Faculty: Law
Study area: Law, notaryship and criminology
Program: Master in Intellectual Property Rights

"I see I see what you don't see – Civil use of drones in a surveillance context"

Master thesis submitted by
Jana BEYENS
Student number: r0262400

To obtain the degree of
Master in Intellectual Property Rights

Word count: 15 575
Promoter: Els KINDT

Academic year **2015 - 2016**

"I confirm that this paper is my own work, is not copied from any other person's work (published or unpublished), and is in conformity with the anti-plagiarism rules explained at http://www.kuleuven.be/plagiarism/"

Jana Beyens

Abstract

Surveillance is everywhere in modern day life, even though you may not always be aware of it. Cameras are installed in shops, at your workplace and even during a marathon cameras might be watching you. Fixed surveillance cameras have become normal in our lives, however also mobile cameras are being increasingly deployed. Mobile surveillance cameras have mainly been used by law enforcement bodies in their mission to reduce crime and the law has been particularly focused thereon. However, with the emergence of new advanced technologies, more and more surveillance material becomes affordable and therefor also available to the general public, meaning that established regulation may need to be revised in order to address these modern day issues. This master thesis therefor concerns the regulation on the use of camera-equipped UAVs by civilians for surveillance purposes and whether the current regulation in force is adequate to address privacy and data protection concerns related thereto. Fully developed specific legislation on UAVs seems to be non-existent, and therefor surveillance legislation regarding CCTV has to be taken into consideration. This means that the same principles need to be respected, such as the respect for the reasonable expectation of privacy of individuals, the obligation to put up a sign warning individuals that they may be filmed and the registration of the surveillance drone at a competent authority. However, UAVs are not in every way the same as CCTV cameras and therefor also other safeguards have to be put into place. This may be achieved by using technology to its advantage by designing drones with artificial intelligence or geofencing features, and by providing data subjects their privacy right by building it into the system by default.

Acknowledgements

I would hereby like to thank everyone that has either directly or indirectly helped to realize this master thesis. I would like to thank my promoter, prof. ELS KINDT, for giving me the opportunity to write about this interesting topic. Furthermore, I would like to thank my supervisor, NIELS VANDEZANDE, for guiding me through this web of regulations and for steering me in the right direction. I would also like to thank my family, partner and friends for withstanding all the moments of stress. And especially I would like to thank my parents, for giving me the opportunity to have an extra year of education, something I will never take for granted. And finally, I would like to thank my brother, NICK BEYENS, my girlfriend, KATRIEN SMETS and my friend, INE SWOLFS, for reading some of the versions of my master thesis and correcting my mistakes.

Content

List of abbreviations

- OECD Organisation for Economic Co-operation and Development
- UDHR Universal Declaration of Human Rights
- ICCP International Covenant on Civil and Political Rights
- ECHR European Convention of Human Rights
- EEA European Economic Area
- DPA Data Protection Authority
- CJEU Court of Justice of the European Union
- EDPS European Data Protection Supervisor
- GDPR General Data Protection Regulation
- DPWP Data Protection Working Party
- UAVs Unmanned Aerial Vehicles
- CCTV Closed-Circuit Television
- RPAS Remotely Piloted Aircraft System
- MAV Micro Air Vehicle
- AAR Autonomous Aerial Robotics
- SUAS Small Unmanned Aircraft System
- ICAO International Civil Aviation Organisation
- CAA Civil Aviation Authority
- FAA Federal Aviation Administration
- DAPTA Drone Aircraft Privacy and Transparency Act
- PETs Privacy-Enhancing Technologies

Introduction

1. INTRODUCTION – Surveillance has become a rather normal part of our day-to-day life. There are surveillance cameras in shops, in the subway but also during manifestations, we are being surveilled by helicopters. Also more and more civilians install surveillance cameras on their private property to prevent burglary. However, the use of mobile surveillance cameras by private parties is less known, though not impossible to imagine since new technologies are becoming affordable. This master thesis will generally discuss the influence of drones on existing privacy and data protection rights and furthermore go into detail whether civilians should be given the possibility to use mobile cameras, more in particular drones, for surveillance purposes, even though this might pose privacy and data protection infringements. To be able to come to a conclusion, all relevant legislation, case law and legal doctrine on privacy, data protection and the use of drones will be taken into account. Drones are a relatively new concept and problem in society, since civil use of it has only come up recently. Therefor, it might be necessary to take already established concepts, like the fact that civilians cannot use mobile cameras for surveillance purposes, into question. New technologies come with new questions, but also old established facts may sometimes need to be revised. At first, this master thesis will briefly mention the relevant general legislation and case law on the right to privacy and data protection that exists upon international level, EU level and in the United States. Afterwards, that legislation will be applied to drones specifically and concrete legislation and case law on drones and surveillance material upon international level, in the EU, and more specifically in Belgium and the UK, and in the US will be discussed. Then, it will be discussed whether it would be possible to allow civilians to use new technology materials such as drones for surveillance purposes, and if so, under which conditions.

CHAPTER 1. What is privacy?

2. DEFINITION – The first questions that need to be asked are: What is privacy? And what falls under the concept of privacy? A general consensus exists on the fact that 'privacy' cannot be exactly defined and no one can articulate what it means, though in general it is accepted that it is the right to be let alone.[1] However, authors agree that privacy is a much more complex concept than that, and that it comprises multiple dimensions of related concepts, such as privacy of the person, privacy of personal communication, but also privacy of personal data.[2] Protection of personal data is thus a spin-off of the right to privacy, though it are two separate concepts each with their own legislation, which will be discussed in the following paragraphs.[3] Personal data then includes every kind of information about an identified or identifiable individual touching his private and family life.[4]

---

[1] R. CLARKE, "The regulation of civilian drones' impacts on behavioural privacy", *Computer Law & Security Review* 2014, 287; B.H.M. CUSTERS, J.J. OERLEMANS en S.J. VERGOUW, *Het gebruik van drones: een verkennend onderzoek naar onbemande luchtvaartuigen*, Meppel, Boom Lemma Uitgevers, 2015, 103; P. DE HERT, *Handboek privacy: persoonsgegevens in België*, Brussel, Politeia, 2003, 14; R.L. FINN and D. WRIGHT, "Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications", *Computer Law & Security Review* 2012, 185; R.L. FINN, D. WRIGHT and M. FRIEDEWALD, "Seven types of privacy", in S. GUTWIRTH, R. LEENES, P. DE HERT and Y. POULLET, *European data protection: coming of age*, Dordrecht, Springer, 2013, 3; B.J. GOOLD, "Surveillance and the political value of privacy", *Amsterdam Law Forum* 2009, 1; D. KLITOU, *Privacy-invading technologies and privacy by design*, The Hague, Asser Press, 2014, 14; D.J. SOLOVE, *Understanding privacy*, Cambridge, Harvard University Press, 2008, 12; U. VOLOVELSKY, "Civilian uses of unmanned aerial vehicles and the threat to the right to privacy – An Israeli case study", *Computer Law & Security Review* 2014, 306; X., *Common law right to privacy*, privacy.uslegal.com.

[2] R.L. FINN and D. WRIGHT, "Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications", *Computer Law & Security Review* 2012, 185; R.L. FINN, D. WRIGHT and M. FRIEDEWALD, "Seven types of privacy", in S. GUTWIRTH, R. LEENES, P. DE HERT and Y. POULLET, *European data protection: coming of age*, Dordrecht, Springer, 2013, 5-6; B.J. GOOLD, "Surveillance and the political value of privacy", *Amsterdam Law Forum* 2009, 1; U. VOLOVELSKY, "Civilian uses of unmanned aerial vehicles and the threat to the right to privacy – An Israeli case study", *Computer Law & Security Review* 2014, 312-313.

[3] P. DE HERT and V. PAPAKONSTANTINOU, "The Council of Europe data protection convention reform: analysis of the new text and critical comment on its global ambition", *Computer Law & Security Review* 2014, 635; G. GONZALEZ FUSTER, *The emergence of personal data protection as a fundamental right of the EU*, Dordrecht, Springer, 2014, 271; V. KOSTA, *Fundamental rights in EU internal market legislation*, Oxford, Hart Publishing, 2015, 93.

[4] CJEU 6 November 2003, C-101/01, Lindqvist; G. GONZALEZ FUSTER, *The emergence of personal data protection as a fundamental right of the EU*, Dordrecht, Springer, 2014, 34; E.J. KINDT, *Privacy and data protection issues of biometric applications: a comparative legal analysis*, Dordrecht, Springer, 2013, 93-94; V. KOSTA, *Fundamental rights in EU internal market legislation*, Oxford, Hart Publishing, 2015, 92.

§1 Historical background

3. HISTORICAL BACKGROUND – After World War II, various legal instruments regarding the right to privacy started to emerge. At first at the international level with the United Nations implementing the Universal Declaration of Human Rights and afterwards article 17 of the International Covenant on Civil and Political Rights.[5] On the European level, legislation also started to emerge due to initiatives of the Council of Europe, namely article 8 of the European Convention on Human Rights and later on also case law regarding that article.[6] It is hard for national legislation to escape the obligation of guaranteeing the right to privacy since it is coded both on international and European level.[7] Due to emerging new digital technologies in the 1970's, the right to privacy seemed inadequate to protect new issues and effects that followed out of these technologies, so national governments felt the need to also protect the data collected by them. On the international level, the Organisation for Economic Co-operation and Development (hereafter: OECD) guidelines were the first to address the issue of data protection in 1980, which were also adopted by the USA.[8]

---

[5] Article 12 Universal Declaration of Human Rights, *UNTS* 10 December 1948, 217 A (III) (hereafter: UDHR): *"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."*; Article 17 International Covenant on Civil and Political Rights, *UNTS* 16 December 1966, No. 14668 (hereafter: ICCPR): *"1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks.";* D. BAANISAR and S. DAVIES, "Privacy and human rights: an international survey of privacy laws and practice", gilc.org; P. BOILLAT and M. KJAERUM, *Handbook on European data protection law*, http://www.echr.coe.int, 2014, 14; A.F. JACOBSEN, *Human rights monitoring: A field mission manual*, Leiden, Martinus Nijhoff Publishers, 2008, 405; A. RENGEL, *Privacy in the 21st century*, Leiden, Martinus Nijhoff Publishers, 2013, 10; J. TERSTEGGE, "Privacy in the law", in M. PETKOVIĆ and W. JONKER, *Security, privacy, and trust in modern data management*, Berlin, Springer, 2007, 11.

[6] European Convention on Human Rights, *ETS* 4 November 1950, 5 (hereafter: ECHR); A. ALEMANNO and A.L. SIBONY, *Nudge and the law: a European perspective*, Oxford, Hart Publishing, 2015, 182; A.F. JACOBSEN, *Human rights monitoring: A field mission manual*, Leiden, Martinus Nijhoff Publishers, 2008, 405; U. KILKELLY, "The right to respect for private and family life: A guide to the implementation of Article 8 of the European Convention on Human Rights", http://www.coe.int, 2001, 8; J. WALDO, H.S. LIN and L.I MILLETT, *Engaging privacy and information technology in a digital age*, Washington, The National Academies Press, 2007, 382.

[7] A.F. JACOBSEN, *Human rights monitoring: A field mission manual*, Leiden, Martinus Nijhoff Publishers, 2008, 406; J. TERSTEGGE, "Privacy in the law", in M. PETKOVIĆ and W. JONKER, *Security, privacy, and trust in modern data management*, Berlin, Springer, 2007, 11; J. WALDO, H.S. LIN and L.I MILLETT, *Engaging privacy and information technology in a digital age*, Washington, The National Academies Press, 2007, 382.

[8] A. ALEMANNO and A.L. SIBONY, *Nudge and the law: a European perspective*, Oxford, Hart Publishing, 2015, 31; A.F. JACOBSEN, *Human rights monitoring: A field mission manual*, Leiden, Martinus Nijhoff Publishers, 2008, 429; J. WALDO, H.S. LIN and L.I MILLETT, *Engaging privacy and information technology in a digital age*, Washington, The National Academies Press, 2007, 384.

Also on the European level, Convention no. 108 of the Council of Europe implemented the protection of individuals against abuses following out of the collection and processing of personal data.[9] Afterwards, the European Union felt the need to regulate data protection by a Data Protection Directive, soon being replaced by the General Data Protection Regulation, and implemented those provisions into the Charter of Fundamental Rights of the European Union as well.[10] An important role was given to the Article 29 Data Protection Working Party for the interpretation of many concepts and the formulation of opinions on data protection within the EU.[11]

§2 Legislation on privacy and data protection

4. PRIVACY AND DATA PROTECTION – In the following paragraphs, all the relevant general legislation and case law on privacy and data protection on international, European and US level will be discussed.

A. International legislation

1. Privacy

1.1 Universal Declaration of Human Rights

5. ARTICLE 12 UDHR – *Supra* 3, footnote 5.

[9] Convention for the protection of individuals with regard to automatic processing of personal data, *ETS* 28 January 1981, 108 (hereafter: Convention no. 108); A.F. JACOBSEN, *Human rights monitoring: A field mission manual*, Leiden, Martinus Nijhoff Publishers, 2008, 406; J. WALDO, H.S. LIN and L.I MILLETT, *Engaging privacy and information technology in a digital age*, Washington, The National Academies Press, 2007, 383.

[10] 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, *OJEC* 23 November 1995, 281/31 (hereafter: Data Protection Directive 95/46/EC); Charter of Fundamental Rights of the European Union, *OJEC* 18 December 2000, 364/1 (hereafter: EU Charter of Fundamental Rights); A. ALEMANNO and A.L. SIBONY, *Nudge and the law: a European perspective*, Oxford, Hart Publishing, 2015, 182-183; P. BOILLAT and M. KJAERUM, *Handbook on European data protection law*, http://www.echr.coe.int, 2014, 14; A.F. JACOBSEN, *Human rights monitoring: A field mission manual*, Leiden, Martinus Nijhoff Publishers, 2008, 406; J. WALDO, H.S. LIN and L.I MILLETT, *Engaging privacy and information technology in a digital age*, Washington, The National Academies Press, 2007, 383.

[11] A. ALEMANNO and A.L. SIBONY, *Nudge and the law: a European perspective*, Oxford, Hart Publishing, 2015, 183; C. FRITSCH, "Data processing in employment relations; impacts of the European general data protection regulation focusing on the data protection officer at the worksite", in S. GUTWIRTH, R. LEENES and P. DE HERT, *Reforming European data protection law: Issues in privacy and data protection*, Dordrecht, Springer, 2015, 155; D. KLITOU, *Privacy-invading technologies and privacy by design*, The Hague, Asser Press, 2014, 29.

1.2 International Covenant on Civil and Political Rights

6. ARTICLE 17 ICCPR – *Supra* 3, footnote 5.

2. Data protection

2.1 OECD Guidelines

7. OECD GUIDELINES – As already mentioned, the specific right to data protection was first established by national initiatives.[12] In 1970, the German state of Hesse implemented the worldwide first 'modern' data protection legislation.[13] Afterwards also Sweden and France followed.[14] However, these national initiatives on data protection started to raise concerns, because disparities in national legislations could hamper the free cross-border exchange of personal information.[15] So in 1980, an international initiative from the OECD saw the light under the form of non-binding guidelines.[16]

---

[12] *Supra* 3, nr. 3; P. BOILLAT and M. KJAERUM, *Handbook on European data protection law*, http://www.echr.coe.int, 2014, 17; G. GONZALEZ FUSTER, *The emergence of personal data protection as a fundamental right of the EU*, Dordrecht, Springer, 2014, 55.

[13] G. GONZALEZ FUSTER, *The emergence of personal data protection as a fundamental right of the EU*, Dordrecht, Springer, 2014, 56; A. KISS and G.L. SZOKE, "Evolution of revolution? Steps forward to a new generation of data protection regulation", in S. GUTWIRTH, R. LEENES and P. DE HERT, *Reforming European data protection law: Issues in privacy and data protection*, Dordrecht, Springer, 2015, 313; E. PALMER, "Online Privacy Law: Germany", https://www.loc.gov 2012.

[14] N. ATWILL, "Online Privacy Law: France", https://www.loc.gov 2012; G. GONZALEZ FUSTER, *The emergence of personal data protection as a fundamental right of the EU*, Dordrecht, Springer, 2014, 61; A. KISS and G.L. SZOKE, "Evolution of revolution? Steps forward to a new generation of data protection regulation", in S. GUTWIRTH, R. LEENES and P. DE HERT, *Reforming European data protection law: Issues in privacy and data protection*, Dordrecht, Springer, 2015, 313; X., *The personal data act*, http://www.datainspektionen.se.

[15] G. GONZALEZ FUSTER, *The emergence of personal data protection as a fundamental right of the EU*, Dordrecht, Springer, 2014, 79; A. KISS and G.L. SZOKE, "Evolution of revolution? Steps forward to a new generation of data protection regulation", in S. GUTWIRTH, R. LEENES and P. DE HERT, *Reforming European data protection law: Issues in privacy and data protection*, Dordrecht, Springer, 2015, 314; X., *OECD Guidelines on the protection of privacy and transborder flows of personal data*, http://www.oecd.org.

[16] P. DE HERT and V. PAPAKONSTANTINOU, "The Council of Europe data protection convention reform: analysis of the new text and critical comment on its global ambition", *Computer Law & Security Review* 2014, 635; G. GONZALEZ FUSTER, *The emergence of personal data protection as a fundamental right of the EU*, Dordrecht, Springer, 2014, 76; G. GREENLEAF, "The influence of European data privacy standards outside Europe: Implications for globalisation of Convention 108?", *International Data Privacy Law* 2012, 1; E.J. KINDT, *Privacy and data protection issues of biometric applications: a comparative legal analysis*, Dordrecht, Springer, 2013, 90; N. WITZLEB, D. LINDSAY, M. PATERSON and S. RODRICK, *Emerging challenges in privacy law: comparative perspectives*, Cambridge, Cambridge University Press, 2014, 12; X., *Data protection legislation*, https://secure.edps.europa.eu.

The main idea behind these guidelines governing the protection of privacy and transborder flows of personal data was to stipulate how to freely exchange information without too many rules and concerns for privacy in the light of a changing environment caused by new technologies.[17]

B. European legislation

1. Privacy

1.1 European Convention on Human Rights

8. ARTICLE 8 – Article 8 ECHR introduces an individual right to privacy and entails two types of obligations, a positive one and a negative one.[18] The positive obligation requires the adoption of measures by the states to protect the individual's right entailed in article 8 ECHR, especially against interference by others.[19] The negative obligation requires the states to assure an exercise of the right of privacy by every individual free of any interference, unless a justification under article 8, paragraph 2 is applicable.[20]

---

[17] G. GONZALEZ FUSTER, *The emergence of personal data protection as a fundamental right of the EU*, Dordrecht, Springer, 2014, 80; E.J. KINDT, *Privacy and data protection issues of biometric applications: a comparative legal analysis*, Dordrecht, Springer, 2013, 90; J. TERSTEGGE, "Privacy in the law", in M. PETKOVIĆ and W. JONKER, *Security, privacy, and trust in modern data management*, Berlin, Springer, 2007, 13.

[18] Art. 8 ECHR: *"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."*; Communication from the Commission to the European Parliament and the Council, "A new era for aviation: opening the aviation market to the civil use of remotely piloted aircraft systems in a safe and sustainable manner", COM(2014) 207, 7; F. BOEHM, *Information sharing and data protection in the area of freedom, security and justice*, Heidelberg, Springer, 2012, 26; P. DE HERT and S. GUTWIRTH, "Privacy, data protection and law enforcement: opacity of the individual and transparency of the power", in E. CLAES, A. DUFF and S. GUTWIRTH, *Privacy and the criminal law*, Antwerpen, Intersentia, 2006, 71-72; A.F. JACOBSEN, *Human rights monitoring: A field mission manual*, Leiden, Martinus Nijhoff Publishers, 2008, 419.

[19] F. BOEHM, *Information sharing and data protection in the area of freedom, security and justice*, Heidelberg, Springer, 2012, 26; B.H.M. CUSTERS, J.J. OERLEMANS en S.J. VERGOUW, *Het gebruik van drones: een verkennend onderzoek naar onbemande luchtvaartuigen*, Meppel, Boom Lemma Uitgevers, 2015, 107.

[20] F. BOEHM, *Information sharing and data protection in the area of freedom, security and justice*, Heidelberg, Springer, 2012, 26; B.H.M. CUSTERS, J.J. OERLEMANS en S.J. VERGOUW, *Het gebruik van drones: een verkennend onderzoek naar onbemande luchtvaartuigen*, Meppel, Boom Lemma Uitgevers, 2015, 107.

9. JUSTIFICATION - If there has been an interference with article 8 ECHR, a possible justification is provided for in paragraph 2 of that article, namely when the interference was in accordance with the law, when it pursued one of the legitimate aims listed in that paragraph and when it was necessary to do so in a democratic society or it was proportionate to the pursuit of that aim.[21]

10. LEGALITY REQUIREMENT – The first requirement is that the measure that constitutes the interference with article 8 ECHR must be in accordance with the law, both statute and unwritten law.[22] This means that the concerning interference must have a legal basis which is sufficiently precise and contains a measure of protection against arbitrariness by public authorities. Important in this regard is that the law must be foreseeable, *i.e.* that it must be accessible to the persons concerned and formulated with sufficient precision to enable them to reasonably foresee what consequences their actions may entail.[23]

[21] ECtHR 4 December 2008, nr. 30562/04 and 30566/04, S. and Marper/United Kingdom, §58; F. BOEHM, *Information sharing and data protection in the area of freedom, security and justice*, Heidelberg, Springer, 2012, 46; B.H.M. CUSTERS, J.J. OERLEMANS en S.J. VERGOUW, *Het gebruik van drones: een verkennend onderzoek naar onbemande luchtvaartuigen*, Meppel, Boom Lemma Uitgevers, 2015, 108; A.F. JACOBSEN, *Human rights monitoring: A field mission manual*, Leiden, Martinus Nijhoff Publishers, 2008, 417; U. KILKELLY, "The right to respect for private and family life: A guide to the implementation of Article 8 of the European Convention on Human Rights", http://www.coe.int, 2001, 25; V. KOSTA, *Fundamental rights in EU internal market legislation*, Oxford, Hart Publishing, 2015, 92.

[22] F. BOEHM, *Information sharing and data protection in the area of freedom, security and justice*, Heidelberg, Springer, 2012, 47; B.H.M. CUSTERS, J.J. OERLEMANS en S.J. VERGOUW, *Het gebruik van drones: een verkennend onderzoek naar onbemande luchtvaartuigen*, Meppel, Boom Lemma Uitgevers, 2015, 109.

