowed the information to be available at one place no matter who the individual. Before that, the information was scattered in individual hard drives or other personal storage devices. Therefore, the pattern of ownership is

[247] See page 41, 'Global Internet Report 2016 – Internet Society' (Internetsociety.org 2016) <www.internetsociety.org/globalinternetreport/2016/#first-d> accessed 19 November 2017.

changing. We are no more the owners of the storage medium although we still own the content. The storage medium is owned by corporations and they are in possession of all our visual and alphanumeric information. So, when we upload pictures to Facebook it is being stored in the company's servers. But we trust them. By this we can assume that corporations exude confidence. Similarly, the visual information collected by drones may be stored in the camera's electronic memory or transferred to the cloud. The amount of visual information generated by drones will surpass anything that we know of today. This will have a major impact on the information systems responsible for the management of data.[248]

Google recently announced, that it was changing its policy towards unlimited photo storage, by restricting the amount of space an individual could use on its platform, due to the massive amount of 28 billion new photos and videos uploaded to its platform every week, which is unsustainable for the long run.[249] If the cloud is running out of storage, we must find a new medium to store visual information.

[248] '7 key considerations before your UAS operation takes to the sky' (Virtual Air Boss) <www.virtualairboss.com/7-key-considerations-before-taking-your-drone-operation-to-the-sky-data-management/> accessed 5 January 2018.
[249] Google photos abandons unlimited uploads amid storage changes (BBC November 2020) < https://www.bbc.com/news/technology-54919165> accessed 15 November 2020.

4. VISUAL PRIVACY

While the previous chapter dealt with the elements of visual privacy invasion by drones, this chapter will explore the concept of visual privacy and what it means. As rightly stated by Pinterest founder, Ben Silbermann, ‘A lot of the future of search is going to be about pictures instead of keywords.’ Due to this fundamental change, we need to understand privacy from a new perspective, that is visual privacy. As ultimately, what keeps things private are the human senses. The ever-growing environment of civilian drone use, surveillance, the use of facial recognition technologies, and the collection and combining of visual information from different sources for further use, strengthens the need to understand visual privacy.

4.1 Introduction

A lot can be said by looking at a person’s face. Not just the normal information that one would gather, like mostly, the identity, ethnicity, race, sex, colour, appearance but also their intricate emotions, like, anger, happiness, confusion, grief, and other natural human expressions. These are visual indicators or markings. However, one should not judge the book by its cover as these indicators can be deceptive sometimes.

The first thing that comes to mind, when talking about the word visual, is a pair of eyes, where images are processed and stored in the visual cortex (the part of the brain responsible for storing visual information). Eyes are a biological camera which has evolved through millions of years, perfecting itself, much like the modern-day cameras,[250] the only difference being the permanence in the recording. While a person takes with him his faded memory, digital footprints are not prone to fade and are difficult to erase.

To a blind, lacking in eyesight, these visual markings are absent as they are unable to visually perceive the world around them. Although unable to perceive visually, there are still other senses of perception, the four other traditional senses. For example, by touching a chair a blind person can identify the chattel by going through its shape, by listening to the waves he can ascertain how close he is to the sea and if he knows the smell or the taste of a mango, he can identify the fruit by smelling or tasting it.

Therefore, a person's image is not the only kind of visual data through which a person can be identified. Images of vehicle license plates, or a house or of personal belongings can easily be identified

[250] The late 1800s was a pivotal moment in history with the invention of the camera or more precisely, rolled film. In 1888, George Eastman invented film that could be put on a spool, preloaded in easy-to-handle cameras, and sold much like today's disposable cameras. The technical innovation of this new film and packaging allowed for cameras to become more portable, and thus allowed more people access to becoming 'Kodakers' or photographers. These technical advances also allowed photographers to include people who did not necessarily desire their behaviour to be captured on film. In other words, it allowed for the mass invasion of visual privacy.

to an individual, given the proper processing tools, an outcome that artificial intelligence has facilitated.

Thus, visual privacy is keeping away unwelcomed observations, the ability to be obscure, subject to reasonableness, from natural persons and imaging technologies, of personal physical visual information, and their subsequent recording, publishing, and further use.

Privacy has been discussed from many perspectives, like, data privacy, privacy as a fundamental right, privacy as a right to be let alone,[251] privacy as the claim of an individual to determine what information about himself or herself should be known to others,[252] privacy as an intrusion upon a person's seclusion or solitude,[253] privacy as building intimacy,[254] privacy as our concern over our accessibility to others,[255] privacy as contextual integrity,[256] and many others. The problem with having so many concepts, as stated by Daniel J. Solove,[257] is that privacy has become a concept in disarray.

To overcome this disarray, a suggested solution would be to shift the existing concepts into a concept dictated by the human senses, for example, visual privacy for the sense of sight and aural privacy

[251] Samuel D. Warren and Louis D. Brandeis, 'The Right to Privacy' (1890) 4 Harvard Law Review, 193.
[252] Alan F. Westin, Privacy and Freedom (New York: Athenum 1967).
[253] William L. Prosser, 'Privacy' (1960) 48 California Law Review 383.
[254] Julie C. Inness, Privacy, Intimacy, and Isolation (Oxford University Press 1992).
[255] Ruth Gavison, 'Privacy and the Limits of Law' (1980) 89 Yale Law Journal 421.
[256] Helen Nissenbaum, 'Privacy as Contextual Integrity' (2004) 79 Washington Law Review.
[257] ibid Solove, 'A Taxonomy of Privacy'

for the sense of hearing. The existing concepts can be accommodated, without any friction, into a concept based on the human senses, because, ultimately, privacy boils down to whether it has been perceived by the human senses. If that is unworkable, then privacy needs to be studied from a new perspective, which is visual privacy, in addition to the existing perspectives. Emerging technologies like drones, facial recognition, and health imaging point towards its necessity. There is extant literature discussing visual privacy, but it is little and scattered.[258] The discussions if any on this topic has been treated as interdisciplinary research involving, law, sociology, architecture, anthropology, information technology and a few others, cited throughout this section.

Although Louis and Brandeis are said to be the first to recognise the right to privacy, as known in the western world, it existed and was recognised in many forms in many different cultures across the world, even prior to the publication of their seminal article in the Harvard Law Review. For example, visual privacy was practised in India since time immemorial in the form of the *'Parda'* system, even before British colonialism.[259] It will be futile to dig into the origins of visual privacy, or privacy in general, because it will be

[258] For example, Seth F. Kreimer, 'Pervasive Image Capture and the First Amendment: Memory, Discourse, and the Right to Record' (2011) 159 University of Pennsylvania Law Review 335; Bert J. Koops and others, 'The Reasonableness of Remaining Unobserved: A Comparative Analysis of Visual Surveillance and Voyeurism in Criminal Law' (2018) 43 Law and Social Inquiry 1210; Sarah Brayne, Karen Levy, Bryce Clayton Newell, 'Visual Data and the Law' (2018) 43 Law and Social Inquiry 1149.

[259] Tasneem Chowdury, 'Segregation of Women in Islamic Societies of South Asia and its Reflection in Rural Housing - Case Study in Bangladesh' (1993) McGill University Student Thesis; Elizabeth H. White, 'Purdah' (1977) 2 Frontiers: A Journal of Women Studies 31.

misleading. With so many forms of its existence in different cultures over a long time-period and known by different names in different languages, one is bound to not cover it properly. The reasonable thing to do will be to discuss it in relation to the present times.

4.2. Determinant factors of visual privacy

A few factors have been identified and consolidated that determine visual privacy or its standards. The influence of these factors on visual privacy is unquestionable. One or more factors may overlap but they can be treated separately as they can stand on their own. Broadly, it is the thread of culture that influences most of the factors mentioned below. However, admitting early on, that this list is not exhaustive and there may be other factors that have an influence which have not been identified.

4.2.1. Culture and Architecture

Culture plays an important role in determining the extent of visual privacy. Culture is defined as the ideas, customs, and social behaviours of people or society.[260] We can say that privacy is culturally common as well as specific.[261] It means that a woman living behind a curtain (a Pardanashin woman) is culturally specific,

[260] 'Culture | Definition of Culture in English by Oxford Dictionaries' (Oxford Dictionaries | English) <https://en.oxforddictionaries.com/definition/culture> accessed 4 May 2017.
[261] Irwin Altman, 'Privacy Regulation: Culturally Universal or Culturally Specific?' (1977) 33 Journal of Social Issues 66.

and a woman wanting to control access to her bedroom is culturally common.

It is common knowledge that India was once a part of the British Empire. The system of laws introduced in India during the time was the common law prevalent in England. But the law as imported from England did not always meet the needs of the people back in India. The culture in India and England were different. In *Gokal Prasad v Radho,*[262] which dealt with a case of visual privacy of Pardanashin women, Justice Mahmood remarked, '[…] the parda system prevails alike among Hindus and Muhammadans, and that both these sections of the community by immemorial usage and custom, regard invasion of privacy as actionable […] that the importation of the English law, as to the invasion of privacy being un-actionable, is not only not justified, but positively opposed to the customs, habits, and conditions of life of the populations […]. Even in Europe, countries whose principles of law are derived from or founded on the civil law recognise invasion of privacy as an actionable wrong […]'.[263]

In this case, the Plaintiff alleged, that the Defendant had built a new house in such a way that a veranda and certain doors of that house, interfered with the privacy of the portions of the Plaintiff's house which were occupied by Pardanashin women of the Plaintiff's family. The Plaintiff wanted the veranda removed and the doors

[262] Gokal Prasad v. Radho, (1888) 10 Indian Law Reports Allahabad Series, 358-389.
[263] ibid 388; also see, Courtney Stanhope Kenny, A Selection of Cases Illustrative of the English Law of Tort, Fifth Edition (Cambridge University Press 1928) 367.

closed of the newly built house of the defendant, to protect the visual privacy of the female members of his family. The court while holding, that the plaintiff had enjoyed his privacy before the new house was built by the Defendant, and as the new house materially interfered with the visual privacy of the Pardanashin female members of the Plaintiff's family, allowed the Plaintiff's application.

The ideas, customs and social behaviours are manifested in various forms, such as accessibility and architecture. This is evident in housing designs and access or restricted access to one another.

The *Mehinaku* are an indigenous tribe which reside in central Brazil.[264] As evidenced in literature, their social structure is totally transparent when looked at from the outside. They have communal huts which are shared by families.[265] But no family encroaches upon the living area of another, although, visible to one another.[266] However, during the birth of a child, the mother, father and the child remain behind a wooden plank in their living area, visually isolated from the rest.[267] This is an instance of visual privacy which supposedly, fosters intimacy among the members of the family. Visual privacy was also observed in the Mehinaku Indians, when boys and girls reached the age of puberty.[268] They were kept isolated in a hut behind wooden planks for one to two years.[269]

[264] ibid Altman 72.
[265] ibid Altman 73.
[266] ibid.
[267] ibid.
[268] ibid.
[269] ibid.

Reaching the age of puberty is also celebrated in other cultures, a sing of maturity and a reason to be more responsible.

In the Japanese culture, visual privacy is prioritised. One can see light weight semi-transparent moveable screens and partitions, made from wood and paper, which allows the passage of light but blocks the detailed shape of a person on the other side of the screen.[270]

In traditional Islamic homes, residential visual privacy is explicitly guarded. The homes are inwardly facing, having a courtyard, while the outer walls have no windows.[271] Even when the windows are at a height they are covered by wooden screens where the outside world is visible to the women of the house but the inside world of the women is protected from the outside glaze.[272] In Seyhulislam Feyzullah Efendi's (1639-1703) fatwa collection, in fatwa number 2481, he argues that 'if the window of a newly built second floor room overlooks the neighbouring house's women's quarter and if the responsible party has already put a wooden curtain to block his illegitimate view, then the other party cannot force him to wall the window.'[273]

[270] 'Housing in Japan' (En.wikipedia.org) <https://en.wikipedia.org/wiki/Housing_in_Japan> accessed 4 May 2017.
[271] Kheir Al-Kodmany, 'Women's Visual Privacy in Traditional and Modern Neighbourhoods in Damascus' (2000) 17 Journal of Architectural and Planning Research 283.
[272] ibid.
[273] Ali Sipahi, 'Window-Conflicts in the Ottoman Empire and Turkey: Visual Privacy, Materiality and Right to the City' (2016) 52 Journal of Middle Eastern Studies 588.

Buildings with terraces have been common throughout history across cultures which restrict visual privacy. Therefore, climate plays a part in determining the amount of visual privacy standards in housing designs. People living close to the equator or on a hot geographical belt will tend to have more open houses as evidenced in Malay housing designs.[274]

The European culture is very individualistic in nature and values visual privacy. Their residences are protected by walls, doors, and fences to prevent visual or auditory invasion. They usually have large windows and balconies so one may believe that they are open to visual intrusions, but that line of thinking could not be more wrong as is evident from image rights in Europe. Dutch people have windows facing the street and rarely use curtains, if at all, giving a passer-by a complete anatomy of their living area.[275] On the other end of the spectrum the architectural styles of southern Europe enhance visual privacy. For example, the Moorish style of architecture, which has influenced Spain and Portugal, have courtyards similar to the Islamic culture.[276] Germany's interior minister, Thomas de Maizière, in the year 2010 had invited politicians, regulators and technology companies to diffuse a tension that had resulted when Google announced that it would

[274] Zaiton Abdul Rahim, 'The Influence of Culture and Religion on Visual Privacy' (2015) 170 Procedia - Social and Behavioural Sciences 537.
[275] Hilje Van Der Horst and Jantine Messing, 'It's Not Dutch to Close the Curtains' (2006) Volume 3 Home Cultures 21.
[276] 'Moorish Architecture' (National Geographic Society 2012) <www.nationalgeographic.org/media/moorish-art/>.

introduce its street view service in 20 largest cities in Germany.[277] The tension was a result when citizens protested against their residential buildings from being photographed.

Residential architecture and housing designs are culturally private spheres of activity but even in the public sphere the importance of visual privacy is evident from modern office designs.[278] Organisations which require more demanding work from their employees requiring them to use a lot of intellect usually have partition style offices like in law firms and universities, and organisations that demand less have more open office settings such as call centres. Open offices with no partitions afford the least visual privacy; open offices with cubicles generally afford more visual privacy and corridor style offices which consist of rooms on either side of the corridor, afford the maximum visual privacy. Modern cubicle office allows for personal space, for the occupants of the office. One of the functions that a modern cubicle office accomplishes is to give visual privacy to an occupant of a cubicle from the other occupants of the office. This allows for a greater degree of isolation and the personal development of each of the occupant of the cubicles.

[277] 'No pixels, please, we're German' (The Economist 2010) <www.economist.com/node/17103679> accessed 14 October 2017.

[278] The ideas in this paragraph have been taken from a few scholarly texts on workplace privacy and office designs. Some of my references are, Teresa A. Bellingar and V. Kupritz, 'Privacy Matters' (Workwellpartners.com 2011) <https://workwellpartners.com/wp-content/uploads/2014/10/privacy-matters1-pdf-28565.pdf> accessed 7 November 2017; Virginia W. Kupritz, 'Privacy Management at Work: A Conceptual Model' (2000) 17 Journal of Architectural and Planning Research 47-63.

One may contend that it is wasteful expenditure and that open offices without cubicles provide the same amount of personal development. This can be argued, however, cubicles do help in increasing the levels of concentration of the occupants, as there are lesser disturbances. The reason for this statement is that there are lesser interactions and distractions among the occupants of the cubicles, than, when people work in a fully open office. Now the amount of visual privacy will depend on the height of the panels. If the panels are short it will not serve its purpose and if the panels are too high it might give a feeling of solitary confinement and hamper the controlled interpersonal interactions between the employees, which will have a negative effect on productivity. So, the optimum height must be maintained in order to serve the purpose of office productivity, which being, the average height of a man.

However, these cubicles do not have doors, but certain occupants in the offices are given this privilege, such as the CEOs', and Managers. They occupy areas of the office which are enclosed on all four sides which run from the floor to the ceiling, have opaque windows, and these enclosures have doors which can be shut to give the person sitting inside the enclosure, total visual privacy.

Why don't all the occupants of the office have similar enclosures? The answers lie in the control of interaction or interpersonal relationship between the occupants of the office. It is generally agreed that Managers need to take important decisions or work with information which might not be suitable for everyone to see, moreover, they have to monitor other employees and having

frequent interaction with them will lead to the breakdown of their privileged relationship with their employees and for that reason there is a need for greater visual privacy for Managers to maintain their authority, for if he is too visual, somehow, psychologically, his authority diminishes among the occupants of the office.

Architectural styles are distinctively regional, based on local culture and customs. But on account of the mixing of cultures there has been a lot of mixing of architectural styles as well. For example, we can see Persian architectural styles in India, such as, the Taj Mahal. But as the world is getting smaller (metaphorically), architecture has taken on a global style. A global style is where the distinctiveness based on cultures is fast vanishing and architecture in the different cities look more alike. For example, Dubai an Islamic city in the Middle East has high rise buildings with shiny exteriors made of glass (which makes the inside more visible to a drone irrespective of the height) common in North America. This is also true of architectural styles of international airports (which have the same construction style no matter from which city the flight is boarded), hotels, office designs and departmental stores, all follow the same pattern. Therefore, due to the mixing of culture and architectural styles, the standard of visual privacy is levelling up.

An interesting scenario with respect to visual privacy emerges when two cultures collide. The contention being, that it could lead either to the enhancement of visual privacy or the reduction of visual privacy, depending on whether the dominant culture is liberal or strict. This can happen when there is an annexation or a voluntary

mixing of cultures. Voluntary mixing of cultures can happen when cultures mix on account of trading with one another. In the event of a forceful takeover of a culture and if the dominant culture is morally strict and repressive, in most probability the passive culture, even though liberal, will have to adhere to the standards of visual privacy imposed by the dominant culture. For example, Islamic culture stresses on the visual privacy for women, and assuming they take over a culture which allows its women personal autonomy in clothing and societal interactions, then, the liberal culture will have to adhere to the standards imposed by the dominant culture, thereby, reducing the personal autonomy of the people of the liberal culture, which will include visual privacy for women. On the other hand, when cultures mix voluntarily, in this instance when two cultures mix on account of trading with one another, the level of visual privacy may remain the same, each culture adhering to its own standard of visual privacy, or it could lead to a total disregard for visual privacy as both cultures are treated equally. In such a scenario, the liberal culture could imitate the stringent culture and vice versa.

But when the mixing is not voluntary nor by annexation, for example, people migrating from one culture to another, or from one city to another or from one neighbourhood to another, with differential visual privacy standards, looking for work or other employment, will the migrating culture be looked with suspicion and abhorrence? In such a situation two levels of visual privacy could coexist in a society with a degree of animosity against the migrating culture. The French example of the ban on *burqa* is apt to

describe the situation, where Islamic women wear a burqa when out on French streets while French women, from a more liberal culture, wear more revealing clothes. But cultures and the prevalent society norms may undergo transformations, overtime, resulting in less concern about visual privacy.

A study was undertaken by Kheir Al-Kodmany wherein he discussed women's visual privacy in traditional and modern neighbourhoods in Damascus, Syria.[279] This study argued that when women migrated from the traditional villages to Damascus, Damascene women needed more privacy, in other words, their desire for visual privacy increased as women from other traditional villages moved to Damascus. This argument was supported by the fact that the original women inhabitants of Damascus had a reduced interaction with women from traditional villages and other cities. They tended to spend more time at home. While the other side of the argument, was, that the need for visual privacy was reduced because of the mixing of women, from other cities and villages with the women from Damascus as interactions between them increased in schools, universities, and workspaces. The writer concludes, after basing his arguments on several parameters, like, whether the women preferred inward facing homes or outward facing homes, whether they preferred a front yard to a courtyard, whether they preferred windows facing the street or windows facing the courtyard, that women in general, whether Damascene women or from traditional neighbourhoods, preferred a good amount of visual privacy no matter from where they came from.

[279] ibid Kodmany.

4.2.2. Religion

There is a lot of similarity between religion and culture. Culture is influenced by religion and vice versa. Dress codes are a prime example where the influence of culture and religion are both existent. Religion can be said to be a subset of the culture they represent.[280] The intention here is not to favour any religion or to ridicule another. Major religions of the world have played an important role in the development of the social norms they were a part of. They play an important role in determining visual privacy standards. Islam stresses on visual privacy. It is moral for women to cover up and for men and women not to gaze at each other. For an Islamic woman it is moral for her to reveal herself only to her husband, and to a lesser extent, to her close family members. This is still in practise in many Islamic countries. Islam also gives importance to residential visual privacy, as evidenced in housing designs. In an authentic hadeeth Prophet Mohamed said, 'He who looks into another's house without the occupant's permission and they puncture his eyes will have no right to demand a fine or ask for punishment'.[281]

Covering up is also the norm in Christianity where nuns cover their hair with a veil. The female hair is a sign of femininity and it is required of them to cover to maintain their modesty. Flaunting is looked like a sign of vanity. Christianity is associated with western

[280] Inna Reddy Edara, 'Religion: A Subset of Culture and an Expression of Spirituality' (2017) 07 Advances in Anthropology 273.
[281] Sabir bin Nabeeh Nu'man, 'A Unified Architectural Theory for Islamic Architecture' (2016) 10 International Journal of Architectural Research: ArchNet-IJAR 100-112.

ideas, society, and values. In Genesis, chapter 3, verse 7, it is mentioned, about Adam and Eve, 'Then the eyes of both of them were opened, and they knew that they were naked; and they sewed fig leaves together and made themselves loin coverings.'[282] Covering one's private parts is an instance of visual privacy and it is moral because exposing oneself may lead to unnecessary sexual distraction, a form of mind control.

When Christian missionaries and colonialists travelled to far and distant lands, and came across tribes where the women were bare chested, where people had no sense of their nakedness, they passed their idea of morality and dress codes, on to the tribes, which is evident in many literatures.[283] The once tribal belt of Northeast India was influenced by the Christian missionaries.[284] It is not that the tribes did not have a moral conduct but that the missionaries thought of their level of visual morality, to be inadequate.

The Jewish religion is replete with instances of visual privacy. It even has a term for visual privacy, which is, 'hezek r'iyah'. The Mishna,[285] in Baba Bathra (60a), says that 'one should not create a new doorway or window which faces one's neighbour's door or

[282] '6. Paradise Lost (Genesis 3:1-7)' (Bible.org) <https://bible.org/seriespage/6-paradise-lost-genesis-31-7> accessed 8 May 2017.
[283] For example, W.W. Hunter, The Indian Empire: Its People, History and Products (Routledge 2000) 56.
[284] H.K Barpujari, The American Missionaries and North-East India, 1836-1900 A.D. (Spectrum Publications 1986).
[285] The term Mishnah is used in many ways but when used as a proper noun 'The Mishnah,' it designates the collection of rabbinic traditions redacted by Rabbi Judah ha-Nasi at the beginning of the third century CE. Mostly written in Hebrew, it is a code of Jewish law which together with the Gemara, makes up the Talmud. Refer to <www.jewishvirtuallibrary.org/mishnah> for more information, accessed on 8th May 2017.

window on the opposite side of the courtyard'.[286] The Rashbam[287] explains that the requirement to stagger windows and doorways so that they should not face each other stems from the need to preserve visual privacy.[288] When doors or windows face the street privacy is disturbed, by the passers-by, who can see into the house.[289] Therefore, no private activities are performed in front of the window.[290] A commentary by Rema,[291] in the Shulchan Aruch (Choshen Mishpot 154:7), adds that it is forbidden to stand at the window and look into the neighbour's courtyard, 'lest he harm him by looking.'[292] The herem (ban) of Rabbenu Gershom Me'or Hagolah (Germany, 960-1028), a reputed author of a series of takkanot–rabbinic enactments, governing various aspects of Jewish life, in one of the takkanot attributed to him, says that, 'One should not read his friend's letter' and some versions add, 'without his knowledge and without his permission.'[293]

---

[286] The 'Talmud' (Halakhah.com) <https://halakhah.com/pdf/nezikin/Baba_Bathra.pdf> accessed 31 October 2017.

[287] It is a Hebrew acronym for Rabbi Shmuel Ben Meir who was a leading French commentator on the Talmud. For more information refer to 'Rashbam' (En.wikipedia.org) <https://en.wikipedia.org/wiki/Rashbam> accessed 8 May 2017.

[288] Rashbam's commentary on Baba Bathra (60a).

[289] Baba Bathra (60a).

[290] ibid.

[291] Moses Isserles is commonly referred to as Rema. An eminent Polish Rabbi, he is known for his notes to the Shulchan Aruch by Yosef Karo.

[292] Michelle Finneran Dennedy, Jonathan Fox and Thomas R Finneran, The Privacy Engineer's Manifesto: Getting from Policy to Code to QA to Value (Apress 2014) 5.

[293] 'First Legal Recognition of Privacy: Mishnah, the code of Jewish law' (Guarding Data 2014) <https://guardingdata.wordpress.com/2014/01/10/first-legal-recognition-of-privacy/> accessed 11 May 2017.

However, as we see the decline of religiosity around the world, due to the importance accorded to science and liberal education, we see that the need for visual privacy has been greatly reduced. The strict standard of visual morality, according to religions, has been overcome, and men and women do wear revealing clothes without being shamed. This is more evident in western countries, as social changes, due to scientific findings, have had a greater effect on the people and shifted them from thinking in the direction of God and morality to thinking in a more liberal and scientific direction. The numbers of atheists are increasing, and their thought process is becoming free from the chains of religious morality.

4.2.3. Affluence

Affluence can be defined as a state of having a great deal of money and overall wealth.[294] Generally, wealth and religiosity are not proportionate to one another, since the richer a person is, the lesser religious he is going to be[295] and, as discussed, religion plays an important role in determining visual privacy standards. Taking this reasoning, rich people are less religious and because they are less religious, they have liberal visual privacy standards. However, this might not always be the case, as there is more visual privacy to be found in affluent societies and neighbourhoods than compared to

[294] Cambridge and Oxford Online Dictionaries.

[295] Pew Research Center 2008 <https://www.pewresearch.org/wp-content/uploads/sites/2/2008/09/Pew-2008-Pew-Global-Attitudes-Report-3-September-17-2pm.pdf> accessed 1 November 2020; Kazi Stastna, 'Do countries lose religion as they gain wealth?' (CBC News 2013) <www.cbc.ca/news/world/do-countries-lose-religion-as-they-gain-wealth-1.1310451> accessed 8 November 2017.

poor societies and neighbourhoods. One of the reasons is the density of the population.

Property prices in affluent societies are more expensive than poorer societies. As a result, fewer people can afford a home in affluent societies. For example, in Bangladesh, the population density is so high that the amount of visual privacy available to people living there will be minimal, due to overcrowding. Historically, the abundance of resources was the reason for the flourishing and later the overcrowding of regions like ancient Mesopotamia and the Indus Valley Civilisation. Contrast that to northern Europe where the density of the population is less which results in greater visual privacy, whether it is desired or not is another concern. But overcrowding also makes the land scarce and a percentage of the people who want more visual privacy in those crowded neighbourhoods or regions must work harder to acquire more land and space to reign in the disappearance of visual privacy. This will result in the prices of land skyrocketing as there is not enough for everyone to have a decent amount of spatial privacy. As a result, there is an emergence of affluent and poor neighbourhoods in the same society.

The point being that people living in affluent neighbourhoods have a greater degree of visual privacy, despite being less religious due to modern education, and, therefore, caring less about visual privacy. In such cases the visual privacy is a by-product of wanting a larger space to live. In ancient times women of royalty covered themselves when going out in public from the glances of the commoners. It was

a status symbol and it existed in all cultures. This is analogous to the people living in affluent societies and neighbourhoods. As the saying goes, one should resist washing dirty laundry in public. It is only the rich who can afford to hide their dirty laundry.

The slums in India are so overcrowded that there is hardly any space between two dwellings. Families living in these slums get little to no visual privacy. It is not unusual that a room in a house in a slum could be shared by up to five people or more. The only way these people can maintain visual privacy is by maintaining good neighbourly conduct. Good neighbourly conduct in general reduces the need to have more visual privacy as a person gets more comfortable with the people surrounding him. He starts trusting others with his visual privacy. People in affluent societies experience isolation and loneliness because of high amount of visual privacy. But people living in high societies prefer this sort of isolation as they have a lot to hide and maintain their expensive reputation. In poorer societies or people living in the shanty towns, have nothing to hide, so even if they are uncomfortable with low levels of visual privacy and desire moving to a neighbourhood which secures them the desired levels, this does not impede their functioning.

Another characteristic of poorer societies are that high-rises and shanty towns co-exist in the same area. This further reduces the amount of visual privacy available to the people living in the shanty towns, as they are over exposed. Their daily chores, like washing, cleaning, and cooking become visible to the people living in the

high rises. To give an example, a person standing at the top of a minaret and looking down has a bird's eye view of the events unfolding beneath him. At such heights he may be a witness to a stabbing or a pickpocketing although the person committing the crime assumes no one is watching.

4.2.4. Gender

Throughout history, we have seen that social power has rested in the males, in most societies, termed by some as the patriarchal system.[296] It is a system where, moral authority, property ownership, and social privileges are mostly enjoyed by the male members; it is they who decide what is permissible.[297] Gender based visual privacy exists across cultures, to a lesser or to a greater degree. In other words, gender based visual privacy exists regardless of culturally based gender visual privacy.

Under the Medieval English law, women were considered the chattels of men having no independent identity.[298] It is the dominance of the male gender over the female gender which is partly responsible for deciding what an appropriate dress code is for women. Why the male gender is more dominant, has to do with their physical traits. There is no shame for men to expose their chest, but it will be highly inappropriate for women to walk bare bosom.

---

[296] Craig A. Lockard, Societies, Networks, and Transitions: A Global History, Volume I: to 1500 (Houghton Mifflin Company 2007) 111-114.
[297] ibid.
[298] Claudia Zaher, 'When a Woman's Marital Status Determined Her Legal Status: A Research Guide on the Common Law Doctrine of Coverture' (2002) 94 Law Library Journal 459, 459-486.

In medieval societies or where morality was adhered to stringently, covering up the skin, particularly applicable to female members of the society, was the norm. This fact is evident across societies with small variations. In some societies, the covering up extended to the face, where women were obliged to ensure that no male, outside the family, could see her facial symmetry. For example, women of the *'Marwari'* caste in India had to cover their faces (traditionally known as a *Ghoonghat*), with a saree in the presence of a male stranger, similarly, a burqa is a dress adorned by some Muslim women which covers them from head to toe when they are out in public.

In modern societies, however, particularly in the western world, women are given much leeway in terms of personal autonomy. It is more egalitarian than in the past. In this respect tribal primitive societies are egalitarian in terms of dress code, where there are many instances, where men and women do not cover their chest, let alone their faces.

The shape of a female's body is another visually sensitive data, as males are biologically programmed to get attracted towards the opposite sex. In some societies it is a taboo to wear a dress which reveals the curves of a female body and instead they resort to wearing gowns, much like the burqa, while in other societies, those norms may be frowned upon and taken as a mark of backwardness. With the advent of modernity, it became normal for women, in western societies, to flaunt their shapes and flash their skins and wear revealing clothes, like leggings, short skirts, and skin hugging

jeans, thus, in such societies the need for visual privacy reduces to a more intimate environment and activity. The reason for such liberal visual privacy norms may lie in the increased social interactions between men and women in such societies, which to state, is open-minded. So even among women the need for visual privacy will differ across societies.