[23] F. BOEHM, *Information sharing and data protection in the area of freedom, security and justice*, Heidelberg, Springer, 2012, 47; B.H.M. CUSTERS, J.J. OERLEMANS en S.J. VERGOUW, *Het gebruik van drones: een verkennend onderzoek naar onbemande luchtvaartuigen*, Meppel, Boom Lemma Uitgevers, 2015, 109; U. KILKELLY, "The right to respect for private and family life: A guide to the implementation of Article 8 of the European Convention on Human Rights", http://www.coe.int, 2001, 26.

11. LEGITIMACY REQUIREMENT – When the interference is found to be in accordance with law, the Court will proceed to the second requirement, *i.e.* whether the interference pursues one of the legitimate aims listed in paragraph 2 of article 8 ECHR, *i.e.* the interest of national security, public safety and the economic well-being of the country, as well as the prevention of disorder or crime, the protection of health, morals or the rights and freedoms of others.[24] Though, a wide margin of appreciation is given to the Member States and in most cases the Court will rarely reject the legitimate aim identified and will accept that the State was acting for a proper purpose, even if it is disputed by the applicant.[25]

12. NECESSARY IN DEMOCRATIC SOCIETY – The final requirement of paragraph 2 of article 8 ECHR is to determine whether the interference was necessary in a democratic society. This key principle means that a pressing social need was present for the interference, and that the measure was relevant, sufficient and efficient.[26] The principle of proportionality plays an important role in this regard to determine whether a balance was achieved between the rights of the individual and the public interest, and that the infringement on the privacy of the individual was not disproportionate to the aim being pursued.[27] Potential benefits for the public interest are hereby being balanced against intrusion and important private-life interests.

---

[24] F. BOEHM, *Information sharing and data protection in the area of freedom, security and justice*, Heidelberg, Springer, 2012, 56; U. KILKELLY, "The right to respect for private and family life: A guide to the implementation of Article 8 of the European Convention on Human Rights", http://www.coe.int, 2001, 30.

[25] ECtHR 4 December 2008, nr. 30562/04 and 30566/04, S. and Marper/United Kingdom, §102; F. BOEHM, *Information sharing and data protection in the area of freedom, security and justice*, Heidelberg, Springer, 2012, 56; B.H.M. CUSTERS, J.J. OERLEMANS en S.J. VERGOUW, *Het gebruik van drones: een verkennend onderzoek naar onbemande luchtvaartuigen*, Meppel, Boom Lemma Uitgevers, 2015, 108; U. KILKELLY, "The right to respect for private and family life: A guide to the implementation of Article 8 of the European Convention on Human Rights", http://www.coe.int, 2001, 30.

[26] F. BOEHM, *Information sharing and data protection in the area of freedom, security and justice*, Heidelberg, Springer, 2012, 57; B.H.M. CUSTERS, J.J. OERLEMANS en S.J. VERGOUW, *Het gebruik van drones: een verkennend onderzoek naar onbemande luchtvaartuigen*, Meppel, Boom Lemma Uitgevers, 2015, 109.

[27] F. BOEHM, *Information sharing and data protection in the area of freedom, security and justice*, Heidelberg, Springer, 2012, 57-58; R. CLARKE, "The regulation of civilian drones' impacts on behavioural privacy", *Computer Law & Security Review* 2014, 287; B.H.M. CUSTERS, J.J. OERLEMANS en S.J. VERGOUW, *Het gebruik van drones: een verkennend onderzoek naar onbemande luchtvaartuigen*, Meppel, Boom Lemma Uitgevers, 2015, 109; U. KILKELLY, "The right to respect for

1.2 Case Law

13. CASE LAW – When a right of the ECHR is infringed upon and all national remedies are exhausted, individuals will have a remedy at the European Court of Human Rights.[28] On the subject of an individual's privacy, the Court has come to the conclusion that a reasonable expectation of private life must always be protected, even when the collection of personal data is carried out in public places.[29] According to the judgment of the European Court of Human Rights in *Von Hannover vs Germany*, a zone of interaction of a person with others exists, even in a public context, which may fall within the scope of the private life.[30] With regard to data protection purposes, the Court has derived a right to data protection from the right to privacy under article 8 ECHR, releasing significant case law that furthered individual data protection.[31] However, the biggest disadvantage is that the Court cannot deal with complaints against individuals or private institutions, but merely against state infringement.[32]

---

private and family life: A guide to the implementation of Article 8 of the European Convention on Human Rights", http://www.coe.int, 2001, 31; V. KOSTA, *Fundamental rights in EU internal market legislation*, Oxford, Hart Publishing, 2015, 92-93.

[28] Article 35 ECHR; P. DE HERT and V. PAPAKONSTANTINOU, "The Council of Europe data protection convention reform: analysis of the new text and critical comment on its global ambition", *Computer Law & Security Review* 2014, 635; G. GREENLEAF, "The influence of European data privacy standards outside Europe: Implications for globalisation of Convention 108?", *International Data Privacy Law* 2012, 24; V. KOSTA, *Fundamental rights in EU internal market legislation*, Oxford, Hart Publishing, 2015, 93; M. KUIJER, "Effective remedies as a fundamental right", www.ejtn.eu 28 april 2014, 1.

[29] B.H.M. CUSTERS, J.J. OERLEMANS en S.J. VERGOUW, *Het gebruik van drones: een verkennend onderzoek naar onbemande luchtvaartuigen*, Meppel, Boom Lemma Uitgevers, 2015, 107-108.

[30] ECtHR 7 February 2012, nr. 40660/08 and 60641/08, Von Hannover/Germany, §95.

[31] P. DE HERT and V. PAPAKONSTANTINOU, "The Council of Europe data protection convention reform: analysis of the new text and critical comment on its global ambition", *Computer Law & Security Review* 2014, 635; V. KOSTA, *Fundamental rights in EU internal market legislation*, Oxford, Hart Publishing, 2015, 93.

[32] Article 34 ECHR; V. KOSTA, *Fundamental rights in EU internal market legislation*, Oxford, Hart Publishing, 2015, 94; X., *Article 34 ECHR – admissibility of individual applications*, echr-online.info; X., *Questions and answers*, www.echr.coe.int.

2. Data Protection

2.1 Convention no. 108

14. CONVENTION no. 108 – The Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data of the European Council, also known as Convention no. 108, was the first international legally binding instrument dealing explicitly with data protection and formed the basis for the Data Protection Directive 95/46/EC.[33] It adopted several resolutions on the protection of personal data, referring to the right to privacy in article 8 ECHR.[34] This convention applies to a group of 48 countries, which is larger than merely the EU countries.

15. CONTENT – Convention no. 108 regulates all data processing carried out by both the private and public sector, such as the judiciary and law enforcement bodies.[35] Its aim is to protect individuals against abuses that can be made with the collection and processing of personal data by demanding fair and lawful collection and automatic processing of data, to be stored for specified legitimate purposes and not to be used for ends incompatible with these purposes, nor to be kept for longer than is necessary.[36]

---

[33] P. BOILLAT and M. KJAERUM, *Handbook on European data protection law*, http://www.echr.coe.int, 2014, 14; P. DE HERT and V. PAPAKONSTANTINOU, "The Council of Europe data protection convention reform: analysis of the new text and critical comment on its global ambition", *Computer Law & Security Review* 2014, 634; G. GONZALEZ FUSTER, *The emergence of personal data protection as a fundamental right of the EU*, Dordrecht, Springer, 2014, 89; G. GREENLEAF, "The influence of European data privacy standards outside Europe: Implications for globalisation of Convention 108?", *International Data Privacy Law* 2012, 1; E.J. KINDT, *Privacy and data protection issues of biometric applications: a comparative legal analysis*, Dordrecht, Springer, 2013, 91; N. WITZLEB, D. LINDSAY, M. PATERSON and S. RODRICK, *Emerging challenges in privacy law: comparative perspectives*, Cambridge, Cambridge University Press, 2014, 12; X., *Data protection legislation*, https://secure.edps.europa.eu.

[34] P. BOILLAT and M. KJAERUM, *Handbook on European data protection law*, http://www.echr.coe.int, 2014, 15; G. GONZALEZ FUSTER, *The emergence of personal data protection as a fundamental right of the EU*, Dordrecht, Springer, 2014, 84.

[35] Article 3(1) Convention no. 108; P. BOILLAT and M. KJAERUM, *Handbook on European data protection law*, http://www.echr.coe.int, 2014, 16; G. GONZALEZ FUSTER, *The emergence of personal data protection as a fundamental right of the EU*, Dordrecht, Springer, 2014, 90.

[36] P. BOILLAT and M. KJAERUM, *Handbook on European data protection law*, http://www.echr.coe.int, 2014, 16; G. GONZALEZ FUSTER, *The emergence of personal data protection as a fundamental right of the EU*, Dordrecht, Springer, 2014, 88; G. GREENLEAF, "The influence of European data privacy standards outside Europe: Implications for globalisation of Convention 108?", *International Data Privacy Law* 2012, 22; E.J. KINDT, *Privacy and data protection issues of biometric applications: a comparative legal analysis*, Dordrecht, Springer, 2013, 91; X., *Data protection legislation*, https://secure.edps.europa.eu.

The convention also regulates the quality of the data, *i.e.* that it must be adequate, relevant, accurate and not excessive, and concerning sensitive data, such as for example a person's race or sexual life, it must provide sufficient guarantees.[37] It also enshrines an individual's right to know that his personal information is being stored, and if necessary to have that information corrected. Restrictions on these rights are possible when overriding interests are at stake, such as state security. The convention also seeks to regulate the transborder flow of personal data and provides for a free flow between State Parties to the convention.[38] However, some restrictions may apply on these flows to states where national legislation does not provide equivalent protection.[39]

16. ENFORCEMENT – The adoption of the Convention no. 108 set a milestone in the development of the legislation throughout Europe on the processing of personal data.[40] Its ratification was supported by the European Commission and today, all EU Member States have ratified Convention no. 108.[41] However, the instrument is non self-executing, *i.e.* that the countries willing to ratify Convention no. 108 need to integrate it into their own legal systems in compliance with its content.[42]

---

[37] Article 5 Convention no. 108; G. GONZALEZ FUSTER, *The emergence of personal data protection as a fundamental right of the EU*, Dordrecht, Springer, 2014, 90; G. GREENLEAF, "The influence of European data privacy standards outside Europe: Implications for globalisation of Convention 108?", *International Data Privacy Law* 2012, 22.

[38] F. BOEHM, *Information sharing and data protection in the area of freedom, security and justice*, Heidelberg, Springer, 2012, 94; G. GONZALEZ FUSTER, *The emergence of personal data protection as a fundamental right of the EU*, Dordrecht, Springer, 2014, 89; N. WITZLEB, D. LINDSAY, M. PATERSON and S. RODRICK, *Emerging challenges in privacy law: comparative perspectives*, Cambridge, Cambridge University Press, 2014, 13.

[39] P. BOILLAT and M. KJAERUM, *Handbook on European data protection law*, http://www.echr.coe.int, 2014, 16; G. GREENLEAF, "The influence of European data privacy standards outside Europe: Implications for globalisation of Convention 108?", *International Data Privacy Law* 2012, 1; N. WITZLEB, D. LINDSAY, M. PATERSON and S. RODRICK, *Emerging challenges in privacy law: comparative perspectives*, Cambridge, Cambridge University Press, 2014, 12.

[40] F. BOEHM, *Information sharing and data protection in the area of freedom, security and justice*, Heidelberg, Springer, 2012, 92; G. GONZALEZ FUSTER, *The emergence of personal data protection as a fundamental right of the EU*, Dordrecht, Springer, 2014, 92; G. GREENLEAF, "The influence of European data privacy standards outside Europe: Implications for globalisation of Convention 108?", *International Data Privacy Law* 2012, 28.

[41] G. GONZALEZ FUSTER, *The emergence of personal data protection as a fundamental right of the EU*, Dordrecht, Springer, 2014, 93; G. GREENLEAF, "The influence of European data privacy standards outside Europe: Implications for globalisation of Convention 108?", *International Data Privacy Law* 2012, 22.

[42] F. BOEHM, *Information sharing and data protection in the area of freedom, security and justice*, Heidelberg, Springer, 2012, 92; G. GONZALEZ FUSTER, *The emergence of personal data protection as a fundamental right of the EU*, Dordrecht, Springer, 2014, 93; G. GREENLEAF, "The influence of European data privacy standards outside Europe: Implications for globalisation of Convention 108?", *International Data Privacy Law* 2012, 23.

The consequence is that the Member States arrived at rather different outcomes, in some cases even imposing restrictions on data flows to other Member States.[43] Convention no. 108 provides that a person must have a remedy of access or correction rights, but itself does not say anything about whether individuals must have a right of individual action to enforce rights, or access to the Courts.[44] No right is thus provided by the Convention of individual complaint against a State party to any Court or other body, so in other words, no effective method in the Convention is given by which individuals can test whether a member state's implementation of the principles are sufficient, or its enforcement methods are appropriate. This stands in contrast to the possibility of remedy at the European Court of Human Rights whenever a right of the ECHR is infringed upon.[45]

2.2 Data Protection Directive 95/46/EC

17. *LEX GENERALIS* - As mentioned before, the Data Protection Directive followed after the initiative of the Council of Europe and has used Convention no. 108 as a basis to try to achieve harmonisation of data protection laws in the EU.[46] However, this directive applies only to the Member States of the EU, *i.e.* 28 countries.[47]

---

[43] P. HUSTINX, "EU data protection law: the review of Directive 95/46/EC and the proposed general data protection regulation", https://secure.edps.europa.eu, 2013, 9; N. WITZLEB, D. LINDSAY, M. PATERSON and S. RODRICK, *Emerging challenges in privacy law: comparative perspectives*, Cambridge, Cambridge University Press, 2014, 14.

[44] Article 8 Convention no. 108; G. GREENLEAF, "The influence of European data privacy standards outside Europe: Implications for globalisation of Convention 108?", *International Data Privacy Law* 2012, 23-24.

[45] *Supra* 9, nr. 13; G. GREENLEAF, "The influence of European data privacy standards outside Europe: Implications for globalisation of Convention 108?", *International Data Privacy Law* 2012, 24; M. KUIJER, "Effective remedies as a fundamental right", www.ejtn.eu 28 april 2014, 1.

[46] *Supra* 3-4, nr. 3; P. BOILLAT and M. KJAERUM, *Handbook on European data protection law*, http://www.echr.coe.int, 2014, 17; G. GONZALEZ FUSTER, *The emergence of personal data protection as a fundamental right of the EU*, Dordrecht, Springer, 2014, 128; P. HUSTINX, "EU data protection law: the review of Directive 95/46/EC and the proposed general data protection regulation", https://secure.edps.europa.eu, 2013, 17; E.J. KINDT, *Privacy and data protection issues of biometric applications: a comparative legal analysis*, Dordrecht, Springer, 2013, 92; D. KLITOU, *Privacy-invading technologies and privacy by design*, The Hague, Asser Press, 2014, 28; V. KOSTA, *Fundamental rights in EU internal market legislation*, Oxford, Hart Publishing, 2015, 99; L. SCAIFE, *Handbook of social media and the law*, New York, Informa Law from Routledge, 2015, 243.

[47] P. BOILLAT and M. KJAERUM, *Handbook on European data protection law*, http://www.echr.coe.int, 2014, 18; V. KOSTA, *Fundamental rights in EU internal market legislation*, Oxford, Hart Publishing, 2015, 99; L. SCAIFE, *Handbook of social media and the law*, New York, Informa Law from Routledge, 2015, 243.

Due to fast developing technologies and the demand from both companies and governments to review the directive to better fit the needs of new technologies, the Data Protection Directive has been adapted into a Data Protection Regulation.[48] The Data Protection Directive is *lex generalis* that applies to the private and the public sector, although some exceptions are foreseen for governments in specific situations.[49] The Data Protection Directive gives an explanation to often used terms such as 'personal data', 'controller', etc. The Directive also describes detailed rights and obligations for the processing of personal data in the EU, as well as the need for an adequate level of protection when personal data is transferred to third countries.[50] One of the most important obligations is the information obligation towards the data subject and the supervising authority, *i.e.* the DPA.[51] There is also the need for a legal basis, so that lawful processing of the collected data can be guaranteed. This directive also gives rights of access and correction to the data subject.[52]

[48] *Infra* 17, nr. 22; P. DE HERT and V. PAPAKONSTANTINOU, "The Council of Europe data protection convention reform: analysis of the new text and critical comment on its global ambition", *Computer Law & Security Review* 2014, 633.

[49] Art. 13 Data Protection Directive 95/46/EC; L. COLONNA, "Europe versus Facebook: an imbroglio of EU data protection issues", in S. GUTWIRTH, R. LEENES and P. DE HERT, *Data protection on the move: Current developments in ICT and privacy/data protection*, Dordrecht, Springer, 2016, 45; G. GONZALEZ FUSTER, *The emergence of personal data protection as a fundamental right of the EU*, Dordrecht, Springer, 2014, 136; P. HUSTINX, "EU data protection law: the review of Directive 95/46/EC and the proposed general data protection regulation", https://secure.edps.europa.eu, 2013, 10; C. KUNER, *European data privacy law and online business*, New York, Oxford University Press, 2003, 17 and 19.

[50] B.H.M. CUSTERS, J.J. OERLEMANS en S.J. VERGOUW, *Het gebruik van drones: een verkennend onderzoek naar onbemande luchtvaartuigen*, Meppel, Boom Lemma Uitgevers, 2015, 104-105; G. GONZALEZ FUSTER, *The emergence of personal data protection as a fundamental right of the EU*, Dordrecht, Springer, 2014, 130; P. HUSTINX, "EU data protection law: the review of Directive 95/46/EC and the proposed general data protection regulation", https://secure.edps.europa.eu, 2013, 11; V. KOSTA, *Fundamental rights in EU internal market legislation*, Oxford, Hart Publishing, 2015, 99.

[51] P. DE HERT and V. PAPAKONSTANTINOU, "The Council of Europe data protection convention reform: analysis of the new text and critical comment on its global ambition", *Computer Law & Security Review* 2014, 639; G. GONZALEZ FUSTER, *The emergence of personal data protection as a fundamental right of the EU*, Dordrecht, Springer, 2014, 138; G. GREENLEAF, "The influence of European data privacy standards outside Europe: Implications for globalisation of Convention 108?", *International Data Privacy Law* 2012, 1; P. HUSTINX, "EU data protection law: the review of Directive 95/46/EC and the proposed general data protection regulation", https://secure.edps.europa.eu, 2013, 11; V. KOSTA, *Fundamental rights in EU internal market legislation*, Oxford, Hart Publishing, 2015, 101-102; C. KUNER, *European data privacy law and online business*, New York, Oxford University Press, 2003, 20.

[52] G. GONZALEZ FUSTER, *The emergence of personal data protection as a fundamental right of the EU*, Dordrecht, Springer, 2014, 138; C. KUNER, *European data privacy law and online business*, New York, Oxford University Press, 2003, 18-19.

18. IMPLEMENTATION – The Data Protection Directive needs to be implemented by national law in order to make it consistent with EU law.[53] However, this is often conceived as a problem since each member state has its own idea of what privacy means. For example, in France and Belgium privacy is linked to the right of freedom and liberty, whereas in other Member States, such as Germany, the right to human dignity is seen as the basis to the right of privacy.[54] Another problem is the lack of harmonisation given that the Directive is adopted with generally formulated concepts and open standards.[55] It thus still gave Member States a wide discretion on its transposition resulting in an interpretation based on different traditions and different concepts which led to different outcomes of similar cases in different EU Member States.[56] However, everything is becoming more and more global and many services are coming from outside the EU. Non-EU service providers are finding it complex to consider all 28 different legislations. In principle, the law of the place of the establishment is applicable, which makes it less problematic.[57] However, since the SCHREMS case, the CJEU has weakened this principle because of the data protection issues involved, making the national privacy law applicable from the EU Member State whenever a local establishment in that Member State is inextricably linked to the activities of the body responsible for the processing of the data.[58] By the end of 2018, when the General Data Protection Regulation needs to be fully in force in all the Member States, this issue will not be as important anymore.[59]

---

[53] V. KOSTA, *Fundamental rights in EU internal market legislation*, Oxford, Hart Publishing, 2015, 99; C. KUNER, *European data privacy law and online business*, New York, Oxford University Press, 2003, 28; X., *European Union Directives*, eur-lex.europa.eu.

[54] P. DE HERT and S. GUTWIRTH, "Data protection in the case law of Strasbourg and Luxembourg: constitutionalisation in action", in S. GUTWIRTH, Y. POULLET, P. DE HERT, C. DE TERWANGNE and S. NOUWT, *Reinventing data protection?*, Berlin, Springer, 2009, 10; V. KOSTA, *Fundamental rights in EU internal market legislation*, Oxford, Hart Publishing, 2015, 93.

[55] E.J. KINDT, *Privacy and data protection issues of biometric applications: a comparative legal analysis*, Dordrecht, Springer, 2013, 92; V. KOSTA, *Fundamental rights in EU internal market legislation*, Oxford, Hart Publishing, 2015, 93.

[56] P. HUSTINX, "EU data protection law: the review of Directive 95/46/EC and the proposed general data protection regulation", https://secure.edps.europa.eu, 2013, 9; E.J. KINDT, *Privacy and data protection issues of biometric applications: a comparative legal analysis*, Dordrecht, Springer, 2013, 93.

[57] Brussel 9 november 2015, *Computerr.* 2016, 62; Opinion 08/2015 on applicable law, Article 29 Data Protection Working Party, 0836-02/10/EN, WP 179, 16 December 2010, 10-11.

[58] CJEU 6 October 2015, C-362/14, Maximillian Schrems/Data Protection Commissioner, §41; Brussel 9 november 2015, *Computerr.* 2016, 63; X., *Het vonnis in de zaak Facebook*, www.privacycommission.be.

[59] *Infra* 18, nr. 23.

19. ARTICLE 6, PARAGRAPH A – Article 6 of the Data Protection Directive sets out some principles relating to the quality of the data. Firstly, paragraph a) states that Member States must provide that personal data is processed fairly and lawfully.[60] Recital 38 further states that for the processing of the data to be fair, the data subject must be in a position to learn from the existence of a processing operation and he must be given accurate and full information when data is collected from or of him. As concerns the 'lawfully' requirement, it is not clarified whether it should be lawful according to the Directive, to all (additional) laws or to fundamental rights.

20. ARTICLE 6, PARAGRAPH B – Paragraph b) states that the personal data must be collected for specified, explicit and legitimate purposes and should not be processed incompatible with those purposes, this is known as the purpose specification principle.[61] Whereas the requirement for a specificity and explicit nature will usually only be relevant at the start, the legitimacy requirement will be more susceptible to the passing of time.[62] Collecting information from a person infringes his privacy, however when all rules of the purpose specification principle are followed, it provides for a legal justification and the issue of privacy will be set aside.

---

[60] Article 6(a) Data Protection Directive 95/46/EC; P. CAREY, *E-privacy and online data protection*, Amsterdam, LexisNexis, 2002, 54; E. FRANTZIOU, "Further developments in the right to be forgotten: The European Court of Justice's judgment in case C-131/12, Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de datos", *Human Rights Law Review* 2014, 762; T.K. HERVEY and J.V. MCHALE, *Health law and the European Union*, New York, Cambridge University Press, 2004, 169; E. MORDINI and P. DE HERT, *Ageing and invisibility*, Amsterdam, IOS Press, 2010, 126; J. TERSTEGGE, "Privacy in the law", in M. PETKOVIĆ and W. JONKER, *Security, privacy, and trust in modern data management*, Berlin, Springer, 2007, 13.

[61] F. BOEHM, *Information sharing and data protection in the area of freedom, security and justice*, Heidelberg, Springer, 2012, 132; E. FRANTZIOU, "Further developments in the right to be forgotten: The European Court of Justice's judgment in case C-131/12, Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de datos", *Human Rights Law Review* 2014, 762; T.K. HERVEY and J.V. MCHALE, *Health law and the European Union*, New York, Cambridge University Press, 2004, 169; D. KLITOU, *Privacy-invading technologies and privacy by design*, The Hague, Asser Press, 2014, 37; P. KORENHOF, J. AUSLOOS *et al*., "Timing the right to be forgotten: a study into 'time' as a factor in deciding about retention or erasure of data", in S. GUTWIRTH, R. LEENES and P. DE HERT, *Reforming European data protection law*, Dordrecht, Springer, 2015, 182; J. TERSTEGGE, "Privacy in the law", in M. PETKOVIĆ and W. JONKER, *Security, privacy, and trust in modern data management*, Berlin, Springer, 2007, 13; G. SKOUMA and L. LÉONARD, "On-line behavioral tracking: what may change after the legal reform on personal data protection", in S. GUTWIRTH, R. LEENES and P. DE HERT, *Reforming European data protection law*, Dordrecht, Springer, 2015, 47; J. STEVOVIC, E. BASSI, A. GIORI, F. CASATI and G. ARMELLIN, "Enabling privacy by design in medical records sharing", in S. GUTWIRTH, R. LEENES and P. DE HERT, *Reforming European data protection law*, Dordrecht, Springer, 2015, 402.

[62] P. BOILLAT and M. KJAERUM, *Handbook on European data protection law*, http://www.echr.coe.int, 2014, 69; P. KORENHOF, J. AUSLOOS *et al*., "Timing the right to be forgotten: a study into 'time' as a factor in deciding about retention or erasure of data", in in S. GUTWIRTH, R. LEENES and P. DE HERT, *Reforming European data protection law*, Dordrecht, Springer, 2015, 182.

However, as mentioned before, privacy and data protection are not necessarily the same, so in certain situations it is advised to look at both the specific legislation on data protection and the general privacy legislation of the ECHR and the EU Charter of Fundamental Rights.[63]

21. ARTICLE 6, PARAGRAPH C – Paragraph c) states that Member States must provide that personal data is adequate, relevant and not excessive in relation to the purpose for which they are collected and/or further processed.[64] This provision, also known as the data minimization principle, stands in close relation to the finality principle. Its importance was often underestimated before the Google Spain case.[65] In that case it was decided that when the collected information is no longer relevant, it has to be deleted, which is known as the right to be forgotten.[66] Article 6, paragraph c) gained a lot of importance due to this case, and the right to be forgotten that followed out of it is now explicitly included in the General Data Protection Regulation which will replace the Directive 95/46/EC.[67]

[63] *Supra* 2, nr. 2.
[64] F. BOEHM, *Information sharing and data protection in the area of freedom, security and justice*, Heidelberg, Springer, 2012, 158; P. BOILLAT and M. KJAERUM, *Handbook on European data protection law*, http://www.echr.coe.int, 2014, 70; E. FRANTZIOU, "Further developments in the right to be forgotten: The European Court of Justice's judgment in case C-131/12, Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de datos", *Human Rights Law Review* 2014, 762; T.K. HERVEY and J.V. MCHALE, *Health law and the European Union*, New York, Cambridge University Press, 2004, 169.
[65] CJEU 13 May 2014, C-131/12, Google Spain/Spanish Data Protection Agency (AEPD); E. FRANTZIOU, "Further developments in the right to be forgotten: The European Court of Justice's judgment in case C-131/12, Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de datos", *Human Rights Law Review* 2014, 761.
[66] E. FRANTZIOU, "Further developments in the right to be forgotten: The European Court of Justice's judgment in case C-131/12, Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de datos", *Human Rights Law Review* 2014, 761.
[67] *Infra* 18, nr. 23.

2.3 General Data Protection Regulation

22. PROPOSAL GDPR – In January 2012, the European Commission proposed a data protection reform package which included a Proposal for a General Data Protection Regulation, which intends to replace the Data Protection Directive 95/46/EC and has as aim to reinforce data protection rights of individuals, to facilitate the free flow of personal data in the digital single market and reduce administrative burden.[68] This reform package came because of the need for modernization of the current rules on data protection in the light of rapid technological changes and globalization.[69] The core element is protecting the individual's privacy even though his awareness of it is low, and even in cases when the individual does not take steps himself in order to have his privacy protected.[70] The Regulation comes with new definitions and new obligations. For example, a data breach notification has become mandatory as well as data protection impact assessments, and a Data Protection Officer needs to be appointed in every Member State. The emphasis is clearly shifting from the rights of privacy and data protection of the data subjects to the duties being put on data controllers.[71]

---

[68] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 2012/0011 (COD), 15039/15; P. BOILLAT and M. KJAERUM, *Handbook on European data protection law*, http://www.echr.coe.int, 2014, 21; C. KUNER, F.H. CATE *et al*., "The data protection credibility crisis", *International Data Privacy Law* 2015, 161; L. SCAIFE, *Handbook of social media and the law*, New York, Informa Law from Routledge, 2015, 249.

[69] P. BOILLAT and M. KJAERUM, *Handbook on European data protection law*, http://www.echr.coe.int, 2014, 21; A. KISS and G.L. SZOKE, "Evolution of revolution? Steps forward to a new generation of data protection regulation", in S. GUTWIRTH, R. LEENES and P. DE HERT, *Reforming European data protection law: Issues in privacy and data protection*, Dordrecht, Springer, 2015, 311; L. SCAIFE, *Handbook of social media and the law*, New York, Informa Law from Routledge, 2015, 244.

[70] A. KISS and G.L. SZOKE, "Evolution of revolution? Steps forward to a new generation of data protection regulation", in S. GUTWIRTH, R. LEENES and P. DE HERT, *Reforming European data protection law: Issues in privacy and data protection*, Dordrecht, Springer, 2015, 311; M. VAN LIESHOUT, "Privacy and innovation: from disruption to opportunities", in S. GUTWIRTH, R. LEENES and P. DE HERT, *Data protection on the move: Current developments in ICT and privacy/data protection*, Dordrecht, Springer, 2016, 210.

[71] P. DE HERT and V. PAPAKONSTANTINOU, "The Council of Europe data protection convention reform: analysis of the new text and critical comment on its global ambition", *Computer Law & Security Review* 2014, 638; A. KISS and G.L. SZOKE, "Evolution of revolution? Steps forward to a new generation of data protection regulation", in S. GUTWIRTH, R. LEENES and P. DE HERT, *Reforming European data protection law: Issues in privacy and data protection*, Dordrecht, Springer, 2015, 312.

23. IMPLEMENTATION – Directive 95/46/EC will thus be replaced by a regulation, which has as a result that more harmonisation will be possible to achieve since all Member States are bound by it due to its direct effect, and they will thus need to adjust their national law as far as necessary for the coherence of the law.[72] In April 2016, the proposal for the GDPR of the European Commission was finally accepted by the European Council and European Parliament and the GDPR eventually came into force in May 2016.[73] The Member States will have another two years to comply with the obligations set forth in the GDPR.

2.4 Art. 29 Data Protection Working Party

24. ART. 29 WORKING PARTY – The Article 29 Data Protection Working Party was set up under the Directive 95/46/EC for interpretation thereof and for the protection of individuals regarding the processing of their personal data.[74] It is composed of representatives of the national data protection authorities (DPA), the European data protection supervisor (EDPS) and the European Commission.[75] The Working Party is an important platform for cooperation.

[72] Regulation of the European Parliament and of the Council 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, *OJEU* 4 May 2016, 119/1 (hereafter: GDPR); A. ALEMANNO and A.L. SIBONY, *Nudge and the law: a European perspective*, Oxford, Hart Publishing, 2015, 184.

[73] L. CROPPER, "GDPR gets the final seal of approval", privacylawblog.fieldfisher.com 15 April 2016; R. ULDALL, "Data protection reform – Parliament approves new rules fit for the digital era", http://www.europarl.europa.eu 2016; X., *Reform of EU data protection rules*, ec.europa.eu; X., *The general data protection regulation*, www.consolium.europa.eu.

[74] C. FRITSCH, "Data processing in employment relations; impacts of the European general data protection regulation focusing on the data protection officer at the worksite", in S. GUTWIRTH, R. LEENES and P. DE HERT, *Reforming European data protection law: Issues in privacy and data protection*, Dordrecht, Springer, 2015, 155; D. KLITOU, *Privacy-invading technologies and privacy by design*, The Hague, Asser Press, 2014, 29; C. KUNER, *European data privacy law and online business*, New York, Oxford University Press, 2003, 9; L. SCAIFE, *Handbook of social media and the law*, New York, Informa Law from Routledge, 2015, 244.

[75] L. COLONNA, "Europe versus Facebook: an imbroglio of EU data protection issues", in S. GUTWIRTH, R. LEENES and P. DE HERT, *Data protection on the move: Current developments in ICT and privacy/data protection*, Dordrecht, Springer, 2016, 27; C. FRITSCH, "Data processing in employment relations; impacts of the European general data protection regulation focusing on the data protection officer at the worksite", in S. GUTWIRTH, R. LEENES and P. DE HERT, *Reforming European data protection law: Issues in privacy and data protection*, Dordrecht, Springer, 2015, 155.

Its main tasks are to provide expert advice on data protection matters from the national level to the European Commission, to promote the uniform application of the Directive 95/46/EC in the EU and EEA, and to advise the Commission on any European Community law that affects the right to protection of personal data.[76]

25. EFFECT OF ADVICE - The interpretative materials issued by the Article 29 Working Party have a non-binding, advisory status and act independently from the position of the European Commission.[77] Its opinions tend to be quite influential and even have some sort of crystallization of legal opinion as effect.[78] The opinions of the Art. 29 Data Protection Working Party will remain relevant when the GDPR comes into force.

2.5 Charter of Fundamental Rights of the European Union

26. EU CHARTER – What distinguishes the Charter of Fundamental Rights from the Data Protection Directive is its ability to recognize different traditions and allow them to be maintained when interpreting the fundamental rights.[79] The consequence is that article 52 of the Charter will be interpreted via the traditions of national states, which makes it disparate again. The result is the same as under the Data Protection Directive in the sense that a common legal approach on the right to privacy in Europe is non-existent.

---

[76] C. FRITSCH, "Data processing in employment relations; impacts of the European general data protection regulation focusing on the data protection officer at the worksite", in S. GUTWIRTH, R. LEENES and P. DE HERT, *Reforming European data protection law: issues in privacy and data protection*, Dordrecht, Springer, 2015, 155-156; X., *Article 29 Working Party*, https://secure.edps.europa.eu.

[77] C. FRITSCH, "Data processing in employment relations; impacts of the European general data protection regulation focusing on the data protection officer at the worksite", in S. GUTWIRTH, R. LEENES and P. DE HERT, *Reforming European data protection law: issues in privacy and data protection*, Dordrecht, Springer, 2015, 156; C. KUNER, *European data privacy law and online business*, New York, Oxford University Press, 2003, 10; X., *Article 29 Working Party*, http://ec.europa.eu.

[78] A. ALEMANNO and A.L. SIBONY, *Nudge and the law: a European perspective*, Oxford, Hart Publishing, 2015, 183; C. KUNER, *European data privacy law and online business*, New York, Oxford University Press, 2003, 9.

[79] F. BOEHM, *Information sharing and data protection in the area of freedom, security and justice*, Heidelberg, Springer, 2012, 125; V. KOSTA, *Fundamental rights in EU internal market legislation*, Oxford, Hart Publishing, 2015, 93-94; J. TERSTEGGE, "Privacy in the law", in M. PETKOVIĆ and W. JONKER, *Security, privacy, and trust in modern data management*, Berlin, Springer, 2007, 11.

An example of this phenomenon is article 22 of the Belgian Constitution, which is more stringent than article 8 ECHR and article 7 of the EU Charter, whereas in other Member States it is possible that a less stringent approach has been chosen to implement.

27. ARTICLE 7 – Article 7 of the Charter of Fundamental Rights of the European Union states the fundamental right to respect for privacy, *i.e.* respect for his or her private and family life, home and communications.

28. ARTICLE 8 – Article 8 of the Charter of Fundamental Rights explicitly recognizes the right to the protection of data in addition to the right of respect for private life.[80] Similar to the Data Protection Directive, the Charter of Fundamental Rights states a purpose specification rule and a right of access for the person of whom the data is collected.[81] Article 8 adds a control by an independent authority.[82] This fundamental data protection includes fair processing, consent, access to data and the right to rectification.[83]

29. ARTICLE 52(1) – Article 52(1) of the Charter of Fundamental Rights stipulates the scope of the rights guaranteed in the Charter. It states that both article 7 and 8 as rights recognized by the Charter need to be provided for by law and their essence needs to be respected.

---

[80] F. BOEHM, *Information sharing and data protection in the area of freedom, security and justice*, Heidelberg, Springer, 2012, 125; P. HUSTINX, "EU data protection law: the review of Directive 95/46/EC and the proposed general data protection regulation", https://secure.edps.europa.eu, 2013, 16; V. KOSTA, *Fundamental rights in EU internal market legislation*, Oxford, Hart Publishing, 2015, 94.

[81] F. BOEHM, *Information sharing and data protection in the area of freedom, security and justice*, Heidelberg, Springer, 2012, 125; S. PEERS, T. HERVEY, J. KENNER and A. WARD, *The EU charter of fundamental rights: A commentary*, Oxford, Hart Publishing, 2014, 259.

[82] F. BOEHM, *Information sharing and data protection in the area of freedom, security and justice*, Heidelberg, Springer, 2012, 125; P. BOILLAT and M. KJAERUM, *Handbook on European data protection law*, http://www.echr.coe.int, 2014, 20-21; P. HUSTINX, "EU data protection law: the review of Directive 95/46/EC and the proposed general data protection regulation", https://secure.edps.europa.eu, 2013, 16; V. KOSTA, *Fundamental rights in EU internal market legislation*, Oxford, Hart Publishing, 2015, 94.

[83] F. BOEHM, *Information sharing and data protection in the area of freedom, security and justice*, Heidelberg, Springer, 2012, 125; R.L. FINN and D. WRIGHT, "Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications", *Computer Law & Security Review* 2012, 192; P. HUSTINX, "EU data protection law: the review of Directive 95/46/EC and the proposed general data protection regulation", https://secure.edps.europa.eu, 2013, 16; V. KOSTA, *Fundamental rights in EU internal market legislation*, Oxford, Hart Publishing, 2015, 94.

The proportionality principle is seen as a very important element. Limitations to these provisions may only be made when they are necessary and genuinely meet objectives of general interest recognized by the Union.[84] These objectives of general interest are clearly broader than the six elements enumerated under the European privacy provisions in article 8 ECHR, namely the interests of national security, public safety or the economic well-being of the country, the prevention of disorder or crime, the protection of health or morals or the protection of rights and freedoms of others.[85]

C. US legislation

30. US LEGISLATION – The US Federal Constitution does not explicitly mention privacy or data protection.[86] However, throughout history, starting with the article written by BRANDEIS and WARREN, the need for privacy and data protection has become more apparent, especially in case law.

1. Brandeis and Warren article

31. BRANDEIS AND WARREN – At the end of the 19th century, a new technology called instantaneous photography started to emerge, which made it possible to make photographs of people on the street.[87] This given combined with the upcoming newspapers and press, which made it possible to distribute photographs on a large scale, brought privacy questions to the attention.

[84] F. BOEHM, *Information sharing and data protection in the area of freedom, security and justice*, Heidelberg, Springer, 2012, 125; S. PEERS, T. HERVEY, J. KENNER and A. WARD, *The EU charter of fundamental rights: A commentary*, Oxford, Hart Publishing, 2014, 259.
[85] *Supra* 8, nr. 11.
[86] G. GREENLEAF, "The influence of European data privacy standards outside Europe: Implications for globalisation of Convention 108?", *International Data Privacy Law* 2012, 3; D. KLITOU, *Privacy-invading technologies and privacy by design*, The Hague, Asser Press, 2014, 15; J. KOKOTT and C. SOBOTTA, "The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR", *International Data Privacy Law* 2013, 223; X., *Common law right to privacy*, privacy.uslegal.com.
[87] M.R. CALO, "The drone as privacy catalyst", *Stanford Law Review Online* 12 December 2011; R.L. FINN, D. WRIGHT and M. FRIEDEWALD, "Seven types of privacy", in S. GUTWIRTH, R. LEENES, P. DE HERT and Y. POULLET, *European data protection: coming of age*, Dordrecht, Springer, 2013, 3; D. KLITOU, *Privacy-invading technologies and privacy by design*, The Hague, Asser Press, 2014, 15.

BRANDEIS and WARREN were the first to argue in a Harvard Law Review article that the law must evolve in response to technological change and must recognize the right to privacy because, when information about a person's private life is made available to the public, it tends to influence and may even hurt the very core of an individual's personality.[88]

2. Amendments to the US Constitution

32. FIRST AMENDMENT – The First Amendment to the United States Constitution provides the right to the free exercise of religion, freedom of speech and the freedom to assemble and petition the government for a redress of grievances.[89]

33. FOURTH AMENDMENT – The Fourth Amendment to the United States Constitution protects citizens from unreasonable searches by law enforcement bodies, particularly in areas where individuals may have a reasonable expectation of privacy, such as their home.[90] Due to the fact that airways are public, materials or activities on the ground may be surveilled by aerial vehicles such as helicopters, as long as those materials and activities are visible to the naked eye.[91]

---

[88] M.R. CALO, "The drone as privacy catalyst", *Stanford Law Review Online* 12 December 2011; B.H.M. CUSTERS, J.J. OERLEMANS en S.J. VERGOUW, *Het gebruik van drones: een verkennend onderzoek naar onbemande luchtvaartuigen*, Meppel, Boom Lemma Uitgevers, 2015, 104; D.J. GLANCY, "The invention of the right to privacy", *Arizona Law Review* 1979, 2; D. KLITOU, *Privacy-invading technologies and privacy by design*, The Hague, Asser Press, 2014, 15; L. SCAIFE, *Handbook of social media and the law*, New York, Informa Law from Routledge, 2015, 238; U. VOLOVELSKY, "Civilian uses of unmanned aerial vehicles and the threat to the right to privacy – An Israeli case study", *Computer Law & Security Review* 2014, 311; S.D. WARREN and L.D. BRANDEIS, "The right to privacy", *Harvard Law Review* 15 December 1890.

[89] First Amendment to the United States Constitution: *"Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances."*.

[90] Fourth Amendment to the United States Constitution: *"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."*; R.L. FINN and D. WRIGHT, "Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications", *Computer Law & Security Review* 2012, 192; D. GALIANO, *The fourth amendment: unreasonable search and seizure*, New York, The Rosen Publishing Group, 2011, 6; T.N. MCINNIS, *The evolution of the Fourth Amendment*, Plymouth, Lexington Books, 2010, 233; S. NOUWT, B.R. DE VRIES and C. PRINS, *Reasonable expectations of privacy? Eleven country reports on camera surveillance and workplace privacy*, Den Haag, TMC Asser Press, 2005, 10.

[91] M.R. CALO, "The drone as privacy catalyst", *Stanford Law Review Online* 12 December 2011; R.L. FINN and D. WRIGHT, "Unmanned aircraft systems: Surveillance, ethics and privacy in civil

3. Case law

34. CASE LAW – In *Olmstead v United States* of 1928 the Supreme Court held that the use of wiretapped private telephone conversations, obtained by federal agents without judicial approval and subsequently used as evidence, did not constitute a violation of the Fourth Amendment.[92] However, BRANDEIS wrote a dissenting opinion on the verdict and in 1967 it was reversed by *Katz v United States,* which extended the Fourth Amendment protection to all areas where a person has a reasonable expectation of privacy.[93]

4. The Privacy Act of 1974

35. PRIVACY ACT 1974 – The Privacy Act of 1974 was created in response to concerns about individuals' privacy rights in the context of the creation and use of computerized databases.[94] The Act safeguards privacy through the creation of procedural and substantive rights in personal data.[95] Amongst others, it requires public agencies to follow certain fair information practices when collecting and handling personal data and it places restrictions on how the individual's data can be shared with other people and public agencies.[96]

---

applications", *Computer Law & Security Review* 2012, 192; T.N. MCINNIS, *The evolution of the Fourth Amendment*, Plymouth, Lexington Books, 2010, 233-234.

[92] US Supreme Court, 277 U.S. 438 (1928), Olmstead/United States; D. GALIANO, *The fourth amendment: unreasonable search and seizure*, New York, The Rosen Publishing Group, 2011, 42-43; T.N. MCINNIS, *The evolution of the Fourth Amendment*, Plymouth, Lexington Books, 2010, 28.

[93] US Supreme Court, 389 U.S. 347 (1967) Katz/United States; H.B. FÄRBER, "Eyes in the sky & privacy concerns on the ground", *Scitech Lawyer* 2015, 7-8; T.N. MCINNIS, *The evolution of the Fourth Amendment*, Plymouth, Lexington Books, 2010, 187; S. NOUWT, B.R. DE VRIES and C. PRINS, *Reasonable expectations of privacy? Eleven country reports on camera surveillance and workplace privacy*, Den Haag, TMC Asser Press, 2005, 10.