The veil is not gender specific and, in some societies, it can cross genders. The *"Tuareg"* are nomadic people who live in Northern Africa and in their tribe, it is the men who cover their faces.[299] However, the reasons why they cover their faces may be different from why women adhere to coverings.

Gender specific visual privacy is not restricted to one's physical self. Critically sensitive information may have far greater repercussions on the female gender than the male gender.[300] For example, Muslim women are more culpable to the dissemination of sensitive information concerning them than their female counterparts in western societies. A letter revealing an extra marital affair will be more culpable to women than men, in general. But in Saudi Arabia the repercussions will be far greater, than say, Spain. This is because of the differences in the role played by women in both the societies. Islamic women were (the same with western

[299] Jeremy H. Keenan, 'The Tuareg Veil' (1977) 13 Middle Eastern Studies 3.
[300] See for example, Special issue on feminist data protection (Internet Policy Review) <https://policyreview.info/node/1470> accessed 10 December 2020.

women) confined to that of housekeeping and making sure that the husband was satisfied in all the senses.[301]

As some feminist scholars have advanced, privacy is more valuable to women than men, since a decision, whether to have a child or not with their partners, is crucial, as they will be the ones left to care if the husband turns out to be a waste.[302] As a decision about bearing a child is also crucial, visual privacy becomes all the more valuable to them.[303] Therefore, visual privacy, or the lack of it, is valuable for women because it acknowledges their autonomy with respect to their physical self.[304] But the same cannot be said that of a man, although he partakes in all of the above intimate decisions, because of his physical and mental makeup. It is the women who bear children and not the men.

4.2.5. Age

Age determines the standard of visual privacy. As asserted above, women require more visual privacy than men, in other words, visual privacy is gender specific. But another point to consider is that females need more visual privacy when they are younger. Psychologically, they are more conscious about their sexuality after they reach the age of puberty. It is then when they start to distinguish themselves from the boys, in other words they start to understand themselves. Sexual age of consent varies between

[301] 'Part 1: The Duties of Women' (Al-Islam.org) <www.al-islam.org/principles-marriage-family-ethics-ayatullah-ibrahim-amini/part-1-duties-women> accessed 4 May 2017.
[302] Julie C. Inness, Privacy, Intimacy, and Isolation (Oxford University Press 1992).
[303] ibid.
[304] ibid.

countries, but usually, it is within the bracket of fourteen to eighteen years. It is this period during which they must be careful about physically exposing themselves to the outside world. For example, a nude picture of a sixteen-year-old leaked online and circulated among her large circle of friends and strangers will put her into a highly emotional state of mind and damage her young reputation. Many at that age are not able to deal with the trauma of being publicly exposed. Young women do voluntary share nude pictures of themselves to their boyfriends to create intimate relationships. Sexting images are common in the digital culture and many partake voluntarily. This trust between friends is sometimes broken and the nude pictures of young women and adolescents begin to circulate on social media platforms.[305] A woman in her mid-thirties will be able to handle the matter much more maturely, although rarely women that age indulge in such behaviour.

As discussed above, culture has an important role to play, as with the case of the girls in the Mehinaku tribe when they reach the age of puberty. In Islam women must observe modesty once they reach the age of puberty. The veil is worn by women in Islamic societies and not by very young girls. However, this is the norm and variations might occur due to societal pressure. But as a person ages and the older she gets, when the hair starts to grey and the skin starts to wrinkle, many tend to let go of the restrictions that once ruled them. The Quran, in chapter 24 *sūrat l-nūr* verse 60, says, 'And the Qawa'id among women who do not hope for marriage, it

[305] Michael Salter, 'Privates in the online public: Sex(ting) and reputation on social media' (2016) 18 New Media and Society 2723.

is no sin on them if they discard their (outer) clothing in such a way as not to show their adornment…'[306] Some of the exegesis to this verse explains that Qawa'id refers to those women who cannot bear children and thus who do not hope to be married.[307]

Also, young women and adolescents are more susceptible to their visual privacy violations than a woman who is in her seventies. It is a common understanding that peeping toms will not be preying upon aged women unless they want to blackmail them for their reputation. Young women are more desirable than the old is the nature's way of making them more susceptible to visual privacy violations. It is hardly news, that women between the age brackets of fifty to seventy years have committed suicide due to the revelation of their nude pictures, but it is often in the news that adolescents and young women have committed suicide and are blackmailed because somebody has spied on their nudity.[308] This visual information whether it be tangible, or intangible serves as a bargaining chip for future misconducts. If the misconduct gets unbearable, the consequences are severe for the victim.

[306] 'Do old Women have to Wear Hijab?' (Shariahprogram.ca) <www.shariahprogram.ca/islam-qa-women/old-women-hijab.shtml>; also see, 'The Quranic Arabic Corpus – Translation' (Corpus.quran.com) <http://corpus.quran.com/translation.jsp?chapter=24&verse=60>, accessed 11 May 2017.

[307] ibid.

[308] Aina M. Gassó and others, 'Sexting, Mental Health, and Victimization Among Adolescents: A Literature Review' (2019) 16 International Journal of Environmental Research and Public Health 2364.

4.2.6. Type of activity

The need for visual privacy also depends on the daily activities. Some activities require more than the others. Bathing and natures call, for most, require the maximum amount of visual privacy. Even when people defecate in the open, in Asian countries, the need to find visual privacy is integral to the activity. In India, for example, people living in rural areas tend to hide themselves in the agricultural fields behind vegetation. If someone happens to take a train ride, they might even, unknowingly, blow their cover.

In contrast, one can see how the Ephesians defecated in communal buildings (public toilets) in the ancient site of Ephesus in Turkey.[309] Even communal bathing was common during the Roman times.[310] We may say that requiring visual privacy during bathing and natures call is a contemporary phenomenon. But then athletes in contemporary times bathe naked in communal spaces, as evident in the health clubs in the Nordic regions. It is also evident in the saunas in the cold regions. However, visual privacy achieved by the segregation of the sexes is common. Gender wise, women need more visual privacy in their activity than men for obvious reasons. Men can bathe in the open but for women to bathe in the open will attract unwanted attention. However, nudist beaches existing around the world will go against this reasoning.

---

[309] 'Ephesus Latrines (Public Toilets)' (Ephesus.ws) <http://www.ephesus.ws/ephesus-latrines-public-toilets.html> accessed 9 November 2017.

[310] 'Ancient Roman bathing' (En.wikipedia.org) <https://en.wikipedia.org/wiki/Ancient_Roman_bathing> accessed 9 November 2017.

Sleeping is another activity that requires visual privacy. Unless a person is homeless, he will have a comfortable bed in his room to sleep, and while sleeping he would like to be alone or with his spouse, with doors shut for a sound and safe sleep. It will be very difficult to sleep in a noisy crowd consciously thinking about the people watching. It is possible to dose off for a bit when extremely exhausted, but that would be it. Sleeping in dormitories one might assume that there is no visual privacy. But when the lights are turned out the darkness guarantees visual privacy.

Eating meals may not need visual privacy but still, everyone enjoys a meal with family and friends. The group may want visual privacy from strangers for the most part except on occasions when dining out. Dressing oneself requires a certain amount of visual privacy. Some people have areas allotted in their homes for this activity while others usually get it done in their bedroom or their bathroom. These are areas in the homes that allow for maximum visual privacy. Personal hygiene requires a good amount of visual privacy. Although, men can do with little visual privacy in terms of their hygiene, women need more due to their biological make up.

The occupation determines the amount of visual privacy. For example, a researcher will have to expend more lone time, as he excludes himself visually from the society, to focus on data which requires a lot of mental resources. But this sort of visual privacy is beneficial to the society as it not only increases the quality of human resources but also assists in innovation. On the other hand, a civil servant spends more time visually exposed taking care of

societal functions. A scientist on a scientific observation of the arctic, whether studying climate change and the declining habitat of the polar bears or the ozone layer, must be mentally prepared to be visually isolated for months at a stretch.

The type of activity can also be differentiated between activities that are exclusively performed in the private sphere and activities that are performed in the public sphere. Generally, visual privacy is necessary to a lesser degree in the latter than in the former because our expectations of visual privacy in a public setting are far lesser than in a private setting.

4.2.7. Technology

In no age was our visual privacy so compromised than the present age, and it can be said with some certainty, that it is only going to get worse. We are surrounded by camera electronics. Our laptops have cameras, our smartphones have cameras, and cameras surround us on the streets, in the banks, in the departmental stores, at airports, at railway stations and even at the bus stations. Cameras are carried on helicopters and airplanes. We live in an age of visual transparency.

Social networking sites are filled with personal pictures and even dating sites have personal images. They are a digital database for identification purposes, regardless of the gender. It has become easier to identify a person from an anonymous photograph. For example, by no means can a person be identified in a photograph without an information trail. So, to identify a criminal whose image has been captured by the CCTV cameras, that visual information

needs to be run against an existing police database and if there is no possible match then that image can be distributed to the public in newspapers, to help identify the person. But without help it will not be possible to know the person in the photograph, if not already known. We may know the person in the photograph if he is 'Brad Pitt' but not otherwise.

But computer algorithms have become so sophisticated that it has become much easier to obtain personal information, as they help to search the entire internet to identify a person behind the picture. But it is us who are assisting the algorithms as we voluntarily upload our personal information into the databases.

AI can guess whether an individual is gay or straight from a photograph.[311] This is information that many of us would like to keep it a secret as society and religion frown upon those who are not straight. This information is by no means shared voluntarily but adduced by AI. Deepfake internet porn bots, using AI, allow users to upload pictures of women with their attires, and returns them, with manipulated pictures of those same women naked.[312] Technology has blurred the lines between what is real and what is fake. Although manipulated, the images can be used negatively.

---

[311] Yilun Wang and Michal Kosinski, 'Deep neural networks are more accurate than humans at detecting sexual orientation from facial images' (Open Science Framework 2017) <https://osf.io/zn79k/> accessed 9 November 2017.

[312] Morgan Meaker, 'Deepfake porn bot targets thousands of women on Telegram' (The Telegraph 2020) <https://www.telegraph.co.uk/technology/2020/10/21/deep-fake-porn-bot-targets-thousands-women-telegram/> accessed 15 November 2020.

Are we supposed to hold AI liable for the infringement of our visual privacy? The answer may not be so straight forward. The user who is using the AI, in the porn bot case, should be held accountable along with the developer. But in most cases the nefarious consequences of AI will be unintentional. To whom the liability should attach in cases where machines take a decision is an evolving legal discipline.

Samsung and Apple have both introduced facial recognition technologies in their smartphones where the phone recognizes the facial symmetry of the owner with the help of the phone's camera, to unlock the phone. Facial recognition technology is also being used for payment transactions. Facebook intends to launch a facial recognition technology which helps users of their social network to log in without the use of a password, with the assistance of the device's camera. So, it has become even more important to guard visual information, like one's image, which can be used to hack into electronic devices. We cannot stop the advancing technology but what we can do is protect ourselves from their capabilities to negatively impact us, in one way or another.

4.3. The nature of visual privacy

The need for visual privacy exists in a private as well as a public space. The expectation is higher in private spaces than public spaces. Public space will include workplace and other spaces that are shared with strangers or mere acquaintances. Private space will

include spaces shared with family and loved ones such as a home. Although, as courts like the ECtHR have stressed, the difference between the public and the private sphere is getting narrower[313] (workplace tending to be more private), the distinction still exists. However, regardless of the space, the subject matter of visual privacy is a natural person directly, or indirectly through information which is capable of being visualised and attributed to a natural person.

A certain amount of personal space is therefore necessary to maintain visual privacy. We all live in houses, whether it being big or small, which have spaces allotted for different purposes, for example, a kitchen, a toilet, a bedroom, and a living room. These houses have doors and windows which, even though it varies with

[313] See, in this regard, Niemietz v. Germany, Series A, no. 251-B, ECHR 1992.: '30. As regards the word "home", appearing in the English text of Article 8 (art. 8), the Court observes that in certain Contracting States, notably Germany (see paragraph 18 above), it has been accepted as extending to business premises. Such an interpretation is, moreover, fully consonant with the French text, since the word "domicile" has a broader connotation than the word "home" and may extend, for example, to a professional person's office. In this context also, it may not always be possible to draw precise distinctions, since activities which are related to a profession or business may well be conducted from a person's private residence and activities which are not so related may well be carried on in an office or commercial premises. A narrow interpretation of the words "home" and "domicile" could therefore give rise to the same risk of inequality of treatment as a narrow interpretation of the notion of "private life" (…). 31. More generally, to interpret the words "private life" and "home" as including certain professional or business activities or premises would be consonant with the essential object and purpose of Article 8 (art. 8), namely, to protect the individual against arbitrary interference by the public authorities (see, for example, the Marckx v. Belgium judgment of 13 June 1979, Series A no. 31, p. 15, para. 31). Such an interpretation would not unduly hamper the Contracting States, for they would retain their entitlement to "interfere" to the extent permitted by paragraph 2 of Article 8 (art. 8-2); that entitlement might well be more far-reaching where professional or business activities or premises were involved than would otherwise be the case'.

culture, serve a common purpose. Assuming a bedroom which has a window faces a narrow street. When the owner of that space is tired of the outside world he retreats to that bedroom. Passer-by's on the street can notice the bedroom window but that hardly infringes the owner's visual privacy. There is simply a threat of invasion without an actual invasion taking place. To infringe his visual privacy the glances towards the bedroom window must be more severe. Like when a person stares in the room for a definite period through the bedroom window. If the owner happens to notice the person, the immediate reaction of the owner will be that of discomfort. That is because the person staring has invaded the spatial privacy in turn invading the visual privacy of the owner of the room.

In a public space, for the most part, people do not expect spatial privacy and hence no visual privacy. When a person is walking on a pedestrian street, he has no legal right to stop other people from glancing at him. If that makes him uncomfortable, he may as well retreat to his housing. The defence when a person stares through the bedroom window will be to either walk to another room in the house or hide behind or underneath objects in the room, for example, a closet or a bed. Or still, approach and reprimand the staring person. If too concerned about people staring into the bedroom, a permanent solution will be to use a blind. This will make it futile for anyone to look in the room from the window as getting past through the blind is not possible with a human eye.

But what if a person got a piece of technology that can look past the blind? Supposing a machine is used that can see through solid

objects, the person using the machine can precisely see the owner inside the room. But the owner is totally unaware of the loss of his visual privacy. With the machine it is possible to see the owner in a compromising position, which if not for the machine would be hidden from the world. It is only because the owner is unaware of the invasion that his behaviour remains unchanged. He may continue to indulge in the compromising behaviour, unknowingly, while he is being observed. But that does not mean that his visual privacy has not been infringed. It has, the only difference being that before he knew about the invasion, whereas in the second case, he is totally unaware.

By using a car, a person gets a certain amount of visual privacy on the road, but that too does not entitle him to a claim of invasion if someone stared at the car windows. At the maximum he can question him politely, or, if he felt uncomfortable, he could drive away. It is due to the nature of the place that he does not have a legal right to take action. However, if his car was parked in his garage and some stranger walked up and started peeping through his car windows, and if he happened to be inside the car, that certainly entitles him to a claim of invasion. Therefore, visual privacy is tied to the space, a private or a public space. It all depends on the reasonable expectation.

Reasonable expectation predicates not to have visual privacy in a temple, church, or a mosque. But even in a public space there might be instances where it is expected. For example, while making a confession in a confession box, in a church, one expects visual

privacy from the priest, as the confession made may be of such a damning act, that if exposed to the priest visually, a person would not regurgitate a word. Taking another example of a private space but this time without the machine, someone makes a tiny hole through the wall that sees a person inside the bathroom, like in the 1959 American novel 'Psycho', even though the peeping tom can see the person's nakedness, the behaviour of the person inside the bathroom remains unchanged. This is because he thinks he is alone, whereas from a practical standpoint, indeed, there are two persons in the bathroom. In an online context, hacking someone else's laptop camera, results in similar findings. Hence, to violate a person's visual privacy it is not necessary that there should be a change in behaviour.

Etymologically, private meant non-public, not being involved in state matters.[314] To be deprived or uninvolved in state affairs, in those times, was not praiseworthy and looked down upon.[315] Retire from public life has a similar connotation, but not the same. Retire suggests that it is a voluntary act whereas the former is more imposed. The root of the word privacy, however, is indicative. It can be traced to the Latin adjective prīvus[316], meaning single, individual, one's own, private, peculiar or particular, deprived of and without.[317] This suggests that visual privacy cannot exist in

[314] Richard A. Posner, 'Privacy, Secrecy and Reputation' (1979) 28 Buffalo Law Review 1, 3.
[315] ibid.
[316] Jack Hirshleifer, 'Privacy: Its Origin, Function, and Future' (1980) 9 The Journal of Legal Studies 649.
[317] Charlton T. Lewis and Charles Short, 'A Latin Dictionary, prīvus' (Perseus.tufts.edu)

isolation, meaning, it exists as a claim against people. If a person is the last surviving human on the planet, there is no need for visual privacy as no one is there to take advantage by visually accessing him or his private things. He might want to visually hide from the animals, due to the fear of becoming a meal, but not in the sense that it will tarnish his reputation.

Solitude and isolation, in the narrowest sense, is an act of visually hiding oneself from other people, it could be, friends, family members, or complete strangers. Thus, the claim to have solitude or isolation is against other people. This is not achievable if the thought of existence of other people did not cross the mind. If it did not then there will be no intimate moments or possessions that one would like not, to be accessed by others, as there will be no others who can see the private moments or possessions. Therefore, visual privacy is demanded from the society who has something to gain from another's loss, like reputation. Visual privacy is needed because there are watchers. Like kidnappers watching a family to determine the number of children, or friends watching others go to a secret hide out to find a sign to tarnish each other's reputation, like one meeting with a woman outside marriage. These are all instances of invasion of visual privacy.

The degree of intimacy of the information, in each setting, is also important. Take for example an individual who is with his clothes on, and another individual, who is with his clothes off. The individual who is wearing his clothes will come across as normal to

---

<www.perseus.tufts.edu/hopper/text?doc=Perseus:text:1999.04.0059:entry=privus> accessed 12 May 2017.

most observers. He may come across a little weird if he is wearing the wrong clothes at the wrong time. But an individual who is not wearing clothes at all, will be shocking to most observers, if he is naked in a public sphere. However, there are places where things take the opposite turn, where wearing clothes will shock most observers and walking naked will be considered normal, for instance, at a nudist beach.

By knowing the behaviour of a person, it is possible to predict his next move. Algorithms which help in predictive analytics is real. So, behaviour forms an integral part of visual privacy. A short-tempered person, in most probability, if he gets into an argument he will land into a fight. This knowledge if in the hands of some miscreant, he can use it to his advantage. In a hypothetical situation, where a person is observed visually day and night, by this observation, knowledge can be gained of the fact that he leaves his home at eight in the morning and returns in the evening by seven. Now if someone wanted to commit a robbery, this would be the ideal time. Knowledge might also be gained of the fact that he fears authority, so that might give the robber more incentive to commit the crime, as in most probability, it will go unreported. A company or a corporation, by observing the behaviour of a person, may induce him into buying products which he may not need. If it is observed that the behaviour of a woman signals that she is pregnant, then a company might target her for their baby products, however, these products she will need. But her autonomy to choose from the various products in the market will be infringed, as the company with the information, will be able to take advantage of this prior

knowledge. The State may arrest a person before he has committed a crime by observing his daily behaviour, like in the 1956 pre crime detection, science fiction novel, 'Minority Report.'

This sort of action whether by the State, corporations, or individuals, has a drawback; it restricts a person's autonomy to make independent decisions. It robs them of their secrecy. But if the watched knows that there are watchers watching him, like in a situation when a person knows that he is under CCTV surveillance at a railway station, it even restricts the growth of a person's natural personality. Overtime, it may be that his senses get used to the surveillance, but still his personality may undergo a change and take a lesser form than otherwise. The thought process gets restricted as the mind become less adventurous. In front of a camera a person tends to put his best face forward even though that might not be his true face. There is a tendency to give up many emotions, like anger, and behave friendlier in order to be agreeable to societal norms. Whether it is a good thing, or a bad thing, is debateable. On a personal level the personality shrinks but on a societal level it could be beneficial if everyone is docile.

The thing about visual privacy is that the dominant classes are more able to secure it. It could either be a class of race, a class of socially affluent people or a class of people in authority. History is abounding with numerous instances which support this statement. The slave trade which brought the black people from the African to the American continent is a fine example. The social stigma attached to being Black in White America was such that it was a

social misdemeanour to have an eye contact with White people.[318] They were meant to lower their gaze when a White man passed by for fear of being physically battered.[319] The Jews during the Second World War wore armbands that visually identified them as being Jews.[320] They were visually exposed. In medieval times it was the norm to lower the gaze when people of royalty, especially Kings and Queens, passed by. Eye contact being one of the most basic forms of human interaction is jeopardised in a class society.

It is normal for lovers to look into each other's eyes while expressing their desire for love. A person's physical image is, therefore, meant to be broadcasted to the public, in order to have normal social interactions. It will be absurd if people walked around wearing a mask or having no right to see another person's face (however, image rights are granted to individuals). If it were then the normal everyday sight would be that of people walking and interacting with each other with their eyes glued to the ground, which would make life unliveable. The hardships that this would cause would be unsurmountable. So, having a balance, between visual privacy and making it public, is necessary, to maintain normal social functions.

But where does one draw the line? We can forget about wearing masks to stay anonymous as it is impractical. In this respect, some

---

[318] Sherene Razack, 'What Is to Be Gained by Looking White People in the Eye? Culture, Race, and Gender in Cases of Sexual Violence' (1994) 19 Signs: Journal of Women in Culture and Society 894.
[319] ibid.
[320] 'The Yellow Star' (Bl.uk) <www.bl.uk/learning/histcitizen/voices/info/yellowstar/theyellowstar.html> accessed 9 November 2017.

help can be taken from the elements outlined in chapter 3 above. Anything observable from a public sphere, so long as it is not systematic, should be taken as harmless. So, if by an innocent gush of wind, one was to observe the undergarments of a woman wearing a skirt in a public street, it should be taken in jest. But the moment any recording comes into the picture, with the limitations outlined above, should be actionable.

As an adjective, 'Secret' is defined as 'not known or seen or not meant to be known or seen by others'.[321] As a noun it is defined as 'something that is kept or meant to be kept unknown or unseen by others.'[322] It originates from the Latin word 'Secretus' which means separate or set apart.[323] We all have secrets which we keep hidden from others. Why we keep secrets is a more tantalizing question. The primary reason why we keep secrets is because of deviant human behaviour. That deviancy if known to others will inflict harm or cause loss to the person keeping the secret, for example ill gotten money being kept a secret from the tax authorities. In order to keep that money secret, it is necessary not to disclose it in the tax returns. It is akin to concealment of facts and material things. Concealment signifies the action like when concealing evidence. That evidence may or may not be a secret. It is even possible to conceal a secret camera like concealing it in the briefcase when the camera is unattached. It will still be called a secret camera in

[321] 'Secret | Definition of secret in English by Oxford Dictionaries' (Oxford Dictionaries | English) <https://en.oxforddictionaries.com/definition/secret> accessed 21 May 2017.
[322] ibid.
[323] ibid.

normal parlance because that is its function, not meant to be seen by others.

In the information age it is very difficult to hide, physically as well as mentally. It is only secret till the time it is in the head, once the thought is captured on a medium it does not remain a secret for long as there are more chances that there will be an information leak. Even when talking about intellectual property, people might want to keep the invention a secret but that too is a form of deviant behaviour as society demands, it be disclosed for the benefit of the many. Intellectual property rights are granted in order to generate more innovation in a society and to reward a person's idea. It is a result of balancing the right of the public against the right of one's creation. But it can also be said that people with ideas, do not necessarily, have the capital, and usually, the idea is financed by the public. So, to give an absolute right, to one's own creation, is also questionable.

We are being constantly monitored and the people's perceptions are becoming comfortable with this kind of monitoring, for one reason or another, as they feel they have nothing to hide.[324] In other words, they have no secrets, they do not indulge in deviant behaviours which could damage their reputation or land them into trouble with the authorities, if known. That is what many in western societies tend to think. I could compare them to the group of people living in the shanty towns who also have nothing to hide. One way to put it is, they do not have any secrets because they cannot afford one. It is

[324] Daniel J. Solove, Nothing to Hide: The False Trade-off between Privacy and Security (Yale University Press 2011).

possible to even have a group secret, as against a single person. So, the way the word secret is interpreted is important, but, in all cases, it will involve an aberration from the normal. It is a normal human characteristic to have aberrational behaviours and what is normal is defined by the society. It is also true that what is normal in one society may be deviant in another.

The world is so vivid around us, filled with different colours, and it would be boring if we did not have the gift of sight. It will still be dreary, despite having eyes, if we did not have memories to reminisce. Without technology, the only way to share our visual experiences is by words or drawings. But by words or drawings is not the same thing as pictures in our visual cortex. Humans ingeniously invented the camera[325] to get as close to mimicking our eyes. The advantage of having this paraphernalia is that information processed by it is capable of being shared as it is and not by word of mouth. Through it, we can capture all the intimate moments of our lives, like our marriage, having our children, the places we have visited, and even when our memories have faded, the pictures are refreshing reminders of how we have spent our lives.

Although, having numerous benefits, the invention of the camera can rightfully be said to be the genesis of the mass invasion of visual privacy. Our expectation of visual privacy after the invention of the camera has reduced. We are more open about flaunting our looks and keeping in touch with fashion. Technology has also made it much easier to disseminate visual information. Paparazzi's

[325] ibid (n) 250.

photographing known personalities, for a small gain, without their permission, is an acknowledged fact. Due to the internet, these unsolicited photographs reach a far greater audience than would have been possible. This digitalisation also raises concerns about visual privacy. Before that, an act of adultery could only be captured by the naked eye. The information about the adultery then could only be circulated by passing on that knowledge by mouth. Without any tangible or digital evidence, the personality of the witnesses bore weight. People would readily believe a person of stature than a commoner. In such times, therefore, the only form of invasion would have been in flesh. But in the present times, the invasion has become technological.

Visual privacy of an individual can be invaded either in flesh, like physically prying into other people's physical lives, physically prying into other people's technological devices, or invaded with the help of cameras and visual sensors, on the ground and in the air. In the case of invasion by technological means, it is permanent. In some instances, it may require a person to operate the cameras and the sensors physically, and yet in other instances, it may be controlled remotely.

The intention to invade matters less because even though, unintentionally, a person is seen with an unsocial element, when a stranger suddenly enters his house without warning, his visual privacy has still been invaded. A knock or a cough before entering would have had him better prepared. To say that behaviour has not changed, in certain situations of visual invasion, and thus there has

not been an infringement of visual privacy, is a fallacy. It has been invaded but only in secret.

Let us assume that A wants to kill B, without anyone knowing it. Finding that B is alone in his house, A goes to B's house, takes out a pistol with a silencer, and shoots B. As a result, B dies. If no one saw A shoot B, then that incident is visually private to only A. We can say that only A knows who murdered B. But, if, despite A's thorough observation that no one was watching, but in fact, there was an eyewitness in the wardrobe, who saw A shoot B (but unknown to A), it can be loosely said that the murder is also visually private to the eyewitness.

However, technically, the incident has lost all visual privacy. This is because the eyewitness may interact with his sister after the incident and divulge to her what he saw. Now the eyewitness's sister is also a party to the secret, and she may interact with someone else and divulge what her brother told her, and this can carry on.

Thus, once the information leaves it source, it is no more a secret. However, it can be controlled as to who has access to it. For A to expect absolute privacy, from the eyewitness, or his sister, or other individuals down the line, will be foolish at best.

Further assume, that A saw the eyewitness after he had shot B, but the eyewitness managed to escape. In this case, A feels that his visual privacy is lost. This is not the case when A is unaware of the eyewitness or there is no eyewitness to begin with. He wants to get back his visual privacy, and to do so, he must kill the eyewitness, or get hold of an equally damning piece of information about the

eyewitness, to maintain an equilibrium, and thus, his visual privacy in the act of murder.

Now even if the information about B's murder is passed down the chain, from the eyewitness to his sister and so on and so forth, the urge to kill the eyewitness will be greater than anyone down the chain. This is because, what the eyewitness saw, others only heard.

In all this, there are opposing interests to uncover A's visual privacy, for example, the police may want to know who the murderer is. The success of the police will depend on the evidence left behind, including any eyewitness and DNA samples. If there was no eyewitness and A was very careful about not leaving any other pieces of evidence, then it is absolute visual privacy for A. But if there was an eyewitness, then it is a reduced form of visual privacy. The eyewitness may disclose A's identity to the police or may not disclose. But if A's visual privacy is dependent on the eyewitness's behaviour, then it is not visually private in the strict sense.

4.4. Classification of visual information

To open a bank account, an individual must mandatorily disclose his/her address. Banks may need more personal information, depending on the type of account being opened, but in most cases the data is alpha numeric, such as, date of birth, sex, marital status and so on. This *alpha numeric information*, when printed on a paper or displayed on a screen is also visible. But what is visible, is so

lacking in physical characteristics, that one would not associate it with *physical visual information*, like, the shape of a person's nose, his built etc. Alpha numeric information has a two-dimensional character, whereas physical visual information has a three-dimensional character. Physical visual information may acquire a two-dimensional character, like a photograph of a mountain, a person, an animal, or anything that has a mass, on the other hand, alpha numeric information may acquire a three-dimensional character, like, when alphabets and numbers are given shape for the purposes of advertisement.

But despite this vice versa, alpha numeric information is two-dimensional from its inception and rarely acquires a three-dimensional character, whereas physical visual information is three-dimensional and becomes two-dimensional only in the form of photographs or drawings. Physical visual information is more real as it excites the senses much more than the boring alpha numeric information. So, we can differentiate between pure alpha numeric information and pure visual information.

Yet, there is another kind of information that sits in the middle of the two. It is neither strictly alpha numeric information nor physical visual information. It has all the characteristics of alpha numeric information though. They are, graphs and other forms of pictorial representations of alpha numeric information. Under this category will fall pictorial representations of an individual's health statistics, license plate numbers etc.

On a study desk there is a personal diary, but the alpha numeric information capable of tarnishing a person's reputation, is scribbled on page eighty-four. If someone wanted to get to that information, he would have to physically pick up the diary, and flip to the relevant page. By just looking at the cover when the diary is placed on the table, he is not infringing anyone's privacy, it is only when he decides to flip the pages, he intends to infringe. Let us assume that the pages are not numbered and so getting to that piece of information would require some investigation. But eventually he will get to it. In either case, it boils down to seeing the information. But it is more than just seeing as it also involves reading and understanding. If an individual does not know how to read, even if he gets to that piece of information, and has seen it, the privacy of the information scribbled in the personal diary remains intact.

So, there are marked differences between alpha numeric information being visualised and thus made a subject of visual privacy, and visual privacy in physical visual information. Making alpha numeric information a subject of visual privacy because it must be seen it order for the information to lose privacy, will unduly make visual privacy the beginning and the end. Thus, it is necessary to know the limits of visual information as that information is going to be the subject matter of visual privacy.