[94] D. KLITOU, *Privacy-invading technologies and privacy by design*, The Hague, Asser Press, 2014, 221; A.J. MARCELLA JR. and C. STUCKI, *Privacy handbook: guidelines, exposures, policy implementation and international issues*, New Jersey, John Wiley & Sons Inc., 2003, 134; X., *The Privacy Act of 1974*, www.epic.org.

[95] A.J. MARCELLA JR. and C. STUCKI, *Privacy handbook: guidelines, exposures, policy implementation and international issues*, New Jersey, John Wiley & Sons Inc., 2003, 134; X., *The Privacy Act of 1974*, www.epic.org.

[96] D. KLITOU, *Privacy-invading technologies and privacy by design*, The Hague, Asser Press, 2014, 222; S. NOUWT, B.R. DE VRIES and C. PRINS, *Reasonable expectations of privacy? Eleven country reports on camera surveillance and workplace privacy*, Den Haag, TMC Asser Press, 2005, 23; X., *The Privacy Act of 1974*, www.epic.org.

However, some exceptions exist to the Privacy Act, for example government agencies that are involved in law enforcement can excuse themselves from the Act's rules. The Act is also not likely to serve as a general barrier to the use of video surveillance other than for some First Amendment activities.[97]

CHAPTER 2. Applied to drones

36. APPLIED TO DRONES – This chapter will first explain what drones are, for which purposes they can be used and what the current issues are concerning them. Afterwards, it will be explained why protection is needed from the rise of UA systems, especially if they could be used for surveillance purposes, as well as the possible problems that come with it regarding consent of the data subject. After addressing these problems, this master thesis will have a look at the current legislation on drones for private and surveillance purposes and whether they are adequate to address the concerns raised about it.

§1 What are drones?

37. UNMANNED AIRCRAFTS – Drones are unmanned aircrafts, which means that it are devices that are flown without a pilot on board.[98] The vehicles are reusable and are steered from a distance using a joystick or digital interface supported by automatic control, which can be close enough to still be in sight, but which can also be thousands of kilometers away.[99]

---

[97] S. NOUWT, B.R. DE VRIES and C. PRINS, *Reasonable expectations of privacy? Eleven country reports on camera surveillance and workplace privacy*, Den Haag, TMC Asser Press, 2005, 23; X., *The Privacy Act of 1974*, www.epic.org.

[98] R. CLARKE, "Understanding the drone epidemic", *Computer Law & Security Review* 2014, 230; R. CLARKE and L.B. MOSES, "The regulation of civilian drones' impacts on public safety", *Computer Law & Security Review* 2014, 272; R.L. FINN and D. WRIGHT, "Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications", *Computer Law & Security Review* 2012, 184; S.E. KREPS, *Drones: What everyone needs to know*, New York, Oxford University Press, 2016, 6; P. MCBRIDE, "Beyond Orwell: The application of unmanned aircraft systems in domestic surveillance operations", *Journal of Air Law and Commerce* 2009, 628; C. SCHLAG, "The new privacy battle: how the expanding use of drones continues to erode our concept of privacy and privacy rights", *Journal of Technology, Law & Policy* 2013, 3.

[99] R. CLARKE and L.B. MOSES, "The regulation of civilian drones' impacts on public safety", *Computer Law & Security Review* 2014, 272; R.L. FINN and D. WRIGHT, "Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications", *Computer Law & Security Review* 2012, 187; C.L. WASHBOURNE and C. NATH, "Civilian drones", *Postnote* 2014, 1.

Drones are known under several abbreviations such as: UAV (Unmanned Aerial Vehicle), RPAS (Remotely Piloted Aircraft System), MAV (Micro Air Vehicle), or SUAS (Small Unmanned Aircraft System). For convenience's sake, this master thesis will be solely using the terms 'drones' and 'UAV'.

A. Different uses of drones

38. DIFFERENT USES – In this paragraph, the possible uses of drones will be explained. First of all, drones can be used for military and police purposes, which is known as state aircraft, as well as for environmental purposes, and increasingly also for private and commercial purposes.

1. Military and police use

39. MILITARY USE – The first uses of drones were made in the military sector, where unmanned aerial rockets were used to lead themselves to targets.[100] In the Second World War, drones were also used as a diversion to keep manned aerial vehicles safe. Today, more than 50 nations use drones for military reconnaissance, intelligence-gathering and targeting.[101] Military applications have been, and still remain today a strong driver of drone developments.[102]

[100] R. CLARKE, "Understanding the drone epidemic", *Computer Law & Security Review* 2014, 238; R. CLARKE, "The regulation of civilian drones' impacts on behavioural privacy", *Computer Law & Security Review* 2014, 286; T. DUNLAP, "We've got our eyes on you: When surveillance by unmanned aircraft systems constitutes a Fourth amendment search", *South Texas Law Review* 2009, 176; R.L. FINN and D. WRIGHT, "Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications", *Computer Law & Security Review* 2012, 185; C. SCHLAG, "The new privacy battle: how the expanding use of drones continues to erode our concept of privacy and privacy rights", *Journal of Technology, Law & Policy* 2013, 3; C.L. WASHBOURNE and C. NATH, "Civilian drones", *Postnote* 2014, 1.

[101] Policy department C: citizens' rights and constitutional affairs, "Privacy and data protection implications of the civil use of drones: in-depth analysis for the LIBE Committee", PE.519.221, www.europarl.europa.eu, June 2015, 10; R.L. FINN and D. WRIGHT, "Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications", *Computer Law & Security Review* 2012, 185; C. SCHLAG, "The new privacy battle: how the expanding use of drones continues to erode our concept of privacy and privacy rights", *Journal of Technology, Law & Policy* 2013, 6.

[102] M.R. CALO, "The drone as privacy catalyst", *Stanford Law Review Online* 12 December 2011; R. CLARKE, "Understanding the drone epidemic", *Computer Law & Security Review* 2014, 231; S.E. KREPS, *Drones: What everyone needs to know*, New York, Oxford University Press, 2016, 1.

40. POLICE USE – Around 2006, drones were starting to be used for societal purposes, such as searching for survivors of natural disasters like hurricanes, or survivors of car accidents.[103] Unmanned aircrafts fitted with cameras or sensors are also being deployed by law enforcement bodies for surveillance purposes against civilians and border controls.[104] Police forces may use unmanned aircrafts to monitor large crowds, for example during festivals, to prevent or detect crime, for example a drone was used during the house searches relating counter-terrorism investigations in Belgium, and to assist in incident responses, for example assisting police in pursuits.[105]

2. Scientific use

41. SCIENTIFIC USE – Drones have proven to be helpful especially for environmental purposes, such as meteorological forecasting, forest fire detection and contamination measurement.[106] Furthermore, drones are being used in biology to follow up erosion, logging or the migration of certain species.[107]

---

[103] R. CLARKE, "Understanding the drone epidemic", *Computer Law & Security Review* 2014, 238; B.H.M. CUSTERS, J.J. OERLEMANS en S.J. VERGOUW, *Het gebruik van drones: een verkennend onderzoek naar onbemande luchtvaartuigen*, Meppel, Boom Lemma Uitgevers, 2015, 115; C. SCHLAG, "The new privacy battle: how the expanding use of drones continues to erode our concept of privacy and privacy rights", *Journal of Technology, Law & Policy* 2013, 9; C.L. WASHBOURNE and C. NATH, "Civilian drones", *Postnote* 2014, 2; D. WRIGHT, "Drones: Regulatory challenges to an incipient industry", *Computer Law & Security Review* 2014, 227.

[104] R. CLARKE, "The regulation of civilian drones' impacts on behavioural privacy", *Computer Law & Security Review* 2014, 286; R.L. FINN and D. WRIGHT, "Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications", *Computer Law & Security Review* 2012, 184-185 and 188; C. SCHLAG, "The new privacy battle: how the expanding use of drones continues to erode our concept of privacy and privacy rights", *Journal of Technology, Law & Policy* 2013, 10; U. VOLOVELSKY, "Civilian uses of unmanned aerial vehicles and the threat to the right to privacy – An Israeli case study", *Computer Law & Security Review* 2014, 313.

[105] R.L. FINN and D. WRIGHT, "Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications", *Computer Law & Security Review* 2012, 189; G. MCNEAL, "Drones and aerial surveillance: considerations for legislators", *Brookings* November 2014, 3.

[106] ICAO Circular 328-AN/190, Unmanned Aircraft Systems (UAS), 8; R. CLARKE, "Understanding the drone epidemic", *Computer Law & Security Review* 2014, 238; R. CLARKE, "The regulation of civilian drones' impacts on behavioural privacy", *Computer Law & Security Review* 2014, 286; B.H.M. CUSTERS, J.J. OERLEMANS en S.J. VERGOUW, *Het gebruik van drones: een verkennend onderzoek naar onbemande luchtvaartuigen*, Meppel, Boom Lemma Uitgevers, 2015, 64; R.L. FINN and D. WRIGHT, "Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications", *Computer Law & Security Review* 2012, 188; C. SCHLAG, "The new privacy battle: how the expanding use of drones continues to erode our concept of privacy and privacy rights", *Journal of Technology, Law & Policy* 2013, 8; C.L. WASHBOURNE and C. NATH, "Civilian drones", *Postnote* 2014, 2.

[107] N. AVERETT, "Drones take off as wildlife conservation tool", www.audubon.org 2014; B.H.M. CUSTERS, J.J. OERLEMANS en S.J. VERGOUW, *Het gebruik van drones: een verkennend onderzoek naar onbemande luchtvaartuigen*, Meppel, Boom Lemma Uitgevers, 2015, 65.

The success of UAVs exists in the fact that they can reach remote locations under harsh conditions or altitudes which manned aircrafts cannot reach, such as the rainforest of the Amazon.[108]

3. Commercial and civilian use

42. COMMERCIAL USE – Commercial use of drones used to be forbidden without a permit of airworthiness or guarantee that the civil air traffic would not be in danger.[109] However, both on national and European, as well as on international level, legislation has recently been adapted to meet the needs of companies to use drones for commercial purposes and make it easier to comply with the law, whilst at the same time uphold privacy rights and safety measures.[110] Mainly private companies have already used drones for security, loss prevention, goods transportation and various other purposes.[111] For example, Google uses drones for developing internet-based street view maps and obtain map data, National Geographic has used drones to collect wildlife and nature information, and recently Amazon announced its intention to use UAVs to deliver packages as soon as the regulations permit.[112]

---

[108] ICAO Circular 328-AN/190, Unmanned Aircraft Systems (UAS), 9; B.H.M. CUSTERS, J.J. OERLEMANS en S.J. VERGOUW, *Het gebruik van drones: een verkennend onderzoek naar onbemande luchtvaartuigen*, Meppel, Boom Lemma Uitgevers, 2015, 65; R.L. FINN and D. WRIGHT, "Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications", *Computer Law & Security Review* 2012, 187; U. VOLOVELSKY, "Civilian uses of unmanned aerial vehicles and the threat to the right to privacy – An Israeli case study", *Computer Law & Security Review* 2014, 313; D. WRIGHT, "Drones: Regulatory challenges to an incipient industry", *Computer Law & Security Review* 2014, 226-227.

[109] B.H.M. CUSTERS, J.J. OERLEMANS en S.J. VERGOUW, *Het gebruik van drones: een verkennend onderzoek naar onbemande luchtvaartuigen*, Meppel, Boom Lemma Uitgevers, 2015, 83; W. VERHEYEN, "Commercieel gebruik van drones: bedreig(en)de vogels?", *De Juristenkrant* 2014, 20.

[110] ICAO Circular 328-AN/190, Unmanned Aircraft Systems (UAS), 9; W. VERHEYEN, "Commercieel gebruik van drones: bedreig(en)de vogels?", *De Juristenkrant* 2014, 20.

[111] R. CLARKE, "Understanding the drone epidemic", *Computer Law & Security Review* 2014, 238; B.H.M. CUSTERS, J.J. OERLEMANS en S.J. VERGOUW, *Het gebruik van drones: een verkennend onderzoek naar onbemande luchtvaartuigen*, Meppel, Boom Lemma Uitgevers, 2015, 62; C. SCHLAG, "The new privacy battle: how the expanding use of drones continues to erode our concept of privacy and privacy rights", *Journal of Technology, Law & Policy* 2013, 11; U. VOLOVELSKY, "Civilian uses of unmanned aerial vehicles and the threat to the right to privacy – An Israeli case study", *Computer Law & Security Review* 2014, 306.

[112] B.H.M. CUSTERS, J.J. OERLEMANS en S.J. VERGOUW, *Het gebruik van drones: een verkennend onderzoek naar onbemande luchtvaartuigen*, Meppel, Boom Lemma Uitgevers, 2015, 62; H.B. FÄRBER, "Eyes in the sky & privacy concerns on the ground", *Scitech Lawyer* 2015, 6; S.E. KREPS, *Drones: What everyone needs to know*, New York, Oxford University Press, 2016, 1; C. SCHLAG, "The new privacy battle: how the expanding use of drones continues to erode our concept of privacy and privacy rights", *Journal of Technology, Law & Policy* 2013, 11; U. VOLOVELSKY, "Civilian uses of unmanned aerial vehicles and the threat to the right to privacy – An Israeli case study", *Computer Law & Security Review* 2014, 307.

43. CIVILIAN USE – Not only companies were attracted to the possibilities of UAVs, but also more and more citizens found it interesting tools to work with.[113] With the growing importance of social networks in our everyday life, *selfies* taken with phones are not sufficient anymore, people want more extreme and unique photos and video clips to share with their friends, like for example pictures taken from the sky by drones.[114] The civilian use of unmanned aircrafts is also rapidly increasing because technology is improving at a fast pace and what was once unaffordable is getting more accessible.[115] The biggest challenges for the use of drones by civilians are the safe and effective integration with the other users of the airspace mentioned above, as well as insurance and more importantly privacy, as fast-pace technological developments expand the capacity of others to invade personal space.[116]

B. Different issues with drones

44. DIFFERENT ISSUES – As discussed in the previous paragraphs, unmanned aircrafts are used for many purposes and may provide many advantages.[117] They did not always contain a camera installed on top of them, because in the beginning they were generally used as a decoy or as a rocket in the military sector.

---

[113] M.R. CALO, "The drone as privacy catalyst", *Stanford Law Review Online* 12 December 2011; U. VOLOVELSKY, "Civilian uses of unmanned aerial vehicles and the threat to the right to privacy – An Israeli case study", *Computer Law & Security Review* 2014, 306.

[114] B.H.M. CUSTERS, J.J. OERLEMANS en S.J. VERGOUW, *Het gebruik van drones: een verkennend onderzoek naar onbemande luchtvaartuigen*, Meppel, Boom Lemma Uitgevers, 2015, 61; J. LUYCKX, "Sleutelgaten en drones", *Limburgs Rechtsleven* 2015, 253; D. WRIGHT, "Drones: Regulatory challenges to an incipient industry", *Computer Law & Security Review* 2014, 226.

[115] R. CLARKE, "Understanding the drone epidemic", *Computer Law & Securit wy Review* 2014, 239; R. CLARKE and L.B. MOSES, "The regulation of civilian drones' impacts on public safety", *Computer Law & Security Review* 2014, 272; R. CLARKE, "The regulation of civilian drones' impacts on behavioural privacy", *Computer Law & Security Review* 2014, 288; B. PALMER, "Hey, you! Get off of my cloud! How much of the airspace above your home do you own?", *Slate* 11 July 2013; C. SCHLAG, "The new privacy battle: how the expanding use of drones continues to erode our concept of privacy and privacy rights", *Journal of Technology, Law & Policy* 2013, 1; B. VAN ALSENOY, "The evolving role of the individual under EU data protection law", *ICRI Working Paper* 23/2015, 24; C.L. WASHBOURNE and C. NATH, "Civilian drones", *Postnote* 2014, 2.

[116] R. CLARKE, "The regulation of civilian drones' impacts on behavioural privacy", *Computer Law & Security Review* 2014, 288; S.E. KREPS, *Drones: What everyone needs to know*, New York, Oxford University Press, 2016, 2; C.L. WASHBOURNE and C. NATH, "Civilian drones", *Postnote* 2014, 1.

[117] *Supra* 25, nr. 38 etc.; U. VOLOVELSKY, "Civilian uses of unmanned aerial vehicles and the threat to the right to privacy – An Israeli case study", *Computer Law & Security Review* 2014, 314.

However, since cameras have been installed on unmanned aircrafts, and since they have gotten extended flying capabilities, issues of privacy, data protection and surveillance as well as ethical issues started to emerge.[118] Drones are not solely being used in the military sector anymore, also civilians and commercial organisations as well as police forces started to use them, which gave rise to aviation issues since the activity in the aerial space is increasing. In the following paragraphs, these issues of privacy, surveillance and airspace will be discussed in light of the civil use of drones.

1. Privacy issues

45. PRIVACY – Regarding the deployment of unmanned aircrafts, privacy arises as one of the key civil liberties, especially when they are modified to carry high-megapixel or infrared cameras.[119] Issues especially arise when those camera-equipped drones gather personal data on individuals.[120] Concerns about privacy have been mitigated by claiming that UAVs are not so different from existing surveillance systems, such as CCTV.[121] However, drones significantly differ given the angles and the reach they can film, meaning that the argument does not take into account the complexity of UA systems and the fact that its capabilities may likely develop even more and at a fast pace in the future.[122]

---

[118] R.L. FINN and D. WRIGHT, "Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications", *Computer Law & Security Review* 2012, 189; R.L. FINN, D. WRIGHT and M. FRIEDEWALD, "Seven types of privacy", in S. GUTWIRTH, R. LEENES, P. DE HERT and Y. POULLET, *European data protection: coming of age*, Dordrecht, Springer, 2013, 15; C. SCHLAG, "The new privacy battle: how the expanding use of drones continues to erode our concept of privacy and privacy rights", *Journal of Technology, Law & Policy* 2013, 13; U. VOLOVELSKY, "Civilian uses of unmanned aerial vehicles and the threat to the right to privacy – An Israeli case study", *Computer Law & Security Review* 2014, 314.

[119] R.L. FINN and D. WRIGHT, "Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications", *Computer Law & Security Review* 2012, 191; C. SCHLAG, "The new privacy battle: how the expanding use of drones continues to erode our concept of privacy and privacy rights", *Journal of Technology, Law & Policy* 2013, 15-16.

[120] R. CLARKE, "What drones inherit from their ancestors", *Computer Law & Security Review* 2014, 248; U. VOLOVELSKY, "Civilian uses of unmanned aerial vehicles and the threat to the right to privacy – An Israeli case study", *Computer Law & Security Review* 2014, 313-314.

[121] R.L. FINN and D. WRIGHT, "Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications", *Computer Law & Security Review* 2012, 191; R.L. FINN, D. WRIGHT and M. FRIEDEWALD, "Seven types of privacy", in S. GUTWIRTH, R. LEENES, P. DE HERT and Y. POULLET, *European data protection: coming of age*, Dordrecht, Springer, 2013, 15; C. SCHLAG, "The new privacy battle: how the expanding use of drones continues to erode our concept of privacy and privacy rights", *Journal of Technology, Law & Policy* 2013, 19.

[122] B.H.M. CUSTERS, J.J. OERLEMANS en S.J. VERGOUW, *Het gebruik van drones: een verkennend onderzoek naar onbemande luchtvaartuigen*, Meppel, Boom Lemma Uitgevers, 2015, 105; N.N. GOMES DE ANDRADE and S. MONTELEONE, "Digital natives and the metamorphosis of the European

2. Surveillance issues

46. SURVEILLANCE – The aforementioned privacy concerns are closely connected to the issue of the use of unmanned aircraft systems for surveillance purposes in civil applications.[123] Unmanned aircrafts raise issues when they are being used for surveillance purposes because people can be monitored, photographed, tracked and targeted at any time and over a certain period of time regardless of whether their activities warrant suspicion, without them even knowing.[124] Such intrusions by UAVs bring about physical, psychological and social effects and could have a self-disciplining effect, where individuals adapt their behavior as if they are being watched at all times.[125] In particular, UAV surveillance has more potential of being covert than CCTV and helicopter surveillance to which it has been compared to, resulting in the aforementioned effects, which as a consequence may erode society's expectation of privacy.[126]

---

information society. The emerging behavioral trends regarding privacy and their legal implications", in GUTWIRTH, S., LEENES, R., DE HERT, P. and POULLET, Y., *European data protection: coming of age*, Dordrecht, Springer, 2013, 141; C. SCHLAG, "The new privacy battle: how the expanding use of drones continues to erode our concept of privacy and privacy rights", *Journal of Technology, Law & Policy* 2013, 19.

[123] R.L. FINN and D. WRIGHT, "Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications", *Computer Law & Security Review* 2012, 184; S.E. KREPS, *Drones: What everyone needs to know*, New York, Oxford University Press, 2016, 47.

[124] M.R. CALO, "The drone as privacy catalyst", *Stanford Law Review Online* 12 December 2011; R. CLARKE, "What drones inherit from their ancestors", *Computer Law & Security Review* 2014, 258; R. CLARKE, "The regulation of civilian drones' impacts on behavioural privacy", *Computer Law & Security Review* 2014, 287-288; H.B. FÄRBER, "Eyes in the sky & privacy concerns on the ground", *Scitech Lawyer* 2015, 6; R.L. FINN and D. WRIGHT, "Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications", *Computer Law & Security Review* 2012, 190; R.L. FINN, D. WRIGHT and M. FRIEDEWALD, "Seven types of privacy", in S. GUTWIRTH, R. LEENES, P. DE HERT and Y. POULLET, *European data protection: coming of age*, Dordrecht, Springer, 2013, 15; J.W. WHITEHEAD, "Drones over America: Tyranny at home", *The Rutherford Institute* 28 June 2010.

[125] *Infra* 33, nr. 50; F. BOEHM, *Information sharing and data protection in the area of freedom, security and justice*, Heidelberg, Springer, 2012, 33; R. CLARKE, "What drones inherit from their ancestors", *Computer Law & Security Review* 2014, 259; R. CLARKE and L.B. MOSES, "The regulation of civilian drones' impacts on public safety", *Computer Law & Security Review* 2014, 263; R. CLARKE, "The regulation of civilian drones' impacts on behavioural privacy", *Computer Law & Security Review* 2014, 287; R.L. FINN and D. WRIGHT, "Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications", *Computer Law & Security Review* 2012, 191; R.L. FINN, D. WRIGHT and M. FRIEDEWALD, "Seven types of privacy", in S. GUTWIRTH, R. LEENES, P. DE HERT and Y. POULLET, *European data protection: coming of age*, Dordrecht, Springer, 2013, 16; U. VOLOVELSKY, "Civilian uses of unmanned aerial vehicles and the threat to the right to privacy – An Israeli case study", *Computer Law & Security Review* 2014, 314.