The proposition here is to include physical visual information (having excluded pure alpha numeric information) leaving graphical or other pictorial representations of alpha numeric information on the borderline, as the subject of visual privacy, provided, that the

visual information can be identified to a particular individual. Thus, a picture of a house which can be identified to a particular individual can be a subject of visual privacy. The same with license plate numbers, personal photographs, health image data etc.

Physical visual information consists of everyday objects, like someone's car and physical self, and it is not necessary for them to be printed on a paper or displayed on a screen to be visualised. We live in a physical world so anything contained within it will fall under physical visual information. Without seeing there can be no invasion of a person's visual privacy. Information whether alpha numeric or physical is collected and processed by machines, like cameras and computers, but as machines are not natural persons, there is no invasion of visual privacy. But if the physical visual information is processed by a machine with the intention of being observed at some other time than the time at which it is processed, it will amount to an invasion. So, an audience consisting of natural persons is necessary.

We can further distinguish between physical visual information that is *recorded* and *unrecorded*. Recorded visual information can either be *open* or *closed*. To give an example, open recorded information will be a physical photograph (apparent) and closed recorded information will be a digital photograph stored on chips or other storage devices (hidden), capable of being open only when displayed on a screen or printed. There are instances where video cameras are connected to a screen, which captures live visual information, through the lens, but that information is not being

recorded or stored on a storage device for later use. This can be termed as *transient projected physical visual information*. As the visual information is displayed on a screen for a person to see, although not capable of seeing at a choosing, in a sense, it still violates a person's right to visual privacy. This is because it is an extension by technological means of our natural human abilities. The camera, and the screen where the image is projected may be a distance apart. It just happens that the violation is not of a permanent nature (not recorded for future use), but, anyway, it may result in repercussions on the subject (a natural person) of visual privacy. There is a threat of violation, but that threat has chances of materialising into an actual invasion.

This might happen, if someone close to the subject, who happens to see, might disseminate that information by word of mouth to some other close acquaintance. And if the subject is confronted with that piece of information it will alter his behaviour to his disadvantage. It is possible that the subject becomes reserved if the information consists of acts that will portray him in a poor light. It might also be disastrous for the relatives that come across such information. It may also be that no one is behind that live screen and it has not captured the eyes of anyone and as a result that information passes into oblivion. Then we can say that there was a threat of invasion of visual privacy without an actual invasion taking place. If the subject knows about the existence of the camera, he will presume someone is behind the screen and that the physical information is being recorded. Irrespective whether someone is behind the screen or not

or whether the information is recorded, the behaviour of the subject will change.

Physical visual information, specifically, an image of a person, captured on an open or a closed medium, is a result of relationships, like images generated during intimate moments with family and friends, or images generated between friends and foes. Visual information generated out of intimate moments with family and friends will include pictures clicked by parents of their children during a birthday party or of a boyfriend clicking intimate pictures of his girlfriend. Feelings are usually attached to these relationships, unlike pure commercial relationships. Those feelings might be positive or negative. It is acknowledged that a police officer and a criminal do not share a positive relationship but there are feelings, although negative, towards one another. In the case of State and its citizens there is a relationship of positive feelings as the State in theory is made up of its citizens.

Without relationships, it is difficult to imagine that anyone will be interested in capturing another's image, except for unsocial purposes, like peeping for mischief. Even the CCTV cameras installed are generating images and videos out of the relationship between the State and its citizens. By ensuring law and order, by identifying the bad elements, the State ensures the safety of its citizens. Companies and corporations demand large amounts of information from the markets they serve, to identify people on ethnic or racial grounds. One of the reasons for this is to find out the efficacy of their products, which is commercial in nature, for

example, fairness products are advertised and mainly sold in regions where people are dark skinned and tanning products are sold where people are white skinned.

Other visual data, like a number plate of a car, is a result of commercial relationships, someone buying the car, then going to the license authority to get permission to use the car on the road, and once the permission is granted, then visiting the number plate dealer to imprint that number on a tangible medium.

Therefore, visual information is generated out of four kinds of relationships, positive, negative, neutral, and commercial.

4.4.1. Positive relationships

Visual information generated out of love and positive relationships are easily identifiable. Parents love their children, and it is normal for them to capture moments they spend together. We all click pictures with our friends when on a holiday or on special occasions with them. The consent to capture one's image is implied in these kinds of relationships. An individual would dare not click a picture of a stranger as it is awkward and bizarre without a context. It also amounts to being rude. It is not always necessary or possible to be physically together with the ones we love and care, so we keep them in our memories.

A relationship between lovers is one that is intimate; they know each other physically and mentally. It is normal for them to capture images together. We all love ourselves as well, and this has never been truer than with the present generation and the proof is in the

number of selfies we take. In this category we voluntarily agree to capture and share our visual information with our near ones. We all upload personal pictures on social networking and dating sites and we do this in order to share our intimate moments with family and friends.

4.4.2. Negative relationships

This is kind of rare as a person would not like to remember people they dislike. Nor would they share moments of their life with them and so there is very little opportunity, if at all, to capture or share images. However, visual information out of negative relationships can be generated out of the need for safety. The State and its institutions require visual information for identification purposes, like police officers clicking pictures (informally known as mugshots) of criminals or the CCTV cameras visually recording the citizens to filter out the bad people from the midst of the law-abiding citizens.

In one way or another, this visual information is generated out of negative feelings. Such negative feeling may have a corresponding positive feeling, like a police officer's positive feelings towards the society. This sort of image collection and dissemination is involuntary as we our forced against our will. A criminal hasn't given his consent voluntarily for his mugshot nor has he given his consent that his mugshot be displayed. The same can be said about the CCTV cameras where the citizens have not given their consent to the collection and utilisation of their visual information, individually. The consent has been forcefully thrusted upon them.

4.4.3. Neutral relationships

Neutral relationships are ones that exist towards fellow human beings, like strangers. They are not related to us, either in a positive or a negative way. There are no feelings attached towards one another. Clicking a picture at a rattlesnake round up, in the US, may unintentionally capture visitor's image in the photograph. This is highly probable as the round up attracts a lot of adults and children alike. They have not given their permission to be photographed but are included in the photograph, unintentionally, in a secondary or accessorial manner. The same can also be said when pictures are taken on the sly of strangers. However, photographs unintentionally taken of people, while attending cruel beheadings of rattlesnakes, may have negative repercussions on the stranger in the photograph if the photograph lands up in the public domain. People who know the stranger or are related to him may categorise him as cruel. It may also happen that an image generated out of neutral relationships in one context is used in a different context, for example, a person's image used in an un-charming way like in a poster of a refugee when the context in which the picture was taken was local culture.

4.4.4. Commercial relationships

Still, a fourth category of visual information is generated out of relationships that are commercial in nature. Transactions can mean a whole lot of different things but basically it means an exchange. Even an exchange of ideas can be termed as a transaction in the sense of an interaction between people. A police officer and a

criminal are transacting with each other, a company is transacting with its market or the government is transacting with its citizens. However, over here it is used as meaning, a commercial exchange. The examples in this category will include car number plates, health statistics, image data acquired by companies for advertisement purposes etc.

In this case, it is obligatory to part with the information in order to function. For example, without displaying the number plate on a car, it will be illegal to use it on the road, or without letting the health monitoring machines read physical statistics, it will be impossible for the doctor to know a patient's condition, and without physical images of people, it will be difficult for companies to advertise their line of clothing or beauty products. Images generated off the public domain, whether in magazines or newspapers, are also a result of transactions as one is paid to click a picture. It could also happen when private detectives are hired to gain visual knowledge of the activities of our near ones in case there is a reason for suspicion.

More and more these days' corporations are moving towards the acquisition of physical visual information, like imaging cities for navigational apps, despite the already vast collections of alphanumeric information. This collection of information could be from varied sources, like satellites or smartphone cameras. Therefore, our hunger for visual information has increased tremendously. We can truly say that we are living in a visual world inside of a visual word. We are constantly staring at screens,

whether it being on a laptop, smartphone, or augmented reality headset. We are also consuming and creating more image and video-based information instead of the traditional alphanumeric data. That itself is not a major problem but with advancements in image and object recognition technology, it becomes a major concern.

For example, snapchat has filed a patent for an object recognition system which identifies the object in an image.[326] What this means is if a person is standing at Sagrada Familia and decides to click a picture next to it then the object recognition software by recognising that public monument can recommend other monuments by the same architect or even suggest restaurants in the area. Facebook has experimented with a similar technology where pictures uploaded to the social networking website are categorised according to what is contained in the picture.[327] For example, if the picture has been taken in a forest it can recognise that there are trees and if the image contains a car it could recognise the make and model.

This is suggestively to benefit blind people, but it will not be long before the person is identified in an image. This will be extremely invasive to visual privacy as the algorithm identifying individuals, with all their details, will become available to the public at large.

[326] 'US20160203586A1 - 'Snapchat Object Recognition Based Photo Filters Patent Application' (Scribd) <www.scribd.com/document/318282319/Snapchat-Object-Recognition-Based-Photo-Filters-Patent-Application#from_embed> accessed 23 June 2017.

[327] Joaquin Quiñonero Candela, 'Building scalable systems to understand content' (Facebook Code 2017) <https://code.facebook.com/posts/1259786714075766/building-scalable-systems-to-understand-content/> accessed 23 June 2017.

This way any image can be picked up from the public domain and searched for personal information even by strangers. Strangers will be in possession of the entire life history of an individual from a single image, including criminal records and much more.

By recognising the objects in the image, it will also be possible to pinpoint the location information of the subject in the photograph. Facebook has even filed a patent to detect facial expressions by spying through an individual's smartphone, laptop, or tablet camera.[328] Visual privacy invasion is not just a threat but a creeping reality. The benefit that Facebook expects to derive from this is in the content and advertising domain. If a person happens to smile seeing a particular picture content, then Facebook will prioritise that and anything related to that content will be shown in the news feed. This is not only invasive to visual privacy but also unethical.

4.5. Reasonable expectation of privacy

Visual privacy, like other forms of privacy, will depend upon reasonable expectation of an individual. Reasonable expectation varies depending on different aspects, such as, space (public, private), activity, technology (drones), culture, religion, or gender.[329] Although, reasonable expectation of privacy is a Western legal concept, it must be discussed in the context of the mundane

[328] 'US20150242679A1 - Techniques for Emotion Detection and Content Delivery - Google Patents' (Google.com) <http://www.google.com/patents/US20150242679> accessed 23 June 2017.
[329] See supra section 4.2.

world. After all, it is only a reasonable expectation of an individual, in the world he is in, nothing fancy about it. What may be reasonable for a Western family may not be reasonable for a Middle Eastern or Asian family. So, although, a legal concept, it must exist outside of the Western legal realm.

For example, culture as an aspect regulates the reasonable expectation of privacy, from an objective standpoint. The subjective expectation, therefore, is based on that objective expectation. Objectively, Islamic society expects women to show no skin and that objective expectation affects the subjective expectation of visual privacy of women. So even though culture is a determining factor of visual privacy, within it, the reasonable expectation of that visual privacy, of an individual, is also shaped by the same culture.

According to the western legal concept, reasonable is determined, not according to one's arbitrary thinking, but, according to what a prudent person would expect in a similar situation. On the other hand, one may say, what is reasonable in an Islamic society is determined by the Quran. Objectively, it is what the society thinks is reasonable and, subjectively, it is what an individual will think is reasonable. It is possible, that there can be many outcomes to an issue, which are all reasonable in their own respective sense and the one that a person will chose depends upon his subjective satisfaction, like judges choosing one interpretation of the law over another interpretation.

Why chose an objective standard over a subjective one? A good way to answer this question is by asking another question. Why is

mistake of law not a defence in law? If mistake of law were to be a defence, then nobody would know the law, in other words, everyone will pretend not to know the law. Similarly, if a subjective standard were to be applied, then an individual will always have a reasonable expectation of privacy, irrespective of what anybody else thinks. An objective standard is also moderated, because of the presence of, reasonable expectation of privacy, of more than a single individual.

The concept of reasonable expectation of privacy was born out of the jurisprudence of the US, by the judges who debated on the fourth amendment to the Constitution of the US, specifically, search and seizure.[330] In Katz v. United States,[331] where the concept germinated, the requirement is twofold, first, that a person must have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as reasonable. Thus, a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements, that he exposes to the 'plain view' of outsiders are not 'protected' because no intention to keep them to himself has been exhibited. On the other hand, conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable.

The European continental system relies less on the reasonable expectation of an individual as the grounds on which the privacy of

[330] Bert-Jaap Koops and Ronald Leenes, 'Code and the Slow Erosion of Privacy' (2005) 12 Michigan Telecommunications and Technology Law Review 115, 128.
[331] 389 US 347 (1967).

an individual can be compromised is explicitly mentioned in the CFREU and other legal instruments applicable in Europe. Nevertheless, reasonable expectation does play a role as European courts recognise the concept without disregarding it.[332] For example, the Spanish Constitutional Court has applied the concept of reasonable expectation of privacy in work places, in a case where it held, that storing messages in the hard drive of a publicly accessible computer, waives one's right to privacy as this act expressly permits others, to have access to it.[333] In other words, an employee should not have any expectation of privacy when the hard drive is public. However, it will be difficult to ignore the US cases (cited below) that have played a vital role in the development of the concept of reasonable expectation.

New technologies have continuously altered our reasonable expectation of visual privacy. From the time since the camera was invented till the ubiquitous use of CCTV cameras, our reasonable expectation has shifted from being completely expected to, somewhat expected. With the advent of civilian drones this shift is going to be even more profound. But is there a reasonable expectation of visual privacy from drones? Does our reasonable expectation of visual privacy from aerial surveillance change depending on whether it is a public or a private space? What happens when a technology is used so widely that is becomes unreasonable to expect visual privacy?

---

[332] See case P.G. and J.H. v. the United Kingdom, no. 44787/98, ECHR 2001-I, para 57.

[333] STC 241/2012, the decision is available in Spanish at, <http://hj.tribunalconstitucional.es/docs/BOE/BOE-A-2013-614.pdf>

It should not be unreasonable to expect visual privacy, from aerial surveillance, within the confines of a private property. An outwardly sign, to show that visual privacy is reasonably expected, within the confines of a home, will be to construct a wall around the property. This helps to keep the property private from ground level observations. But a drone flying at 400 feet can compromise the wall. This should not necessarily mean that visual privacy is not expected from the airspace above and it should not require an individual to build a shed to protect his property from an aerial observation, unlike the reasoning in the US cases.[334] From a perspective, an individual who builds a wall to protect his property from ground level observations, the protection from aerial observation is implicit in the act of building the wall. Whether he could fathom the invasion of his visual privacy, from the airspace above his property, is another question altogether.

If one were to follow the US cases closely, it will come to light that it requires a physical trespass to hold that a person's privacy has been violated.[335] But in an age where technological progress is doubling every decade,[336] it has become possible to invade an individual's visual privacy without the need for a physical trespass.[337] As high airspace is considered public highways, drones

[334] See cases, California v. Ciraolo, 476 US 207 (1986); Dow Chemical Co. v. United States, 476 US 227 (1986); and Florida v. Riley, 488 US 445 (1989).
[335] See, Olmstead v. United States, 277 US 438 (1927); Goldman v. United States, 316 US 129 (1942); On Lee v. United States, 343 US 747 (1952); and Silverman v. United States, 365 US 505 (1961).
[336] Ray Kurzweil, 'The Law of Accelerating Returns' (Kurzweilai.net 2001) <www.kurzweilai.net/the-law-of-accelerating-returns>
[337] See Katz v. United States, 389 US 347 (1967).

will never fit the definition of a trespasser. But they will be capable of surreptitiously invading an individual's visual privacy from the airspace above.

Gone are the days of physical trespass because present technological advancements have made it possible to invade an individual's visual privacy without even physically trespassing into his personal property. Visual and auditory trespass is gaining traction without even an iota of physical encroachment.

Reasonable expectation of privacy, although higher in private spaces, can also exist in public spaces.[338] US jurisprudence on the subject or accords lesser degree of protection to curtilages of homes on the logic that the sphere is not private.[339] Open fields on the other hand, are totally excluded from protection.[340] Open fields are unoccupied lands whereas curtilages are areas immediately surrounding a home.

In the villages in rural Asia, where the toilets are not attached to the main house, but are constructed rudimentarily in the same compound, but some distance away from the main habitation, an individual's expectation of visual privacy thereby does not reduce when visiting the toilet, even if located some distance away from the main habitation. The European cases treat workplaces as private spheres of activity where a person has a reasonable expectation of privacy against searches, monitoring of telephone calls and emails

[338] Bert-Jaap Koops, 'Privacy Spaces' (2018) 121 West Virginia Law Review 612.
[339] See Hester v. United States, 265 US 57 (1924).
[340] ibid.

initiated at the workplace.[341] Thus, the activity is no less important to determine the reasonable expectation of visual privacy, although, the location will play a mitigating role. If a private activity, like having sex, is performed in a public space, it will be unwise to expect no public.

It has become so necessary to disclose personal information, that without disclosure, a major portion of the economic machinery will come to a standstill, as it is so dependent on information. But just because it is necessary for information to exist in the public domain does not mean that our expectations towards that information should be diminished.[342] An individual who drives a car uses the public highway. So, we are willingly giving up, a part of the privacy to the location of the car, as it is in the public domain. However, inherently we still think, for the most part, that we are not being followed. Among a sea of cars, it will be difficult, if not impossible, to track down the move of the car without the help of technology. There could be other cars of the same make and model and of the same colour, at the same time and place, which will help to preserve the visual privacy of the car and from being followed around.

[341] See Copland v. the United Kingdom, no. 62617/00, ECHR 2007-I; Halford v. the United Kingdom, 25 June 1997, Reports 1997-III; and Bărbulescu v. Romania, no. 61496/08, ECHR 2016.

[342] See, Case C-131/12 Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, (google was required to remove links from its search engine which directed users to information which was already publicly available); Case C-362/14 Maximillian Schrems v. Data Protection Commissioner; Case C-311/18 Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems.

Once a thing becomes a practise, we start to lose all inhibitions. The US cases, dealing with the reasonable expectation of privacy and the fourth amendment, were decided on the basis of the general use criteria, on the logic that if a technology is in general use then the public cannot expect privacy if information has been revealed using that technology.[343] A drone with cameras is such a technology that is in general use or will be. But only because it is in general use is no reason why the public should not expect visual privacy if visual information has been processed, stored, or revealed using that technology. An individual should be protected from emerging technologies that render his once held expectations obsolete.

There are so many technologies which are in general use, from the internet to the computing devices, still there are rules and regulations to control the information flow. People still expect not to be spied through their web cameras and they still expect when they are holding private conversations that no third person is eavesdropping. But if someone did interfere, with the help of modern technology, we will be left unguarded. However, a defence that people can put up against technologies that invade our visual privacy is to adopt a counter technology. For instance, surveillance by drones could be fought by Sousveillance, a term coined by Steve Mann.[344] Sousveillance is defined as inverse panopticon, where, with the help of technologies, the observed can observe the

[343] Kyllo v. United States, 533 US 27 (2001).
[344] Steve Mann and others, 'Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments' (2003) 1 Surveillance and Society 331.

observer.[345] But counter technologies are socially costly. So, they are not practical from a social welfare perspective.

Privacy is fundamental in developing individual behaviours and personality and this development should be unrestricted even amidst new technology. Closed Circuit Television cameras surround us, in the streets, at the railway stations, at airports and even in commercial stores. We expect them to be there at banks and even installed in most of the public areas. Usually, such installations come with a visual warning that the area is under surveillance. We have allowed this, as a society, to happen under one pretext or another. This has diminished our expectation of visual privacy collectively as a society. But surveillance technologies have now gotten new wings wherein it can piggyback on drones and take to the air. We still do not expect to come under the sphere of constant surveillance from the airspace and reasonably expect not to be watched from above, so in this respect our expectations of privacy have not yet diminished. But it will be if we allow it and passively submit to new technologies trespassing into our personal lives. We will have no opportunity, unlike ground level surveillance, to even know who the person behind the camera is, as there will be no warnings that the area is under surveillance from the airspace above.

It is said ignorance is bliss, but that ignorance can cause great damage. A drone is an addition in the list of technologies where ignorance might seem bliss when it is flying in navigable airspace,

[345] ibid.

but it has the capacity to strip the clothes off a person. There are instances of airplanes and helicopters invading our visual privacy from the airspace, so there is nothing inherently new with drones. But we should keep in mind that the frequency of visual invasion will increase. As a piece of consumer electronic technology, it will be within the reach of millions. The cost of launching a drone into the airspace is a fraction of what it costs for a single flyby of an airplane or a helicopter. The small size of the drone needs to be considered as well.

Where once we roamed the streets, highly secure in our feelings, thinking that the only person watching us from above is God, has changed.

5. THE FUNDAMENTAL DIMENSIONS OF VISUAL PRIVACY

While the previous chapter discussed the concept of visual privacy, this chapter will discuss visual privacy within the fundamental rights framework in Europe. There are two major frameworks, at the EU level, namely, the ECHR and the CFREU. Although distinct, they share a common bond, with regards to the meaning and interpretation of the legal Articles, contained within them. There is no specific right to visual privacy under the two frameworks, thus, visual privacy will be discussed under the available and broad, right to privacy and data protection. The first part of this section will enumerate and discuss the sources protecting the right to privacy and data protection, while the second part of this section, will discuss how visual privacy and its offshoots, like image rights, are interpreted by the European courts.

5.1. Sources and their relationship

5.1.1. European Convention on Human Rights

The ECHR, in Article 8, contains the right to respect for private and family life, in other words, the right to privacy. Article 8 of the ECHR states:

> ‘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.’

At the time when the ECHR was enacted, there was little data processing, compared to today. People were more concerned about invasion of their physical privacy and their physical space by physical beings and not data privacy by technological means. So, unlike the CFREU, the ECHR does not contain a right to data protection. The ECHR is an international framework and applies to member countries of the Council of Europe (COE), which includes, all EU member States.[346] Matters arising in relation to the ECHR are dealt with by the ECtHR which sits in Strasbourg.

Article 8 (2) of the ECHR negatively states that there shall be no interference by a public authority, however, the traditional meaning of public authority is blurred in present times. There are many private entities that provide public services. Due to the dwindling government budgets around the world, privatisation of public entities is the norm. From water companies, national airlines, banks,

[346] It is an international organisation consisting of 47 member countries, including all EU Member States. To know more about the COE visit <https://www.coe.int/en/web/about-us/our-member-states>

railways, etc., which were once under the control of national governments, are now in the hands of multinational corporations. A breed of corporations further detached from the traditional meaning of public services but providing a public service in a broad sense of the word, are the likes of Facebook. However, in a recent English case, it was held that Facebook cannot be assumed to be a hybrid public authority.[347]

There is still some time before corporations are made directly liable under the ECHR for human rights violations. But as corporations become more powerful, and adopt new technologies to process data, to exert an influence, it is the necessary to include them within the meaning of public authority. Governments may delegate data processing to private companies for the provision of public services, and in these circumstances, it should not be unholy to hold private companies accountable. Drone use by private corporations, even though it would mean extending the meaning of public authority, should be circumscribed within these limits for an effective protection of privacy and data protection rights of private individuals.

5.1.2. Charter of Fundamental Rights of the European Union

The CFREU, in Article 7, contains the right to privacy. It states:

> 'Everyone has the right to respect for his or her private and family life, home and communications.'

[347] Richardson v Facebook/ Richardson v Google, [2015] EWHC 3154 (QB).

Additionally, the CFREU, in Article 8, also contains the right to data protection. It states:

> '1. Everyone has the right to the protection of personal data concerning him or her.
>
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
>
> 3. Compliance with these rules shall be subject to control by an independent authority.'

By including the right to data protection in Article 8, shows, that it has come of age since the first legislations protecting data appeared in Europe, like Hessen in Germany which passed the first data protection statute in 1970,[348] followed by, the Swedish Data Protection Act.[349] The CFREU is a regional framework and applies to institutions of the EU and to the member States only when implementing EU law.[350] Matters arising in relation to the CFREU are dealt with by the Court of Justice of the European Union (CJEU) which sits in Luxembourg.

[348] Fred H. Cate, The EU Data Protection Directive, Information Privacy, and the Public Interest (1995). Articles by Maurer Faculty. Paper 646
[349] Swerige Datalagen 1973.
[350] Article 51 of the Charter.

5.1.3. Interrelationship between the ECHR and the CFREU

Due to the dual framework, for the protection of, the right to privacy, it is normal for an individual to think that dual standards will exist. To an extent, it is unavoidable for there to exist differential standards as they are two different, but parallel frameworks. The ECHR is of the year 1950 having come into force in the year 1953,[351] whereas the CFREU is of the year 2000 having come into force only in the year 2009.[352] In this respect, the ECHR has a richer collection of case laws than compared to the CFREU for obvious reasons. Pragmatically then, to avoid any kind of a rift between the two fundamental rights frameworks, the rights in the CFREU, which corresponds to rights in the ECHR, should be interpreted as it is meant under the ECHR. In this respect, Article 52 (3) of the CFREU states:

> 'In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection.'

In other words, the above provision is meant to avoid a rift between the two frameworks by interpreting the CFREU in harmony with

[351] https://www.coe.int/en/web/conventions/full-list

[352] David Anderson Q. C. and Cian C. Murphy, The Charter of Fundamental Rights: History and Prospects in Post-Lisbon Europe (2011) European University Institute law repository < https://cadmus.eui.eu//handle/1814/17597>

the ECHR. So, unless there is a camaraderie between the two frameworks, the chances of having a sour relationship exists. But if the CFREU is to be interpreted according to the standards developed by the ECtHR, then the role of the CJEU in interpreting the CFREU is minimum. The CJEU is left with full autonomy, in the domain of human rights, only in cases where the CFREU contains rights which does not have a corresponding right in the ECHR, for example, Article 8 of the CFREU does not have a corresponding right in the ECHR. So, Article 8 of the CFREU can have a meaning and scope which is independent of the ECHR, while Article 7 of the CFREU will have the same meaning and scope as that of Article 8 of the ECHR, including the limitation. In other words, Article 7 of the CFREU is limited by Article 8 (2) of the ECHR, by virtue of Article 52 (3) of the CFREU. Article 8 of the CFREU has its own limitation clause.

However, the ECtHR has held that Article 8 of the ECHR also encompasses personal data protection.[353] This broad interpretation by the ECtHR magically creates a right to data protection within the existing Article 8 of the ECHR. Now does this mean that Article 8 of the CFREU, which does not have a corresponding right in the ECHR, must be interpreted according to the scope developed by the ECtHR. But the right to data protection as enshrined in Article 8 of the CFREU looks to be of a higher standard and more specific.

[353] Z v. Finland, Reports 1997-I, ECHR 1997.

In the case of *Antović and Mirković v. Montenegro*,[354] which involved camera surveillance of auditoriums where classes were held and which amounts to processing of personal data under Article 8 of the CFREU, the ECtHR decided the case purely based on Article 8 of the ECHR. The court held the auditoriums to be a private sphere and therefore infringed the right to private life of the complainants. It could not have decided the case based on the principles of data protection as there is no corresponding right to data protection under the ECHR. Assuming the case was brought before the CJEU under Article 8 of the CFREU, then the case would be decided based on a separate set of principles, different from those based on privacy.

One way of looking at it is that the ECHR is the minimum standard to which the CFREU must be compared.[355] But the CFREU can incorporate standards that are higher than the ECHR,[356] below which the CFREU cannot go. Thus, if the standards under the ECHR were to increase, the CFREU will have to follow. This could result in a tug of war.

At present, the EU is not a party to the ECHR, so both the frameworks have parallel applicability. One is not superior to the other in hierarchy. But if the EU were to become a party to the ECHR, then it will be answerable to the ECtHR, and because the

[354] Antović and Mirković v. Montenegro, no. 70838/13, ECHR 2017.
[355] Elena Butti, The Roles and Relationship between the two European Courts in Post-Lisbon EU Human Rights Protection (2013) < https://www.jurist.org/commentary/2013/09/elena-butti-lisbon-treaty/>
[356] ibid.

CJEU is an institution of the EU, its authority will also be diminished in human rights cases.

5.1.4. Does privacy and data protection mean the same thing?

It is also not clear whether the right to privacy and the right to data protection mean the same thing. If it meant the same thing then there would be no need to include it as a separate Article 8 in the CFREU. In other words, it does not mean the same thing and that is why it is included as a separate Article 8 in the CFREU. One way of looking at it is to say that the right to privacy is a broader right, in the sense that an infringement of the right to data protection also infringes the right to privacy but an infringement of the right to privacy does not necessarily infringe the right to data protection. But in some instances, these two rights may overlap.

However, from one perspective they are similar and yet they differ. For example, Article 7 CFREU guarantees the privacy of communications, which will include electronic communications, which to state the least will also be covered under the right to data protection. But privacy simpler, minus information privacy, cannot be accommodated under the right to data protection. A similar provision that equates privacy with data protection can be found in the EU Data Protection Directive (DPD),[357] where Article 1 states:

[357] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31 (repealed).

> ‘In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.’

Therefore, there is a link between the two rights, but it falls short of being the same. However, the GDPR omits any reference to privacy whatsoever. The most compelling distinction between the right to privacy and the right to data protection has been given by Serge Gutwirth and Paul De Hert. In their scholarly article, they have defined privacy as a tool for opacity (creating zones of non-interference) and data protection as a tool for transparency.[358] In other words privacy is prohibitive in nature while data protection is permissive.

With regards to data protection, the CJEU is at the forefront in the development of this right through case laws. As the ECHR does not contain a right to data protection, the lead is obvious. However, the ECtHR has inferred a right to data protection in Article 8 of the ECHR.[359] The CJEU has done something similar in a few cases wherein it has equated the right to privacy with the right to data protection, and in a few other cases, it sees the two rights as separate and distinct. For example, in the case of Tele2 Sverige AB,[360] the CJEU in para 129 of the judgement notes:

---

[358] Paul De Hert and Serge Gutwirth, ‘Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power’ (in E. Claes, A. Duff and S. Gutwirth eds, Privacy and the Criminal Law, Antwerp/Oxford, Intersentia, 2006) 61-104.

[359] ibid Antović and Mirković v. Montenegro

[360] CJEU Joined Cases C-203/15 and C-698/15.

> 'Article 8 of the Charter concerns a fundamental right which is distinct from that enshrined in Article 7 of the Charter and which has no equivalent in the ECHR.'

In Digital Rights Ireland,[361] the CJEU equates the two rights,[362] while at the same time sees that the principles underlying both the rights are distinct.[363]

If both the rights are understood to mean the same thing, then the minimum standards as prescribed by Article 8 of the ECHR are to be followed, against the reasoning that Article 8 of the CFREU has no equivalence in the ECHR and as such can have a standard independent of the ECHR. The question is not just about minimum standards but also about the principles behind the two rights, which are distinct.

Knowing the difference between the two rights is necessary as drones are going to have an impact on both, the right to privacy and the right to data protection; and because of this, it is important to know when a drone has only violated the right to privacy, or only violated the right to data protection, or both.

[361] CJEU Joined Cases C-293/12 and C-594/12.
[362] ibid para 48, herein the CJEU acknowledges the important role played by the protection of personal data in the light of the fundamental right to respect for private life; also see Case C-275/06, Promusicae v. Telef´onica de Espana SAU at para 68 of the judgement and Joined Cases C92/09 & C93/09, Schecke v. Land Hessen at para 52 of the judgement.
[363] ibid Digital Rights Ireland, para 32-37 and 39-40.

5.1.5. Convention 108 and Convention 108+

Convention 108[364] was enacted to protect individuals, among others, from the automation in the processing of personal data. There was an absence of an international data protection framework, at that time, which was filled by Convention 108. Article 1 of the Convention states:

> 'The purpose of this Convention is to secure […] for every individual […] respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him (data protection).'

It is also an international framework and applies to member countries of the COE. However, European non-member States, and non-European non-member States can accede to this Convention.[365] Due to the challenges posed by new technologies, Convention 108 has been modernised into Convention 108+.[366] Some of the new enhanced provisions in the modernised Convention 108 are, application of the privacy by design principle, application of data protection principles to all processing activities including for national security reasons, new rights for individuals in an

[364] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 1981 (entered into force in 1985).
[365] https://www.coe.int/en/web/conventions/full-list
[366] Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 2018 (Convention 108+) < https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223>

algorithmic decision making process by an artificial intelligence, stronger accountability for data controllers, and more.[367]

5.1.6. Multi-level system of protection

Fundamental rights are also included in Constitutions around the world. For instance, the German Basic Law[368] guarantees basic rights, as enshrined in Articles 1 to 19. The fundamental rights contained in Constitutions are enforceable against State actors as a matter of policy, like in the ECHR and the CFREU. However, the Portuguese Constitution states in Article 18 paragraph 1, that the provisions 'regarding rights, freedoms and guarantees are directly applicable to and binding on public and private persons and bodies.' This is an example of direct application of human rights on private individuals at a national level.

Due to the multi-level system existing in the EU, (ECHR, CFREU, and the EU member States Constitutions), for the protection of fundamental rights, the friction between the three levels, for autonomy and authority is only further exacerbated. This friction is ameliorated between the ECHR and CFREU, to an extent, by Article 52 (3) of the CFREU. In the case of fundamental rights contained in national Constitutions of member States of the EU, they are hierarchically below the CFREU. Given this, one would understand that the constitutional courts of the member States are duty bound to apply the CFREU in matters relating to fundamental rights. To an extent, it is true.

[367] ibid.
[368] Grundgesetz für die Bundesrepublik Deutschland 1949.

In the case of *Åkerberg Fransson*,[369] the CJEU in para 29 of the judgement noted:

> 'where a court of a Member State is called upon to review whether fundamental rights are complied with by a national provision or measure which, in a situation where action of the Member States is not entirely determined by European Union law, implements the latter for the purposes of Article 51(1) of the Charter, national authorities and courts remain free to apply national standards of protection of fundamental rights, provided that the level of protection provided for by the Charter, as interpreted by the Court, and the primacy, unity and effectiveness of European Union law are not thereby compromised'

Article 51 (1) of the CFREU states, 'The provisions of this Charter are addressed to the […] Member States only when they are implementing Union law.' In other words, when the EU member States are not implementing Union law, they are free to exercise their own discretion, but when they are implementing Union law, they have no discretion as hierarchically they are inferior.

Fundamental right to privacy and data protection, in the case of civilian drone use, can also have multilevel protection standards where each member State of the EU has its own national rules on the protection of the right to privacy from civilian drones,[370] by virtue of Article 56 (8) of the new basic law governing drones.

[369] Case C-617/10.

[370] Joaquín Sarrión, Actual challenges for fundamental rights protection in the use of drone technology (2018).

Article 56 (8) states that there is a 'possibility for Member States to lay down national rules to make subject to certain conditions the operations of unmanned aircraft for reasons falling outside the scope of this Regulation, including public security or protection of privacy and personal data in accordance with the Union law.'

In the case of *Stefano Melloni*,[371] the CJEU in para 60 of the judgement noted:

> 'It is true that Article 53 of the Charter confirms that, where an EU legal act calls for national implementing measures, national authorities and courts remain free to apply national standards of protection of fundamental rights, provided that the level of protection provided for by the Charter, as interpreted by the Court, and the primacy, unity and effectiveness of EU law are not thereby compromised.'

The CFREU mandates that the fundamental rights contained in the EU member States Constitutions, should be, as far as possible, interpreted in harmony with the CFREU. In this regard, Article 53 of the CFREU states:

> 'Nothing in this Charter shall be interpreted as restricting or adversely affecting human rights and fundamental freedoms as recognised, […] by the Member States' constitutions.'

From the above, it can be said that the relationship between fundamental rights contained in the EU member States constitutions and the CFREU, will depend on three situations. First, where the

[371] Case C-399/11.

subject matter is fully harmonised by EU law, second, where the subject matter is not harmonised by EU law, and third, where the subject matter is fully harmonised by EU law but at the same time EU member States are given a margin of appreciation (leeway) to adapt the subject matter according to their national requirements. In the case of drones, it is of the third kind, where the right to privacy and data protection is fully harmonised by EU law, but at the same time, EU member States are given a leeway to adapt the provisions according to their national needs.[372]

With regards to the three situations, the German Constitutional court adopts a dual approach.[373] Where the subject matter is fully harmonised by EU law, CFREU prevails and domestic fundamental rights have no role to play, but where the subject matter is not harmonised by EU law, or where, even though it is fully harmonised, EU member States are given a leeway, then the CFREU and the domestic fundamental rights are parallelly applicable, the CFREU acting as a standard of review.[374]

The problem with this system, when it comes to drones, is that differential standards of visual privacy protection will exist in the EU member States.

---

[372] See Article 56 (8) of Regulation (EU) 2018/1139.

[373] Dana Burchardt, 'Backlash against the Court of Justice of the EU? The Recent Jurisprudence of the German Constitutional Court on EU Fundamental Rights as a Standard of Review' (2020) 21 German Law Journal 1; also see, 1 BvR 16/13 and 1 BvR 276/17, the twin cases decided by the Federal Constitutional Court of Germany regarding the relationship between domestic fundamental rights and CFREU.

[374] ibid.

In this multi framework protection of fundamental rights, the hierarchy is quite evident, regardless of the camaraderie between the three frameworks. The ECHR comes out as the Godfather, followed by the CFREU, and then the domestic fundamental rights.

5.1.7. Drittwirkung and the problem of applicability to private relations

Although fundamental rights are primarily enforceable against the State, Article 8 of the ECHR has been indirectly applied between private parties. In the EU, there is a concept of *Drittwirkung*, born out of the German jurisprudence, which means that an individual can rely on the national bill of rights to sue another individual for the violation of those rights.[375] In other words, it allows for the horizontal application of human rights between private individuals rather than the vertical application between individuals and the State.

In *X and Y v The Netherlands*[376] where criminal proceedings were unavailable against the perpetrator of sexual assault on a minor girl who was mentally handicapped, the ECtHR reasoned that the State has not only a negative obligation to not interfere with the ECHR rights but also a positive obligation to protect individuals from interference from others. In *Reklos and Davourlis*, cited earlier, a case where a picture was taken by a private professional photographer the ECtHR held that there was an infringement of

[375] 7 BVerfGE 198 (Lüth case 1958); also see Andrew Clapham, Human Rights in the Private Sphere (Clarendon Press 1993).
[376] X and Y v. the Netherlands, 26 March 1985, Series A, no. 91; also see Reklos and Davourlis v. Greece, no. 1234/05, ECHR 2009 (para 35).

Article 8 of the ECHR. Thus, it is not inconceivable that private persons can come within the ambit of the ECHR, but indirectly, through the State.

In *Schüth v Germany*[377] the ECtHR noted:

> 'The Court further observes that, although the object of Article 8 is essentially that of protecting the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private life. These obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves'[378]

Despite this claim, Article 1 of the ECHR states, 'The High Contracting Parties shall secure to everyone within their jurisdiction the rights and freedoms defined in Section 1 of this Convention.' The High Contracting Parties are Nation States and not private persons. Exceptionally, the EU as a supranational union may be a party to the ECHR, by virtue of Article 59. A plain reading of Article 1 does not say much against whom the rights shall be secured, whether public authorities, private corporations, or individuals. It is inferred from Article 1 that the High Contracting Parties have a positive obligation to secure rights against any entity

[377] Schüth v. Germany, no. 1620/03, ECHR 2010.
[378] ibid para 55.

that encroaches, within their jurisdiction, whether natural or legal, in addition to a negative obligation not to encroach upon the rights of individuals by the High Contracting Parties themselves.

Article 19 of the ECHR states, 'To ensure the observance of the engagements undertaken by the High Contracting Parties […]' which means that primarily the ECtHR is set up to redress violations by nation States. This argument is even more strengthened by Article 34 of the ECHR which states, 'The Court may receive applications from any person […] claiming to be the victim of a violation by one of the High Contracting Parties […]' and not private individuals. Going through the ECHR one can say that it is directed towards the States who are members of the Council of Europe. The States secure the rights under the ECHR by providing the legal forum to address violations as and when they arise, like legislations and courts.

For example Article 7 of the ECHR states, that 'No one shall be held guilty of any criminal offence on account of any act or omission which did not constitute a criminal offence under the national or international law at the time when it was committed […]' In the case of *X and Y v The Netherlands*, cited above, there was a gap in the national law which prevented the perpetrator of the crime from being prosecuted, it was the fault of the legislature and so the State is liable to enact provisions to prevent encroaching of rights by private persons. It is not always that the States are aggressors but people in their private capacities may also encroach

upon the rights of others. The State can however fail in its obligations to provide a forum to address those aggressions.

Article 13 of the ECHR states, 'Everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy […] notwithstanding that the violation has been committed by persons acting in an official capacity,' which means that the ECHR also does consider that it is not always that persons in official capacity are aggressors, private persons may as well violate the rights and freedoms. So, we may say, as an instrument, the ECHR is addressed not only to the States but also to individuals in their private capacities. However, the States have the primary responsibility to ensure its adherence between private relationships. In other words, the ECHR is indirectly applicable between private persons and not directly.

Moreover, the preamble to the ECHR directs the governments of European countries to enforce certain of the rights stated in the Universal Declaration of Human Rights but the Universal Declaration in its preamble proclaims the Declaration as the common standard of achievement for all peoples and nations meaning that it is directed even towards private persons and not just the State. Article 29 of the Declaration expresses in paragraph 1 that everyone has duties towards the community and not just State actors. Further in Article 30 of the Declaration it is explicitly mentioned that private persons have duties and responsibilities to not engage in activities that destroy the fundamental rights of

others. So, the Declaration, as a general rule, imposes obligations directly on private persons and not indirectly.

The preamble to the CFREU states, 'Enjoyment of these rights entails responsibilities and duties with regard to other persons […]' and so, as the rights are enjoyed by private persons, they have to act in a way that does not violate other's fundamental rights. But in Article 51 of the CFREU, the rights are ensured primarily against the institutions and bodies of the EU and secondly to EU member States only when they are implementing Union law and no obligation has been fastened onto private persons. However, Article 52 in paragraph 3 of the CFREU, states that the meaning and scope of the rights contained in the CFREU, which corresponds to the rights guaranteed by the ECHR, shall be the same as in the ECHR. In other words, as member States of the EU are primarily liable for the infringement of the fundamental rights contained in the ECHR (as they are part of the Council of Europe) by extension they are primarily liable under the CFREU as well. And as the ECHR is indirectly applicable to private persons, so is the CFREU.

Nation States are becoming more toothless with the rise of transnational corporations and supranational organisations like the EU. The traditional approach is that the Nation States are responsible under international law for international human rights violations, as they are the ones who make the rules. But the waning authority of the political system and the influence of economically mighty transnational corporations in the legislative and decision-

making process makes us want to rethink whether the obligations imposed on the States alone are sufficient.

Andrew Clapham reasons that the State centric approach should be retained, but additionally, obligations are also directly applicable on non-state actors such as transnational corporations.[379] They are not rule makers but the obligations arising out of the rules apply to non-state actors directly as they are powerful enough to exploit human rights.[380] But those who favour the State centric approach feel that it will dilute the responsibility of the States to protect human rights if obligations arising out of international law directly applied to non-state actors.[381] But under international criminal law private individuals are directly responsible if they have committed the crime of genocide or other crimes against humanity.[382]

If human rights obligations are imposed on private individuals directly then there will be a multitude of human rights violations as any wrongful act in most circumstances will violate another's human right and some so trivial as a parent scolding their children for holding a different opinion. This will impose a massive burden on international human rights court.

The point of this discussion above, is to determine, whether the fundamental right to privacy and data protection as enshrined in the ECHR and the CFREU, is enough to deal with infringements of

[379] Andrew Clapham, Human Rights Obligations of Non-State Actors (Gráinne de Búrca, Brunno de Witte, Francesco Francioni, eds., Oxford University Press 2006) 25-58.
[380] ibid.
[381] ibid.
[382] ibid.

visual privacy by private individuals and corporations using civilian drones. It will not be enough if we hold that only States are responsible for fundamental rights violations, but on the other hand, if we are to dilute the States responsibility and hold even private individuals liable for fundamental rights violations it will result in unmanageable litigation. An additional problem lies with the multilevel system of protection as this will give rise to differential standards of privacy protection at the national level.

It is not easy, to give an answer to the question, whether the current frameworks can handle the infringement of the visual privacy, if there were substantial cases, due to private individuals using civilian drones. The contradictions in scholarships are very evident where on the one hand fundamental rights can only be enforced against the States, while on the other, based on indirect application, it can also be enforced between private individuals. Direct application, however, will be more convenient for a victim of visual privacy infringement by private individuals using civilian drones, rather than indirect application. However, direct application falls within the margin of appreciation of the Contracting States which gives rise to differential standards of privacy protection in a multilevel system.

5.2. Visual privacy and its offshoots within the two frameworks

In section 4, we discussed that there are two kinds of physical visual information, one which is recorded and one which is unrecorded. Recorded visual information is treated like alphanumeric information under the right to data protection (discussed further below). As physical visual information, in any form, which can be identified to a particular individual, is the subject matter of visual privacy, we will discuss it within the two fundamental rights frameworks. The offshoots of visual privacy are, physical privacy, image rights, and visual data protection.

5.2.1. Visual privacy

Visual privacy has been extensively discussed in the previous sections 3 and 4, so the aim here is to be brief. Visual privacy is required for the development of intimate family relationships, intimate activities like sexual intercourse, the development of personality, the protection of personal integrity, and it even extends to personal belongings. Privacy from visual surveillance by private individuals, corporations and governments will also fall under the category of visual privacy.

But as discussed, it can be infringed, either in flesh or by technological means. A physical invasion of visual privacy (for instance, an individual seeing through a keyhole, a passionate sexual intercourse between a husband and wife without their consent), where the visual information has not been processed or

recorded by technological means, fits within the protection of Article 8 of the ECHR and Article 7 of the CFREU. But it cannot be protected by Article 8 of the CFREU as it is not data until it has been processed or recorded.

There is also a grey area, where technology is used, to project the physical visual information, which is at a distance, so that it is within the VLOS of the observer, without the information being recorded. It is like seeing through a binocular, the physical lives of others, when the natural ability to see is not enough. In this case, the challenges to protection faced are, firstly, it is covert, meaning, an individual will be ignorant that he and his physical space is being projected somewhere else, and secondly, there is no right of action under the ECHR or the CFREU as that observation is treated as harmless.

But once that physical visual information is processed or recorded, it comes within the ambit of Article 8 of the CFREU, which accords ample protection to the processing and recording. The processed or recorded information is additionally protected by even Article 8 of the ECHR and Article 7 of the CFREU.[383]

In the case of Söderman v Sweden,[384] which involved covert filming of a minor, the ECtHR held it to be a violation of Article 8 of the ECHR. The ECtHR also referred in this judgement, to the Supreme Court of Sweden's observation, that the ECHR did not impose duties on individuals and an individual could not be obliged

[383] See Z v. Finland, 25 February 1997, Reports 1997-I.
[384] Söderman v Sweden, no. 5786/08, ECHR 2013

to compensate another individual directly on the basis of the ECHR.[385] The Supreme Court of Sweden's observation implies, that visual privacy infringements by civilian use of drones, cannot be solved by the two frameworks directly. The protection of visual privacy needs to be achieved indirectly at the national level of the EU member States.

But if it is to be achieved indirectly, then individual EU member States have a margin of appreciation and must abide by the principle of proportionality while balancing the right to visual privacy from drones with other fundamental rights.

Visual privacy and physical privacy overlap to a certain extent, as visual privacy can relate to the physical self. In this respect, physical visual privacy is violable even without a physical trespass. In such a case, despite there being a violation of physical visual privacy, most cases will be unactionable.

5.2.2. Physical privacy

Keeping in mind the technology in discussion, we are concerned with the relationship between physical privacy and trespass. Basically, physical privacy denotes privacy of the person within a physical space, in other words, inaccessibility of the physical self to the outside world. It can aptly be described by the saying 'a man's home is his castle.' A person is free to defend his home and in turn his person from unjustified intrusion or trespass. That intrusion or trespass may be by an individual or a machine, like a drone. An

[385] ibid para 47

individual who enters another's home, to cause violence to the owner of the home, is violating the physical privacy of the owner.

But physical privacy extends beyond violence to a person and includes visual and auditory intrusion of a person. Physical privacy intrusion does not have an element of publication or distribution of information. It is complete as soon as the intrusion takes place. Using of civilian drones may result in the infringement of physical privacy whether flown over private property or not.

Physical privacy is protected by article 8 of the ECHR. Article 8(2) of the ECHR specifically prohibits intrusions by public authorities into homes, if it is not within the confines of that article. With regards to intrusions by private individuals, although not covered directly under Article 8 of the ECHR, it is covered indirectly as States not only have a negative obligation to not interfere, but also a positive obligation to ensure that private individuals do not intrude into other people's homes.

It is not always that an actual trespass or intrusion into a private property will infringe physical privacy. It may only result in a claim of trespass or sanctions under the criminal law, like house breaking. But a trespass into homes to clandestinely install video cameras for the purposes of evidence gathering, will result in the violation of physical privacy. The case for infringement of physical privacy will be stronger if the property comes within the meaning of a home. Home has a more personal connotation than just private property. It is also not necessary to own the property to call it home. A house may be on rent or on a lease but if it is there that a person resides

with his family building intimate relationships then it will be called a home irrespective of the status of legal ownership.

In the case of *López Ostra v Spain*,[386] a case of nuisance (environmental pollution) affecting the right to physical privacy, the ECtHR held it to be a violation of Article 8 of the ECHR. In this case, the applicant complained about the pollution (gas fumes, pestilential and irritant smells, repetitive noise, and contamination) from a plant for the treatment of liquid and solid waste, which affected her family's quality of life (nausea, vomiting, allergic reactions, anorexia). Although, this case has little to do with visual privacy, it is important to show the extent of protection accorded to physical privacy by the ECtHR.

Article 1 of Protocol number 1 to the ECHR contains the right to property. It states:

> 'Every natural or legal person is entitled to the peaceful enjoyment of his possessions. No one shall be deprived of his possessions except in the public interest and subject to the conditions provided for by law and by the general principles of international law.
>
> The preceding provisions shall not, however, in any way impair the right of a State to enforce such laws as it deems necessary to control the use of property in accordance with the general interest or to secure the payment of taxes or other contributions or penalties.'

[386] López Ostra v. Spain, no. 16798/90, ECHR 1994.

In some instances, a violation of this right by trespass into homes, may have a bearing on Article 8 of the ECHR and physical privacy, as in the case *Cyprus v Turkey* cited above.[387] Article 17 of the CFREU, containing the right to property corresponds to Article 1 of Protocol number 1 to the ECHR. It will be safe to assume that the relationship between trespass or intrusion and physical privacy violation will be the same in the CFREU as it is in the ECHR.

5.2.3. Image rights

5.2.3.1. Concept

Image rights is a subset of visual privacy because visual privacy has a wider scope of application than image rights. An image is a replication of the physical visual information in a 2 D form. Image rights are mostly restricted to images of natural persons (with a few exceptions of personal belongings) whereas visual privacy, without exception, will include all images, like, images of houses, car number plates and physical visual information which has not yet been transformed into a photograph. There are some marked differences between the two rights, for example, the taking of images or video recording is not necessary for a violation of visual privacy whereas the taking of pictures and video recordings is necessary for a violation of image rights. The subsequent use of the taken pictures and video recordings will solidify the violation of image rights. Additionally, image rights in some instances protects

[387] Cyprus v. Turkey, no. 25781/94, ECHR 2001; also see Affaire Halabi v. France, no. 66554/14, ECHR 2019, wherein it was held that public officials who entered a home without the consent of the occupier or owner violated Article 8 of the Convention.

the monetary value in an image whereas it is absent in visual privacy (publicity rights).

An image of a person has a distinct characteristic as no two person's images is the same. They may look alike, in the case of twins, but there are always some characteristics that differentiate one from the other, for example, one of them having a mole. A person grows in his image, meaning that some become public personalities, famous figures, sport stars, actors, and musicians while others must be content with an anonymous existence. So, the value in an image is proportional to the hard work and labour put into making oneself successful. Luck too plays a role as the right circumstances are necessary for the success of any person. It is not always necessary that labour is the reason why a person is famous. A person can be born into fame.

The masses which consist of anonymous people emulate the people who have gained success and fame as deep within they wish they were like them, for instance, individuals wanting to have a David Beckham haircut. So, it is normal for successful people to commercialise their image. This is done by endorsing brands of food, medicine, clothing, sports gear, and many others in the industry. Through endorsements they are paid the monetary value of their image. Some are paid more than the others as they are more successful. It is reasonable then for them to object if their image is used without their consent as it could ruin the personality that they have established for themselves. Mother Teresa's image being used

in advertisements of right-wing political parties will be contrary to the saintly image which she established for herself.

Images of anonymous people do not have monetary value as the public is least interested in what they do, except for the people who know them. However, although their image is not capable of being commercialised, it is still protected if it is abused and affects their dignity. Therefore, image rights protect both the dignity and the monetary value in an image.

In the EU, the rationale behind image rights is basically to protect the dignity of an individual. Monetary value in a person's image has generally been accorded less importance than dignity. Image rights emanate from the ECHR and property rights in Europe. Property rights because image is treated as a commercial product which has a monetary value, in few cases. However, monetary value is not the sole criteria to grant image right protection in the EU.[388] The legal right to protection of one's image, however, is not uniform in the EU. The EU member States have their own independent provisions for the protection of image rights.

In Spain, image rights are Constitutional rights guaranteed by Article 18 of the Constitution. The 1982 law on the protection of Honour, Privacy and Image accords civil law protection to image

[388] The Spanish Supreme Court dealt with a case involving a booklet titled 'Respeto a los mayores' (Respect for seniors) published by the City of Madrid. The case was brought by persons whose photos appeared in the booklet which were taken in a public place without their consent. The court held that although the publication of the booklet and the picture was for non-commercial purposes, it anyway was publication within the meaning of Article 7.6 of the 1982 Organic law.

rights in Spain.[389] In France, it originates from personality rights established by case laws.[390] It enables individuals to prevent unauthorised fixation and reproduction of their image. In Germany, a specific right to one's own image is contained in Section 22 of the Kunsturhebergesetz (copyright in works of art and photography). Image rights in Germany can also be inferred from the rights in personality.[391] In Italy, image rights emanate from the Italian Civil Code and Copyright law.[392] Netherland protects image rights through the Copyright law.[393]

Image rights are fundamental rights as they emanate from Article 8 of the ECHR, (although not expressly appearing in the Article) but at the same time, they are also protected by the Civil law systems of the member States of the EU. Therefore, image rights are enforceable not only against the State but even between private individuals directly. Thus, we can say that recorded physical visual information, in the form of an image, has a wider degree of protection, when it comes to violations by private individuals, than unrecorded visual information.

Images can take various forms. It can be in the form of a still picture, in the form of moving pictures or in the form of an art, like

[389] Ley Orgánica 1/1982 de 5 de mayo de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen.
[390] Elisabeth Logeais and Jean-Baptiste Schroeder, 'The French Right of Image: An Ambiguous Concept Protecting the Human Persona' (1998) 18 Loyola of Los Angeles Entertainment Law Review 511.
[391] Susanne Bergmann, 'Publicity Rights in the United States and Germany: A Comparative Analysis' (1999) 19 Loyola of Los Angeles Entertainment Law Review 479.
[392] See Article 10 of the Civil Code and Articles 96 and 97 of the Copyright Law.
[393] See particularly Article 21 of the Copyright Act.

a painting or a caricature. With the help of technology images can also be manipulated and abused. The swapping of faces onto another person's body is also possible with a digital image. Using of images of underage girls and boys on dating websites, where the minimum age required to use the services of the website is 18 years, or, posting images of someone else's property on Airbnb for rent are all examples of image abuse. Therefore, there is no reason to restrict image rights to just the face of a natural person. Immovable as well as personal movable properties should all be accorded the protection of image rights, provided it can be identifiable to an individual.

The limitations, like does image rights exist in an edited picture cannot be answered concisely. It is possible to identify the natural person in an edited picture from the body shape, the clothes that are worn in the picture, the posture, or the skin tone. But the issue is whose image right is at stake? Is it the person whose face appears in the image or the person whose face has been swapped? The answer should be that if the image can be identified, irrespective of the degree of edition, then image rights should be granted and not otherwise. But it will also be difficult to determine whose image rights are we protecting here, the person with the face or the person to whom the body belongs. For example, a well-known politician has been clandestinely photographed going to a psychologist, but the image has been manipulated with someone else's face. Now whose reputation is at stake, the person whose face appears in the image or the physical body of the actual person in the photograph?

One may immediately jump to the conclusion that the person whose face appears in the photograph is the person whose reputation is tarnished, but that is far from being reasonable. It could also be the person whose body appears in the photograph whose reputation is tarnished, depending on various factors, like, the individual who is analysing the photograph, the context of the photograph, the precision of the edited picture etc.

It is not always that publishing of images will result in image rights violations. Visual privacy rights, including image rights, must be balanced with the right to freedom of expression as contained in Article 10 of the ECHR. But will it make a difference if the image is, of a known personality or anonymous individual, taken in a public space or a private space, altered or original, taken with consent or without consent, a drawing, or a picture, identifiable or non-identifiable, of family life or public life and blurry or sharp? These variables determine the scope of image rights. The number of variables increase when there is a combination of two or more variables, like, when a blurry image is taken without consent in a public space of a known personality. As can be seen from the history of judgements of the ECtHR, the variables do make a difference in determining image rights.

5.2.3.2. ECtHR's case laws on image rights

There is a plethora of cases dealing with image rights violations in the EU. However, we will select only a few of them to understand the subject of image rights better. The cases have been classified broadly under two categories, where image rights violations have

been upheld and where image rights violations have not been upheld and instead given way to the right to expression.

Cases where image right violations have been upheld:

In the first *Von Hannover v Germany*[394] case, which involved a series of photographs, decided by the ECtHR, photographs of Princess Caroline of Monaco taken by German paparazzi in a public place, breached her privacy. In this first case, Princess Caroline applied to the German courts for preventing further publication of her photographs in German magazines relating to her private life. Her application was partially allowed relating to a few photographs, but the rest dismissed by the German courts and as a result she filed an application with the ECtHR. She alleged that her right to respect for private life (Article 8 of the ECHR) had been infringed as the photographs were taken without her consent. The German courts had concluded that the photographs were taken in a public place and Princess Caroline being a public figure of contemporary society had to be more open about the publication by the entertainment press, as the public had a right to know.[395] The ECtHR on the other hand

[394] Von Hannover v. Germany, no. 59320/00, ECHR 2004-VI.

[395] See also Judgment 18/2015 of the Spanish Constitutional Court of 16 February 2015, wherein it overturned a decision of the Spanish Supreme Court and held that the Constitutional protection to freedom of information requires that the information have public relevance even if the information is true referring to the Von Hannover v. Germany case. The Spanish case involved a famous person who was in a private moment in public with his partner and his image was captured and disseminated without his consent by television gossip programmes. The Supreme Court came to the finding that he dragged his relationship in the public domain and did not take the necessary measures to keep it private and so he could not complain about the infringement of his image rights; also see Judgment 518/2012 of the Spanish Supreme Court of 24 July 2012 wherein it was held that the dissemination of secretly captured images

held that there had been a violation of Article 8 of the ECHR and reasoned that the general public interest in her life and the commercial interest and the right to freedom of expression of the magazine had to give way to her right to respect for private life.

In *Axel Springer AG and RTL Television GmbH v. Germany*[396] the applicants Axel Springer and RTL television alleged an infringement of their right to expression under Article 10 of the ECHR. The case involved a defendant who was charged and arrested for killing his parents and dismembering the bodies and flushing it down the toilets. The defendant confessed to the crime during the investigation and it was at this time that pictures taken when he was younger was published by German newspapers reporting on this case. At the trial of the defendant, photographers representing the applicant companies attended the hearings to take still photographs and video recordings of the defendant. Prior to the start of the hearing, however, the presiding judge orally made it clear that the defendant's face had to be unidentifiable by technological means before any pictures of him are published. The ECtHR held that the presiding judge's order was not an infringement of their right to the freedom of expression and that the judge had rightfully balanced the right of the public to know and the personality rights of the defendant.

---

of Spanish model Elsa Pataky during a professional photoshoot in an isolated part of a beach violated her image rights.

[396] Axel Springer AG and RTL Television GmbH v. Germany, no. 51405/12, ECHR 2017.

In *Bogomolova v. Russia*[397] the ECtHR was faced with the question, whether the use of a minor's image, on the cover of a booklet meant to inform the public about the local authorities' efforts to protect orphans and families looking to adopt, without parental authorisation, constituted a violation of Article 8 of the ECHR. The court concluded that it did violate the child's right to private life as the child's mother had only consented to her child being photographed without consenting that the photograph be published. The court also noted that false impressions were likely that the child was an orphan and abandoned by his parents.

In *Kurier Zeitungsverlag und Druckerei GmbH (no. 2) v. Austria*[398] and *Krone Verlag GmbH v. Austria*,[399] the two cases involved compensation proceedings brought by a mother and child against two publishing companies, on account of their newspapers publishing the dispute of the parents over the custody of the child. The article published revealed the child's identity and gave details of his personal and family life along with a photograph that showed him in a state of despair. The ECtHR held that given the fact that the parents of the child were not public figures it was not essential to publish the child's photograph to understand the case. The court was not convinced by the publishing companies' arguments (the applicants) that it was necessary to publish the picture in order to draw attention to the issue.

[397] Bogomolova v. Russia, no. 13812/09, ECHR 2017.
[398] Kurier Zeitungsverlag und Druckerei GmbH (no. 2) v. Austria, no. 1593/06, ECHR 2012.
[399] Krone Verlag GmbH v. Austria, no. 27306/07, ECHR 2012.

In a recent case between the *Duchess of Cambridge and the celebrity magazine 'Closer,'* a court in France upheld the right to privacy of the Duchess and her husband the Duke of Cambridge, when their photographs were taken and published without their consent by the magazine.[400]

Cases where image right violations have not been upheld:

In the second *Von Hannover v Germany* case[401] which related to photos of Princess Caroline and her husband on a skiing holiday, published alongside an article about the health of her father Prince Rainier III of Monaco, the German courts held that there was no infringement of the right to respect for private life as the pictures were published in relation to an article of general public interest. The ECtHR upheld the reasoning of the German courts and concluded there had been no violation of Article 8 of the ECHR. They reasoned that the photographs were published in relation to an article of general debate and that the right to respect for private life had to be balanced with the right of expression of the magazine. It also concluded that the EU member States enjoyed a margin of appreciation when balancing the two opposing rights.