[126] R. CLARKE, "The regulation of civilian drones' impacts on behavioural privacy", *Computer Law & Security Review* 2014, 288; T. DUNLAP, "We've got our eyes on you: When surveillance by unmanned aircraft systems constitutes a Fourth amendment search", *South Texas Law Review* 2009, 202; H.B. FÄRBER, "Eyes in the sky & privacy concerns on the ground", *Scitech Lawyer* 2015, 6; R.L. FINN and D. WRIGHT, "Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications", *Computer Law & Security Review* 2012, 191; R.L. FINN, D. WRIGHT and M. FRIEDEWALD, "Seven

3. Aviation issues

47. AVIATION ISSUES – The application of drones in a civil context creates a wide range of benefits, but it also creates sources of harm and possibility of collisions in the airspace.[127] The difficulty is that UAVs are not being monitored by a central dispatch, therefor other aircrafts cannot be warned when such vehicles come into the same aerial space, neither is there a sense-and-avoid compatibility generally available yet, meaning that collisions with other objects cannot be avoided automatically.[128] Although civil drones may not fly higher than a certain height and may not fly within a certain range of an airport, they have been spotted several times in those unlawful areas.[129] A recent example is the near miss of a Lufthansa jumbo with a drone over Los Angeles, which could have had far reaching consequences.[130] Also at UK airports there have been several near-misses between drones and passenger planes, which clearly indicates the necessity to undertake action to avoid possible collisions in the future, but this master thesis will not go further into that discussion.[131]

---

types of privacy", in S. GUTWIRTH, R. LEENES, P. DE HERT and Y. POULLET, *European data protection: coming of age*, Dordrecht, Springer, 2013, 16.

[127] R. CLARKE and L.B. MOSES, "The regulation of civilian drones' impacts on public safety", *Computer Law & Security Review* 2014, 264; B.H.M. CUSTERS, J.J. OERLEMANS en S.J. VERGOUW, *Het gebruik van drones: een verkennend onderzoek naar onbemande luchtvaartuigen*, Meppel, Boom Lemma Uitgevers, 2015, 74.

[128] K.E. BOON and D.C. LOVELACE JR., *The domestic use of unmanned aerial vehicles*, New York, Oxford University Press, 2014, 241; B.H.M. CUSTERS, J.J. OERLEMANS en S.J. VERGOUW, *Het gebruik van drones: een verkennend onderzoek naar onbemande luchtvaartuigen*, Meppel, Boom Lemma Uitgevers, 2015, 74; S.E. KREPS, *Drones: What everyone needs to know*, New York, Oxford University Press, 2016, 56; X., *6th sense and avoid*, www.dronesense.com.

[129] R. CLARKE and L.B. MOSES, "The regulation of civilian drones' impacts on public safety", *Computer Law & Security Review* 2014, 264; B.H.M. CUSTERS, J.J. OERLEMANS en S.J. VERGOUW, *Het gebruik van drones: een verkennend onderzoek naar onbemande luchtvaartuigen*, Meppel, Boom Lemma Uitgevers, 2015, 74; A. ZAVRŠNIK, *Drones and unmanned aerial systems: legal and social implications for security and surveillance*, Heidelberg, Springer, 2016, 252.

[130] B.H.M. CUSTERS, J.J. OERLEMANS en S.J. VERGOUW, *Het gebruik van drones: een verkennend onderzoek naar onbemande luchtvaartuigen*, Meppel, Boom Lemma Uitgevers, 2015, 74; X., "Lufthansa jumbo reports near miss with drone over Los Angeles", *The Guardian* 21 March 2016.

[131] B.H.M. CUSTERS, J.J. OERLEMANS en S.J. VERGOUW, *Het gebruik van drones: een verkennend onderzoek naar onbemande luchtvaartuigen*, Meppel, Boom Lemma Uitgevers, 2015, 74; X., "Drone over Heathrow was 'wingspan away' from collision with jet", *The Guardian* 26 February 2016; A. ZAVRŠNIK, *Drones and unmanned aerial systems: legal and social implications for security and surveillance*, Heidelberg, Springer, 2016, 252.

§2 Problems in Practice

48. PROBLEMS IN PRACTICE – As mentioned before, many law enforcement organisations have argued that surveillance by an UA system is not so different from surveillance done by any other equipment, such as CCTV or helicopter surveillance.[132] However, many authors are of a different opinion since drones can be invisible and inaudible and thus the breadth and scope of data which a UAV can capture is much more far reaching than the capabilities of traditional surveillance tools.[133] This section will focus on the practical problems which may arise out of the use of UA systems for surveillance purposes and the need for protection, and the practical problems that come with that concerning the acquisition and giving of consent.

A. Need for protection

49. NEED FOR PROTECTION – This paragraph will address the modern day issues that come with the use of drones and why we would need protection. At first, it will be discussed how drones may cause a chilling effect, then it will be discussed how drones may play a role in the every day use of social media and finally the risks of fast-evolving technologies will be discussed.

[132] *Supra* 29, nr. 45; R.L. FINN and D. WRIGHT, "Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications", *Computer Law & Security Review* 2012, 192; C. SCHLAG, "The new privacy battle: how the expanding use of drones continues to erode our concept of privacy and privacy rights", *Journal of Technology, Law & Policy* 2013, 19.

[133] B.H.M. CUSTERS, J.J. OERLEMANS en S.J. VERGOUW, *Het gebruik van drones: een verkennend onderzoek naar onbemande luchtvaartuigen*, Meppel, Boom Lemma Uitgevers, 2015, 76; H.B. FÄRBER, "Eyes in the sky & privacy concerns on the ground", *Scitech Lawyer* 2015, 6; R.L. FINN, D. WRIGHT and M. FRIEDEWALD, "Seven types of privacy", in S. GUTWIRTH, R. LEENES, P. DE HERT and Y. POULLET, *European data protection: coming of age*, Dordrecht, Springer, 2013, 15-16; B. SCHERMER, "An eye in the sky: privacy aspects of drones", *Criminal Law and Criminology* 20 June 2013; U. VOLOVELSKY, "Civilian uses of unmanned aerial vehicles and the threat to the right to privacy – An Israeli case study", *Computer Law & Security Review* 2014, 310; D. WRIGHT, "Drones: Regulatory challenges to an incipient industry", *Computer Law & Security Review* 2014, 227.

1. Prevent chilling effect

50. BIG BROTHER - The fact that technology is getting so advanced that cameras can be placed on materials that are inaudible and invisible, has raised a lot of concerns.[134] This was already heavily debated when the regulation on CCTV came into force, and will certainly be relevant in the discussion on UAVs. The biggest concern is that society will evolve towards a surveillance society, where the public will behave in a different way out of fear of being filmed and out of fear of behaving in a criminal way.[135] The public will have the feeling of being watched everywhere all the time, also known as a Big Brother society.[136] Especially new technologies such as snake bots, which are unmanned vehicles in the shape of a snake that can be fitted with cameras or audio sensors and that can climb, swim and even go through small holes, have raised serious privacy concerns.[137]

---

[134] R. CLARKE, "The regulation of civilian drones' impacts on behavioural privacy", *Computer Law & Security Review* 2014, 290; D. DE BOT, "Eye in the sky – Het gebruik van drones en privacy", *Rechtskundig Weekblad* 2014-2015, 1362; B.H.M. CUSTERS, J.J. OERLEMANS en S.J. VERGOUW, *Het gebruik van drones: een verkennend onderzoek naar onbemande luchtvaartuigen*, Meppel, Boom Lemma Uitgevers, 2015, 76; H.B. FÄRBER, "Eyes in the sky & privacy concerns on the ground", *Scitech Lawyer* 2015, 6; R.L. FINN and D. WRIGHT, "Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications", *Computer Law & Security Review* 2012, 187; R.L. FINN, D. WRIGHT and M. FRIEDEWALD, "Seven types of privacy", in S. GUTWIRTH, R. LEENES, P. DE HERT and Y. POULLET, *European data protection: coming of age*, Dordrecht, Springer, 2013, 15.

[135] M.R. CALO, "The drone as privacy catalyst", *Stanford Law Review Online* 12 December 2011; R. CLARKE, "The regulation of civilian drones' impacts on behavioural privacy", *Computer Law & Security Review* 2014, 287; B.H.M. CUSTERS, J.J. OERLEMANS en S.J. VERGOUW, *Het gebruik van drones: een verkennend onderzoek naar onbemande luchtvaartuigen*, Meppel, Boom Lemma Uitgevers, 2015, 108; D. DE BOT, "Eye in the sky – Het gebruik van drones en privacy", *Rechtskundig Weekblad* 2014-2015, 1362; R.L. FINN, D. WRIGHT, L. JACQUES and P. DE HERT, "Study on privacy, data protection and ethical risks in civil Remotely Piloted Aircraft Systems operations – final report", http://ec.europa.eu 2014, 7; U. VOLOVELSKY, "Civilian uses of unmanned aerial vehicles and the threat to the right to privacy – An Israeli case study", *Computer Law & Security Review* 2014, 314.

[136] M.R. CALO, "The drone as privacy catalyst", *Stanford Law Review Online* 12 December 2011; B.H.M. CUSTERS, J.J. OERLEMANS en S.J. VERGOUW, *Het gebruik van drones: een verkennend onderzoek naar onbemande luchtvaartuigen*, Meppel, Boom Lemma Uitgevers, 2015, 108; A. KISS and G.L. SZOKE, "Evolution of revolution? Steps forward to a new generation of data protection regulation", in S. GUTWIRTH, R. LEENES and P. DE HERT, *Reforming European data protection law: Issues in privacy and data protection*, Dordrecht, Springer, 2015, 312; P. LEWIS, "CCTV in the sky: Police plan to use military-style spy drones", *The Guardian* 23 January 2010; O. RUDGARD, "Should you install CCTV outside your home?", *The Telegraph* 22 May 2015.

[137] M.R. CALO, "The drone as privacy catalyst", *Stanford Law Review Online* 12 December 2011; R.L. FINN and D. WRIGHT, "Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications", *Computer Law & Security Review* 2012, 187; S.E. KREPS, *Drones: What everyone needs to know*, New York, Oxford University Press, 2016, 122.

51. PROBLEMS - New problems have arisen in privacy law as well, such as celebrities being chased by paparazzi drones, making it easier for paparazzi to obtain footage, but at the same time making it harder for celebrities to obtain at least some part of their life private.[138] Their only option remains to exercise their privacy right by taking measures to keep those activities private that they do not want to expose to the public view.[139] An example is the footage that has been collected by a UAV from Tina Turner's wedding, and an incriminating picture of Barbra Streisand.[140] Also in criminal law new technologies have led to an easier commitment of crimes, such as the crime of stalking or voyeurism.[141]

52. CIVIL LIBERTIES – Privacy seems to be inadequate to address all the problems of surveillance that come with new technologies, since also other civil liberties, in addition to privacy, raise concerns.[142] For example, the use of surveillance technologies may limit an individual's right to freedom of assembly or freedom of expression due to a chilling effect that discourages participation in social movements or public protests.[143]

---

[138] M.R. CALO, "The drone as privacy catalyst", *Stanford Law Review Online* 12 December 2011; R. CLARKE, "Understanding the drone epidemic", *Computer Law & Security Review* 2014, 240; R. CLARKE, "The regulation of civilian drones' impacts on behavioural privacy", *Computer Law & Security Review* 2014, 289; R.L. FINN and D. WRIGHT, "Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications", *Computer Law & Security Review* 2012, 191; R.L. FINN, D. WRIGHT and M. FRIEDEWALD, "Seven types of privacy", in S. GUTWIRTH, R. LEENES, P. DE HERT and Y. POULLET, *European data protection: coming of age*, Dordrecht, Springer, 2013, 16; U. VOLOVELSKY, "Civilian uses of unmanned aerial vehicles and the threat to the right to privacy – An Israeli case study", *Computer Law & Security Review* 2014, 307.

[139] R.L. FINN, D. WRIGHT and M. FRIEDEWALD, "Seven types of privacy", in S. GUTWIRTH, R. LEENES, P. DE HERT and Y. POULLET, *European data protection: coming of age*, Dordrecht, Springer, 2013, 16; P. MCBRIDE, "Beyond Orwell: the application of unmanned aircraft systems in domestic surveillance operations", *Journal of Air Law and Commerce* 2009, 661.

[140] Los Angeles Superior Court, SC 077 257 (2003), Streisand/Adelman; U. VOLOVELSKY, "Civilian uses of unmanned aerial vehicles and the threat to the right to privacy – An Israeli case study", *Computer Law & Security Review* 2014, 307; X. "Tina Turner's wedding photographed by drones", *The Huffington Post* 8 February 2013.

[141] R. CLARKE, "Understanding the drone epidemic", *Computer Law & Security Review* 2014, 240; R. CLARKE, "The regulation of civilian drones' impacts on behavioural privacy", *Computer Law & Security Review* 2014, 289; B.H.M. CUSTERS, J.J. OERLEMANS en S.J. VERGOUW, *Het gebruik van drones: een verkennend onderzoek naar onbemande luchtvaartuigen*, Meppel, Boom Lemma Uitgevers, 2015, 108; U. VOLOVELSKY, "Civilian uses of unmanned aerial vehicles and the threat to the right to privacy – An Israeli case study", *Computer Law & Security Review* 2014, 315.

[142] R.L. FINN and D. WRIGHT, "Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications", *Computer Law & Security Review* 2012, 186; D. LYON, "Facing the future: Seeking ethics for everyday surveillance", *Ethics and Information Technology* 2001, 176; S. NOUWT, B.R. DE VRIES and C. PRINS, *Reasonable expectations of privacy? Eleven country reports on camera surveillance and workplace privacy*, Den Haag, TMC Asser Press, 2005, 26.

[143] D. CUNNINGHAM and J. NOAKES, "What if she's from the FBI? The effects of covert forms of social control on social movements", in M. DEFLEM, *Surveillance and governance: Crime control and*

The number of UAVs will probably expand given the fact that they are getting more affordable, and as a consequence, so will the influence of the chilling effect on their behavior, causing changes in people's behavior patterns adversely affecting the fundamental right to human dignity.[144]

2. Social media

53. SOCIAL MEDIA – One of the biggest privacy concerns in modern society are without a doubt social media platforms such as Facebook, Instagram and Twitter.[145] How many times have there been pictures or videos of individuals, filmed without their knowledge, uploaded onto a social media platform and shared with millions of other people? Or how many times have people uploaded pictures or videos of burglars in order to get them caught? This brings positive consequences, but also risks regarding security and trust.[146] Not only the right to privacy is endangered, but also the right to personal data protection.[147] It is not the sharing of information *in se* that constitutes a problem, but rather the fact that it is the sharing of information outside socially agreed contextual boundaries.[148]

---

beyond, Bingley, Emerald Group Publishing Limited, 2008, 177; R.L. FINN and D. WRIGHT, "Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications", *Computer Law & Security Review* 2012, 186.

[144] ICO, *In the picture: A data protection code of practice for surveillance cameras and personal information*, https://ico.org.uk 2015, 29; B. PALMER, "Hey, you! Get off of my cloud! How much of the airspace above your home do you own?", *Slate* 11 July 2013; U. VOLOVELSKY, "Civilian uses of unmanned aerial vehicles and the threat to the right to privacy – An Israeli case study", *Computer Law & Security Review* 2014, 314.

[145] A. KISS and G.L. SZOKE, "Evolution of revolution? Steps forward to a new generation of data protection regulation", in S. GUTWIRTH, R. LEENES and P. DE HERT, *Reforming European data protection law: Issues in privacy and data protection*, Dordrecht, Springer, 2015, 315; A. RALLO and R. MARTINEZ, "Data protection, social networks and online mass media", in GUTWIRTH, S., LEENES, R., DE HERT, P. and POULLET, Y., *European data protection: coming of age*, Dordrecht, Springer, 2013, 409-410.

[146] A. OXLEY, *Security risks in social media technologies*, Oxford, Chandos Publishing, 2013, 92-93; A. RALLO and R. MARTINEZ, "Data protection, social networks and online mass media", in GUTWIRTH, S., LEENES, R., DE HERT, P. and POULLET, Y., *European data protection: coming of age*, Dordrecht, Springer, 2013, 410; L. SCAIFE, *Handbook of social media and the law*, New York, Informa Law from Routledge, 2015, 236.

[147] A. RALLO and R. MARTINEZ, "Data protection, social networks and online mass media", in GUTWIRTH, S., LEENES, R., DE HERT, P. and POULLET, Y., *European data protection: coming of age*, Dordrecht, Springer, 2013, 411; L. SCAIFE, *Handbook of social media and the law*, New York, Informa Law from Routledge, 2015, 236.

[148] R.L. FINN, D. WRIGHT and M. FRIEDEWALD, "Seven types of privacy", in S. GUTWIRTH, R. LEENES, P. DE HERT and Y. POULLET, *European data protection: coming of age*, Dordrecht, Springer, 2013, 5.

3. Technological advancements

54. EVOLVING TECHNOLOGY – Innovation and technological breakthroughs have also led to new economic models and tools influencing the life of the individual, especially in connection to information and communications technologies.[149] This is also the case for UAVs, which combine several technical capabilities as well as existing and future technologies.[150] There is however no certainty anymore about what can be filmed where and when, given that new technologies like infrared cameras can indicate the presence of a person, even through the walls. Furthermore, UAVs are also susceptible for abuse of their capabilities, like hijacking and taking control of the vehicle as well as of its photographic capabilities, which means the collected data will come into the hands of not only the owner of the UAV, but also of the hijacker.[151] This has as a result that there is no certainty as to whom will get the data as well as to whom one must address himself to protest against the use of his personal data, indicating again the potential dangers that must be addressed.

B. Practical problems

55. PRACTICAL PROBLEMS – One of the most practical issues with the use of drones is the giving of consent. In the next paragraphs it will be explained why consent of the data subject is necessary and whether it must be obtained at all times.

[149] N.N. GOMES DE ANDRADE and S. MONTELEONE, "Digital natives and the metamorphosis of the European information society. The emerging behavioral trends regarding privacy and their legal implications", in GUTWIRTH, S., LEENES, R., DE HERT, P. and POULLET, Y., *European data protection: coming of age*, Dordrecht, Springer, 2013, 133; B. VAN ALSENOY, "The evolving role of the individual under EU data protection law", *ICRI Working Paper* 23/2015, 24; U. VOLOVELSKY, "Civilian uses of unmanned aerial vehicles and the threat to the right to privacy – An Israeli case study", *Computer Law & Security Review* 2014, 314.

[150] S.E. KREPS, *Drones: What everyone needs to know*, New York, Oxford University Press, 2016, 122; U. VOLOVELSKY, "Civilian uses of unmanned aerial vehicles and the threat to the right to privacy – An Israeli case study", *Computer Law & Security Review* 2014, 314.

[151] L. CHANG, "How easy is it to hijack a drone?", *Digital Trends* 2 March 2016; A. HERN, "Skateboards, drones and your brain: everything got hacked", *The Guardian* 11 August 2015; U. VOLOVELSKY, "Civilian uses of unmanned aerial vehicles and the threat to the right to privacy – An Israeli case study", *Computer Law & Security Review* 2014, 314; X., *Wat met hacking van drones?,* www.privacycommission.be.

1. Consent to use information

56. CONSENT – The data subject's control and consent as a legal ground for data processing became a key issue in data protection legislation.[152] The Article 29 Data Protection Working Party has stated in an opinion that the notion of consent is traditionally linked with the idea that the data subject should be in control of the use that is being made of his personal data and his consent hereto must be given freely.[153] The role of consent was explicitly recognised in article 8(2) of the EU Charter of Fundamental Rights and article 5(3) of the Data Protection Directive as an essential element of the protection of personal data.[154] However, consent has not been deemed as the only legal ground enabling personal data processing operations.[155]

[152] P. DE HERT and V. PAPAKONSTANTINOU, "The Council of Europe data protection convention reform: analysis of the new text and critical comment on its global ambition", *Computer Law & Security Review* 2014, 637; N.N. GOMES DE ANDRADE and S. MONTELEONE, "Digital natives and the metamorphosis of the European information society. The emerging behavioral trends regarding privacy and their legal implications", in GUTWIRTH, S., LEENES, R., DE HERT, P. and POULLET, Y., *European data protection: coming of age*, Dordrecht, Springer, 2013, 135; A. KISS and G.L. SZOKE, "Evolution of revolution? Steps forward to a new generation of data protection regulation", in S. GUTWIRTH, R. LEENES and P. DE HERT, *Reforming European data protection law: Issues in privacy and data protection*, Dordrecht, Springer, 2015, 315; G. SKOUMA and L. LÉONARD, "On-line behavioral tracking: what may change after the legal reform on personal data protection", in S. GUTWIRTH, R. LEENES and P. DE HERT, *Reforming European data protection law*, Dordrecht, Springer, 2015, 48.

[153] Opinion 15/2011 on the definition of consent, Article 29 Data Protection Working Party, 01197/11/EN, WP 187, 13 July 2011, 8; A. ALEMANNO and A.L. SIBONY, *Nudge and the law: a European perspective*, Oxford, Hart Publishing, 2015, 195; N.N. GOMES DE ANDRADE and S. MONTELEONE, "Digital natives and the metamorphosis of the European information society. The emerging behavioral trends regarding privacy and their legal implications", in GUTWIRTH, S., LEENES, R., DE HERT, P. and POULLET, Y., *European data protection: coming of age*, Dordrecht, Springer, 2013, 135; A. KISS and G.L. SZOKE, "Evolution of revolution? Steps forward to a new generation of data protection regulation", in S. GUTWIRTH, R. LEENES and P. DE HERT, *Reforming European data protection law: Issues in privacy and data protection*, Dordrecht, Springer, 2015, 315.

[154] Opinion 15/2011 on the definition of consent, Article 29 Data Protection Working Party, 01197/11/EN, WP 187, 13 July 2011, 5; G. SKOUMA and L. LÉONARD, "On-line behavioral tracking: what may change after the legal reform on personal data protection", in S. GUTWIRTH, R. LEENES and P. DE HERT, *Reforming European data protection law*, Dordrecht, Springer, 2015, 48.