In *Schüssel v. Austria*[402] the Deputy Prime Minister of Austria complained, relying on Article 8 of the ECHR, that the use of his picture on stickers, which were half overlapped with a picture of a

[400] K Corcoran, 'French court orders fines in Kate photos case' (Business Insider 2017) <www.businessinsider.com/ap-the-latest-french-court-orders-fines-in-kate-photos-case-2017-9> accessed 8 October 2017.
[401] Von Hannover v. Germany (no.2), nos. 40660/08 and 60641/08, ECHR 2012.
[402] Schüssel v. Austria, no. 42409/98, ECHR 2002.

right-wing politician, with the slogan, 'The social security slashers and the education snatchers share a common face,' infringed his right. The ECtHR found his application inadmissible and reasoned that the Austrian Supreme Court had correctly balanced his right of image with the general interest in a political debate protected by Article 10 of the ECHR.

In *Vereinigung Bildender Kunstler v. Austria*,[403] the ECtHR had to deal with an art exhibition where one of the works on display was a painting entitled 'Apocalypse' by Austrian artist Otto Mühl. The painting contained sexual depictions of public figures, including Mother Teresa and various members of the Austrian Freedom Party. One of the former Freedom Party member depicted was Mr. Meischberger gripping the ejaculating penis of Jörg Haider (a Freedom Party member) while being touched by two other Freedom Party members and ejaculating on Mother Teresa. Mr. Meischberger sued the artist association who organized the art exhibition seeking an order to prevent the further exhibition of the painting contending that the painting depicted him as a loose character. The Vienna court of appeal reversed the trial court order and granted a perpetual injunction against the artist's association from exhibiting the painting again in line with image rights. The artist's association filed an application with the ECtHR claiming that their right to freedom of expression under Article 10 of the ECHR had been violated. The ECtHR agreed with the artist's association's claim of infringement of their right to expression. It noted that Mr. Meischberger was a political figure who must

[403] Vereinigung Bildender Kunstler v. Austria, no. 68354/01, ECHR 2007.

display a wider degree of tolerance in respect of criticisms having satirical elements.

Couderc and Hachette Filipacchi Associés v. France[404] is a case where the publication director and publisher of the weekly magazine Paris Match were convicted after they published a ten-page article headlined 'Albert de Monaco: Alexandre, l'enfant secret', which also contained several photographs. The ECtHR held that there had been a violation of Article 10 of the ECHR and given the nature of the information it could be understood that it contributed to a subject of public interest.

5.2.3.3. Reference to cases from the Common law jurisdictions:

The Common law jurisdictions, such as the US and the UK, protect the monetary value in an image and not dignity. In the US, a right in one's own image is protected by the right of publicity. It is different from image rights in Europe as it is more economically oriented. It was in *Haelan Laboratories v. Topps Chewing Gum*[405] where the right of publicity was first acknowledged in 1953 and which related to the publication of pictures of baseball players. It was felt in *O'Brien v. Pabst Sales Co.,*[406] where the right to privacy was applied in a case where a photograph of a famous football player was used in a beer advertisement, that the right to privacy did not protect images of personalities from being used by others for

[404] Couderc and Hachette Filipacchi Associés v. France, no. 40454/07, ECHR 2015.
[405] Haelan Laboratories v. Topps Chewing Gum, 202 F.2d 866 (2nd Cir. 1953).
[406] O'Brien v. Pabst Sales Co., 124 F.2d 167 (5th Cir. 1941).

commercial gains. As the footballer was a public figure, he was not harmed by the publicity which he personally sought.

In the United Kingdom there is no specific right to one's own image. Usually, the person who is aggrieved, must bring an action based on one of the torts, like the tort of passing off or breach of confidence.[407] The principles of these torts are modified to accommodate new situations. In *Irvine v. Talksport Ltd.*,[408] a race car driver filed a lawsuit, alleging a tort of passing off, against a radio station which used his image in a promotional brochure. In a tort of passing off there must be a common field of activity between the plaintiff and the defendant whereby the consumers are led into confusion because of the use of another's goodwill. However, in this case although the race car driver and the radio station did not share a common activity the court held it was not necessary for there to be a common activity for the applicability of this tort. It is enough if the use of someone's goodwill and reputation is unlicensed.

The fundamental difference we can draw from our discussion on image rights is that the EU has far broader protection, meaning that it protects not just the commercial value but also the dignity in an image, whereas the focus of the Common law jurisdictions is on the commercial value.

---

[407] See cases, Douglas v Hello, [2005] EWCA Civ 595, [2005] 4 All ER 128, [2005] 3 WLR 881, [2006] QB 125; Campbell v Mirror Group Newspapers Ltd, [2004] UKHL 22, [2004] 2 WLR 1232, [2004] 2 AC 457, [2004] UKHRR 648, [2004] EMLR 15, 16 BHRC 500, [2004] HRLR 24, [2004] 2 All ER 995.

[408] Irvine v Talksport, [2003] EWCA Civ 423, [2003] 2 All ER 881, [2003] EMLR 538.

It may be noted that the image rights are, more often than not, contested by personalities and famous people. But their image rights are also restricted as personalities must be more open to criticisms about their persona. It may also happen that instead of their image, things that are associated with a personality, like a particular hat, walking stick, car or even a phrase used by a celebrity may be used in reference to the person.[409] The purpose of using objects is to get around the idea of image rights but the public perception doesn't change. The public still associate the objects with the image of the personality and so the courts have repeatedly treated it as an infringement of image rights. However, images used as an art are protected by copyright even though it is the using of another's image. It could be in the form of parody, caricature, or other enhancements to the image. So, copyrights limit the extent of image rights. But can edited pictures be considered a form of art?

5.2.4. Visual data protection

Protection against the unlawful processing of visual data is robust, comprising layers of protection in the EU. Article 8 of the CFREU is the innermost layer containing the fundamental right to data protection. The EU, in fulfilment of its positive obligations under the CFREU, has legislated the GDPR, an outer layer, which is an EU level regulation. Its predecessor was the DPD. The GDPR, although outside the league of fundamental rights, is applicable throughout all the member States of the EU without there being a

[409] Motschenbacher v. R.J. Reynolds Tobacco Company, 498 F.2d 821 (9th Cir. 1974).

need to transpose it into the national laws, while the DPD needed to be transposed. Then there is Convention 108+ for protection against the automatic processing of personal data.

Due to a broad interpretation by the ECtHR, Article 8 of the ECHR also includes the right to data protection, as stated above. As the scope of the CFREU rights are the same as those in the ECHR, it means that the right to data protection is also protected by Article 7 of the CFREU. Processing visual data with the help of a drone and its camera will be covered by the layers.

The GDPR implements Article 8 of the CFREU and details the conditions necessary for the processing of personal data and the rights that an individual can have against another individual or a corporation. What this means is that the EU has provided the measure at an EU level for the protection of personal data from unauthorised processing by private individuals and corporations. Now if the GDPR were to fall short of its intended purpose and individuals not protected from unauthorised personal data processing, for example, new technologies which process personal data in ways not anticipated under the GDPR, an individual should be able to bring an action against the EU for failing to provide the necessary measures to protect an individual's right to data protection under Article 8 of the CFREU.

Article 8 right of the CFREU (in the form of GDPR), is enforceable against not only corporations but even private individuals. So, for an individual who has a right of action against a drone enthusiast or a corporation for the infringement of his visual privacy, he can

totally skip basing his action under Article 7 of the CFREU and instead wholly rely on Article 8 of the CFREU, which provides a private individual a safety net in the form of the GDPR, as drones even relaying data without any recording, are covered under the broad definition of processing in the GDPR. Therefore, there is no need for an individual to contest his right to privacy which offers him little protection from individuals and corporations.

A more detailed discussion on visual data protection has been undertaken below in the section GDPR.

Summary: -

Even though the use of drones will infringe the right to privacy and the right to data protection, these rights cannot be enforced against private individuals or corporations under the CFREU or the ECHR directly, for stated reasons. The recourse that an individual has is to rely on the GDPR, national camera surveillance legislations, or the civil law of the member States of the EU which grants them image rights.

6. THE SOLUTIONS

6.1 Legislative

As of now, the number of civilians using drones is limited. But this number will explode as drones become more popular and affordable, just like cars. In fact, some time down the line, every teenager may want to own one. To manage the insane number of cars, we built roads, parking lots, road signals, and freeways, to help us not only in maintaining safety but also to ensure that they flow freely. Cars come with license plates to identify who is the owner of the vehicle for various reasons, one such reason is, in case a crime is committed involving a car. We have rules regarding age where individuals only above a certain age can drive. By this we can generally conclude that when there is an increase in numbers there is a greater need to regulate. Regulation ensures the minimum level of harm.

The theory of the car equally applies to drones when used by civilians. The need for regulating it is undeniable. We yet do not know the impact of this technology when used on a grand scale. We not only have to be prepared for any eventualities that might arise from its use but also from the use of ancillary technologies that forms a part of the machine.

A few of the legislative solutions have been outlined in section 2.4.2 above. However, those legislations (new basic law, implementing regulation, delegated regulation) are more concerned

with the safety of drone use rather than regulating the processing of visual data when using drones. But those legislations do state that the use of drones must abide by the fundamental right to privacy and data protection.

The specific rules on drones, such as, the certification requirements, registration of the remote operator and the drone, licencing requirements of the remote pilot, obligations on the manufacturers of the drones to inculcate privacy by design and default features, will have a very positive impact on protecting the right to privacy and data protection, for example, Annex IX paragraph 1.3. of the new basic law states:

> '[…] the unmanned aircraft must have the corresponding and specific features and functionalities which take into account the principles of privacy and protection of personal data by design and by default. According to the needs those features and functionalities must ensure easy identification of the aircraft and of the nature and purpose of the operation; and must ensure that applicable limitations, prohibitions or conditions be complied with, in particular with respect to the operation in particular geographical zones, beyond certain distances from the operator or at certain altitudes.'

Trespass and nuisance laws serve a limited purpose. They alone are insufficient to deal with visual data processing by drones. As stated earlier, the right to privacy and data protection can both be infringed without trespass or nuisance being applicable. In other words, tort

law assists in the protection of the right to privacy and data protection with other general frameworks which are applicable, like the GDPR. The GDPR is the most comprehensive legislation at the EU level which will have an impact on the processing of visual information by drones and which is discussed in detail below.

6.1.1 The General Data Protection Regulation

With regards to visual information processed by drones, the GDPR takes the lead. How far will the GDPR go in addressing the concerns of processing of visual information by drones, will be discussed below. If a processing is not covered by the limitations mentioned in the GDPR (the household exemption and exemption from record keeping for organisations employing less than 250 employees), then the GDPR applies to such processing activities. It applies to individuals and corporations alike who process personal data for commercial or professional purposes.

Recital 6 acknowledges the fact, that due to rapid technological developments, the scale of processing and sharing activities has increased. This poses new challenges to protect an individual's visual data. One such technological development is the internet which facilitates the sharing of visual information on a mass scale. No matter which corner of the world an individual is, the information posted on websites is available to a large audience. Although the GDPR does not address drones specifically, recital 15 mentions that the GDPR is technologically neutral. It states, 'to prevent creating a serious risk of circumvention, the protection of

natural persons should be technologically neutral and should not depend on the techniques used […]'.

By this we can assume, that the processing of personal data by drones, whether it is number plates of vehicles or facial images of people, is covered by the GDPR. However, it is to be noted that the GDPR is geared mainly towards online activity.[410] Therefore, the application of its provisions to novel technologies, like drones, is not tailor made.

6.1.1.1. The two competing objectives

The GDPR has two objectives according to Article 1 paragraph 1,[411] the protection of personal data and on the one hand, and on the other, the free flow of personal data. They are very opposing objectives. Article 1 paragraph 2[412] acknowledges the fundamental right to data protection as enshrined in Article 8 of the CFREU. Recital 2 states that the principles and rules of data processing should respect a natural person's fundamental rights and freedoms. Therefore, it is not just the fundamental right to data protection but considers other fundamental rights as well.

Recital 4 goes on to say that the processing of personal data should serve mankind. It further goes on to say that the fundamental right to data protection is not an absolute right and it must be balanced with other fundamental rights and freedoms, such as, the fundamental right to respect for private and family life, the

[410] See recital 9 of the GDPR.
[411] See also recital 170 of the GDPR.
[412] See also recital 1 of the GDPR.

fundamental right to freedom of expression and information and the freedom to conduct a business. Therefore, if looked at it from the business side, corporations are entitled to process information using drones for business activities.

The only restriction is that the processing should abide by the provisions of the GDPR. It would have been more appropriate to name it the *'General Data Processing Regulation'* instead of, the *'General Data Protection Regulation'* as the GDPR is more in favour of processing activities rather than the protection of individuals' data. For example, even when there is no consent of the data subject the controller can still process data on other grounds, like public interest and legitimate interest. Article 6 paragraph 1 (f)[413] states legitimate interests as a lawful ground as, 'processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.'

An instance when a data subject's interest will override those of the controller is when the data subject has no reasonable expectation of the processing. But if he has a relationship with the controller then that reasonable expectation could be assumed. However, Article 21 paragraph 1[414] says that the controller can demonstrate that its legitimate interest overrides the fundamental rights and freedoms of

[413] See also recital 47 of the GDPR.
[414] See also recital 69 of the GDPR.

the natural person. Therefore, it is the right to processing against the right to protection.

6.1.1.2. The position of visual information in the GDPR

The GDPR does not distinguish between alphanumeric or physical visual information. It accords no special importance to images of people. It treats all recorded information equally. Recital 26 says that data protection principles should apply equally to any information concerning an identified or an identifiable natural person. Therefore, information incapable of being related to a natural person (anonymous data) does not fall within the ambit of the GDPR. By virtue of recital 27, personal data of deceased persons are also not covered by the GDPR. However, image rights have been accorded to dead people in the EU.[415]

But is it possible for information to truly remain anonymous? To an extent, one can say that alphanumeric information may be capable of remaining anonymous, but for visual information, like an image of a person, it is difficult for it to remain completely anonymous. There are hundreds of ways in which an anonymous photograph can be identified to an individual, some as mundane as publishing it in the newspapers and assigning a reward to the person who can identify the individual.

Therefore, recorded physical visual information, in many instances, will be information concerning an identifiable natural person. More

[415] Elisabeth Logeais and Jean-Baptiste Schroeder, 'The French Right of Image: An Ambiguous Concept Protecting the Human Persona' (1998) 18 Loyola of Los Angeles Entertainment Law Review 511, 514.

so, because of the existence and access to numerous databases where information has been and is uploaded voluntarily and the technology that is available to link the anonymous information to a single person.

Recital 26, however, includes information that has undergone pseudonymisation as personal data falling within the ambit of the GDPR. They are not treated as anonymous information.[416] Article 4 paragraph 5 of the GDPR defines pseudonymisation as, 'the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately […].'

Thus, the GDPR differentiates between fully anonymous and pseudonymous information. Visual information will be pseudonymous when a photograph of a person and the alphanumeric information that assists in the identification of the person are kept separately.[417] Or the photograph is blurred or pixelated and the key to bringing the photograph to its original form

[416] See for example, Khaled El Emam, Sam Rodgers, and Bradley Malin, 'Anonymising and sharing individual patient data' (2015) 350 British Medical Journal; Sophie Stalla-Bourdillon and Allison Knight, 'Anonymous Data V. Personal Data - A false debate: An EU perspective on anonymization, pseudonymization, and personal data' (2017) Wisconsin International Law Journal; Runshan Hu and others, Bridging Policy, Regulation, and Practice? A Techno-Legal Analysis of Three Types of Data in the GDPR, in 'Data Protection and Privacy: The Age of Intelligent Machines' Edited by Ronald Leenes Rosamunde van Brakel, Serge Gutwirth and Paul De Hert (Hart Publishing 2017); Samson Esayas, 'The Role of Anonymisation and Pseudonymisation Under the EU Data Privacy Rules: Beyond the 'All or Nothing' Approach' (2015) 6 European Journal of Law and Technology.

[417] ibid.

is kept separately. So, in order to identify the person, first bring the photograph to its original form and then link the photograph with the alphanumeric information.

The effort required to re-identify the information which has undergone pseudonymisation needs to be considered, because if it is impossible to re-identify, then it will be considered as anonymous.[418] Let us suppose, a person is flying his drone for recreation, and in the video recording, faces of a few individuals have been captured. What will be the status of this physical visual information? Will it fall under anonymous or pseudonymous information?

With the help of available technology and with a good amount of effort it is possible to identify the faces. But it is doubtful that such technology will be readily available to an average person. May be an average person will have to buy access to numerous online databases and assemble a team of experts in the field of re identification of information. But nobody is going to go to such a length if the purpose of identification is void. Or one might not have to go so far in identifying the faces and asking someone in the neighbourhood might do the trick.

Going by the risk-based approach there is no risk to an adult, but it may still pose a risk to a minor. Recital 38 says that 'children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned […] protection should, in particular, apply to the use of personal data of

[418] ibid.

children for the purposes of […] creating personality or user profiles […].'

But even decent adult images can be used out of context and abused against the dignity of the person. It is all possible with today's technology. In most probability the view of the many will be to treat such information as anonymous as it is at the point of collection that it is unidentifiable. If it was identifiable at source and then later de identified, then there is no doubt that that information is pseudonymous.

The GDPR specifically mentions in recital 51, that photographs should not be considered as special categories of personal data. However, in Article 9 paragraph 1 of the GDPR, the following are relevant to visual information and considered to be special categories of data, which reveal, racial or ethnic origin, religious beliefs, political opinions, health conditions, sex life, sexual orientation, and biometric data. A photograph of a person to a large extent reveals his racial or ethnic origin. One will be able to determine, at a minimum, whether a person is African, Asian, or White. It is not the nationality we are discussing here. A person could be African and yet have a North American citizenship.

In a sense then photographs should be treated as a special category of data requiring extra protection. But recital 51 also mentions that racial origin does not have the same meaning as separate human races. This is puzzling because on the one hand data revealing racial or ethnic origin has been classified as a special category of data, and on the other, the meaning of racial origin is not the same as we

understand as separate human races. But even if we understand it in a scientific way, Homo sapiens as a human race, any natural person's photograph will still be revealing Homo sapiens. Therefore, it should still be covered under special category of data.

Now for religious beliefs and political opinions, a photograph can reveal both. Religious belief of a person may be revealed by the clothes he wears, whether he keeps his beard trimmed or unshaven and as a photograph captures a person with his entire clothing one can make out whether he is a follower of the Islamic faith, Buddhist faith, Jewish faith, Christian faith and so on. Even when these identifiers are absent, a person may be caught in a photograph going to a church or other place of worship which reveals his religious affiliations.

Similarly, a person may be caught in a photograph participating in a political demonstration which reveals his political opinions. Even health conditions are capable of being determined by a photograph, for example psoriasis. The imaging sensors on drones themselves can reveal data concerning the health of an individual.[419] Recital 35 says that personal data concerning health should include all data pertaining to the health status of a natural person which reveal information relating to the past, current or future physical or mental health. Sex life or sexual orientation can be captured on camera or revealed by a photograph through advanced image analysis, like whether a person is gay or straight from a photograph.

[419] Jane Wakefield, 'Drone detects heartbeat and breathing' (BBC News 2017) <http://www.bbc.com/news/technology-41427529> accessed 7 January 2018.

A qualification to photographs, in recital 51, is made for biometric data. According to Article 4 paragraph 14 of the GDPR, 'biometric data means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images […].' Therefore, photographs are covered by the definition of biometric data only when it allows for the unique identification of a natural person and when processed through specific technical means. A normal photograph processed by a camera, therefore, will fall outside the protection of biometric data.

But what does specific technical means mean? Will it include a drone with facial recognition abilities? Thus, in a way, photographs are and are not considered as a special category of data, depending on the context. Hence, the provisions applicable to special categories of data would apply even to photographs.

6.1.1.3. The approach to the analysis of the relevant Articles

If we treat most of the visual data recorded by a drone as anonymous data, then there is no point in discussing further, as anonymous data is outside the ambit of the GDPR. It is only when we do not treat such data as anonymous, and the controller is held liable, that there is a point in discussion. An assumption is made that the drone has a camera or other visual sensors that can record or transmit identifiable visual information.

There will be two categories of data collected, data collected in transit and data collected of the data subject. For example, Amazon

Prime Air delivers a parcel to the data subject (one who orders the goods). During the flight, the drone may record visual information and once it has reached its destination, it may record visual information relating to the data subject, such as the entrance to the home, or children playing in the backyard or even the image of the person who has ordered the goods. Now will the GDPR apply to the whole of the data during the flight or only the data relating to the data subject, as the rest of the data will be anonymous, or identifiable, depending on the way one looks at it. The approach adopted here is that all of the data is regulated by the GDPR. This way the discussion is more interesting.

6.1.1.3.1. Applicability of the grounds of processing

Article 6 paragraph 1 states the grounds on which the processing is lawful. A processing is lawful when, **a.** the data subject has given consent […], **b.** is necessary for the performance of a contract to which the data subject is a party […], **c.** is necessary for compliance with a legal obligation to which the controller is subject, **d.** is necessary in order to protect the vital interests of the data subject […], **e.** is necessary for the performance of a task carried out in the public interest […], and, **f.** is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject, which require protection of personal data, in particular where the data subject is a child.

Now if Amazon Prime Air delivers a parcel to the data subject and visually processes the data subject or his home it is a lawful processing. This processing can either be based on the consent of the data subject, for the performance of a contract to which the data subject is a party, compliance with a legal obligation (contractual obligation) to which the controller is subject or on the legitimate interests pursued by the controller. However, the visual information processed of children playing in the backyard or the people in transit is unlawful processing.

So, Amazon needs to come up with a way to avoid processing unnecessary information. This will help them to fulfil the principle of data minimisation wherein the data processed should be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. In an online environment, these kinds of scenarios do not play out. In the case of CCTV cameras installed by public authorities,' public interest is a lawful ground to process data, but for drones used for commercial purposes, this ground is not available. One way to comply with the GDPR in such a scenario, is to adopt technological measures where, either one is not using a camera to deliver parcels (which is highly unlikely) or one is processing only that is required for the performance of the contract.

Therefore, as of now, the use of drones will involve processing, where some of the data processed is lawful while the rest of the data has been processed unlawfully. It is like finding the way home by partially trespassing onto another's property. Basically, the grounds

mentioned in Article 6 paragraph 1 will not be fulfilled and make the whole processing unlawful. However, processing on the grounds of legitimate interests pursued by the controller could be applied by stretching the concept. But even then, applicability will depend on the balancing of the interests of the controller with that of individuals whose data has been processed unlawfully. It will be safe to assume that individuals will include children which will make it more difficult to abide by the GDPR.

6.1.1.3.2. Applicability of the consent requirements

It is very difficult to get consent or to give consent to the processing of data which may take place in transit. According to Article 4 paragraph 11, 'consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.' In no way can the controller satisfy these conditions or the requirements of Article 7 which lays down the conditions for consent.

If the visual information falls under special categories of personal data (Article 9 GDPR) then the requirement of consent is even more stringent. It needs to be explicit. However, Article 9 paragraph 2 subparagraph e states that special categories of personal data can be processed if the 'processing relates to personal data which are manifestly made public by the data subject.' This provision relates to our discussion on reasonable expectation of privacy in a public place. Privacy is seldom recognised in a public place. So, the

assumption here is that by being in a public place, the data subject has manifestly made him-self public. Therefore, it should be possible to process data as the processing will be lawful. If this is the case with special categories of data, then it must be the case with normal categories of data, like a car number plate.

This provision has a profound impact. It would allow Amazon Prime Air, to deliver parcels, even though visual data is processed in transit because the individuals, who are processed, manifestly made themselves public. But this will apply only to individuals who are processed in a public sphere, like roads or parks, but individuals who have been processed in a private sphere, like the back yard or front yard of a home, may not be covered. But if we understand public as anything visible from a public sphere then such data may also be covered.

Recital 32 says that consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subjects agreement to the processing of personal data relating to him or her. In an online environment it is easy to show that one's consented to the processing of his/her personal data, for example, by clicking on an accept button or ticking a box.

However, problems arise when visual data is processed by drones. This is because neither the person processing the data is aware of who all will be processed, nor the person being processed is aware that he is the subject of processing. So, it is difficult to get consent or to give consent. As, according to recital 32, silence and inactivity

cannot be regarded as consent, other methods must be devised to make known that data processing activity is being undertaken and that all individuals affected are to give consent, in a particular manner, to satisfy the provisions of the GDPR.

One way of fulfilling the provisions of the consent requirement is to copy the style of the CCTV cameras by putting up signage where data processing takes place, like, the area is being used for recreation and images may be processed by a drone. If one enters the area, he/she impliedly consents to the processing of his/her image. This will inform the people that their images may be processed if they are present within the area of the VLOS.

But unlike CCTV cameras, drones have no fixed area of surveillance. It is very difficult to circumscribe an area of surveillance. However, with geo fencing software it is possible to circumscribe an area. The use of the signage is still complicated due to the nature of the space. A public space does not privately belong to anyone and so putting up signage of drone activity in a park or a beach will restrict others right to the enjoyment of the public space. It will also restrict the right to free movement which is protected by Article 2 of Additional Protocol Number 4 to the ECHR. This leaves an individual with his/her private space where he/she can put signage which will mean little.

Recital 42 of the GDPR puts the onus on the controller, in this case the drone operator that he be able to demonstrate that the data subject has given consent. To the maximum what the drone operator can do is treat the acquiescence of the data subjects with the signage

that there is consent. It will be unmanageable if he must hand out pre formulated declaration of consent to everyone, present and future.

Recital 62 states that the obligation to provide information to the data subjects regarding the processing of their personal data can be excused if it proves impossible or would involve a disproportionate effort. This has relevance where personal data are processed by drones as it is impossible to identify beforehand whose data may be processed and as such would be impossible or will involve a disproportionate effort to provide information.

Regarding consent, recital 46 says that 'the processing of personal data should be regarded to be lawful where it is necessary to protect an interest which is essential for the life of the data subject […] processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes […] humanitarian emergencies, in particular in situations of natural and man-made disasters.'

This is particularly applicable where drones are used in medical emergencies, like a car crash or a heart attack. If a drone is relaying visual information about the condition of the patient in a car crash to the hospital, then such processing activities are considered as lawful, even if there is no consent of the data subject. It is understandable, that in such situations, it may be difficult to get the consent of the data subject as he may be unconscious. Thus, such visual information will be grouped under special category of data as

it reveals the health condition of the data subject. Therefore, such processing will be covered by Article 9 paragraph 2 subparagraph c of the GDPR.

6.1.1.3.3. Applicability of the obligation to inform the data subject and profiling

It is common understanding that without knowing what the rights are, it will be difficult to exercise them. The nature of processing personal data by drones makes it difficult for the data subjects to exercise their rights under the GDPR. In an online environment, a website can be identified to a natural or legal person. CCTV cameras are stationary and thus it is possible to locate the control room with a reasonable amount of effort. So, in both these instances if a person has an issue with the processing of his personal data, theoretically, it is possible to approach the concerned natural person. It is possible to request a deletion or rectification of their personal data. However, in the case of a drone, which has a nature opposite to being stationary, in most cases it will not be possible to identify a drone to a natural person, unless there is a system assigning a number plate. But even physical number plates will be near to impossible to comprehend from the ground and therefore some kind of a digital number plate is required.

Article 12 provides for the controller to inform the data subjects about the processing. This information should be provided in line with the transparency criteria as mentioned in Article 5 paragraph 1 (a) and recital 39 and 58 of the GDPR. The principle of transparency requires that any information addressed to the public

be concise, easy to understand, in a plain language and include the name and address of the controller or processor, the rights of the data subjects, the purpose of the processing etc.

There will be no issue in providing information to the data subject who has ordered the goods. He could be informed of his rights while he is placing an order online, that the drone would process visual information in his private sphere. But such an opportunity will not be available to individuals who are processed having nothing to do with the transaction.

The information to be provided to the data subject has been clubbed under two categories, the first, where data is collected from the data subject himself, and second, where the data has been collected from some other controller, or from someone other than the data subject. In this case, Article 13 will apply, as the visual data would be collected from the data subjects. Article 13 provides that at the time when personal data are obtained, the controller shall provide information to the data subject, such as, the identity and contact details of the controller and the data protection officer, the purpose and the legal basis for the processing, the recipients of the personal data, whether the data will be transferred to a third country, for how long the data will be stored, the data subjects right (of access (Article 15), to rectification (Article 16), to erasure (Article 17), to restriction of processing (Article 18), to data portability (Article 20), to object (Article 21)) and the existence of profiling.

These are complex pieces of information and thus require individualised attention. Using signage to convey such information

to a mass audience will fall short of the intended purpose of informing the data subject. It is impossible to provide information to everyone who may be visible, from 300 or 400 feet above in the air.

If the route is regular, it may even come within the meaning of regular processing in the GDPR. For example, a person walks to work and walks back home. He takes the same route every day, but it so happens that the flight path of a drone is also the same. The operator of the drone happens to notice the person after a few deliveries. So, in a way, patterns tend to emerge, and the identity of the anonymous person is on the cusp of being disclosed. This will even come within the meaning of regular monitoring in the GDPR. So, it is vital that such individuals also be informed, or their data not processed. Article 22, regarding automated decision making and profiling, will also become applicable.

The issue of profiling by drones:

Profiling is another area that drones will be highly competent in. Article 4 paragraph 4 of the GDPR defines profiling as ‘any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning […] behaviour, location or movements.’ The processing however needs to be automated, which a drone is fully capable of, and if equipped with advanced analytics software, it can evaluate personal aspects as well. Recital 60 says that the controller should inform the data subject of the existence of profiling and the consequences of

such profiling. In cases where there is automated processing and profiling, according to recital 71, a data subject has a right not to be subject to a decision based solely on such processing which significantly affects him or her.

What kind of automated decisions can a drone make? In an online context, it is easy to see how this applies when a housing loan application is rejected solely based on the credit profile that is present in the system. It is easy to come up with examples in the law enforcement sector where a drone starts beeping on seeing suspicious behaviour, whether it turns out to be accurate is another question. But in the civilian sphere, it is more difficult.

One decision making process, based on automated processing by a drone, could be to monitor individuals for financial standing. So for example, drones could visually monitor the living standards of a person, like how a person travels to work, whether he uses a fancy car or a worn down one, whether he lives in a nice house or a shack, and accordingly, cross check and update the company systems whether the subject has enough collateral to finance a loan. However, for there to be profiling it is not necessary that there should be a decision taken based on such profiling. According to Article 29 working party guidelines on automated decision making and profiling, it is enough if there is collection of data for the creation of profiles.[420]

[420] Article 29 Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' 17/EN, WP251, adopted 3 October 2017.