[155] Opinion 15/2011 on the definition of consent, Article 29 Data Protection Working Party, 01197/11/EN, WP 187, 13 July 2011, 5-6; P. DE HERT and V. PAPAKONSTANTINOU, "The Council of Europe data protection convention reform: analysis of the new text and critical comment on its global ambition", *Computer Law & Security Review* 2014, 637; A. KISS and G.L. SZOKE, "Evolution of revolution? Steps forward to a new generation of data protection regulation", in S. GUTWIRTH, R. LEENES and P. DE HERT, *Reforming European data protection law: Issues in privacy and data protection*, Dordrecht, Springer, 2015, 315; E. KOSTA, *Consent in European data protection law*, Leiden, Martinus Nijhoff Publishers, 2013, 229; A. MURRAY, *Information technology law: the law and society*, Oxford, Oxford University Press, 2013, 526.

The EU Charter also explicitly recognises that the law may lay down other legitimate grounds, which is the case in article 7 of Directive 95/46/EC.[156] Personal data processing may only take place if one of the six legal grounds conditions is met, of which consent is mentioned as one of them, since the legal grounds are enumerated by using 'or'.[157] If no consent or one of the other legal grounds is present, then no personal data processing may take place because no lawful basis for the processing of the data is established.[158] But even when the aims of a data processing are legitimate according to article 7 of the Directive, it will only be legal if the data collected is processed in line with the article 6 requirements.[159] This leads to the conclusion that the article 6 principles are predominant, which implies a reduction of the importance of consent in data protection issues to its real proportions, namely to one of the six possibilities listed in article 7 of the Directive that make a data processing legitimate.[160] In other words, Directive 95/46/EC recognizes the legitimate interest of the data controller as a possible justification for the processing of personal data, so no principle of a data subject's consent exists.[161]

---

[156] Opinion 15/2011 on the definition of consent, Article 29 Data Protection Working Party, 01197/11/EN, WP 187, 13 July 2011, 6; A. ALEMANNO and A.L. SIBONY, *Nudge and the law: a European perspective*, Oxford, Hart Publishing, 2015, 184; P. DE HERT and V. PAPAKONSTANTINOU, "The Council of Europe data protection convention reform: analysis of the new text and critical comment on its global ambition", *Computer Law & Security Review* 2014, 637.

[157] A. ALEMANNO and A.L. SIBONY, *Nudge and the law: a European perspective*, Oxford, Hart Publishing, 2015, 184; P. BOILLAT and M. KJAERUM, *Handbook on European data protection law*, http://www.echr.coe.int, 2014, 57; P. DE HERT and V. PAPAKONSTANTINOU, "The Council of Europe data protection convention reform: analysis of the new text and critical comment on its global ambition", *Computer Law & Security Review* 2014, 638.

[158] A. ALEMANNO and A.L. SIBONY, *Nudge and the law: a European perspective*, Oxford, Hart Publishing, 2015, 186; P. DE HERT and V. PAPAKONSTANTINOU, "The Council of Europe data protection convention reform: analysis of the new text and critical comment on its global ambition", *Computer Law & Security Review* 2014, 638.

[159] *Supra* 15-16, nr. 19-21; P. DE HERT and V. PAPAKONSTANTINOU, "The Council of Europe data protection convention reform: analysis of the new text and critical comment on its global ambition", *Computer Law & Security Review* 2014, 638; S. GUTWIRTH, "Short statement about the role of consent in the European data protection directive", http://works.bepress.com/serge_gutwirth 2012, 2.

[160] S. GUTWIRTH, "Short statement about the role of consent in the European data protection directive", http://works.bepress.com/serge_gutwirth 2012, 3; P. DE HERT and S. GUTWIRTH, "Data protection in the case law of Strasbourg and Luxembourg: constitutionalisation in action", in S. GUTWIRTH, Y. POULLET, P. DE HERT, C. DE TERWANGNE and S. NOUWT, *Reinventing data protection?*, Berlin, Springer, 2009, 32-33.

[161] CJEU 11 December 2014, C-212/13, Ryneš/Office for Personal Data Protection, §11-12; P. BOILLAT and M. KJAERUM, *Handbook on European data protection law*, http://www.echr.coe.int, 2014, 57; B. VAN ALSENOY, "The evolving role of the individual under EU data protection law", *ICRI Working Paper* 23/2015, 11.

57. CONSENT DATA SUBJECT – Prior consent may thus be needed as a legal ground for processing data, of the person who is subject to the data information retention.[162] However, some difficulties arise both on the side of the person needing to give consent as well as on the side of the person needing the consent to be able to use the information when that data is collected via camera-equipped drones.

1.1 Person needing to give consent

58. GIVING CONSENT – Data subjects should be given some information, namely the identity of the controller of the drone and of his representative, the purposes of the processing for which the data is collected, and any further information such as the categories of data, recipients or categories of recipients of the data, the existence of the right of access to and the right to specify and correct the data concerning the subject.[163] However, even though the information must be provided, in practice it remains difficult for the person needing to give the consent to know when he is being filmed and by whom.[164] It is easier when it concerns CCTV, since persons or companies using CCTV are obliged to warn the public in a general context that they are being filmed.[165] On the same warning, they are also obliged to formulate contact details to make it possible for the subject that is being filmed to object against the use of their information.

---

[162] A. ALEMANNO and A.L. SIBONY, *Nudge and the law: a European perspective*, Oxford, Hart Publishing, 2015, 184; R.L. FINN, D. WRIGHT, L. JACQUES and P. DE HERT, "Study on privacy, data protection and ethical risks in civil Remotely Piloted Aircraft Systems operations – final report", http://ec.europa.eu 2014, 8; G. SKOUMA and L. LÉONARD, "On-line behavioral tracking: what may change after the legal reform on personal data protection", in S. GUTWIRTH, R. LEENES and P. DE HERT, *Reforming European data protection law*, Dordrecht, Springer, 2015, 48; P. BOILLAT and M. KJAERUM, *Handbook on European data protection law*, http://www.echr.coe.int, 2014, 57.

[163] Opinion 01/2015 on privacy and data protection issues relating to the utilisation of drones, Article 29 Data Protection Working Party, 01673/15/EN, WP 231, 16 June 2015, 15; P. BOILLAT and M. KJAERUM, *Handbook on European data protection law*, http://www.echr.coe.int, 2014, 59; E. KOSTA, *Consent in European data protection law*, Leiden, Martinus Nijhoff Publishers, 2013, 202.

[164] P. BOILLAT and M. KJAERUM, *Handbook on European data protection law*, http://www.echr.coe.int, 2014, 59; S. NOUWT, B.R. DE VRIES and C. PRINS, *Reasonable expectations of privacy? Eleven country reports on camera surveillance and workplace privacy*, Den Haag, TMC Asser Press, 2005, 105.

[165] R.W. BELLABY, *The ethics of intelligence: A new framework*, New York, Routledge, 2014, 62; S. NOUWT, B.R. DE VRIES and C. PRINS, *Reasonable expectations of privacy? Eleven country reports on camera surveillance and workplace privacy*, Den Haag, TMC Asser Press, 2005, 103-104.

However, since the technology of drones is advanced in such a way that it sometimes may be impossible to see or even hear them, the public does not always know if and when they are being filmed, as well as by whom they are being filmed.[166] It is therefor impossible for them to object against the use of their information.

1.2. Person needing consent for data processing

59. OBTAINING CONSENT – On the other hand, the person or organisation that owns the camera-equipped drone needs the consent of the data subjects on the footage.[167] This may be difficult to obtain, especially *a priori*, since people are often being filmed by coincidence and they are not intended to be the main subject of the footage, or the data controller and processor may be many kilometers away from the area that is being filmed.[168] However, as mentioned before, consent is not always necessary to be obtained when the data controller can prove that another legitimate ground is present.[169] For example, the domestic use of surveillance drones may be legitimate on the ground of article 7(f) of the Directive 95/46/EC, if the data controller were to prove that the processing of personal data is in his legitimate interest. [170] In order for this ground for processing to apply, that legitimate interest must be weighed against the interests for fundamental rights and freedoms of the data subject.[171]

---

[166] R.W. BELLABY, *The ethics of intelligence: A new framework*, New York, Routledge, 2014, 62; S. CURTIS, "Drone laws in the UK – what are the rules?", *The Guardian* 18 April 2016; B. SCHERMER, "An eye in the sky: privacy aspects of drones", *Criminal Law and Criminology* 20 June 2013.

[167] Opinion 15/2011 on the definition of consent, Article 29 Data Protection Working Party, 01197/11/EN, WP 187, 13 July 2011, 4; P. BOILLAT and M. KJAERUM, *Handbook on European data protection law*, http://www.echr.coe.int, 2014, 56; X., *Legal matters and obtaining consent*, www.andfestival.org.uk.

[168] ICO, *In the picture: A data protection code of practice for surveillance cameras and personal information*, https://ico.org.uk 2015, 30; T. WESSING, "Drones and data", united-kingdom.taylorwessing.com March 2015.

[169] *Supra* 37, nr. 56; Opinion 15/2011 on the definition of consent, Article 29 Data Protection Working Party, 01197/11/EN, WP 187, 13 July 2011, 7; E. KOSTA, *Consent in European data protection law*, Leiden, Martinus Nijhoff Publishers, 2013, 229.

[170] Article 7(f) Data Protection Directive 95/46/EC; S. PEERS, T. HERVEY, J. KENNER and A. WARD, *The EU charter of fundamental rights: A commentary*, Oxford, Hart Publishing, 2014, 252; J. TERSTEGGE, "Privacy in the law", in M. PETKOVIĆ and W. JONKER, *Security, privacy, and trust in modern data management*, Berlin, Springer, 2007, 13.

[171] S. PEERS, T. HERVEY, J. KENNER and A. WARD, *The EU charter of fundamental rights: A commentary*, Oxford, Hart Publishing, 2014, 252; J. TERSTEGGE, "Privacy in the law", in M. PETKOVIĆ and W. JONKER, *Security, privacy, and trust in modern data management*, Berlin, Springer, 2007, 13.

In this example, a balancing act thus needs to be done between the right of the controller to protect one's own private property and the right of privacy of the data subject whose personal data is being collected. Moreover, the data controller must also adhere to the requirements mentioned in article 6 of the Directive 95/46/EC.[172]

2. Solutions

60. SOLUTIONS – The general solution to make it easier to comply to the consent requirement is to make it obligatory for companies to put their logo on the drones, so that the public knows who they need to contact to object.[173] However, civilian users will not have logos, and there is of course also the problem of invisible and inaudible drones. Another possible solution, which can also be applied to civilian users, is the obligation of license plates for every drone, so that complaints can be made by giving the license plate of the drone that invaded a person's privacy to an organisation that administers the license applications.[174] However, also here the main problem remains the invisibility and inaudibility of many drones.

[172] *Supra* 15-16, nr. 19-21; Opinion 15/2011 on the definition of consent, Article 29 Data Protection Working Party, 01197/11/EN, WP 187, 13 July 2011, 6.
[173] Opinion 01/2015 on privacy and data protection issues relating to the utilisation of drones, Article 29 Data Protection Working Party, 01673/15/EN, WP 231, 16 June 2015, 15; D. KLITOU, *Privacy-invading technologies and privacy by design*, The Hague, Asser Press, 2014, 240.
[174] Opinion 01/2015 on privacy and data protection issues relating to the utilisation of drones, Article 29 Data Protection Working Party, 01673/15/EN, WP 231, 16 June 2015, 15; C. DE LOOPER, "License plates for drones will make drone operators accountable for their actions", *Tech Times* 22 August 2015; T. SIMONITE, "Drones could make rogue operators accountable", *MIT Technology Review* 18 August 2015.

§3 For privacy purposes vs. for surveillance purposes

61. REGULATION UAVs – The numerous uses that can be made of UAVs and the relevant concerns regarding privacy and surveillance demonstrate that the use of these devices needs to be regulated. However, technology is developing at a faster pace than lawmakers and courts can regulate.[175] The question then arises whether the development of technology should be permitted, since it clearly seems to threaten our privacy.[176] However, it is impossible to stop this fast-developing technology and the right to privacy is not absolute, therefor it might be advised to control new technologies and to introduce very tight regulatory regimes wherein drones can only be used in socially acceptable applications.[177] Important documents regulating drones are: on the international level the Chicago Convention on International Civil Aviation and advices from the International Civil Aviation Organisation (ICAO), a UN body that oversees the development of air transport, on European level the opinions of the Data Protection Working Party and case law, and on national level the Belgian Royal Decree on RPAS, the '*Privacywet'* and the '*Camerawet'*, the UK Air Navigation Order 2009 and guidance from the UK CAA, the Data Protection Act 1998 and the CCTV Surveillance and Privacy Legislation, and the US amendments to the constitution, the FAA Regulations and the Drone Aircraft Privacy and Transparency Act of 2015, which will be discussed in following paragraphs.

[175] H.B. FÄRBER, "Eyes in the sky & privacy concerns on the ground", *Scitech Lawyer* 2015, 6; A. KISS and G.L. SZOKE, "Evolution of revolution? Steps forward to a new generation of data protection regulation", in S. GUTWIRTH, R. LEENES and P. DE HERT, *Reforming European data protection law: Issues in privacy and data protection*, Dordrecht, Springer, 2015, 316; U. VOLOVELSKY, "Civilian uses of unmanned aerial vehicles and the threat to the right to privacy – An Israeli case study", *Computer Law & Security Review* 2014, 312.

[176] K.K. STYLIANOU, "Hasta la vista privacy, or how technology terminated privacy", in C. AKRIVOPOULOU and A.E. PSYGKAS, *Personal data privacy and protection in a surveillance era: technologies and practices*, New York, Information Science Reference 2011, 51; D. WRIGHT, "Drones: Regulatory challenges to an incipient industry", *Computer Law & Security Review* 2014, 226.

[177] K.K. STYLIANOU, "Hasta la vista privacy, or how technology terminated privacy", in C. AKRIVOPOULOU and A.E. PSYGKAS, *Personal data privacy and protection in a surveillance era: technologies and practices*, New York, Information Science Reference 2011, 45; U. VOLOVELSKY, "Civilian uses of unmanned aerial vehicles and the threat to the right to privacy – An Israeli case study", *Computer Law & Security Review* 2014, 319; D. WRIGHT, "Drones: Regulatory challenges to an incipient industry", *Computer Law & Security Review* 2014, 226 and 229.

A. For privacy purposes

62. PRIVATE PURPOSES – As seen in Chapter 1 of this master thesis, the concept of privacy cannot be exactly defined, however this does not necessarily have to be a negative given.[178] An imprecise conceptualisation of privacy might be recommended to maintain a fluidity making it possible for new dimensions of privacy to be identified, understood and addressed in order to be able to respond to rapidly evolving technologies, like for example drones.[179]

1. International legal framework

63. INTERNATIONAL LEGAL FRAMEWORK – At international level, drones fall under the provisions of the Convention on International Civil Aviation. It will be discussed in the following paragraph whether it can give an adequate level of clarity which is needed in drone regulation.

1.1 The Chicago Convention

64. CHICAGO CONVENTION – The Convention on International Civil Aviation, also known as the Chicago Convention, sets out the context for regulation within the individual countries.[180] A UN organisation called the ICAO is responsible to promote the safe and orderly development of international civil aviation throughout the world via standards and recommended practices.[181]

---

[178] *Supra* 2, nr. 2 etc.
[179] R.L. FINN, D. WRIGHT and M. FRIEDEWALD, "Seven types of privacy", in S. GUTWIRTH, R. LEENES, P. DE HERT and Y. POULLET, *European data protection: coming of age*, Dordrecht, Springer, 2013, 4; B. PRENEEL, P. ROGAWAY, M.D. RYAN and P.Y.A. RYAN, "Privacy and security in an age of surveillance", drops.dagstuhl.de 2014 112.
[180] Convention on International Civil Aviation, *UNTS* 7 December 1944, 15-295 (hereafter: Chicago Convention); R. CLARKE and L.B. MOSES, "The regulation of civilian drones' impacts on public safety", *Computer Law & Security Review* 2014, 272; D. MACKENZIE, *ICAO: A history of the International Civil Aviation Organization*, Toronto, University of Toronto Press Incorporated, 2010, 52.
[181] R. CLARKE and L.B. MOSES, "The regulation of civilian drones' impacts on public safety", *Computer Law & Security Review* 2014, 272; D. MACKENZIE, *ICAO: A history of the International Civil Aviation Organization*, Toronto, University of Toronto Press Incorporated, 2010, 53; A. ZAVRŠNIK, *Drones and unmanned aerial systems: legal and social implications for security and surveillance*, Heidelberg, Springer, 2016, 13.

However, aviation regulation has been primarily concerned with piloted aircraft and not so much with unmanned aircrafts. The Chicago Convention states that regulation regarding unmanned aircrafts should be managed by national laws, which should provide for special authorization when a pilotless aircraft wants to fly over the territory of a contracting State.[182] The international framework for drone regulation is however incomplete and immature, and thus it is more advisable to look at the relevant legislation on European and national level, both for privacy as for surveillance purposes.[183]

2. European legal framework

65. EUROPEAN LEGAL FRAMEWORK – At European level, the Article 29 DPWP has issued an opinion on the utilisation of drones and which effects it may have on privacy and data protection of individuals. The applicable law is the Data Protection Directive 95/46/EC, but also national authorities of civil aviation play an important role in minimizing the privacy and data protection risks following the use of drones.

2.1 Opinion 01/2015 of the Art. 29 DPWP

66. OPINION 01/2015 – Opinion 01/2015 on the privacy and data protection issues relating to the utilisation of drones of the Art. 29 DPWP provides guidelines in order to be able to correctly address the data protection rules in the context of drones.[184] The relevant legal framework on the use of drones in Member States is made up by the Data Protection Directive 95/46/EC.[185]

---

[182] Art. 8 Chicago Convention; R. CLARKE and L.B. MOSES, "The regulation of civilian drones' impacts on public safety", *Computer Law & Security Review* 2014, 272; D. WRIGHT, "Drones: Regulatory challenges to an incipient industry", *Computer Law & Security Review* 2014, 227.
[183] R. CLARKE and L.B. MOSES, "The regulation of civilian drones' impacts on public safety", *Computer Law & Security Review* 2014, 273.
[184] Opinion 01/2015 on privacy and data protection issues relating to the utilisation of drones, Article 29 Data Protection Working Party, 01673/15/EN, WP 231, 16 June 2015, 3; A. ZAVRŠNIK, *Drones and unmanned aerial systems: legal and social implications for security and surveillance*, Heidelberg, Springer, 2016, 262.
[185] *Supra* 12-13, nr. 17; Communication from the Commission to the European Parliament and the Council, "A new era for aviation: opening the aviation market to the civil use of remotely piloted aircraft systems in a safe and sustainable manner", COM(2014) 207, 7-8; Opinion 01/2015 on privacy and data protection issues relating to the utilisation of drones, Article 29 Data Protection Working Party, 01673/15/EN, WP 231, 16 June 2015, 8; R.L. FINN, D. WRIGHT, L. JACQUES and P. DE HERT,

Pursuant to article 3(2) of that Directive, the processing of personal data by a natural person in the course of a purely personal or household activity is exempted and is thus permitted.[186] However, when the personal data is published on the internet and the data has been made accessible to an indefinite number of people, this exemption will not apply.[187] This is also the case when drones give rise to a video surveillance system in a way that it involves the constant recording and storage of personal data.[188]

67. APPLICABLE LAW – In accordance with article 6 of the Data Protection Directive 95/46/EC, personal data must be collected for specified, explicit and legitimate purposes and may not further be processed in a way incompatible with those purposes.[189] Applied to drones, this has as a result that when a drone operation involves the processing of personal data, this should comply with applicable law in general, safeguarding personal rights, image, family life and the private sphere, including national regulations on CCTV and the use of drones.[190]

"Study on privacy, data protection and ethical risks in civil Remotely Piloted Aircraft Systems operations – final report", http://ec.europa.eu 2014, 6; B. VAN ALSENOY, "The evolving role of the individual under EU data protection law", *ICRI Working Paper* 23/2015, 24-25; A. ZAVRŠNIK, *Drones and unmanned aerial systems: legal and social implications for security and surveillance*, Heidelberg, Springer, 2016, 115.

[186] Opinion 01/2015 on privacy and data protection issues relating to the utilisation of drones, Article 29 Data Protection Working Party, 01673/15/EN, WP 231, 16 June 2015, 9; B.H.M. CUSTERS, J.J. OERLEMANS en S.J. VERGOUW, *Het gebruik van drones: een verkennend onderzoek naar onbemande luchtvaartuigen*, Meppel, Boom Lemma Uitgevers, 2015, 127; E. KOSTA, *Consent in European data protection law*, Leiden, Martinus Nijhoff Publishers, 2013, 229.

[187] CJEU 6 November 2003, C-101/01, Lindqvist, §47; Opinion 01/2015 on privacy and data protection issues relating to the utilisation of drones, Article 29 Data Protection Working Party, 01673/15/EN, WP 231, 16 June 2015, 9; E. KOSTA, *Consent in European data protection law*, Leiden, Martinus Nijhoff Publishers, 2013, 229; B. VAN ALSENOY, "The evolving role of the individual under EU data protection law", *ICRI Working Paper* 23/2015, 25.

[188] Opinion 01/2015 on privacy and data protection issues relating to the utilisation of drones, Article 29 Data Protection Working Party, 01673/15/EN, WP 231, 16 June 2015, 9; B. VAN ALSENOY, "The evolving role of the individual under EU data protection law", *ICRI Working Paper* 23/2015, 25.

[189] *Supra* 15, nr. 20; Opinion 01/2015 on privacy and data protection issues relating to the utilisation of drones, Article 29 Data Protection Working Party, 01673/15/EN, WP 231, 16 June 2015, 13.

[190] Opinion 01/2015 on privacy and data protection issues relating to the utilisation of drones, Article 29 Data Protection Working Party, 01673/15/EN, WP 231, 16 June 2015, 13.

68. CAA – National Civil Aviation Authorities or CAAs play an important role in certifying drone operators and licensing drone pilots in order to aim to address privacy or data protection aspects related to the use of drones.[191] In most countries, certifications or authorisations which regulate the use of civil drones are granted by CAAs.

3. Belgian legal framework

69. BELGIAN LEGAL FRAMEWORK – In Belgium, the legislation that is important for addressing the privacy risks that follow out of the use of drones, is the general *Privacywet*.[192] Also a Royal Decree has been recently adopted, dividing drone users into different categories and indicating the requirements that should be met. Both will be discussed in the following paragraphs.