With regards to profiling by drones, there are several issues that raise the question of unfairness and bias. For example, the software used for the purposes of profiling may have been developed by a person who thinks only from his perspective. So, for example, if it is software designed to detect human emotions, it is possible that the software identifies dark skin tones with anger and lighter skin tones with more peaceful and calm emotions.

6.1.1.3.4 Applicability of the provisions for controllers and processors

Individuals and companies using civilian drones will come within the meaning of controllers and processors. Article 24 fastens obligation onto the controller to implement organisational and technical measures. Some of the organisational and technical measures have already been discussed. Paragraph 3 of Article 24 encourages the controller to adhere to codes of conduct and certification mechanisms. Codes of conduct could be formulated keeping in mind the special characteristics of processing data by drones. It could be formulated either by the EU member States, supervisory authorities or by an association of controllers or processors who use drones, in line with Article 40 of the GDPR. A specific body could be established under Article 41 to monitor the drone code of conduct.

Data protection certification mechanisms, seals and marks could be applied to drones and controllers, under Article 42, that inculcate technological measures such as data minimisation. Certification bodies that have expert knowledge of the technical know-how of

data processing by drones could be set up under Article 43 of the GDPR, to issue certification marks and seals. Such certification marks or seals should be prominently displayed on the drone. It could be in the form of the colour of the drone. So, for example, data protection certified drones could be painted orange in colour or some other flashy colours that would allow its identification even when airborne.

A controller should be obliged to undertake a data protection impact assessment (DPIA), under Article 35, when operating drones. During the DPIA, consideration should be given to the route the drone takes. Routes which have high concentration of residential areas or schools should be avoided. Routes which pose a danger to the fundamental rights and freedoms of natural persons should only be operated with a prior consultation of the supervisory authority concerned under Article 36 of the GDPR.

With regards to processing of data with new technologies, which would include drones, recital 89 says that mechanism like DPIA should be carried out in case the processing is likely to result in a high risk to the data subjects. Recital 91 gives examples of what might be considered as high risk, such as, the sensitivity of the data processed in relation to the data subject and where the method of data processing renders it more difficult for the data subjects to exercise their right, like in cases of surreptitious monitoring. Recital 91 also mentions that a DPIA is necessary where publicly accessible area is monitored on a large scale by using optic electronic devices.

Known technologies that would fit this requirement are CCTV cameras and drones.

There is a requirement to notify the supervisory authority of a data breach under Article 33 and to the data subject under Article 34. The controller must also ensure the security of the processing under Article 32. With regards to drones, a security measure that could be implemented is data encryption as soon as the data is processed and stored and while the data is transmitted to ground stations for further processing. The security of the on-board storage should also be considered in the event of a crash.

Article 25 imposes an obligation on the controller to implement data protection by design and default, considering the state of technological progress, the cost of implementation, nature and scope of processing and the risk likely to result from the processing. The drone should be programmed in such a way, that by default, it only processes information required for the purposes of the controllers' activities. Whether the obligation, to implement privacy by design features, could be extended to the manufacturers who have no role to play in the processing activities, is doubtful. In most cases, they would want to ensure that their products are available at the most affordable rates and ignore such design features while manufacturing drones. Article 28 imposes a similar liability, like in the case of a controller, on the processor. In fact, there is an obligation on the controller to employ only those processors that abide by the provisions of the GDPR, including implementing technical and organisational measures. So, the situation of the

processor is the same as the controller when processing data using drones. They will face the same difficulties with regards to unnecessary data collection.

6.1.1.3.5. Data transfer to third countries

This has relevance to drones when data processed by it is published on the internet or transferred to the cloud. The rule for online publishing and whether such publishing amounts to a transfer to third countries is complicated, but it has been dealt with in the past. As mentioned earlier, publishing online is in most cases, to an indeterminate number of people as the content is accessible by anyone, even third country nationals. However, in the *Bodil Lindqvist* case the CJEU ruled that if the host with whom the content is stored is in one of the member States of the EU, then such publication will not amount to a transfer of data to a third country.[421] So the main factor is whether the server where the content is stored is within the EU or outside of the EU.

As data from drones, will in most probability, be transferred to the cloud due to the enormous size of visual data and restrictions with internal storage capacities of drones, the traditional understanding of data transfer and its accessibility breaks down. Moreover, the companies that provide the cloud services are established worldwide, they have presence not only in the EU but also outside of the EU. So, to determine in which of the servers the data is stored is a tricky question. There is a possibility that a part of the data is

[421] See case C-101/01, para 71.

stored in a server within the EU and another part in a server outside the EU.

6.1.1.3.6. Applicability of the provisions for supervisory authorities

Article 57 enumerates the tasks of the supervisory authorities. What the supervisory authorities could do is promote public awareness about drones and the risks that arise in using them, from the perspective of the controllers and processors as well as from the perspective of the data subjects. They could also monitor developments in drone technology and advise the controllers and processors accordingly. They should always insist on a DPIA when drones are going to be used by an establishment or an organisation. They should also be involved in implementing certification requirements and codes of conduct for drones. Under Article 58, supervisory authorities could carry out periodic reviews and investigations especially of controllers and processors who use drones. It could also obtain periodically, sets of data processed by drones and go through some of them to see whether the data collected is limited to what is necessary for the purposes they are processed. Recital 132 states, 'awareness-raising activities by supervisory authorities addressed to the public should include specific measures directed at controllers and processors […] as well as natural persons in particular in the educational context.'

The activities undertaken by the supervisory authorities, in relation to drones, should follow the consistency and cooperation mechanism as outlined in chapter VII of the GDPR. As regards chapter VIII, which outlines the remedies available to a data

subject, like filing a complaint with the supervisory authority concerned or filing a complaint with the concerned controller or processor, the challenges with respect to such remedies is the awareness of the processing activities. A data subject may not always be aware that their data is being processed by drones.

6.1.1.3.7. Reasonable expectation and privacy enhancing measures applicable to drones

Another noteworthy aspect of the GDPR is the recognition of the principle of reasonable expectation. Recital 47 says that a legal basis for the processing may be the legitimate interests of a controller. However, the data subject should reasonably expect that such processing will take place based on his relationship with the controller. Therefore, if he does not reasonably expect the data processing then such processing is illegal. The principle of reasonable expectation is also applied in cases, where the data has been collected for one purpose and further used for another purpose. In further using the data for another purpose there should be a reasonable expectation by the data subject, that his data may be used for that other purpose. This is stated in recital 50 of the GDPR. However, assuming the data subject reasonably expects his data to be processed, but the means used to process is beyond his reasonable expectation, will then such processing be legal? The courts in the US, in *Kyllo v. United States* (cited above), came up with the 'general use criteria' meaning that if a technology is in general use, then the public cannot expect privacy, if information

has been processed and revealed using that technology. As drones become more popular, they will be in general use.

A new aspect in the GDPR, which was absent in the DPD, is the explicit mention of data protection by design and default. Simply speaking, it is the inclusion of technological measures which restrict the collection of identifiable information.[422] It is integrated into the technology itself. But while we speak about data protection by design, we are still coming to terms with it. It is like the term PET and is a part of the technological and organisational measures mentioned in the GDPR. We can say that technologies that include data protection by design are PETs. Therefore, it also relates to the principle of data minimisation in the GDPR.

The question to ask is what kind of a design can be incorporated in a drone that will protect an individual's data? The design must be mainly built into the camera and the sensor systems. Electronic monitoring of individuals, when they are under house arrests, is a fine example of data protection by design. The global positioning system, that is used to keep track of an individual's location, only recognises or records the location of the individual when he moves outside the permissible area.[423] Therefore, his location privacy is unaffected when he obeys the area limitation. But from another perspective, his location privacy is still compromised when he

[422] For a more detailed reading see, Lee A. Bygrave, 'Data Protection by Design and by Default: Deciphering the EU'S Legislative Requirements' (2017) 4 Oslo Law Review 105.

[423] Leah Satine, 'Maximal Safety, Minimal Intrusion: Monitoring Civil Protective Orders without Implicating Privacy' (2008) 43 Harvard Civil Rights-Civil Liberties Law Review 267.

obeys the area limitation because if the machine does not record the location of the individual it means he is within the permissible area.

Recital 78 mentions that the controller should adopt measures that meet the requirements of data protection by design and default. It gives examples of data minimisation, pseudonymisation and transparency as some of the measures that meet the requirements. The recital not only imposes obligations on the controllers, but also on the producers of products and services, to consider the principles of data protection, when designing their products and services. But how far they are liable, under the GDPR, if they fail to obey the principles, is not addressed. It is more of a suggestion than an obligation imposed by the GDPR. Therefore, we can see how the principles are interrelated. Data minimisation, pseudonymisation, data protection by design and default and transparency are all part of the technical and organisational measures to be adopted by the controller.

There are technological measures, in place, that minimise visual data collection by drones or enhance the security of data collected by drones. For example, Intel Falcon 8+ drone can be configured as a closed system with only on-board data storage that does not transmit data over the Wi-Fi.[424] This is supposedly to protected data, from interception, when transferred over a network. Intel's Aero Ready to Fly Drone, comes with Intel's real sense technology, which can sense and avoid obstacles and convert raw image data,

[424] 'Intel® Falcon™ 8+ System' (Intel) <www.intel.com/content/www/us/en/products/drones/falcon-8.html> accessed 11 January 2018.

into data necessary for navigation.[425] This would thereby minimise visual data that could be used to identify people. Other measures that could be used are encryption of recorded data, software to blur out facial images of people, or no fly zones incorporated into the firmware of the drone.

A data breach can occur when using a drone or when a drone crashes to the ground for technical or other reasons. In the event of a crash, the on-board storage could be assessed by unknown people, especially in BVLOS scenarios. A breach can also occur while the drone is still processing data and that data is intercepted by hackers. Data breach is defined in Article 4 paragraph 12 of the GDPR as, 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.'

Recital 85 says that a data breach may result in a risk to natural persons, specifically, discrimination, identity theft or fraud, damage to reputation etc. In such an eventuality, the controller has an obligation to notify the supervisory authority concerned. However, in case there is no risk, which would be in most cases, the controller can dispense with the obligation requirement. The controller has a similar obligation to notify the data subject, as mentioned in recital 86.

But the point to consider is the risk factor. In only rare circumstances, anonymous data will be of risk to natural persons.

[425] 'Intel® Aero Ready to Fly Drone' (Intel) <www.intel.com/content/www/us/en/products/drones/aero-ready-to-fly.html> accessed 11 January 2018.

Recital 87 says that it should be ascertained whether technological and organisational measures have been implemented to determine whether a personal data breach has taken place. For example, if the controller has implemented measures, such as encryption, then the breach would be of little risk to the data subject. But the likelihood and the ease with which such encrypted data could be decrypted will also need to be taken into consideration.

6.1.1.4. Limitations

6.1.1.4.1. With regards to processing by individuals

There is little recourse if the right to protection of personal data has been violated by an individual drone enthusiast. Article 2 paragraph 2 (c) states that the GDPR does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity. This is commonly referred to as the household exemption and it existed in the DPD as well. There is no guidance in Article 2 of the GDPR about what a purely personal or household activity means. However, some assistance is provided by recital 18 of the GDPR which clarifies that purely personal or household activities are those that have no connection to professional or commercial activities. It further goes on to include activities such as correspondence and the holding of addresses, or social networking and online activities undertaken within the context of correspondence or the holding of addresses as personal or household activities. These examples are not exhaustive as they are qualified, by the use of the word, could.

This explanation is insufficient as there are innumerable activities that could be classified as personal or household and yet be commercial in nature and professional and commercial and yet be personal or household in nature. For example, posting drone footage of one's home (an aerial view) which also shows one's neighbourhood, for the purpose of selling, in an online property database, is personal and at the same time commercial in nature. The examples given as to what constitutes a purely personal or household activity in recital 18 of the GDPR are too simple for the complexities that could arise due to the use of modern technology.

Recital 18 also states that the controllers or processors who provide the means for processing for such personal or household activities are not exempt. It means that an individual drone enthusiast who processes physical visual information in the course of his leisure activity is exempt from the GDPR, but the person who provides the drones for such leisure activity is not exempt. There are drone rental companies who provide drones for filming purposes for both hobbyists and professionals. But can also manufacturers and retailers of drones be classified as controllers or processors who provide the means for processing for personal activities?

According to Article 4 of the GDPR, paragraph 7, 'controller means the natural or legal person […] which […] determines the purposes and means of the processing of personal data […].' According to paragraph 8 of Article 4 'processor means a natural or legal person […] which processes personal data on behalf of the controller.'

There is no doubt that the operator of the drone is a controller and simultaneously also a processor. He determines the purpose and means of processing of personal data. However, the drone rental companies, and manufacturers don't determine the purpose on behalf of an individual operator, but they provide him the means of processing. But drone rental companies and manufacturers could broadly determine the purpose, for example, determining whether a drone is to be used for recreational or professional purposes.

In this case the person who hires or buys a drone has no choice to determine its hardware and must be satisfied with the restrictions imposed by the rental companies and manufacturers. With such an interpretation it is logical to consider them also as controllers and within the meaning of Article 4 of the GDPR. But why attach liability to controllers and processors who provide the means for processing personal data for personal or household activities?

We can say that they have a non-enforceable duty to ensure that the processing is strictly for personal or household purposes. That duty can be fulfilled by ensuring that privacy by design is embedded in the hardware and software of the drone or the sensors. It could also be fulfilled by entering into an agreement with the individual drone enthusiast who determines the final purposes for which the drone is hired or used, that a kind of drone is used only for a particular purpose. Otherwise, I see no reasons to include controllers and processors who provide the means in recital 18 of the GDPR because if an individual is exempt if he processes data for purely personal or household purposes so will the controllers and

processors who provide the means. It did not form a part of a similar recital 12 in the now annulled DPD as it serves no purpose.

But seen from another angle, a drone is a consumer product and as manufacturers of consumer products, collect data from customers about the use of their products. In the IOT landscape, it is not farfetched to think that drones would be sending back personal data to the manufacturers. Therefore, manufacturers are liable under the GDPR if they deal with personal data sent by drones for improving their products or for other purposes.

The issue of what amounts to processing is also not straightforward. Will the projection of transient physical visual information on a smartphone for the purposes of navigating and manoeuvring a drone, without recording or storage, be considered as processing within the meaning of Article 4 paragraph 2 of the GDPR? Paragraph 2 of Article 4 states, 'processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.'

For example, if a person is having a skype communication with his friend in a public place, the front facing camera of his smartphone may process images of the nearby public unintentionally, and it is not necessary that information needs to be recorded for it to come within the meaning of processing under Article 4 paragraph 2 the

GDPR, as it is very broad in scope. But will this purely personal activity be considered commercial and professional? If the answer is in the affirmative, then he will have to comply with the provisions of the GDPR which will impose an unimaginable burden. He will have to take the consent of the public by anticipating who all will be most affected, inform the public of the processing in the area and even going to the extent of carrying out a privacy impact assessment just for the sake of having a skype communication. If such a burden were to be imposed, people would be wary of using a smartphone for video calling, out in public. It would result in nonsensical restrictions.

Therefore, an additional problem lies in defining what is processing under the GDPR. Is recording necessary for it to come within the ambit of processing? A person with a binocular is processing physical visual information with the help of technology. A person using a video camera, simply to project the visual information onto the small screen of the camera, is processing visual information. The European Data Protection Board, in its guidelines on processing of personal data through video devices, acknowledges that real time monitoring may be very intrusive.[426] But real time monitoring is possible without the help of cameras and technological devices. Any natural person could simply visit the place and observe the same thing with the naked eye, as held in the *Pierre Herbecq* case. It will be absurd, if observation through the

[426] European Data Protection Board, Guidelines 3/2019 on processing of personal data through video devices (version for public consultation), Adopted on 10 July 2019.

naked eye also comes within the ambit of processing in the GDPR. Therefore, simple observation, even by technology, should be excluded from the meaning of processing if it does not include recording, alterations, making available to third parties or any other additional manipulation of the observation.

It has been reiterated earlier, that there is a distinction between the private and the public sphere, even though that distinction may be symbolic. Activities in the private sphere can be equated to purely personal or household activities. But it is also noted that private activities can be performed in a public sphere, like a confession in a church.

A relevant case, which closely assimilates drones and spatial character, is the case of *František Ryneš v Úřad pro ochranu osobních údajů*.[427] In this case Mr. Ryneš installed a CCTV camera for monitoring the entrance of his home. But the public footpath and the entrance of the opposite house was also within the VLOS of the camera. The recorded visual information was stored on a hard disk drive. Strictly speaking, this installation of the camera and the subsequent recording and storing of the visual information should have been covered by the household exemption. However, the Court of Justice of the European Union (CJEU) held that as it also monitored a public sphere and the entrance of the opposite house it did not come within the meaning of processing for a purely personal or household activity.

[427] Case C-212/13 (Judgement of the CJEU of 11/12/2014)

But shouldn't a person have no reasonable expectation of privacy on a public footpath or the entrances of homes? Mr. Ryneš could have simply observed the assailant with the naked eye, or anybody else for that matter could have seen the assailant if they happened to be at that particular place and time, if one were to follow the logic in the *Pierre Herbecq* case. What sets the *Ryneš* case apart from the *Pierre Herbecq* case is the recoding and storing, which was lacking in the latter. But that recording and storing was for personal use and was not published.

In the *Bodil Lindqvist* case,[428] the CJEU, with reference to the household exemption, in para 47 states, 'That exception must therefore be interpreted as relating only to activities which are carried out in the course of private or family life of individuals, which is clearly not the case with the processing of personal data consisting in publication on the internet so that those data are made accessible to an indefinite number of people.'

Therefore, the two main grounds on which the CJEU decided, whether an activity falls within the household exemption was 'space' and 'publication'. But neither of the activity was professional or commercial in nature. What if visual information recorded by a hobbyist using a drone, which also happens to include members of the public, is published on a person's Facebook page? Does the sharing of visual data with friends on Facebook make the friends recipients within the meaning of Article 4 paragraph 9 of the

[428] Case C-101/01 (Judgement of the CJEU of 6/11/2003)

GDPR and in turn a commercial activity because it amounts to publishing?

Friends will be considered recipients within the meaning of Article 4 paragraph 9 of the GDPR which states 'recipient' as meaning a natural or legal person. But will this convert a personal act into a commercial act? The publication on a Facebook page is initially to a definite number of people. But the information will also be available to friends who have been subsequently added, after the publication, and, thus, is indirectly available to an indefinite number of persons. By publishing on Facebook, a person is exercising his fundamental right of expression and even if the visual information recorded by drones contained information that could identify a person, like faces, it will nevertheless require an effort to identify solely based on the photograph, if he is not a celebrity. Moreover, the right to privacy and data protection of the person must be balanced with the right to freedom of expression.

Processing for journalistic or artistic purposes could also exempt individuals from the provisions of the GDPR. Image rights can similarly be curtailed for artistic purposes. And it is not necessary that journalistic or artistic activities be performed by media or artist organisations, respectively. Individuals in their personal capacity can also be considered to come within the meaning of Article 85 of the GDPR, considering the *Satamedia case*.[429]

Article 85 paragraph 1 states that 'Member States shall by law reconcile the right to the protection of personal data pursuant to the

[429] Case C-73/07 (Judgement of the CJEU of 16/12/2008) para 58-62.

GDPR with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression.' Paragraph 2 of Article 85 states, 'For processing carried out for journalistic purposes or the purpose of academic artistic or literary expression, Member States shall provide for exemptions or derogations from Chapter II (principles), Chapter III (rights of the data subject), Chapter IV (controller and processor), Chapter V (transfer of personal data to third countries or international organisations), Chapter VI (independent supervisory authorities), Chapter VII (cooperation and consistency) and Chapter IX (specific data processing situations) if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information.'

Recital 153 explains, 'Member States law should reconcile the rules governing freedom of expression and information, including journalistic, academic, artistic and or literary expression with the right to the protection of personal data pursuant to the GDPR. The processing of personal data solely for journalistic purposes, or for the purposes of academic, artistic or literary expression should be subject to derogations or exemptions from certain provisions of this Regulation if necessary, to reconcile the right to the protection of personal data with the right to freedom of expression and information, as enshrined in Article 11 of the CFREU. This should apply in particular to the processing of personal data in the audio-visual field […]. In order to take account of the importance of the right to freedom of expression in every democratic society, it is

necessary to interpret notions relating to that freedom, such as journalism, broadly.'

In effect, EU member States are allowed discretion, and therefore, the exemptions and derogations may not be harmonious throughout all the EU member States. Video recordings by drones can be considered as a piece of art as the aerial view is quite unique, and recordings of large gatherings posted on YouTube or Facebook to inform people about city congestion could qualify as a journalistic activity, even if it is performed for a commercial purpose.

The recent *Buivids case*,[430] decided by the CJEU, dealt with a video recording of police officers at the police station and its subsequent publication on the internet. Although that case was decided under the DPD, the principles are equally applicable to the GDPR. The main question asked by the referring court was whether this would be covered within the journalistic exception. The CJEU decided that it is for the referring court to determine and balance the right to freedom of expression with the right to privacy. However, it did hint that such an activity may fall within the journalistic exception, adopting a broad interpretation.

The Buivids case is straightforward and it is surprising that the Latvian courts even referred such questions to the CJEU, like whether the DPD is applicable to the given facts of the case and whether the given facts will be covered by the journalistic exceptions. The filming and recording of visual information will be processing within the meaning of the now annulled DPD and it

[430] Case C–345/17

makes little difference whether the police officers were anonymous or not by their name. The police officers were not celebrities and so the identification of each individual police officer would require somewhat of an effort. That being said, the information trails like the colours of their uniform and the rank badges worn by the police officers would make it easier to identify the police officers as it would be easier to identify the country of origin and then in turn the police station to which the police officers belonged to.

Whether this amounts to disproportionate effort in disclosing the identities of the individual police officers would vary depending on to whom the question is asked. For an expert in de-identification, it will require absolutely no effort on his part but for a person with no resources and no computer skills, it will require quite an effort in order to identify the police officers. The discussion on this case law could go on for ever without an end in sight. There are so many pictures of anonymous individuals posted on Facebook and YouTube, as example, travel pictures containing anonymous individuals, and if we are to apply the logic that just because faces of anonymous individuals have been captured, would make nearly the entirety of individuals, who use social media, liable for privacy violations. But should not the publication also factor in the individuals to whom it has been published.

For example, an individual is a traveller and a photography enthusiast, and he regularly posts travel pictures on his personal Facebook page as well as a personal channel that he has on YouTube. The YouTube channel can be subscribed by anyone but

to see his posts on his personal Facebook page, one need to send him a friend request. Therefore, seeing his posts on his Facebook page is dependent on him accepting a friend request. Is the posting on YouTube and Facebook the same or does YouTube amount to publication but posting on Facebook does not?

Therefore, taken together, the exemption for personal or household activity, for journalistic and artistic purposes and the need to balance the right to data protection with the right to freedom of expression gives an individual a lot of space to play with.

It is not clear what can and what cannot be accommodated within the household exemption. Even if the drone is not recording or storing visual information and is simply relaying the visual information to a smartphone or other device, it is still processing within the meaning of the GDPR. But at the same time, it is only observing, and as discussed previously, mere observation is seldom illegal. So, the variables applicable to mere observation should apply to the GDPR as well.

Therefore, to unify our previous analysis of mere observation with the GDPR, the observation must fulfil the conditions of the household exemption, because if it does not fulfil the conditions of the household exemption, then all of the GDPR becomes applicable to an individual. Thus, the inconsistencies are clearly visible where at one end mere observation amounts to nothing, and on the other end, observation by technological means (drones) amounts to processing within the meaning of the GDPR and as such must fulfil the conditions of the household exemption.

If no, then an individual will be liable even for mere observation and to escape any liability he will have to restrict his activity within the airspace above his personal property and at a height which restricts the angle of visibility so that others, even unintentionally, are not drawn into visibility. Or an individual could use his drone where he is sure that he is not going to encounter any people, which is very rare with a population of close to eight billion on the planet. But if observed from above the most likely aspect of a human being that will be visible will be the hair and not the face. But with some tweaking of the camera equipment and adjusting the visibility angle, faces may become apparent. Therefore, it is very important to have a clear idea of the household exemption.

What is logical is that not every processing of someone's image should count. It should be decided based on the intimacy of the activity as casual walking on a public street would have no repercussions on an individual if his image is processed, and the malice behind the processing. The purpose of the overall processing should be taken into consideration rather than the accidental inclusion of an identifiable individual.

So, for example, if a person is making an aerial drone video of his house for the purpose of selling it and accidentally, he captures a few individuals who happen to live in the neighbourhood; this by itself should not transform a purely personal activity into a commercial one. If the captured individuals were performing intimate acts in their backyard and the video is published on a property selling website, their privacy has been invaded and the

controller should be morally liable. In such situations, if the data subjects, whose privacy were invaded were made aware of the processing of their image, before publication of the video, then they could exercise their right to erasure under Article 17 paragraph 2 of the GDPR.

Before posting, a moral obligation should be fastened onto an individual to go through the video footage to see that no unwanted images have been accidentally captured. But the individuals who have been captured performing intimate acts should have been more careful and performed those acts in their bedrooms. So even they have a moral obligation to not perform private acts in public. So, if one is being adventurous, they should also have to face the consequences. From another aspect, if the individuals are unidentifiable, in a sense that they are not public figures, has their privacy still been invaded? As the internet is a public platform the website is accessible not only to people outside of the neighbourhood but also to people of the neighbourhood. So, there is a possibility that someone from the same neighbourhood can access the video.

Article 29 working party's 'Proposals for amendments regarding exemption for personal or household activities',[431] has mentioned the criteria for determining whether a processing falls within the household exemption. The criterions are only illustrative and not

[431] Annex 2, Proposals for Amendments regarding exemption for personal or household activities (Article 29 Working Party 2013) <http://ec.europa.eu/justice/article-29/documentation/other-document/files/2013/20130227_statement_dp_annex2_en.pdf> accessed on 7th January 2018.

exhaustive and are as follows, **a.** 'Is the personal data disseminated to an indefinite number of persons rather than to a limited community of friends, family members or acquaintances?', **b.** 'Is the personal data about individuals who have no personal or household relationship with the person posting it?', **c.** 'Does the scale and frequency of the processing of personal data suggest professional or full-time activity?', **d.** 'Is there evidence of a number of individuals acting together in a collective and organised manner?' and **e.** 'Is there the potential adverse impact on individuals, including intrusion into their privacy?'.[432] They also mentioned that the criteria should not be taken in isolation and that a combination of the criteria should be used to determine whether an activity is for personal or household purpose. We will take them one by one and see what they mean.

The internet has become the main platform for publishing. We have moved away from the more traditional platforms, such as newspapers. But what does indefinite number of persons mean? As mentioned, if I publish on my Facebook page the number of persons to whom it is published is definite but as more friends may be potentially added by me in the future, it has the effect of publishing to an indefinite number of people. In the *Goole Spain* case, Google published a link which was already publicly available to an indeterminate number of persons but still it was liable. But an image which is already publicly available, is reposted from the internet to any social networking sites with an added caption, whether it be neutral or derogatory, should not make the person posting it liable,

[432] ibid.

as there is no reasonable expectation of privacy in a public image. He could be sued for libel if the commentary is derogatory but not for privacy. In the *Bodil Lindqvist* case publishing on a personal webpage amounted to publishing to an indefinite number of people as the information could be accessed by anybody, even third country nationals.

So, publishing on personal pages on the internet is not the determinative factor. Privacy settings on Facebook may turn a personal page into a public page. Therefore, the privacy settings may also determine whether the publishing is to a determinate or an indeterminate number of persons. Generally, anything available on the internet is capable of being accessed by an indeterminate number of persons. Even closed groups attract new members as well as pages where one must pay to be members. The membership is open to the whole world that fulfils the criteria of the membership. Therefore, should we conclude that anything published on the internet is to an indeterminate number of persons? Such a conclusion will not hold ground as we all know that there is a distinction between personal and public cyberspace.

The second criterion based on relationship is also not fully determinative. For example, a group photograph with friends, posted on Facebook, where the friends are tagged, may well fit the criteria but a photograph of graduation day taken along with other students, with whom there was no interaction, and posted on personal social media, in no sense affects their privacy. If an individual is a part of the photograph, he should have full rights to

publish it on his personal social network, as it is a defining day in his life and it will be irrational if the consent of every person included in the photograph had to be taken, assuming that there are over a hundred students. But it is not restricted to photographs of graduation days as travel photographs may also include people who have no personal or household relationship to the person posting it and yet they are personal photographs. These instances are merely examples as there are innumerable instances in our day to day lives where such a possibility could arise.

Regarding the third and fourth criteria, they can be clubbed together. The scale and frequency will in many cases be related to the number of individuals involved in the processing. The scale and frequency of processing by an organisation will be large when compared to an individual. One reason is that an individual has limited resources when compared to an organisation. But an organisation may also consist of a single individual. A family doctor or a lawyer or a psychologist processing data will fall in-between household and commercial. It all depends on how the relationship is interpreted. A private practitioner processes data on an individual basis when compared to an organisation which processes data on a mass scale. An individual practitioner will have a limited number of clients, compared to a large organisation, with whom he keeps a personal relationship.

The last criteria about the impact on individuals is a subjective criterion based on factors such as culture and religion. Islamic women will be sensitive to the publication of their image which

depicts them without their hijab whereas women from more open cultures will not.

So, these criteria are also not certain. They do not live up to fully determining whether an activity is for personal and household purpose or for a commercial purpose. In the *Jehovah's Witness case,*[433] the collection of data by members of the community was not covered under the household exemption even though the data collection was done by individual members of the community without any direction from the community itself as to how and what data should be collected. The basis being that the collection was for the basic objective of Jehovah's Witness.

6.1.1.4.2. With regards to processing by corporations

The GDPR in Article 30 paragraph 5 differentiates between organisations which employ less than 250 persons from an organisation which employ more than 250 persons. Recital 13 explains that micro, small and medium sized enterprises are placed in a special situation and thus derogation is necessary with regards to record keeping. The exemptions for journalistic and artistic purposes will also apply to corporations who are involved in such activities.

Record keeping basically refers to maintaining a record of the processing activities by controllers and processors, like the purposes of the processing, the categories of data, etc. Article 30 paragraph 5 states, 'The obligations referred to in paragraphs 1 and 2 shall not

[433] Case C-25/17.

apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.

What this means is that organisations which employ less than 250 persons are exempt from keeping any written records of their processing activities under the GDPR. This is relevant to drone rental companies or to companies that provide drone services, whether for filming, surveying, or monitoring. They are usually small size companies having fewer than 250 employees. Having no obligations to maintain records puts them in the same league as a private drone enthusiast. They can flout the rules.

It is only when the processing is likely to result in a risk that they must adhere to the provisions. What does risk mean? Is a person playing with his dog on his porch at risk? Is a person walking down a public street at risk? Is a person buying groceries in a grocery store at risk? The foundation of a risk-based approach to data processing is contained in Article 24 of the GDPR. Article 24 paragraph 1 states, ‘Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons [...]. Recital 75 of the GDPR clarifies that, ‘The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to

physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.'

Therefore, if there is no damage to an individual, as is the case when a person is casually walking on a public road when his image is processed, then there is no requirement to keep a record of the processing. However, if the casual walker is processed on a regular basis, then a record must be maintained. This is partly because systematic monitoring reveals behavioural or location patterns of an individual.

But what amounts to occasional is not specified even though it has been used more than a few times in the GDPR. Does processing once a week, once a month or once a year, qualify as occasional? Does processing personal data about the same individual once a month qualify as occasional or the whole of the processing activity of an organisation needs to be considered? Even when processing is on an occasional scale it may still result in a risk to the rights and freedoms of data subjects.

Visual information, particularly the physical image of a person, is almost special categories of data within the meaning of Article 9 paragraph 1 of the GDPR. This is because an image of a person to a large extent reveals his racial or ethnic origin. However, recital 51 clears this ambiguity by mentioning that the processing of visual information, in the form of photographs, should not in itself be considered as processing of special categories of personal data. Photographs are covered by the definition of biometric data only when they are processed by a specific technical means which allows for the identification or authentication of an individual. This means that the vast amounts of physical visual data that would be processed by drones will fall under normal category of data even if it processes images of people. Thus, the risk to an individual, according to the GDPR, when images of people are processed by drones is less, as it does not allow for the identification or authentication of an individual. But drones with facial recognition abilities will allow for the identification and authentication of an individual.

Thus, small organisations are liable under Article 30 of the GDPR if they happen to process data which is likely to result in a risk to the rights and freedoms of natural persons, the processing is regular, the processing includes special categories of data or if the data processed is about criminal convictions and offences.

There are also video surveillance legislations in the EU which are country specific that will apply to visual information gathering by drones, but that is outside the scope of this thesis.

6.2 Technological

Legislation and technology go hand in hand, although, technology is way ahead. In this regard, legislations try to regulate new technologies because most of them have some disruptive potential. For example, in our above discussion of the GDPR, the main aim and purpose of its existence is to regulate data processing because technological advancements have made data processing easier. However, disruptive technologies can be made to be less disruptive by technological solutions itself and only the mandate to use technological measures included in the legislations. For example, the GDPR mandates the use of privacy by design and default, a technological measure.

Facial image of a person can be protected by wearing a mask. The mask to a large extent conceals his identity and can be regarded as a technological measure. Laptops come with privacy panic button which helps to keep the information displayed on the screen

invisible to a person other than the user. They also come with webcam covers to help maintain visual privacy of the user in case his webcam is hacked. The examples of the mask and the laptop reflect the position of protection before an invasion of visual privacy. An imaging technology itself could be limited in capturing identifiable information.

Ramón Padilla-López et.al, in their scholarly article, Visual Privacy Protection Methods[434], has enumerated five technological methods to protected visual privacy. They are intervention, blind vision, secure processing, redaction, and data hiding.[435] In terms of its relevance to drones, they are all applicable. Intervention is a protection method before the image is acquired while the other four are methods after an image has been processed. While intervention interferes with the camera, by means of pulsating light directed towards the lens or by means of software, the other four methods rely on computer algorithms.

Some of the common visual privacy protection measures after an image has been processed are blurring, pixelating, encryption, face de-identification and object removal. These methods of visual privacy protection are well within the meaning of technical and organisational measures mentioned in the GDPR. By applying the aforesaid measures, like blurring, the visual information becomes pseudonymous. Therefore, it will help in the pseudonymisation of

[434] José Ramón Padilla-López, Alexandros Andre Chaaraoui and Francisco Flórez-Revuelta, 'Visual Privacy Protection Methods: A Survey' (2015) 42 Expert Systems with Applications 4177.
[435] ibid.

data which is seen as a mitigating factor for the application of the GDPR. Intervention can be used to protect private space from drones. With the help of light beams which automatically detect camera lenses, could be installed at homes and other private spaces to render the drones ineffective in capturing images when flying over private property.

6.3 Self-Regulation

More than legislative and technological methods, self-regulation is a fundamental solution. But it is also the most difficult to ensure adherence. That may be due to many factors such as lack of knowledge about other's rights and one's own duties. Rights and duties can either be based on morality or written laws. We know privacy as a fundamental human right because it has been written as such in legal instruments. But at one point in time, it existed simply as an idea or practise without it being penned down.

In cultures where privacy existed, it was adhered to by the people as an unwritten norm. The problem with unwritten norms is that only people who are part of the norm have knowledge about the norm. Outsiders cannot be expected to have knowledge because they are not part of the system. Therefore, by etching the norms in written form adherence can be expected even from outsiders. In contemporary times everyone is expected to know the law of the land, even though practically, it is not possible for a person to know all the legal provisions that regulate his behaviour. But still he is

assumed by law to know them. So, if one commits a crime, he cannot say that he did not know the law. He had the ability to know the law by taking the help of a scholar learned in the practise of law.

But one may ask the question that if the norm to be followed is written then what is the role of self-regulation? But even though it is written people may act against the norm. For example, we know murder is a crime and it is written as law in all legal systems. Even though it is written, the crime is still committed. But what if murder as a crime was not written in the legal systems? There is a high probability that the number of murders would increase.

Therefore, written norms help a person in his quest for self-regulation. It makes it easier for a person to know right from wrong. But self-regulation is still at work even though the norms are written, as a person may be aggravated to such an extent that he feels like killing his neighbour but resists the urge as he knows the consequences of his actions. The role of self-regulation is even more pronounced in the case of civil wrongs, like invading others privacy. Unlike murder, the consequences for civil wrongs are less severe and because it is less severe people would more readily commit it. Therefore, the role of self-regulation is indispensable in visual privacy invasions. But the trick is privacy rights must be within the knowledge of the people who are more at risk of undermining them. Because if a person does not know that it is wrong then he will not think twice about what he is doing.

Information about others privacy rights can be disseminated by various methods for an effective self-regulation. One way of getting

the information to drone enthusiasts is by including a pamphlet that enumerates the importance of others visual privacy. So, for instance, a buyer purchases a drone and goes through the pamphlet that specifies the legal provisions of the ECHR and the CFREU, then instantly he becomes conscious about others right to privacy. This way there are more chances that he will abide by the ECHR and the CFREU. But there will be many who would prefer not to read the pamphlet and so other ways of getting the information contained in the pamphlet to the user is necessary. There exists a group of people who do not go through the booklets provided by the manufacturers of smartphones, televisions, or other electronic items. Supervisory Authorities established under the GDPR could fill the lag. They could organise public events for the masses to educate them about privacy risks and drones, the advantages and disadvantages of drone use and the risks to visual privacy weighed against the benefits that the drones will provide to the many industries. A positive public perception is necessary for the success of this technology.

But self-regulation too has its limitations, for example, Facebook although assuring the general-public that self-regulation would be the best for the sector, it did not abide by its words.[436] Therefore, self-regulation seldom works when it goes against self-interest.

[436] Mark Scott, 'Report: Social media networks fail to root out fake accounts' (POLITICO 2019) < https://www.politico.com/news/2019/12/06/social-media-networks-fake-accounts-report-076939> accessed 4 December 2020.

Summary: -

The solutions outlined above do not pre-empt each other. In other words, if one wants to solely rely on trespass, he can do so but proving a trespass in the case of drones will not be easy or, if one wants to solely rely on the fundamental right to privacy, he can do so but the difficulties have been outlined above. Even if one is relying on the GDPR, he will first have to identify the drone to the remote pilot which will be difficult. To give the most effective protection to the right to visual privacy, the reliance will have to be placed on all of the solutions. Relying on just one solution will be inadequate.

7. THE SUMMATION

7.1 Findings

From our discussion above, it is evident that the threat that drones pose to visual privacy, is real. The mass use of civilian drones will encroach upon the privacy rights guaranteed by the ECHR and the CFREU, if not properly regulated. There are currently different layers of legislations in place to ensure that the right to privacy and data protection is respected, but they seem to be, at certain points, in conflict with each other or inadequate to address the problems generated by civilian drones.

The outermost layer of protection are the new EU wide rules for drones, namely, Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, as well as its ancillary regulations. Some of the provisions for making sure that the right to privacy and data protection is not violated are the requirements included therein for the registration of drones which have a camera, and the provision for inclusion of privacy by design and default. These rules resort to an ex-ante regulatory approach to safeguard privacy and data protection. The requirements for registration of the drone and the remote pilot will help in the case of VLOS operations, in the identification of a violator of the fundamental right to privacy. But in the case of BVLOS or extended BVLOS operations, until the

drone can be identified in mid-air, the registration requirements achieve little to identify the violator.

Then comes the layer of protection in the form of the General Data Protection Regulation, which mainly ensures that the visual data processed by drones is lawful and complies with the provisions for the controllers and processors as guided by the principle of accountability. The regulatory approach here combines ex ante obligations with ex post enforcement of compliance. One of the main shortcomings of the GDPR is that individual drone enthusiasts and model aircraft clubs may escape liability for some visual privacy invasions, especially if they are covered by the household exemption or if the activity at stake is based on one the lawful grounds for processing personal data. The GDPR is also not clear about transitional visual information used for personal purposes and whether this amounts to processing. If it is interpreted affirmatively, that is, it amounts to processing then it becomes highly challenging to use drones with cameras. In the years ahead, the CJEU and national courts, as well as data protection supervisory authorities, will have to interpret the GDPR provisions and provide guidance on the said issues.

Other legal issues are also relevant for examining the role of civilian drones in visual privacy. That is the case, for instance, of the problem of whether plain observation with technological means, without trespassing into an individual's private immovable property, amounts to visual privacy infringements. The ECtHR has held that it does not infringe Article 8 of the ECHR as long as there

is no recording of the observation, while on the other hand, it amounts to processing within the meaning of the GDPR. In this context therefore, the position under the GDPR is stricter and in conflict with the ECHR.

The innermost layer of protection is in the form of the ECHR and the CFREU which guarantees the fundamental right to privacy and data protection and which form the general principles of EU law. The regulatory approach resorts here to ex post enforcement via injunctions and damages actions. But to bring an action against an individual violator under the ECHR or the CFREU is challenging as these international instruments are not directly applicable to private relations. Similar actions with grounds on domestic constitutional norms which recognize the fundamental rights to privacy and data protection may also be unavailable in the case of private claims unless the jurisdiction at stake assumes the direct or the indirect effects of these fundamental rights in horizontal private relationships.

Trespass has not been taken into consideration in any of the layers of legislations, but legal doctrines of trespass are fundamental in attaching liability for visual privacy violations by drones. The way the EU drone legislations have tried to avoid trespassing episodes is by banning the use of drones or restricting the use of drones over assemblies of people or through geo awareness software. But this kind of limitation will only hamper the market for drones as hobbyists would be hesitant to buy the product if they are not allowed enough space to use them. This will also be damaging for

the manufacturers, as their sales will be hit hard, discouraging a blossoming nascent drone industry.

Having said that, overall, the EU legislative requirements are in the right direction to address the problems of violations of privacy and data protection, by making registration mandatory for all drones having sensors that can process data, having specific and certified categories for commercial drone operations which are more stringently regulated, making geo awareness (for example, identifying residential areas) software mandatory for certain classes, etc. But the regulations seem too cumbersome and too technical for an average drone enthusiast to fully digest properly. The technological measures required to be adopted in the manufacture of drones, so that they are in conformity with all the EU rules and regulations, will increase the cost of the final product and it is normal for manufacturers to pass on the cost to the buyers which will eventually discourage sales.

The different variables identified in our discussion have not been holistically put to the test. By addressing each variable individually and isolated from the rest does no justice. There is the variable of a public and a private space, wherein, there is little expectation of visual privacy in a public place, so when people observe others in a public place, it does not amount to a violation of the right to privacy in most cases. Even if somebody takes a picture of another in a public place, another variable comes to play that is, whether he is a celebrity or not. If he is a celebrity, then he should be more open about his pictures being taken. Unintentional inclusion of members

of the public in a personal photograph is very common. But whether the unintentional inclusion will amount to violation of privacy rights is difficult to answer. The answer will depend on another set of variables like whether the person can be identified with a reasonable amount of effort or to whom is the publication directed towards. Delimitation of visual privacy is thus case-specific and empirically sensitive to the relevant variables at stake in each situation.

The current legal framework for addressing civil drones' impacts on visual privacy is permeated with several ambiguities. To begin with, what amounts to publication is open to different interpretations. In some cases, providing a link to information which is already in the public domain, on a personal webpage, amounts to publication, whereas on the other hand, anything published on the internet may amount to publication as the content could possibly be assessed by millions of people worldwide, by paying membership fee to the domain where the information is stored.

There is also the difficulty with transitional visual information, where on the one hand, even when images of the public were captured for the personal purpose of maintaining security outside one's home amounted not to violate privacy rights, while on the other, the same facts of the case amounted to the violation of privacy rights. The only difference was that there was a recording in one case and absent in the other.

Thus, there are too many variables and ambiguity that make it uncertain about the position of violation of visual privacy using

civilian drones. Instead of addressing it in a balanced manner, the legislations have addressed the problems by going to the extreme end of highly restricting the use of civilian drones. The only place left for an individual to still enjoy using his drone is within the confines of his home. It is only in this way that he will be able to avoid infringing others right to visual privacy.

But many people do not mind being seen or observed while walking on a street and they certainly might not mind if someone takes a nice picture of them, especially if they are not identifiable or if they are shown attractive or in good light. Therefore, the activity which has been processed or recorded, needs to be given due importance in determining a violation of visual privacy. A stranger may hypothetically well consent to the taking of his photograph if he were approached in the right way.

Private actions for visual privacy violations will also pose a problem because an individual will be hesitant to approach the courts, due to one reason or another. As already mentioned, the possibility of private individuals directly taking action under the ECHR or the CFREU is non-existent. Besides, maybe, financial concerns weigh heavily on the individual victim or maybe the consideration about the chances of success, seeing the number of variables that come into play. With such burdens, problems of collective action enter the picture and maybe ex ante protections as well as public investigation and enforcement should have a more crucial role in disciplining the use of civilian drones. When using such regulatory strategies, individuals may indirectly be benefitted

in the protection of their fundamental right to privacy and data protection. Moreover, some private claims may be available in some jurisdictions with grounds on national norms. In this case, indirect applicability will only truly be meaningful if there is a specific violation of the right to visual privacy by a drone and its remote pilot, at the national level.

The question about dummy drones, which does not observe or record, and whether it amounts to a violation of visual privacy rights is another important contention. Stating again it is not necessary that there should be a change in behaviour for visual privacy violations. This will be in cases where the violation occurs in secret. But what about cases where there is a change in behaviour, but no actual violation takes place. If every change of behaviour, for instance a change in behaviour because of a dummy drone, amounts to visual privacy violations, then we have reached the tipping point of being ludicrous. But the consequences of having dummy drones observe us in our daily lives also cannot be ignored. Whether the rules applicable to real cameras should be extended to dummy cameras, is a matter for the legislature to decide. However, in deciding, one should keep in mind that dummy cameras have the same effect on individuals as if it were a real camera, a chilling effect, unless by plain observation one can make out that in fact it is a ploy.

Adopting technological measures for solving the concerns of visual privacy is still in its infant stage. Although there is ongoing research on ethical drones, for example, how to inculcate ethics into drone

technology at the University of Southern Denmark UAS Centre, it is still a long way from truly being realised. The question of the overall cost of production of ethical drones also cannot be ignored. If the overall costs are too high, then it will dissuade the manufacturers from adopting those ethical designs.

The findings of this study are applicable to other imaging devices.

7.2 Theoretical contributions of this study

There have been previous studies on the privacy and data protection implications of drones upon which this study has been built, from academic articles written by university scholars and students, research conducted by the EU and articles in online magazines, but none have focussed their study on visual privacy. They all have been too oblivious to the nature of privacy infringement. This is the first study that categorically discusses the privacy implications of drones from the standpoint of visual privacy. It is such an important facet of privacy that without it no literature on drones and privacy is complete. In discussing visual privacy, I have given a true account of the determinant factors that apply to visual privacy, classified categories of visual information and even gone to the extent of dividing visual privacy invasion into three elements, it being, plain observation, observation coupled with recording and observation coupled with recording and publishing. Therefore, I divide the invasion according to the degree of the infringement. I have taken account of the cultural factors with specific examples that have an

influence on visual privacy. Further, I have isolated provisions of the GDPR which have relevance to visual information. I have included all of this in a seamless discussion on the topic of privacy implications of civilian drone use.

To add more weight to the study, trespass has been discussed alongside visual privacy. Therefore, the question of infringement of visual privacy from drones has been made dependent on trespass. Aerial trespass, to be more precise, has been discussed considering the relevant international conventions and literature. This study clearly shows the role, trespass has on visual privacy invasion by drones. Furthermore, the effects of this visual privacy invasion on the personality and autonomy of individuals has been discussed. Therefore, a holistic account of drones and privacy, from the type of invasion to its effects on individuals is what this study aimed to investigate.

7.3 Conclusion

The significance of visual information cannot be underestimated. With the increasing use of identification and surveillance technologies, whether it is in the form of drones with facial recognition technologies or going deeper than the layer of the skin, it has become essential to give visual information the importance that it deserves.

Some jurisdictions, like San Francisco in the US, have already realised this importance and taken a step which bans facial

recognition technologies, to preserve civil liberties.[437] Other jurisdictions, like China, have realised the importance of visual information from a different perspective. The Chinese social credit system uses facial recognition technologies to identify people and monitor their daily behaviour to give them points, depending on the passivity of their behaviour.[438] This in turn curbs civil liberties of minorities, like the Uyghur Muslims, due to biases one may have against the community as they are exposed and permanently recorded in the system. A new proposed French law will make the recording and publishing of images of police officers on duty, a crime.[439]

Image capturing technologies are getting more sophisticated, visual information is being processed in new ways, there is more visual data consumption than ever before due to our change in attitude and technology, and because of all this, there is a pressing need to realise that a picture is worth a thousand words.

The way forward is to give recorded physical visual information (which is identifiable or identified to a particular individual), and depending on the variables mentioned in this study, a higher level of protection than alphanumeric information. With regards to physical

[437] Gregory Barber, 'San Francisco bans agency use of facial recognition tech' (Wired.com 2019) < https://www.wired.com/story/san-francisco-bans-use-facial-recognition-tech/> accessed 23 November 2020.
[438] Karen Li Xan Wong and Amy Shields Dobson, 'We're just data: Exploring China's social credit system in relation to digital platform ratings cultures in Westernised democracies' (2019) 4(2) Global Media and China 220.
[439] Proposition de loi nº 3452 relative à la sécurité globale <http://www.assemblee-nationale.fr/dyn/15/textes/l15b3452_proposition-loi#tocUniqueId30> accessed 24 November 2020.

visual information which has not been recorded, as there is no need for a new provision guaranteeing a fundamental right to visual privacy, a direct remedy, accessible to the masses, will go a long way in ensuring peace of mind. At present, due to the multiplicity of legislations (like in tort law or criminal law) that could be applicable in bits and pieces, to visual privacy infringements by drones, an individual is confused as to what action to take or whether there is an any action to take at all.

Bibliography

List of Judgements/Decisions

European

ECtHR

Affaire Halabi v. France, no. 66554/14, ECHR 2019

Antović and Mirković v. Montenegro, no. 70838/13, ECHR 2017

Axel Springer AG and RTL Television GmbH v. Germany, no. 51405/12, ECHR 2017

Bărbulescu v. Romania, no. 61496/08, ECHR 2016

Bogomolova v. Russia, no. 13812/09, ECHR 2017

Copland v. the United Kingdom, no. 62617/00, ECHR 2007-I

Couderc and Hachette Filipacchi Associés v. France, no. 40454/07, ECHR 2015

Cyprus v. Turkey, no. 25781/94, ECHR 2001

Friedl v. Austria, 31 January 1995, Series A, no. 305 B

Halford v. the United Kingdom, 25 June 1997, Reports 1997-III

Kahn v. Germany, no. 16313/10, ECHR 2016

Kurier Zeitungsverlag und Druckerei GmbH (no. 2) v. Austria, no. 1593/06, ECHR 2012

Krone Verlag GmbH v. Austria, no. 27306/07, ECHR 2012

Küchl v Austria, no. 51151/06, ECHR 2012

Laskey, Jaggard and Brown v. the United Kingdom, 19 February 1997, Reports 1997-I

López Ribalda and Others v. Spain, nos. 1874/13 and 8567/13, ECHR 2018

López Ostra v. Spain, no. 16798/90, ECHR 1994

Niemietz v. Germany, 16 December 1992, Series A, no. 251 B

P.G. and J.H. v. the United Kingdom, no. 44787/98, ECHR 2001-I

Peck v. The United Kingdom, no. 44647/98, ECHR 2003-I

Perry v. The United Kingdom, no. 63737/00, ECHR 2003

Reklos and Davourlis v. Greece, no. 1234/05, ECHR 2009

Schüssel v. Austria, no. 42409/98, ECHR 2002 (unreported)

Société de Conception de Presse et d'Edition v. France, no. 4683/11, ECHR 2016

Sciacca v. Italy, no. 50774/99, ECHR 2005-I

Schüth v. Germany, no. 1620/03, ECHR 2010

Söderman v Sweden, no. 5786/08, ECHR 2013

Von Hannover v. Germany, no. 59320/00, ECHR 2004-VI

Von Hannover v. Germany (no.2), nos. 40660/08 and 60641/08, ECHR 2012

Von Hannover v. Germany (no.3), no. 8772/10, ECHR 2013

Vereinigung Bildender Kunstler v. Austria, no. 68354/01, ECHR 2007

Vukota-Bojić v. Switzerland, no. 61838/10, ECHR 2016

X and Y v. the Netherlands, 26 March 1985, ECHR Series A, no. 91

Z v. Finland, 25 February 1997, ECHR Reports 1997-I

Commission Decisions

Friedl v Austria, no. 28/1994/475/556, Commission decision of 1994 (report)

Pierre Herbecq and the Association Ligue des droits de l 'homme v. Belgium, nos. 32200/96 and 32201/96, Commission decision of 14 January 1998 (on admissibility)

CJEU

Judgement of 11 December 2014, *František Ryneš v. Úřad pro ochranu osobních údajů*, C-212/13, EU:C:2014:2428

Judgement of 13 May 2014, *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, C-131/12, EU:C:2014:317

Judgement of 22 January 2013, *Sky Österreich GmbH v. Österreichischer Rundfunk*, C-283/11, EU:C:2013:28

Judgement of 16 December 2008, *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy*, C-73/07, EU:C:2008:727

Judgement of 6 November 2003, *Bodil Lindqvist*, C-101/01, EU:C:2003:596

Judgement of 6 October 2015, *Maximillian Schrems v. Data Protection Commissioner*, C-362/14, EU:C:2015:650

Judgement of 16 July 2020, *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems*, C-311/18, EU:C:2020:559

Judgement of 21 December 2016, *Tele2 Sverige AB*, Joined Cases C-203/15 and C-698/15, EU:C:2016:970

Judgement of 8 April 2014, *Digital Rights Ireland*, Joined Cases C-293/12 and C-594/12, EU:C:2014:238

Judgement of 29 January 2008, *Promusicae v. Telef´onica de Espana SAU*, C-275/06, EU:C:2008:54

Judgement of 9 November 2010, *Schecke v. Land Hessen*, Joined Cases C-92/09 & C-93/09, EU:C:2010:662

Judgement of 26 February 2013, *Åkerberg Fransson*, C-617/10, EU:C:2013:105

Judgement of 26 February 2013, *Stefano Melloni*, C-399/11, EU:C:2013:107

Judgement of 6 November 2003, *Bodil Lindqvist*, C-101/01, EU:C:2003:596

Judgement of 14 February 2019, *Sergejs Buivids*, C-345/17, EU:C:2019:122

Judgement of 10 July 2018, *Jehovah's Witness*, C-25/17, EU:C:2018:551

Spanish

STC 241/2012 (Tribunal Constitutional)

STS, Sala Primera, de lo Civil, Sentencia 600/2019 de 7 Nov. 2019, Rec. 5187/2017

Judgment 18/2015 of the Spanish Constitutional Court of 16 February 2015

In Judgment 518/2012 of the Spanish Supreme Court of 24 July 2012

Respeto a la mayores (Supreme Court)

German

7 BVerfGE 198 (Lüth case 1958)

1 BvR 16/13

1 BvR 276/17

British

Bernstein of Leigh v Skyview & General Ltd, [1977] EWHC QB 1, [1977] 3 WLR 136, [1977] 241 EG 917, [1977] 2 All ER 902, [1978] QB 479

Bury v Pope, (1587) Croke Eliz 118, [1653] EngR 382, (1653) Croke Eliz 118, (1653) 78 ER 375 (B)

Campbell v Mirror Group Newspapers Ltd, [2004] UKHL 22, [2004] 2 WLR 1232, [2004] 2 AC 457, [2004] UKHRR 648, [2004] EMLR 15, 16 BHRC 500, [2004] HRLR 24, [2004] 2 All ER 995

DPP v Jones, [1999] 2 All ER 257

Douglas v Hello, [2005] EWCA Civ 595, [2005] 4 All ER 128, [2005] 3 WLR 881, [2006] QB 125

Ellis v Loftus Iron Company, (1874) LR 10 CP 10

Fay v Prentice, [1845] EngR 79, (1845) 1 CB 828, (1845) 135 ER 769

Fearn v Tate Gallery, [2019] EWHC 246 (Ch)

Harrison v Duke of Rutland [1893] 1 QB 142

Hickman v Maisey, [1900] 1 QB 752

Irvine v Talksport, [2003] EWCA Civ 423, [2003] 2 All ER 881, [2003] EMLR 538

Kenyon v Hart, (1865) 6 Best and Smith's Reports 249

Lowdens v Keaveney, [1903] 2 IR 82

Murray v Express Newspapers plc, [2008] EWCA Civ 446

Pickering v Rudd, [1815] EWHC KB J43, (1815) 4 Camp 219, (1815) 171 ER 70, (1815) 171 ER 400 (B)

Richardson v Facebook/ Richardson v Google, [2015] EWHC 3154 (QB)

The Electric Telegraph Co. v Overseers of Salford, [1855] EngR 552, (1855) 11 Exch 181, (1855) 156 ER 795

Wandsworth Board of Works v United Telephone Company, (1884) 13 QBD 904

American

California v. Ciraolo, 476 US 207 (1986)

Dow Chemical Co. v. United States, 476 US 227 (1986)

Florida v. Riley, 488 US 445 (1989)

Goldman v. United States, 316 US 129 (1942)

Haelan Laboratories v. Topps Chewing Gum, 202 F.2d 866 (2nd Cir. 1953)

Hester v. United States, 265 US 57 (1924)

John David Boggs v. William H. Merideth [2016], In the United States District Court, Western District of Kentucky, Louisville Division, Case No. 3:16-cv-6-DJH

Katz v. United States, 389 US 347 (1967)

Kyllo v. United States, 533 US 27 (2001)

Motschenbacher v. R.J. Reynolds Tobacco Company, 498 F.2d 821 (9th Cir. 1974)

Naruto v. David John Slater et al, No. 3:2015cv04324 - Document 45, N.D. Cal. 2016

O'Brien v. Pabst Sales Co., 124 F.2d 167 (5th Cir. 1941)

Olmstead v. United States, 277 US 438 (1927)

On Lee v. United States, 343 US 747 (1952)

Silverman v. United States, 365 US 505 (1961)

United States v. Causby, 328 U.S. 256 (1946)

Australian

Victoria Park Racing and Recreation Grounds Company Limited v Taylor, [1937] High Court of Australia 45

Bathurst City Council v Saban, [1985] 2 New South Wales Law Reports 704

Indian

Gokal Prasad v Radho, (1888) 10 Indian Law Reports (ILR) Allahabad Series

Treatise/Statutes

International

Convention relating to the Regulation of Aerial Navigation (signed 13 October 1919 at Paris, as amended)

Convention on International Civil Aviation (signed 7 December 1944 at Chicago and entered into force 4 April 1947, as amended)

The Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights (ECHR), as amended).

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 1981 (Convention 108, entered into force in 1985)

Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 2018 (Convention 108+)

International Civil Aviation Organisation Circular 328-AN/190

International Civil Aviation Organisation Doc 10019-AN/507 (Manual on Remotely Piloted Aircraft Systems 2015)

European Union

Charter of Fundamental Rights of the European Union (Charter, CFREU) [2012] OJ C326/391.

Commission, 'Proposal for a Regulation of the European Parliament and of the Council on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and repealing Regulation (EC) No 216/2008 of the European Parliament and of the Council' COM (2015) 613 final, 7 November 2015

Commission, 'Proposal for a Regulation of the European Parliament and of the Council on European data governance' COM (2020) 767 final, 25 November 2020

Directive 2009/48/EC of the European Parliament and of the Council of 18 June 2009 on the safety of toys [2009] OJ L170/1

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to

the processing of personal data and on the free movement of such data [1995] OJ L281/31

Regulation (EC) No 216/2008 of the European Parliament and of the Council of 20 February 2008 on common rules in the field of civil aviation and establishing a European Aviation Safety Agency and repealing Council Directive 91/670/EEC, Regulation (EC) No 1592/2002 and Directive 2004/36/EC [2008] OJ L79/1

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1

Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 [2018] OJ L212/1

Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems [2019] OJ L152/1

Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft [2019] OJ L152/45

European Union Institutional Documents

Article 29 Data Protection Working Party, 'Statement of the Working Party on current discussions regarding the data protection reform package,' (Annex 2, 'Proposals for Amendments regarding exemption for personal or household activities') (2013) <http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130227_statement_dp_annex2_en.pdf> accessed on 7th January 2018

Article 29 Data Protection Working Party, 'Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones' 01673/15/EN, WP 231 (2015)

Article 29 Data Protection Working Party, Guidelines on Automated individual decision- making and profiling for the purposes of Regulation 2016/679, WP 251 (2017)

Article 29 Working Party, Proposals for Amendments regarding exemption for personal or household activities 2013

'Civil UAV Application and Economic Effectiveness of Potential Configuration Solutions' | Projects | FP5-GROWTH | CORDIS | European Commission' (CORDIS | European Commission) <https://cordis.europa.eu/project/rcn/63495_en.html>

'Civilian UAV Thematic Network: Technologies, Applications, Certification' | Projects | FP5-GROWTH | CORDIS | European Commission' (CORDIS | European Commission) <https://cordis.europa.eu/project/rcn/61170_en.html>

Commission, 'Towards a European strategy for the development of civil applications of Remotely Piloted Aircraft Systems (RPAS)', SWD (2012) 259 final, 4th September 2012

Commission, 'An Aviation Strategy for Europe', SWD (2015) 261 final, 7 December 2015

EASA, 'Concept of Operations for Drones: A risk-based approach to regulation of unmanned aircraft' (undated)

EASA Technical Opinion, 'Introduction of a regulatory framework for the operation of unmanned aircraft' (2015) < https://www.easa.europa.eu/document-library/opinions/opinion-technical-nature>

Frost and Sullivan for the European Commission, 'Study Analysing the Current Activities in the Field of UAV' ENTR/2007/065 (2007)

'Innovative Operational UAS Integration' (Transport-research.info) <http://www.transport-research.info/sites/default/files/project/documents/20130111_100721_43303_INOUI_Booklet.pdf>

NPA 2014-09, 'Transposition of Amendment 43 to Annex 2 to the Chicago Convention on remotely piloted aircraft systems (RPAS) into common rules of the air' <www.easa.europa.eu/document-

library/notices-of-proposed-amendments/npa-2014-09> accessed 22 July 2017

NPA 2017-05, ‘Introduction of a regulatory framework for the operation of drones — unmanned aircraft system operations in the open and specific category’<www.easa.europa.eu/document-library/notices-of-proposed-amendment/npa-2017-05> accessed on 24 July 2017

‘Roadmap for the Integration of Civil Remotely Piloted Aircraft Systems into the European Aviation System’ European RPAS Steering Group, June 2013

‘Strategic Aerospace Review for the 21st century (STAR21): Creating a coherent market and policy framework for a vital European industry’ European Commission Enterprise Publications, July 2002

'Unmanned Aerial Systems in European Airspace | Projects | FP7-TRANSPORT | CORDIS | European Commission' (CORDIS | European Commission) <https://cordis.europa.eu/project/rcn/103989_en.html>

‘25 Nations for an Aerospace Breakthrough: European Civil Unmanned Air Vehicle Roadmap’ (2005) <https://www.uvsr.org/Documentatie%20UVS/Publicatii-internationale/EuropeanCivilUnmannedAirVehicleRoadmap1.pdf>

French

Arrêté du 17 décembre 2015 relatif à la conception des aéronefs civils qui circulent sans personne à bord, aux conditions de leur emploi et aux capacités requises des personnes qui les utilisent

Proposition de loi nº 3452 relative à la sécurité globale

Spanish

Constitución Española

Ley Orgánica 1/1982 de 5 de mayo de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen

Ley 18/2014, de 15 de octubre, de aprobación de medidas urgentes para el crecimiento, la competitividad y la eficiencia

Real Decreto 1036/2017, de 15 de diciembre, por el que se regula la utilización civil de las aeronaves pilotadas por control remoto, y se modifican el Real Decreto 552/2014, de 27 de junio, por el que se desarrolla el Reglamento del aire y disposiciones operativas comunes para los servicios y procedimientos de navegación aérea y el Real Decreto 57/2002, de 18 de enero, por el que se aprueba el Reglamento de Circulación Aérea

Real Decreto 2816/1982, de 27 de agosto, por el que se aprueba el Reglamento General de Policía de Espectáculos Públicos y Actividades Recreativas

German

Grundgesetz für die Bundesrepublik Deutschland 1949

American

U.S. Department of Defence press release (Release No: NR-008-17) of 2017, <www.defense.gov/News/News-Releases/News-Release-View/Article/1044811/department-of-defense-announces-successful-micro-drone-demonstration/> accessed 30 October 2017

Reports and Guidelines

Asser Institute, 'Study on sports organisers' rights in the European Union' (Publication office of the European Union 2014)

Pew Research Center 2008 <https://www.pewresearch.org/wp-content/uploads/sites/2/2008/09/Pew-2008-Pew-Global-Attitudes-Report-3-September-17-2pm.pdf> accessed 1 November 2020; Kazi Stastna, 'Do countries lose religion as they gain wealth?' (CBC News 2013) <www.cbc.ca/news/world/do-countries-lose-religion-as-they-gain-wealth-1.1310451> accessed 8 November 2017.