3.1 Privacywet

70. PRIVACYWET – The *Privacywet* is applicable to every complete or partial automated processing of personal data, and to every non-automated processing of personal data that is preserved in a filing system or that is intended to form a part thereof.[193] Camera-equipped drones and every other drone equipped with other instruments that are capable to collect any type of information on an individual, will be considered to be automated processing of data.[194] When that data can be qualified as personal data, then the *Privacywet* will be applicable.

[191] Opinion 01/2015 on privacy and data protection issues relating to the utilisation of drones, Article 29 Data Protection Working Party, 01673/15/EN, WP 231, 16 June 2015, 17; R. ABEYRATNE, *Convention on International Civil Aviation: A commentary*, Cham, Springer, 2014, 423.
[192] Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, *BS* 18 maart 1993 (hereafter: *Privacywet*).
[193] Art. 3 *Privacywet*; F. ROBBEN, "De wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens: toepassingsgebied en begripsdefinities", *www.frankrobben.be* 1994, 1.
[194] X., *Is de Privacywet van toepassing op de informatie die drones verwerken?*, www.privacycommission.be.

According to article 1, §1 of the *Privacywet*, data is considered to be personal data when it contains information about an identified or identifiable natural person by means of an identification number or one or more specific elements that characterise the individual's physical, physiological, psychological, economic, cultural or social identity.[195] The Privacy Commission has confirmed that the *Privacywet* is applicable to camera-equipped drones because it can collect images of persons and of their goods, making it a realistic possibility there is processing of personal data.[196]

3.2 Royal Decree on the use of RPAS in the Belgian Airspace

71. ROYAL DECREE – The Royal Decree on the use of UAVs in the Belgian Airspace makes a distinction between the professional and civil use of drones.[197] When the drone is professionally used, two categories exist. Category 1 is the professional use of drones that weigh between 0 and 150 kg and cannot fly higher than 300 feet resp. 91,5 meters.[198] Pilots will need to obtain a flight brevet, must be at least 18 years old and must register their drones.[199] Category 2 is the professional use of drones that weigh less than 5 kg and cannot fly higher than 150 feet resp. 46 meters.[200] Pilots will have to obtain an attest, must be at least 16 years old and must also register their drones.

---

[195] R.L. FINN, D. WRIGHT, L. JACQUES and P. DE HERT, "Study on privacy, data protection and ethical risks in civil Remotely Piloted Aircraft Systems operations – final report", http://ec.europa.eu 2014, 11; N.N. GOMES DE ANDRADE, "The right to privacy and the right to identity in the age of ubiquitous computing: friends or foes? A proposal towards a legal articulation", in C. AKRIVOPOULOU and A.E. PSYGKAS, *Personal data privacy and protection in a surveillance era: technologies and practices*, New York, Information Science Reference 2011, 33; G. GONZALEZ FUSTER, *The emergence of personal data protection as a fundamental right of the EU*, Dordrecht, Springer, 2014, 34; F. ROBBEN, "De wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens: toepassingsgebied en begripsdefinities", *www.frankrobben.be* 1994, 4.

[196] X., *Is de Privacywet van toepassing op de informatie die drones verwerken?*, www.privacycommission.be.

[197] Koninklijk Besluit van 10 april 2016 met betrekking tot het gebruik van op afstand bestuurde luchtvaartuigen in het Belgisch luchtruim, *BS* 15 april 2016 (hereafter: Royal Decree on drones); F. BRUGGEMAN, "Wettelijke regeling voor drones is klaar", *De Redactie* 31 maart 2015; X., *Het Belgisch Koninklijk Besluit werd zopas gepubliceerd!*, www.drone-kopen.be; X., *Minister Galant heeft aangepast KB Drones rond*, www.drone-kopen.be.

[198] Art. 13, §2 Royal Decree on Drones; F. BRUGGEMAN, "Wettelijke regeling voor drones is klaar", *De Redactie* 31 maart 2015; X., *Overzicht van de drone wetgeving in België*, www.droneblog.be.

[199] Art. 17, §2 Royal Decree on Drones; X., *Het Belgisch Koninklijk Besluit werd zopas gepubliceerd!*, www.drone-kopen.be; X., *Overzicht van de drone wetgeving in België*, www.droneblog.be.

[200] Art. 13, §1 Royal Decree on Drones; X., *Het Belgisch Koninklijk Besluit werd zopas gepubliceerd!*, www.drone-kopen.be; X., *Overzicht van de drone wetgeving in België*, www.droneblog.be.

The civil use of drones is allowed as long as they fly above private property, when necessary with the approval of the owner, not higher than 33 feet resp. 10 meters and with a drone that weighs less than 1 kg.[201] No education, registration or attest is necessary for this private use.[202]

4. UK legal framework

72. UK LEGAL FRAMEWORK – The UK was compelled by European principles to implement a level of protection for the privacy and data protection rights of individuals. They have done so by adapting their notion of breach of confidence and by implementing a Data Protection Act, which both can be applied to the use of drones. Furthermore, they have also issued a Dronecode and a UK Air Navigation Order, which may be applicable to drones as well.

4.1 Breach of Confidence

73. BREACH OF CONFIDENCE – In *Wainwright v Home Office*, the House of Lords held that there is no general right of privacy in the UK.[203] However, the influence of article 8 ECHR has forced the UK courts to broaden the scope of the cause of action for breach of confidence.[204]

---

[201] Art. 3, §2 Royal Decree on Drones; F. BRUGGEMAN, "Wettelijke regeling voor drones is klaar", *De Redactie* 31 maart 2015; X., *Het Belgisch Koninklijk Besluit werd zopas gepubliceerd!*, www.drone-kopen.be; X., *Overzicht van de drone wetgeving in België*, www.droneblog.be.

[202] X., *Het Belgisch Koninklijk Besluit werd zopas gepubliceerd!*, www.drone-kopen.be; X., *Minister Galant heeft aangepast KB Drones rond*, www.drone-kopen.be; X., *Overzicht van de drone wetgeving in België*, www.droneblog.be.

[203] House of Lords, UKHL 53 (2003), Wainwright/Home Office; P. CAREY, *E-privacy and online data protection*, Amsterdam, LexisNexis, 2002, 3; S. NOUWT, B.R. DE VRIES and C. PRINS, *Reasonable expectations of privacy? Eleven country reports on camera surveillance and workplace privacy*, Den Haag, TMC Asser Press, 2005, 108; X., *What do I need to know about the right to privacy?*, http://findlaw.co.uk; K.S. ZIEGLER, *Human rights and private law: Privacy as autonomy*, Oregon, Hart Publishing, 2007, 41.

[204] M. RICHARDSON, M. BRYAN, M. VRANKEN and K. BARNETT, *Breach of confidence: social origins and modern developments*, Cheltenham, Edward Elgar Publishing Limited, 2012, 126; X., *What do I need to know about the right to privacy?*, http://findlaw.co.uk; K.S. ZIEGLER, *Human rights and private law: Privacy as autonomy*, Oregon, Hart Publishing, 2007, 43.

This cause of action can be said to come closest to a right of privacy in the UK under the form of misuse of private information.[205] To bring a claim for misuse of confidential information, the claimant must prove that he had a reasonable expectation of privacy in relation to the personal information in question, which must be private and not public.[206] The use of camera-equipped drones brings about privacy risks for other individuals and thus might constitute a breach of confidence when the collected private personal data is misused.[207]

4.2 Data Protection Act 1998

74. DPA '98 – The Data Protection Act 1998 sets out some principles which have to be complied with when collecting, storing, retrieving or organising personal data, such as measures that have to be taken against unlawful processing of personal data and the principle not to keep the collected personal data for longer than necessary to fulfil the purposes for which it was collected.[208] These principles apply to any collection of personal information, including drone footage.[209] The Data Protection Act is thus applicable to drones equipped with cameras. Besides these principles, the DPA also provides rights for the data subjects, such as the right to prevent others from using your personal data in a way that causes damage.[210]

---

[205] D. BUTLER, "The dawn of the age of the drones – an Australian privacy law perspective", *UNSW Law Journal* 2014, 449; M. RICHARDSON, M. BRYAN, M. VRANKEN and K. BARNETT, *Breach of confidence: social origins and modern developments*, Cheltenham, Edward Elgar Publishing Limited, 2012, 126; X., *What do I need to know about the right to privacy?*, http://findlaw.co.uk; K.S. ZIEGLER, *Human rights and private law: Privacy as autonomy*, Oregon, Hart Publishing, 2007, 204.

[206] ECtHR 28 January 2003, nr. 44647/98, Peck/United Kingdom, §58; V. KOSTA, *Fundamental rights in EU internal market legislation*, Oxford, Hart Publishing, 2015, 92; S. NOUWT, B.R. DE VRIES and C. PRINS, *Reasonable expectations of privacy? Eleven country reports on camera surveillance and workplace privacy*, Den Haag, TMC Asser Press, 2005, 109; X., *What do I need to know about the right to privacy?*, http://findlaw.co.uk; K.S. ZIEGLER, *Human rights and private law: Privacy as autonomy*, Oregon, Hart Publishing, 2007, 197.

[207] D. BUTLER, "The dawn of the age of the drones – an Australian privacy law perspective", *UNSW Law Journal* 2014, 449; ICO, *Drones*, https://ico.org.uk.

[208] P. CAREY, *E-privacy and online data protection*, Amsterdam, LexisNexis, 2002, 10; I. KROENER, *CCTV: A technology under the radar*?, Surrey, Ashgate Publishing Limited, 2014, 106; J. WADHAM, K. HARRIS and G. PERETZ, *Blackstone's guide to the Freedom of Information Act 2000*, Oxford, Oxford University Press, 2011, 98; T. WESSING, "Drones and data", united-kingdom.taylorwessing.com March 2015; X., *What do I need to know about the right to privacy?*, http://findlaw.co.uk.

[209] ICO, *Drones*, https://ico.org.uk; ICO, *CCTV*, https://ico.org.uk; T. WESSING, "Drones and data", united-kingdom.taylorwessing.com March 2015.

[210] I. KROENER, *CCTV: A technology under the radar*?, Surrey, Ashgate Publishing Limited, 2014, 106; J. WADHAM, K. HARRIS and G. PERETZ, *Blackstone's guide to the Freedom of Information Act 2000*,

4.3 Dronecode

75. DRONECODE – The Dronecode is a safety guide issued by the UK CAA for consumers wanting to use a drone in the UK.[211] Some simple steps are enumerated to ensure that the consumer is flying the drone safely and legally, such as for example the consumer has to make sure that he can see the drone at all times and keep it away from airports and airfields.[212] It is also expressed that failure to comply with the applicable legislation may lead to criminal prosecutions, as well as the obligation to take into account privacy laws as they may be infringed upon when images are obtained with a drone.[213]

4.4 UK Air Navigation Order 2009

76. UK AIR NAVIGATION ORDER – The principal order regarding aircrafts currently in force in the UK is the Air Navigation Order 2009, which establishes a system for the mandatory marking and registration of an aircraft and for the certification and licensing of aircraft worthiness.[214] Article 10 of the UK Air Navigation Order states that an aircraft, other than those that may fly without being registered, must have the nationality and registration marks painted or fixed thereon as required by the law of the country in which it is registered.[215]

Oxford, Oxford University Press, 2011, 101; X., *What do I need to know about the right to privacy?*, http://findlaw.co.uk.

[211] T. WESSING, "Drones and data", united-kingdom.taylorwessing.com March 2015; X., *Flying drones: guidance on the safety rules that apply when flying unmanned and model aircraft*, http://www.caa.co.uk; A. ZAVRŠNIK, *Drones and unmanned aerial systems: legal and social implications for security and surveillance*, Heidelberg, Springer, 2016, 263.

[212] X., *Flying drones: guidance on the safety rules that apply when flying unmanned and model aircraft*, http://www.caa.co.uk; A. ZAVRŠNIK, *Drones and unmanned aerial systems: legal and social implications for security and surveillance*, Heidelberg, Springer, 2016, 263.

[213] CAA, *Droneaware*, http://publicapps.caa.co.uk; X., *Flying drones: guidance on the safety rules that apply when flying unmanned and model aircraft*, http://www.caa.co.uk.

[214] 7th Report of 2014-2015 on the Civilian use of drones in the EU, House of Lords, HL 122, 5 March 2015, 16; CAA, *Air navigation: The order and regulations*, https://publicapps.caa.co.uk; G. ODUNTAN, *Sovereignty and jurisdiction in the airspace and outer space: legal criteria for spatial delimitation*, Oxon, Routledge, 2012, 68.

[215] CAA, *Air navigation: The order and regulations*, https://publicapps.caa.co.uk; G. ODUNTAN, *Sovereignty and jurisdiction in the airspace and outer space: legal criteria for spatial delimitation*, Oxon, Routledge, 2012, 69.

Some provisions of the Air Navigation Order apply to all aircrafts, including UAVs, such as the obligation to not recklessly or negligently cause or permit an aircraft to endanger a person or property.[216] For small UAVs that weigh under 20 kilogram, the pilot is required to seek permission from the CAA for aerial surveillance or data gathering work.[217]

5. US legal framework

77. US LEGAL FRAMEWORK – The United States does not have a basic privacy law or specific federal legislation that addresses privacy concerns of civil drone use.[218] However, some political figures, administrative bodies and private interest groups have proposed technology bills that would encompass at least some of the privacy concerns related to drones in domestic airspace.[219] In this paragraph, it will first be investigated whether the Amendments to the Constitution are adequate to accommodate the privacy concerns related to the civil use of drones, as well as what case law has been decided upon this issue. Afterwards, the FAA Regulations will be discussed.

[216] 7th Report of 2014-2015 on the Civilian use of drones in the EU, House of Lords, HL 122, 5 March 2015, 16; CAA, *Air navigation: The order and regulations*, https://publicapps.caa.co.uk.
[217] Art. 166 UK Air Navigation Order 2009; 7th Report of 2014-2015 on the Civilian use of drones in the EU, House of Lords, HL 122, 5 March 2015, 17; CAA, *Air navigation: The order and regulations*, https://publicapps.caa.co.uk.
[218] Surveillance, ethics and privacy in civil applications", *Computer Law & Security Review* 2012, 88; C. SCHLAG, "The new privacy battle: how the expanding use of drones continues to erode our concept of privacy and privacy rights", *Journal of Technology, Law & Policy* 2013, 17.
[219] M.R. CALO, "The drone as privacy catalyst", *Stanford Law Review Online* 12 December 2011; G. MCNEAL, "Drones and aerial surveillance: considerations for legislators", *Brookings* November 2014, 3; C. SCHLAG, "The new privacy battle: how the expanding use of drones continues to erode our concept of privacy and privacy rights", *Journal of Technology, Law & Policy* 2013, 17.

5.1 Amendments to the US Constitution

78. FOURTH AMENDMENT – As is mentioned before, the Fourth Amendment guarantees a certain degree of privacy and prevents excessive government intrusion.[220] However, with the new emerging technologies, the capability of the Fourth Amendment to deal with these new issues have been subject to debate, since the founders could not have foreseen it in the protection they intended.[221] However, most UAV systems are not in general public use, so its use for surveillance purposes will fall under the Fourth Amendment when material is gathered from areas where individuals have a reasonable expectation of privacy.[222]

5.2 Case law

79. CASE LAW – Following *Katz v United States*, the Supreme Court covered the first aerial surveillance case in *California v Ciraolo,* wherein it was held that a warrantless aerial observation of a fenced-in backyard within the curtilage of a home was a reasonable search under the Fourth Amendment.[223]

[220] *Supra* 22, nr. 33; H.B. FÄRBER, "Eyes in the sky & privacy concerns on the ground", *Scitech Lawyer* 2015, 7; T.N. MCINNIS, *The evolution of the Fourth Amendment*, Plymouth, Lexington Books, 2010, 234; C. SCHLAG, "The new privacy battle: how the expanding use of drones continues to erode our concept of privacy and privacy rights", *Journal of Technology, Law & Policy* 2013, 12.

[221] US Supreme Court, 277 U.S. 438 (1928), Olmstead/United States; M.R. CALO, "The drone as privacy catalyst", *Stanford Law Review Online* 12 December 2011; C. SCHLAG, "The new privacy battle: how the expanding use of drones continues to erode our concept of privacy and privacy rights", *Journal of Technology, Law & Policy* 2013, 12-13.

[222] R.L. FINN and D. WRIGHT, "Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications", *Computer Law & Security Review* 2012, 192; S. NOUWT, B.R. DE VRIES and C. PRINS, *Reasonable expectations of privacy? Eleven country reports on camera surveillance and workplace privacy*, Den Haag, TMC Asser Press, 2005, 12.

[223] US Supreme Court, 476 U.S. 207 (1986), California/Ciraolo; M.R. CALO, "The drone as privacy catalyst", *Stanford Law Review Online* 12 December 2011; G. MCNEAL, "Drones and aerial surveillance: considerations for legislators", *Brookings* November 2014, 5; S. NOUWT, B.R. DE VRIES and C. PRINS, *Reasonable expectations of privacy? Eleven country reports on camera surveillance and workplace privacy*, Den Haag, TMC Asser Press, 2005, 12; C. SCHLAG, "The new privacy battle: how the expanding use of drones continues to erode our concept of privacy and privacy rights", *Journal of Technology, Law & Policy* 2013, 13.

Even though the observed area was private, the data subject's backyard was clearly visible and exposed to overhead flights, leading to the conclusion that the owner did not have a reasonable expectation of privacy from air surveillance.[224] In *Kyllo v United States*, the Court held that the use of sense-enhancing technology to gather information regarding the interior of the home, constitutes a search under the Fourth Amendment.[225] In reaching this conclusion, the Court determined that heightened privacy interests exist surrounding the home, especially since the enhanced technology was not available for general public use, individuals could not reasonably expect to protect their private interests from this type of technology.[226] Applying this case law to civil drones, it can be said that individuals are familiar with the use of drones and can even purchase them themselves relatively easy, which might have an impact on society's privacy expectations.[227] The global proliferation of UAVs may weaken the protection described in *Kyllo*, leaving the US citizens vulnerable to intrusions in and around their homes, both by the government as well as by any citizen in possession of a camera-equipped drone.[228]

[224] US Supreme Court, 476 U.S. 207 (1986), California/Ciraolo; M.R. CALO, "The drone as privacy catalyst", *Stanford Law Review Online* 12 December 2011; H.B. FÄRBER, "Eyes in the sky & privacy concerns on the ground", *Scitech Lawyer* 2015, 8; G. MCNEAL, "Drones and aerial surveillance: considerations for legislators", *Brookings* November 2014, 5; C. SCHLAG, "The new privacy battle: how the expanding use of drones continues to erode our concept of privacy and privacy rights", *Journal of Technology, Law & Policy* 2013, 13.

[225] US Supreme Court, 533 U.S. 27 (2001), Kyllo/United States; H.B. FÄRBER, "Eyes in the sky & privacy concerns on the ground", *Scitech Lawyer* 2015, 8; D. GALIANO, *The fourth amendment: unreasonable search and seizure*, New York, The Rosen Publishing Group, 2011, 6; S. NOUWT, B.R. DE VRIES and C. PRINS, *Reasonable expectations of privacy? Eleven country reports on camera surveillance and workplace privacy*, Den Haag, TMC Asser Press, 2005, 14; C. SCHLAG, "The new privacy battle: how the expanding use of drones continues to erode our concept of privacy and privacy rights", *Journal of Technology, Law & Policy* 2013, 14.

[226] US Supreme Court, 533 U.S. 27 (2001), Kyllo/United States; S. NOUWT, B.R. DE VRIES and C. PRINS, *Reasonable expectations of privacy? Eleven country reports on camera surveillance and workplace privacy*, Den Haag, TMC Asser Press, 2005, 16; C. SCHLAG, "The new privacy battle: how the expanding use of drones continues to erode our concept of privacy and privacy rights", *Journal of Technology, Law & Policy* 2013, 14.

[227] M.R. CALO, "The drone as privacy catalyst", *Stanford Law Review Online* 12 December 2011; S. NOUWT, B.R. DE VRIES and C. PRINS, *Reasonable expectations of privacy? Eleven country reports on camera surveillance and workplace privacy*, Den Haag, TMC Asser Press, 2005, 16; C. SCHLAG, "The new privacy battle: how the expanding use of drones continues to erode our concept of privacy and privacy rights", *Journal of Technology, Law & Policy* 2013, 15.

[228] M.R. CALO, "The drone as privacy catalyst", *Stanford Law Review Online* 12 December 2011; H.B. FÄRBER, "Eyes in the sky & privacy concerns on the ground", *Scitech Lawyer* 2015, 8.

5.3 FAA Regulations

80. FAA – The Federal Aviation Administration (FAA) is an organisation to ensure the safe and orderly operation of aircrafts in the American airspace.[229] The FAA also determines where domestic drones can be used and is in charge of domestic licensing of drone operation.[230] However, some recreational drone operators operating drones below 400 feet are not required to obtain a certification.[231] The only major federal legislation controlling domestic use of drones is the FAA Modernization and Reform Act of 2012.[232] A significant number of federal laws have been proposed following the FAA Modernization and Reform Act of 2012 to address drone use. Their primary focus concerns law enforcement's receipt of a warrant prior to initiating surveillance and limiting the scope of drone use.[233] However, none of the federal bills proposed fully address privacy concerns, since they still allow drones to be used for surveillance purposes in an open and visible area, and even to a certain extent when the individual has a certain expectation of privacy in the monitored area.[234]

---

[229] M.R. CALO, "The drone as privacy catalyst", *Stanford Law Review Online* 12 December 2011; R. CLARKE and L.B. MOSES, "The regulation of civilian drones' impacts on public safety", *Computer Law & Security Review* 2014, 275; C. SCHLAG, "The new privacy battle: how the expanding use of drones continues to erode our concept of privacy and privacy rights", *Journal of Technology, Law & Policy* 2013, 2.

[230] R. CLARKE and L.B. MOSES, "The regulation of civilian drones' impacts on public safety", *Computer Law & Security Review* 2014, 276; K. LESWING, "Why your drone can't fly near airports anymore", *Fortune* 18 November 2015; C. SCHLAG, "The new privacy battle: how the expanding use of drones continues to erode our concept of privacy and privacy rights", *Journal of Technology, Law & Policy* 2013, 2 and 17; J. VACEK, "Big Brother will soon be watching – or will he? Constitutional, regulatory, and operational issues surrounding the use of unmanned aerial vehicles in law enforcement", *North Dakota Law Review* 2009, 674; U. VOLOVELSKY, "Civilian uses of unmanned aerial vehicles and the threat to the right to privacy – An Israeli case study", *Computer Law & Security Review* 2014, 307.