Guidelines on the protection of individuals with regard to the processing of personal data in a world of big data (Council of Europe 2017)

The Impact of Big Data and Artificial Intelligence (AI) in the Insurance Sector (OECD 2020)

European Data Protection Board, Guidelines 3/2019 on processing of personal data through video devices (version for public consultation), Adopted on 10 July 2019

Secondary Literature

Books

Barnhart R and others, *Introduction to Unmanned Aircraft Systems* (CRC Press 2012)

Barpujari H, *The American Missionaries and North-East India (1836-1900 A.D.)* (Spectrum Publications 1986)

Bartsch R and others, *Drones in Society: Exploring the Strange New World of Unmanned Aircraft* (Routledge 2017)

Blackstone W, *Commentaries on the Laws of England* (Sharswood G ed, JB Lippincott Company 1893)

Blom D. J., *Unmanned Aerial Systems: A Historical Perspective* (CSI Press 2010)

Chalmeta Torrubia Blanca, *Aeronaves civiles no tripuladas. Contexto y regulación* in Agustí Cerrillo and Miquel Peguera (eds.), *Retos Jurídicos de la Inteligencia Artificial* (Thomson Reuters-Aranzadi 2020)

Clapham A, *Human Rights Obligations of Non-State Actors* (Gráinne de Búrca, Brunno de Witte, Francesco Francioni eds, Oxford University Press 2006)

Clapham A, *Human Rights in the Private Sphere* (Clarendon Press 1993)

Dennedy M and others, *The Privacy Engineer's Manifesto: Getting from Policy to Code to QA to Value* (Apress 2014)

Everett R. H., *Unmanned Systems of World Wars I and II* (The MIT Press 2015)

Finn A and Scheding S, *Developments and Challenges for Autonomous Unmanned Vehicles* (Springer 2010)

Gutwirth S and others, *European Data Protection: Coming of Age* (Springer Netherlands 2013)

Hert P and Gutwirth S, '*Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power'* (in E. Claes, A. Duff & S. Gutwirth eds, Privacy and the Criminal Law, Antwerp/Oxford, Intersentia, 2006)

Hunsaker J, *Biographical Memoir of Elmer Ambrose Sperry, 1860-1930* (National Academy of Sciences 1954)

Hunter W, *The Indian Empire: Its People, History and Products* (Routledge 2000)

Hu Runshan and others, *Bridging Policy, Regulation, and Practice? A Techno-Legal Analysis of Three Types of Data in the GDPR*, in 'Data Protection and Privacy: The Age of Intelligent Machines' Edited by Ronald Leenes Rosamunde van Brakel, Serge Gutwirth and Paul De Hert (Hart Publishing 2017)

Inness J, *Privacy, Intimacy and Isolation* (Oxford University Press 1992)

Kenny C, *A Selection of Cases Illustrative of the English Law of Tort*, Fifth Edition (Cambridge University Press 1928)

Leslie David, *Understanding bias in facial recognition technologies: an explainer* (The Alan Turing Institute 2020)

Lincoln F, *The Legal Background to the Starrs* (London, E. Goldston1932)

Lockard C. A, *Societies, Networks, and Transitions: A Global History*, Volume I: to 1500 (Houghton Mifflin Company 2007)

McNair A, *The Law of the Air* (Butterworth 1932)

Newcome L, *Unmanned Aviation: A Brief History of Unmanned Aerial Vehicles* (American Institute of Aeronautics and Astronautics Inc., 2004)

Norton-Taylor R, *Whose Land is it Anyway? Agriculture, Planning and Land Use in the British Countryside* (Turnstone Press 1982)

Rosa M. and others, *Spain–UK–Belgium Comparative Legal Framework: Civil Drones for Professional and Commercial Purposes.* In: de Miguel Molina M., Santamarina Campos V. (eds) *Ethics and Civil Drones* (Springer Briefs in Law 2018)

Kim Nancy S., *Consentability: consent and its limits* (Cambridge University Press 2019)

Semple J, *Bentham's Prison: A Study of the Panopticon Penitentiary* (Clarendon Press 1993)

Solove D, *Nothing to Hide: The False Tradeoff between Privacy and Security* (Yale University Press 2013)

Tesla Nikola, *My Inventions: The Autobiography of Nikola Tesla* (Experimenter Publishing Company Inc., New York 1919)

Villani Cédric, *For a meaningful artificial intelligence: Towards a French and European strategy* (2018)

Westin A, *The Origins of Modern Claims to Privacy* in Schoeman Ferdinand D ed, *Philosophical Dimensions of Privacy: An Anthology* (Cambridge University Press 2007)

Westin A, *Privacy and Freedom* (New York: Athenum 1967)

Wilson Hughes J, *On Intelligence: The History of Espionage and the Secret World* (Constable 2016)

Journal Articles

‘More about Balloons’ (1849) 4 (26) Scientific American 205

Al-Kodmany K, ‘Women’s Visual Privacy in Traditional and Modern Neighbourhoods in Damascus’ (2000) 17 Journal of Architectural and Planning Research

Altman I, 'Privacy Regulation: Culturally Universal or Culturally Specific?' (1977) 33 Journal of Social Issues 66

Ames J, ‘The History of Trover’ (1897) 11 Harvard Law Review 277

Barocas Solon and Levy Karen, ‘Privacy Dependencies’ (2020) 95 Washington Law Review 555

Beaman A and others, 'Self-Awareness and Transgression in Children: Two Field Studies' (1979) 37 Journal of Personality and Social Psychology 1835

Bentley Jennifer, ‘Policing the Police: Balancing the Right to Privacy Against the Beneficial Use of Drone Technology’ (2018) 70 Hastings Law Journal 249.

Bergmann S, ‘Publicity Rights in the United States and Germany: A Comparative Analysis’ (1999) 19 Loyola of Los Angeles Entertainment Law Review 479

Buolamwini Joy and Gebru Timnit, ‘Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification’ (2018) Conference on fairness, accountability, and transparency

Burchardt Dana, ‘Backlash against the Court of Justice of the EU? The Recent Jurisprudence of the German Constitutional Court on EU Fundamental Rights as a Standard of Review’ (2020) 21 German Law Journal 1

Brayne Sarah and others, ‘Visual Data and the Law’ (2018) 43 Law and Social Inquiry 1149

Bygrave L, 'Data Protection by Design and by Default: Deciphering the EU’S Legislative Requirements' (2017) 4 Oslo Law Review 105

Cate Fred H., ‘The EU Data Protection Directive, Information Privacy, and the Public Interest’ (1995). Articles by Maurer Faculty. Paper 646

Calo Ryan M., ‘The Drone as Privacy Catalyst’ (2011) 64 Stanford Law Review Online 29

Chowdury Tasneem, ‘Segregation of Women in Islamic Societies of South Asia and its Reflection in Rural Housing - Case Study in Bangladesh’ (1993) McGill University Student Thesis

Cooper J, ‘Roman Law and the Maxim Cujus est Solum in International Law’ (1952) 1 McGill Law Journal 23

Deiser G, ‘The Development of Principle in Trespass’ (1917) 27 Yale Law Journal 220

Edara I, 'Religion: A Subset of Culture and an Expression of Spirituality' (2017) 07 Advances in Anthropology 273

Elvin Jesse, ‘The law of Nuisance and the Human Rights Act’ (2003) 62 Cambridge Law Journal 546

Emam Khaled El and others, ‘Anonymising and sharing individual patient data’ (2015) 350 British Medical Journal

Esayas Samson, ‘The Role of Anonymisation and Pseudonymisation Under the EU Data Privacy Rules: Beyond the All or Nothing Approach’ (2015) 6 European Journal of Law and Technology

Farber B. Hillary, ‘Keep Out! The Efficacy of Trespass, Nuisance and Privacy Torts as Applied to Drones’ (2017) 33 Georgia State University Law Review 359

Fox L, ‘The Law of Aerial Navigation’ (1909) 190 The North American Review 101

Gavison Ruth, ‘Privacy and the Limits of Law’ (1980) 89 Yale Law Journal 421

Gevurtz Franklin, ‘Obstruction of Sunlight as a Private Nuisance’ (1977) 65 California Law Review 94

Goodheart B, ‘Tracing the History of the Ornithopter: Past, Present and Future’ (2011) 21 Journal of Aviation/Aerospace Education & Research 31

Gassó Aina and others, ‘Sexting, Mental Health, and Victimization Among Adolescents: A Literature Review’ (2019) 16 International Journal of Environmental Research and Public Health 2364

Hale Benjamin, ‘Identity Crisis: Face Recognition Technology and Freedom of the Will’ (2005) 8 Ethics Place and Environment 141

Hirshleifer J, 'Privacy: Its Origin, Function, and Future' (1980) 9 The Journal of Legal Studies 649

Horst Hilje and Messing Jantine, ‘It’s Not Dutch to Close the Curtains’ (2006) Volume 3 Home Cultures 21

Hutchings Karl W., ‘Finding the Paleoindian Spear Thrower: Quantitative Evidence for Mechanically-Assisted Propulsion of Lithic Armatures during the North American Paleoindian Period’ (2015) 55 Journal of Archaeological Science 34

Kaminski E. Margot, ‘Drone Federalism: Civilian Drones and the Things They Carry’ (2013) 4 California Law Review Circuit 57

Keenan J, ‘The Tuareg Veil’ (1977) 13 Middle Eastern Studies 3

Kreimer Seth, ‘Pervasive Image Capture and the First Amendment: Memory, Discourse, and the Right to Record’ (2011) 159 University of Pennsylvania Law Review 335

Kellermann Robin, ‘Drones for Parcel and Passenger Transportation: A Literature Review’ (2020) 4 Transportation Research Interdisciplinary Perspectives (Elsevier)

Koops B. J. and another, ‘Code and the Slow Erosion of Privacy’ (2005) 12 Michigan Telecommunications and Technology Law Review 115

Koops B. J. and others, ‘The Reasonableness of Remaining Unobserved: A Comparative Analysis of Visual Surveillance and Voyeurism in Criminal Law’ (2018) 43 Law and Social Inquiry 1210

Koops B. J., ‘Privacy Spaces’ (2018) 121 West Virginia Law Review 612

Kupritz V, ‘Privacy Management at Work: A Conceptual Model’ (2000) 17 Journal of Architectural and Planning Research

Lardone F, ‘Airspace Rights in Roman Law’ (1931) 2 Air Law Review 455

Logeais E and another, ‘The French Right of Image: An Ambiguous Concept Protecting the Human Persona’ (1998) 18 Loyola of Los Angeles Entertainment Law Review 511

Mann Steve and others, ‘Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments’ (2003) 1 Surveillance and Society 331

Merrill W. Thomas, ‘Trespass, Nuisance, and the Costs of Determining Property Rights’ (1985) 14 Journal of Legal Studies 13

Molko Robert, ‘The Drones are Coming! Will the Fourth Amendment Stop their Threat to Our Privacy?’ (2013) 78 Brooklyn Law Review 1279

Nettle D and others, ‘Cycle Thieves, We Are Watching You: Impact of a Simple Signage Intervention against Bicycle Theft’ (2012) 7 PLoS ONE

Nissenbaum Helen, ‘Privacy as Contextual Integrity’ (2004) 79 Washington Law Review

Nu’man S., 'A Unified Architectural Theory for Islamic Architecture' (2016) 10 International Journal of Architectural Research: ArchNet-IJAR

Padilla-López J and others, ‘Visual Privacy Protection Methods: A Survey' (2015) 42 Expert Systems with Applications 4177

Palmer T, ‘Intellectual Property: A non-Posnerian Law and Economics Approach’ (1989) 12 Hamline Law Review 261

Penney Jonathon, ‘Chilling Effects and Transatlantic Privacy’ (2019) 25 European Law Journal 122

Posner R, ‘Privacy, Secrecy and Reputation’ (1979) 28 Buffalo Law Review 1

Prosser William, ‘Privacy’ (1960) 48 California Law Review 383

Q. C. David Anderson and Murphy Cian C., The Charter of Fundamental Rights: History and Prospects in Post-Lisbon Europe (2011) European University Institute law repository

Rahim Z, 'The Influence of Culture and Religion on Visual Privacy' (2015) 170 Procedia - Social and Behavioural Sciences 537

Razack S., ‘What Is to Be Gained by Looking White People in the Eye? Culture, Race, and Gender in Cases of Sexual Violence’ (1994) 19 Signs: Journal of Women in Culture and Society 894

Reynolds M. Osborne, ‘Distinguishing Trespass and Nuisance: A Journey through a Shifting Borderland’ (1991) 44 Oklahoma Law Review 227

Stalla-Bourdillon Sophie and Knight Allison, ‘Anonymous Data V. Personal Data - A false debate: An EU perspective on anonymization, pseudonymization, and personal data’ (2017) Wisconsin International Law Journal

Sarrión Joaquín, ‘Actual challenges for fundamental rights protection in the use of drone technology’ (2018) SSRN

Salvador Coderch Pablo, Rubi Puig Antoni, Ramírez Silva Pablo, ‘Imágenes Veladas: Libertad de Información, Derecho a la Propia Imagen y Autocensura de los Medios’ (2011) Vol.1 InDret

Satine L, ‘Maximal Safety, Minimal Intrusion: Monitoring Civil Protective Orders without Implicating Privacy’ (2008) 43 Harvard Civil Rights-Civil Liberties Law Review 267

Sawers Brian, ‘The Right to Exclude from Unimproved Land’ (2011) 83 Temple Law Review 665

Salter M, ‘Privates in the online public: Sex(ting) and reputation on social media’ (2016) 18 New Media and Society 2723

Schick F, ‘Space Law and Space Politics’ (1961) 10 International and Comparative Law Quarterly 681

Selinger Evan and Hartzog Woodrow, ‘The Inconsentability of Facial Surveillance’ (2019) 66 Loyola Law Review 101

Sipahi A, ‘Window-Conflicts in the Ottoman Empire and Turkey: Visual Privacy, Materiality and Right to the City’ (2016) 52 Journal of Middle Eastern Studies 588

Sella-Villa David, ‘Drones and Data: A Limited Impact on Privacy’ (2020) 55 University of Richmond Law Review

Solove Daniel, ‘A Taxonomy of Privacy’ (2006) 154 University of Pennsylvania Law Review 477

Stöcker Claudia and others, ‘Review of the Current State of UAV Regulations’ (2017) 9 Remote Sensing, MDPI Journal

Takahashi T. Timothy, ‘Drones and Privacy’ (2012) XIV Columbia Science and Technology Law Review 72

Villasenor J, ‘Observations from above: unmanned aircraft systems and privacy’ (2013) 36 Harvard Journal of Law and Public Policy 457

Wachter Sandra and Mittelstadt Brent, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' (2019) Issue 2 Columbia Business Law Review

Warren Samuel and Brandeis Louis, 'The Right to Privacy' (1890) 4 Harvard Law Review 193

Watts C. Adam and others, 'Unmanned Aircraft Systems in Remote Sensing and Scientific Research: Classification and Considerations of Use' (2012) 4 MDPI Journal Remote Sensing 1671

White Elizabeth, 'Purdah' (1977) 2 Frontiers: A Journal of Women Studies 31

Wong Karen Li Xan and Dobson Amy Shields, 'We're just data: Exploring China's social credit system in relation to digital platform ratings cultures in Westernised democracies' (2019) 4(2) Global Media and China 220

Zaher C, 'When a Woman's Marital Status Determined Her Legal Status: A Research Guide on the Common Law Doctrine of Coverture' (2002) 94 Law Library Journal 459

Internet Articles and Sources

Ashton K, 'That Internet of Things Thing' (Rfidjournal.com 2009) <www.rfidjournal.com/articles/view?4986> accessed 26 November 2017

Barber Gregory, 'San Francisco bans agency use of facial recognition tech' (Wired.com 2019)

<https://www.wired.com/story/san-francisco-bans-use-facial-recognition-tech/> accessed 23 November 2020

Bellingar T and Kupritz V, 'Privacy Matters' (Workwellpartners.com 2011) <https://workwellpartners.com/wp-content/uploads/2014/10/privacy-matters1-pdf-28565.pdf> accessed 7 November 2017

Braithwaite R, 'The Queen of Bees' (Lightaircraftassociation.co.uk 2012) <www.lightaircraftassociation.co.uk/2012/Magazine/June/QueenBee.pdf> accessed 15 July 2017

Budanovic N, 'The Early Days of Drones - Unmanned Aircraft from World War One and World War Two' (War History Online 2017) <www.warhistoryonline.com/military-vehicle-news/short-history-drones-part-1.html> accessed 11 July 2017

Butti Elena, 'The Roles and Relationship between the Two European Courts in Post-Lisbon EU Human Rights Protection' (JURIST – Dateline, Sept. 12, 2013) <http://jurist.org/dateline/2013/09/elena-butti-lisbon-treaty.php.>

Candela J, 'Building scalable systems to understand content' (Facebook Code 2017) <https://code.facebook.com/posts/1259786714075766/building-scalable-systems-to-understand-content/> accessed 23 June 2017

Corcoran K, 'French court orders fines in Kate photos case' (Business Insider 2017) <www.businessinsider.com/ap-the-latest-

french-court-orders-fines-in-kate-photos-case-2017-9> accessed 8 October 2017

Crouch T, 'On This Spot...' (National Air and Space Museum 2009) <https://airandspace.si.edu/stories/editorial/spot> accessed 15 July 2017

Garvie Clare, 'Garbage In, Garbage Out: Face Recognition on Flawed Data' (The Center on Privacy & Technology at Georgetown Law 2019) < https://www.flawedfacedata.com/#acknowledgements> accessed 4 December 2020

Farivar C, 'Man shoots down neighbour's hexacopter in rural drone shotgun battle' (Ars Technica 2015) <http://arstechnica.com/tech-policy/2015/06/man-shoots-downs-neighbors-hexacopter-in-rural-drone-shotgun-battle/>

Frederiksen H. Marianne and others, 'Drones for Inspection of Infrastructure: Barriers, Opportunities and Successful Uses' (SDU Centre for Integrative Innovation Management 2019) < https://uasdenmark.dk/wp-content/uploads/2019/06/Final_Infrastructure-Memo_30.05.2019.pdf>

Garrett B, 'London's future...public space' (Museumoflondon.org.uk 2017) <www.museumoflondon.org.uk/discover/londons-future-space> accessed 4 November 2017

Kretchmer Harry, ‘How Drones are Helping to Battle Covid-19 in Africa and Beyond’ (Weforum.org 2020) < https://www.weforum.org/agenda/2020/05/medical-delivery-drones-coronavirus-africa-us/> accessed 15 August 2020

Kurzweil R, ‘The Law of Accelerating Returns’ (Kurzweilai.net 2001) <www.kurzweilai.net/the-law-of-accelerating-returns>

Leiner M. Barry and others, ‘Brief History of the Internet’ (Internet Society 1997) < https://www.internetsociety.org/wp-content/uploads/2017/09/ISOC-History-of-the-Internet_1997.pdf> accessed 12 August 2020.

Lewis C and Short C, ‘A Latin Dictionary, prīvus’ (Perseus.tufts.edu) <www.perseus.tufts.edu/hopper/text?doc=Perseus:text:1999.04.0059:entry=privus> accessed 12 May 2017

Meaker Morgan, ‘Deepfake porn bot targets thousands of women on Telegram’ (The Telegraph 2020) <https://www.telegraph.co.uk/technology/2020/10/21/deep-fake-porn-bot-targets-thousands-women-telegram/> accessed 15 November 2020

Momont A, ‘Ambulance Drone’ (TU Delft) <www.tudelft.nl/en/ide/research/research-labs/applied-labs/ambulance-drone/>

Pierce David, ‘The Wired Guide to Drones’ (Wired.com 2018) <https://www.wired.com/story/guide-drones/> accessed 4 August 2020.

Pierce David, ‘Delivery Drones are Coming’ (Theverge.com 2013) <https://www.theverge.com/2013/12/1/5164340/delivery-drones-are-coming-jeff-bezos-previews-half-hour-shipping> accessed 4 August 2020.

Stastna K, ‘Do countries lose religion as they gain wealth?’ (CBC News 2013) <www.cbc.ca/news/world/do-countries-lose-religion-as-they-gain-wealth-1.1310451> accessed 8 November 2017

Syam Piyali, ‘What is the difference between common law and civil law?’ <https://onlinelaw.wustl.edu/blog/common-law-vs-civil-law/> accessed 11 September 2020

Scott Mark, ‘Report: Social media networks fail to root out fake accounts’ (POLITICO 2019) < https://www.politico.com/news/2019/12/06/social-media-networks-fake-accounts-report-076939> accessed 4 December 2020

Waharte Sonia and Trigoni Niki, ‘Supporting Search and Rescue Operations with UAVs’ (University of Oxford Computing Laboratory 2010) < https://www.researchgate.net/publication/228954615_Supporting_Search_and_Rescue_Operations_with_UAVs> accessed 15 August 2020.

Wakefield J, ‘Drone detects heartbeat and breathing’ (BBC News 2017) <http://www.bbc.com/news/technology-41427529> accessed 7 January 2018

Wang Y and Kosinski M, ‘Deep neural networks are more accurate than humans at detecting sexual orientation from facial images’

(Open Science Framework 2017) <https://osf.io/zn79k/> accessed 9 November 2017

'Ancient Roman bathing' (En.wikipedia.org) <https://en.wikipedia.org/wiki/Ancient_Roman_bathing> accessed 9 November 2017

'AP constateert geen misstanden met camera's in onderzochte sauna's' (The Dutch Data Protection Authority 2019), <https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-constateert-geen-misstanden-met-cameras-onderzochte-saunas> assessed 26 November 2019.

'Cuius est solum, eius est usque ad coelum et ad inferos' (En.wikipedia.org) <https://en.wikipedia.org/wiki/Cuius_est_solum,_eius_est_usque_ad_coelum_et_ad_inferos> accessed 28 August 2017

'Culture | Definition of Culture in English by Oxford Dictionaries' (Oxford Dictionaries | English) <https://en.oxforddictionaries.com/definition/culture> accessed 4 May 2017

'Crop Dusting Drones – Making Work Safer and Easier for Farmers' <https://www.dw.com/en/crop-dusting-drones-making-work-safer-and-easier-for-farmers/a-50128698> accessed 15 August 2020

'Do old Women have to Wear Hijab?' (Shariahprogram.ca) <www.shariahprogram.ca/islam-qa-women/old-women-hijab.shtml> accessed 11 May 2017

‘DJI Broadcasts First Drone Video Over Facebook Live’ <https://www.dji.com/newsroom/news/dji-broadcasts-first-drone-video-over-facebook-live> accessed 1 September 2020

‘Ephesus Latrines (Public Toilets)’ (Ephesus.ws) <http://www.ephesus.ws/ephesus-latrines-public-toilets.html>

‘First Legal Recognition of Privacy: Mishnah, the code of Jewish law’ (Guarding Data 2014) <https://guardingdata.wordpress.com/2014/01/10/first-legal-recognition-of-privacy/> accessed 11 May 2017

‘First-person view (radio control)’ (En.wikipedia.org) <https://en.wikipedia.org/wiki/First-person_view_(radio_control)> accessed 11 November 2017

‘Global Internet Report 2016 – Internet Society’ (Internetsociety.org 2016) <www.internetsociety.org/globalinternetreport/2016/#first-d> accessed 19 November 2017

‘Google photos abandons unlimited uploads amid storage changes’ (BBC November 2020) <https://www.bbc.com/news/technology-54919165> accessed 15 November 2020

‘History of Unmanned Aerial Vehicles’ (En.wikipedia.org) <https://en.wikipedia.org/wiki/History_of_unmanned_aerial_vehicles> accessed 15 July 2017

‘Housing in Japan’ (En.wikipedia.org) <https://en.wikipedia.org/wiki/Housing_in_Japan> accessed 4 May 2017

‘Intel® Aero Ready to Fly Drone’ (Intel) <www.intel.com/content/www/us/en/products/drones/aero-ready-to-fly.html> accessed 11 January 2018

‘Intel® Falcon™ 8+ System’ (Intel) <www.intel.com/content/www/us/en/products/drones/falcon-8.html> accessed 11 January 2018

‘Internet of Things Defined - Tech Definitions by Gartner’ (Gartner IT Glossary) <www.gartner.com/it-glossary/internet-of-things/> accessed 26 November 2017

‘L’Entreprenant, Reconnaissance Aircraft, 1794' (Science Photo Library) <www.sciencephoto.com/media/775991/view> accessed 9 July 2017

‘Mars Helicopter’ (Nasa.gov 2020) <https://mars.nasa.gov/technology/helicopter/> accessed 4 August 2020.

‘Michel-Joseph and Montgolfier Jacques-Étienne | French Aviators' (Encyclopaedia Britannica) <https://www.britannica.com/biography/Montgolfier-brothers> accessed 15 July 2017.

‘Mishnah’ (Jewishvirtuallibrary.org) <www.jewishvirtuallibrary.org/mishnah> accessed 8 May 2017

‘Moorish Architecture’ (National Geographic Society 2012) <www.nationalgeographic.org/media/moorish-art/>

‘No pixels, please, we're German’ (The Economist 2010) <www.economist.com/node/17103679> accessed 14 October 2017

‘Part 1: The Duties of Women’ (Al-Islam.org) <www.al-islam.org/principles-marriage-family-ethics-ayatullah-ibrahim-amini/part-1-duties-women> accessed 4 May 2017

‘Radioplane OQ-2’ (En.wikipedia.org) <https://en.wikipedia.org/wiki/Radioplane_OQ-2> accessed 17 July 2017

‘Rashbam’ (En.wikipedia.org) <https://en.wikipedia.org/wiki/Rashbam> accessed 8 May 2017

‘Remote Piloted Aerial Vehicles: The Aerial Target and Aerial Torpedo in the USA’ (Ctie.monash.edu, 2003) <http://www.ctie.monash.edu/hargrave/rpav_usa.html> accessed 11 July 2017

‘Secret | Definition of secret in English by Oxford Dictionaries’ (Oxford Dictionaries | English) <https://en.oxforddictionaries.com/definition/secret> accessed 21 May 2017

'SESAR Joint Undertaking | History' (Sesarju.eu) <http://www.sesarju.eu/discover-sesar/history> accessed 3 August 2017.

‘Snapchat Object Recognition Based Photo Filters Patent Application’ (Scribd) <www.scribd.com/document/318282319/Snapchat-Object-

Recognition-Based-Photo-Filters-Patent-Application#from_embed> accessed 23 June 2017

'Taking Flight: Civilian Drones' Technology Quarterly (The Economist 2017) < https://shop.economist.com/products/technology-quarterly-civilian-drones> accessed 25 August 2020.

'Talmud' (Halakhah.com) <https://halakhah.com/pdf/nezikin/Baba_Bathra.pdf> accessed 31 October 2017

'The Benefits of Electronic Fuel Injection (EFI) - Power4flight' (Power4Flight) <https://power4flight.com/benefits-of-efi/>

'The Emergence of Commercial Drones' (IFLY Infographics) <www.purefunds.com/learn-about-purefunds-etfs/infographics/ifly/> accessed 10 July 2017

'The Quranic Arabic Corpus – Translation' (Corpus.quran.com) <http://corpus.quran.com/translation.jsp?chapter=24&verse=60> accessed 11 May 2017

'The Yellow Star' (Bl.uk) <www.bl.uk/learning/histcitizen/voices/info/yellowstar/theyellowstar.html> accessed 9 November 2017

'Tractate Bava Batra: Chapter 4' (Jewishvirtuallibrary.org) <www.jewishvirtuallibrary.org/tractate-bava-batra-chapter-4> accessed 29 August 2017

‘Use of Drones in Agriculture’ <https://wingtra.com/drone-mapping-applications/use-of-drones-in-agriculture/> accessed 15 August 2020

‘US20150242679A1 - Techniques for Emotion Detection and Content Delivery - Google Patents’ (Google.com) <http://www.google.com/patents/US20150242679> accessed 23 June 2017

‘6. Paradise Lost (Genesis 3:1-7)’ (Bible.org) <https://bible.org/seriespage/6-paradise-lost-genesis-31-7> accessed 8 May 2017

‘7 key considerations before your UAS operation takes to the sky’ (Virtual Air Boss) <www.virtualairboss.com/7-key-considerations-before-taking-your-drone-operation-to-the-sky-data-management/> accessed 5 January 2018