[231] C. SCHLAG, "The new privacy battle: how the expanding use of drones continues to erode our concept of privacy and privacy rights", *Journal of Technology, Law & Policy* 2013, 18; X., *Domestic Unmanned Aerial Vehicles (UAVs) and Drones*, www.epic.org.

[232] H.B. FÄRBER, "Eyes in the sky & privacy concerns on the ground", *Scitech Lawyer* 2015, 6; R. CLARKE and L.B. MOSES, "The regulation of civilian drones' impacts on public safety", *Computer Law & Security Review* 2014, 276; G. MCNEAL, "Drones and aerial surveillance: considerations for legislators", *Brookings* November 2014, 5; C. SCHLAG, "The new privacy battle: how the expanding use of drones continues to erode our concept of privacy and privacy rights", *Journal of Technology, Law & Policy* 2013, 17; U. VOLOVELSKY, "Civilian uses of unmanned aerial vehicles and the threat to the right to privacy – An Israeli case study", *Computer Law & Security Review* 2014, 308.

[233] G. MCNEAL, "Drones and aerial surveillance: considerations for legislators", *Brookings* November 2014, 5; C. SCHLAG, "The new privacy battle: how the expanding use of drones continues to erode our concept of privacy and privacy rights", *Journal of Technology, Law & Policy* 2013, 19.

[234] G. MCNEAL, "Drones and aerial surveillance: considerations for legislators", *Brookings* November 2014, 5; C. SCHLAG, "The new privacy battle: how the expanding use of drones continues to erode our concept of privacy and privacy rights", *Journal of Technology, Law & Policy* 2013, 19.

81. DAPTA – An amendment to the FAA Modernization and Reform Act of 2012 has been made by the Drone Aircraft Privacy and Transparency Act of 2015 (hereafter: DAPTA), which proscribes limits on gathering, retention and sharing of data collected by UAVs and requires certain disclosures regarding the identity of the UAV operator, the flight path, the type of data that will be collected and so on.[235] DAPTA also places restrictions on how long the data can be kept by organisations using UAVs to collect it, as well as whether the data information can be sold, leased or otherwise provided to third parties.[236]

6. Solutions to privacy issues

82. SOLUTIONS PRIVACY ISSUES – During the last ten to fifteen years the world has changed significantly. Technological, social, economic and cultural changes have led to new challenges for the regulation on privacy protection, so reconceptualization and novel concepts seem necessary.[237] Also given the extraordinary capabilities of UAVs, it might be necessary to create a separate and novel set of specific legal controls to ensure privacy.[238] It is crucial to strike the right balance so that society can enjoy the benefits of new technologies without having to sacrifice their privacy and civil liberties upon which they have been relying for centuries.[239]

---

[235] S. 3 DAPTA; K.E. BOON and D.C. LOVELACE JR., *The domestic use of unmanned aerial vehicles*, New York, Oxford University Press, 2014, 259; H.B. FÄRBER, "Eyes in the sky & privacy concerns on the ground", *Scitech Lawyer* 2015, 7.

[236] S. 3 DAPTA; K.E. BOON and D.C. LOVELACE JR., *The domestic use of unmanned aerial vehicles*, New York, Oxford University Press, 2014, 259; H.B. FÄRBER, "Eyes in the sky & privacy concerns on the ground", *Scitech Lawyer* 2015, 7.

[237] N.N. GOMES DE ANDRADE and S. MONTELEONE, "Digital natives and the metamorphosis of the European information society. The emerging behavioral trends regarding privacy and their legal implications", in GUTWIRTH, S., LEENES, R., DE HERT, P. and POULLET, Y., *European data protection: coming of age*, Dordrecht, Springer, 2013, 141; A. KISS and G.L. SZOKE, "Evolution of revolution? Steps forward to a new generation of data protection regulation", in S. GUTWIRTH, R. LEENES and P. DE HERT, *Reforming European data protection law: Issues in privacy and data protection*, Dordrecht, Springer, 2015, 328.

[238] K.E. BOON and D.C. LOVELACE JR., *The domestic use of unmanned aerial vehicles*, New York, Oxford University Press, 2014, 261; H.B. FÄRBER, "Eyes in the sky & privacy concerns on the ground", *Scitech Lawyer* 2015, 9.

[239] H.B. FÄRBER, "Eyes in the sky & privacy concerns on the ground", *Scitech Lawyer* 2015, 9; U. VOLOVELSKY, "Civilian uses of unmanned aerial vehicles and the threat to the right to privacy – An Israeli case study", *Computer Law & Security Review* 2014, 306.

The following paragraphs will discuss whether the legal instruments that govern the use of UAVs in a European context, as well as in the US are sufficient to address modern-life privacy issues. It will also discuss to some extent the possible solutions for addressing potential breaches of privacy arising from the use of UAVs.

6.1 EU

83. NEW APPROACH NEEDED? – Many significant technological, social, economic and cultural changes have occured over the years, and the question remains whether existing legislation and authorities are sufficient to address modern day privacy and data protection issues.[240] Control by data subjects themselves on the collecting of their personal information seems to be inadequate, so a new approach is needed. As stated before, an individual's privacy awareness is rather low and sometimes the individual does not even take action to protect his personal data, so it is deemed necessary to effectively protect an individual's privacy in his place and ensure some kind of background protection.[241] This approach is similar to that of consumer protection, where the users will be provided with much information, and, even if they pay little or no attention to them, a minimum level of protection can be ensured by specially designed authorities and NGOs.[242]

[240] N.N. GOMES DE ANDRADE and S. MONTELEONE, "Digital natives and the metamorphosis of the European information society. The emerging behavioral trends regarding privacy and their legal implications", in GUTWIRTH, S., LEENES, R., DE HERT, P. and POULLET, Y., *European data protection: coming of age*, Dordrecht, Springer, 2013, 141; A. KISS and G.L. SZOKE, "Evolution of revolution? Steps forward to a new generation of data protection regulation", in S. GUTWIRTH, R. LEENES and P. DE HERT, *Reforming European data protection law: Issues in privacy and data protection*, Dordrecht, Springer, 2015, 328.

[241] A. KISS and G.L. SZOKE, "Evolution of revolution? Steps forward to a new generation of data protection regulation", in S. GUTWIRTH, R. LEENES and P. DE HERT, *Reforming European data protection law: Issues in privacy and data protection*, Dordrecht, Springer, 2015, 328.

[242] A. KISS and G.L. SZOKE, "Evolution of revolution? Steps forward to a new generation of data protection regulation", in S. GUTWIRTH, R. LEENES and P. DE HERT, *Reforming European data protection law: Issues in privacy and data protection*, Dordrecht, Springer, 2015, 328.

6.2 US

84. POSSIBLE SOLUTION – Also in the US, to resolve privacy concerns raised by drones it has been advised to develop a new set of statutes, rules and guidelines.[243] A possible solution is to introduce a baseline consumer protection law that points out permissible uses of drones in domestic airspace by both law enforcement bodies and private parties.[244] This approach might be chosen in order to protect the weaker party, *i.e.* the data subject, from the stronger party, which are the data controllers.[245] According to SCHLAG, a specifically developed consumer protection agency or NGO dedicated only to drone technology should take action when an unfair imbalance would exist towards the data controllers and would thus be responsible for implementing and overseeing compliance with the law.[246] A baseline consumer protection law would need to address drone surveillance, data collection and the various drone technological capabilities, and would give an accurate representation of the current expectations of privacy. This would be a guarantee that both governmental and private parties are not using drones in a way that violates an individual's privacy, which would also benefit individual's privacy expectations.[247]

[243] K.E. BOON and D.C. LOVELACE JR., *The domestic use of unmanned aerial vehicles*, New York, Oxford University Press, 2014, 1; C. SCHLAG, "The new privacy battle: how the expanding use of drones continues to erode our concept of privacy and privacy rights", *Journal of Technology, Law & Policy* 2013, 21; U. VOLOVELSKY, "Civilian uses of unmanned aerial vehicles and the threat to the right to privacy – An Israeli case study", *Computer Law & Security Review* 2014, 310; D. WRIGHT, "Drones: Regulatory challenges to an incipient industry", *Computer Law & Security Review* 2014, 229.
[244] C. SCHLAG, "The new privacy battle: how the expanding use of drones continues to erode our concept of privacy and privacy rights", *Journal of Technology, Law & Policy* 2013, 21.
[245] A. KISS and G.L. SZOKE, "Evolution of revolution? Steps forward to a new generation of data protection regulation", in S. GUTWIRTH, R. LEENES and P. DE HERT, *Reforming European data protection law: Issues in privacy and data protection*, Dordrecht, Springer, 2015, 318.
[246] A. KISS and G.L. SZOKE, "Evolution of revolution? Steps forward to a new generation of data protection regulation", in S. GUTWIRTH, R. LEENES and P. DE HERT, *Reforming European data protection law: Issues in privacy and data protection*, Dordrecht, Springer, 2015, 318; C. SCHLAG, "The new privacy battle: how the expanding use of drones continues to erode our concept of privacy and privacy rights", *Journal of Technology, Law & Policy* 2013, 21.
[247] A. KISS and G.L. SZOKE, "Evolution of revolution? Steps forward to a new generation of data protection regulation", in S. GUTWIRTH, R. LEENES and P. DE HERT, *Reforming European data protection law: Issues in privacy and data protection*, Dordrecht, Springer, 2015, 318; C. SCHLAG, "The new privacy battle: how the expanding use of drones continues to erode our concept of privacy and privacy rights", *Journal of Technology, Law & Policy* 2013, 21-22.

7. Interim-conclusion

85. INTERIM-CONCLUSION – Privacy issues exist everywhere, on the EU level, as well as within the Member States, as well as on US level. With the current and upcoming new technologies, it does not get easier to address these issues, forcing legislators to find novel and improved ways to protect an individual's privacy rights. Both at the EU and US level, doctrine has come to the conclusion that the answer may lie in consumer protection law, wherein data subjects need to be protected as the weaker party from the data controller as the stronger party. This system would be able to give guarantees to the data subject that his privacy is respected by the data controller, whom is holding all the power.

B. For surveillance purposes

86. SURVEILLANCE PURPOSES – The 21st century has brought rapid changing technological evolutions making it possible to invade in other parties' privacy, especially with the possibility to use cameras for surveillance purposes.[248] Surveillance is the systematic monitoring of a certain target, which can be an area, an identified individual or a group of people.[249] In order to address invasions on privacy by surveillance cameras, surveillance legislation has been put into place. But the question will be whether these laws can avoid a surveillance society to come into existence, especially when the civil use of drones is becoming more present in everyday life. Another question that can be asked is whether drones even fall under the existing surveillance legislation? And whether they will remain adequate to address the challenges that new technologies may pose in the future?

[248] K.E. BOON and D.C. LOVELACE JR., *The domestic use of unmanned aerial vehicles*, New York, Oxford University Press, 2014, 72; R. CLARKE, "The regulation of civilian drones' impacts on behavioural privacy", *Computer Law & Security Review* 2014, 288; D. LYON, *Surveillance studies: An overview*, Cambridge, Polity Press, 2007, 175.
[249] R. CLARKE, "The regulation of civilian drones' impacts on behavioural privacy", *Computer Law & Security Review* 2014, 288; D. LYON, *Surveillance studies: An overview*, Cambridge, Polity Press, 2007, 13-14.

1. European legal framework

87. EUROPEAN LEGAL FRAMEWORK – As concerns the surveillance issues that come with the use of camera equipment, the Article 29 DPWP has issued an opinion which is not binding, but has a certain importance nonetheless. Besides that, also case law at the level of the European Court of Human Rights has given video surveillance some thought.

1.1 Opinion 04/2004 of the Art. 29 Data Protection Working Party

88. OPINION 04/2004 – In Opinion 04/2004 on the processing of personal data by means of video surveillance, the Art. 29 DPWP stated that images and video clips are considered to be personal data if they provide information that makes an individual identifiable, even when it is done indirectly.[250] Public surveillance materials that record visual data will thus be considered to be personal data under the Charter of Fundamental Rights and the Data Protection Directive, which will be replaced by the GDPR in the near future, and has as a consequence that data subjects will have the rights of information, access and correction of the assembled data concerning them.[251] Data subjects thus need to have access to data collected about them by a UA device, even when it is done indirectly, and they should be given the opportunity to consent to this surveillance.[252]

---

[250] Opinion 04/2004 on the processing of personal data by means of video surveillance, Article 29 Data Protection Working Party, 11750/02/EN, WP 89, 11 February 2004; CJEU 6 November 2003, C-101/01, Lindqvist, §24; B.H.M. CUSTERS, J.J. OERLEMANS en S.J. VERGOUW, *Het gebruik van drones: een verkennend onderzoek naar onbemande luchtvaartuigen*, Meppel, Boom Lemma Uitgevers, 2015, 125; R.L. FINN and D. WRIGHT, "Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications", *Computer Law & Security Review* 2012, 192-193; G. GONZALEZ FUSTER, *The emergence of personal data protection as a fundamental right of the EU*, Dordrecht, Springer, 2014, 34; E.J. KINDT, *Privacy and data protection issues of biometric applications: a comparative legal analysis*, Dordrecht, Springer, 2013, 93-94; V. KOSTA, *Fundamental rights in EU internal market legislation*, Oxford, Hart Publishing, 2015, 92.

[251] P. CAREY, *E-privacy and online data protection*, Amsterdam, LexisNexis, 2002, 57; L. CROPPER, "GDPR gets the final seal of approval", privacylawblog.fieldfisher.com 15 April 2016; R.L. FINN and D. WRIGHT, "Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications", *Computer Law & Security Review* 2012, 193; R. ULDALL, "Data protection reform – Parliament approves new rules fit for the digital era", http://www.europarl.europa.eu 2016; X., *Reform of EU data protection*.

[252] R.L. FINN and D. WRIGHT, "Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications", *Computer Law & Security Review* 2012, 193; S. NOUWT, B.R. DE VRIES and C. PRINS, *Reasonable expectations of privacy? Eleven country reports on camera surveillance and workplace privacy*, Den Haag, TMC Asser Press, 2005, 297.

1.2 Case law

89. NO RECORDING - In *Peck v United Kingdom*, the European Court of Human Rights stated that "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".[253] What the Court thus is stating is that public space surveillance, such as CCTV, is lawful under the Charter of Fundamental Rights.[254] This consideration leads to the conclusion that UAV surveillance that monitors public spaces but does not record, is lawful. However, surveillance that includes the private home would likely require monitoring.[255]

90. RECORDING – Video surveillance, like CCTV, which does record the visual data, falls under the scope of the EU Data Protection Directive of 1995, soon to be GDPR.[256] The consequence is that consent will be needed from the data subject, from whom the information is gathered, to be able to use that information, or another legal ground has to be found.[257]

---

[253] ECtHR 28 January 2003, nr. 44647/98, Peck/United Kingdom, §59; V. KOSTA, *Fundamental rights in EU internal market legislation*, Oxford, Hart Publishing, 2015, 92; S. NOUWT, B.R. DE VRIES and C. PRINS, *Reasonable expectations of privacy? Eleven country reports on camera surveillance and workplace privacy*, Den Haag, TMC Asser Press, 2005, 110; L. SCAIFE, *Handbook of social media and the law*, New York, Informa Law from Routledge, 2015, 238.

[254] R.L. FINN and D. WRIGHT, "Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications", *Computer Law & Security Review* 2012, 192; V. KOSTA, *Fundamental rights in EU internal market legislation*, Oxford, Hart Publishing, 2015, 92; S. NOUWT, B.R. DE VRIES and C. PRINS, *Reasonable expectations of privacy? Eleven country reports on camera surveillance and workplace privacy*, Den Haag, TMC Asser Press, 2005, 110.

[255] R.L. FINN and D. WRIGHT, "Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications", *Computer Law & Security Review* 2012, 192; S. NOUWT, B.R. DE VRIES and C. PRINS, *Reasonable expectations of privacy? Eleven country reports on camera surveillance and workplace privacy*, Den Haag, TMC Asser Press, 2005, 136.

[256] L. CROPPER, "GDPR gets the final seal of approval", privacylawblog.fieldfisher.com 15 April 2016; R.L. FINN and D. WRIGHT, "Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications", *Computer Law & Security Review* 2012, 192; R. ULDALL, "Data protection reform – Parliament approves new rules fit for the digital era", http://www.europarl.europa.eu 2016; X., *Reform of EU data protection*.

[257] *Supra* 37, nr. 56.

91. CCTV AT HOME – In the *Ryneš* case, the ECJ held that continuous video surveillance of a public space cannot fall under the household exemption of article 3(2) Directive 95/46/EC, and thus the Data Protection Directive is fully applicable in this case.[258] The monitoring of a public space requires the surveillance equipment to be directed outwards from the privacy setting of the home, so for example towards a public footpath.[259] The same reasoning can be pursued in application to drones, since the Directive 95/46/EC does not make a distinction between fixed and mobile surveillance cameras, given that they both amount to the automatic processing of personal data. So in parallel in application to drones, as soon as it is flown outdoors, it will record elements outwards from the privacy setting, thus making the data controller automatically subject to Directive 95/46/EC and excluding the household exemption.[260] However, this point of view must be mitigated, since the ECJ reasoned that the number of data subjects involved, the scale and frequency of the processing and the potential adverse effect on the fundamental rights of others must also be taken into account next to the monitoring of a public space, thus not excluding the possible applicability of the household exemption of Directive 95/46/EC.[261]

[258] CJEU 11 December 2014, C-212/13, Ryneš/Office for Personal Data Protection, §35; O. RUDGARD, "Should you install CCTV outside your home?", *The Telegraph* 22 May 2015; H. SIDDIQUE, "Home surveillance CCTV images may breach data protection laws, ECJ rules", *The Guardian* 11 December 2014; B. VAN ALSENOY, "The evolving role of the individual under EU data protection law", *ICRI Working Paper* 23/2015, 26; T. WESSING, "Drones and data", united-kingdom.taylorwessing.com March 2015.

[259] CJEU 11 December 2014, C-212/13, Ryneš/Office for Personal Data Protection, §33; O. RUDGARD, "Should you install CCTV outside your home?", *The Telegraph* 22 May 2015; H. SIDDIQUE, "Home surveillance CCTV images may breach data protection laws, ECJ rules", *The Guardian* 11 December 2014; B. VAN ALSENOY, "The evolving role of the individual under EU data protection law", *ICRI Working Paper* 23/2015, 11.

[260] Opinion 01/2015 on privacy and data protection issues relating to the utilisation of drones, Article 29 Data Protection Working Party, 01673/15/EN, WP 231, 16 June 2015, 8; Policy department C: citizens' rights and constitutional affairs, "Privacy and data protection implications of the civil use of drones: in-depth analysis for the LIBE Committee", PE.519.221, www.europarl.europa.eu, June 2015, 8-9; B. VAN ALSENOY, "The evolving role of the individual under EU data protection law", *ICRI Working Paper* 23/2015, 26.

[261] CJEU 11 December 2014, C-212/13, Ryneš/Office for Personal Data Protection, §34; B. VAN ALSENOY, "The evolving role of the individual under EU data protection law", *ICRI Working Paper* 23/2015, 26.

2. Belgian legal framework

92. BELGIAN LEGAL FRAMEWORK – The legal framework in Belgium regarding video surveillance consists of the *Wet van 21 maart 2007 tot regeling van de plaatsing en het gebruik van bewakingscamera's*.[262] In the following paragraphs it will be discussed whether this regulation may also be applicable to the use of drones for surveillance purposes.

2.1 Camerawet

93. CAMERAWET – Drones are more and more frequently used for surveillance purposes, so they may fall under the existing regulation on the use of surveillance cameras, such as the *Camerawet*.[263] Under this regulation, every fixed or mobile observation system with as aim to prevent, to establish or to trace crimes against persons or goods, or to maintain public order and which for that purpose gathers, administers or preserves images, will be considered to be a surveillance camera.[264] When that surveillance camera is being transferred during the observation in order to film different areas and positions, it will considered to be mobile.[265] It is thus evident that the use of camera-equipped drones will fall under this regulation.[266]

---

[262] Wet van 21 maart 2007 tot regeling van de plaatsing en het gebruik van bewakingscamera's, *BS* 31 mei 2007 (hereafter: *Camerawet*); J. MORTELÉ, H. VERMEERSCH, E. DE PAUW, W. HARDYNS and F. DEPRINS, *Cameratoezicht in de openbare ruimte. Ook wie weg is, is gezien?,* Antwerpen, Maklu, 2013, 24.

[263] W. VERHEYEN, "Onbemande luchtvaartuigen: Vogelvrij of (nu al) gekooid?", *NJW* 2015, 345.

[264] Article 2 *Camerawet*; P. DE HERT and R. SAELENS, "De camerawet: een zoektocht naar een afweging tussen het recht op privacy en het recht op veiligheid", *T. Strafr*. 2007, 93; X., *Wat is een bewakingscamera?,* www.privacycommission.be.

[265] Wetsontwerp houdende wijziging van de wet van 21 maart 2007 tot regeling van de plaatsing en het gebruik van bewakingscamera's, *Parl. St.* Kamer 2008-09, nr. 2076/003, 3; Principenota van 20 januari 2010 betreffende de wet tot regeling van de plaatsing en het gebruik van bewakingscamera's, nr. 2007.2, 8-9.

[266] Aanbeveling nr. 04/2012 van 29 februari 2012 van de Privacycommissie inzake de diverse toepassingsmogelijkheden van camerabewaking, 2; Principenota van 20 januari 2010 betreffende de wet tot regeling van de plaatsing en het gebruik van bewakingscamera's, nr. 2007.2, 18; X., *Is de camerawet van toepassing op drones?*, www.startpuntveiligheid.be.

Important however is to make a distinction between fixed and mobile surveillance cameras, since the law provides for different rules. Furthermore, the *Camerawet* obliges the owner of the surveillance camera to obey the applicable privacy rules.[267]

94. FIXED CAMERA – Fixed surveillance cameras may be placed at a public place or at for the public accessible places.[268] However, the law prohibits to make images with the fixed surveillance camera of public areas or areas for which the owner of the camera is not responsible, when the fixed camera is installed at a for the public non-accessible area.[269] Surveillance cameras may then only film areas for which the owner of the camera is responsible, thus for his private property. For example, if a person wants to install a camera to safeguard his home, the camera must be pointed at the entrance of the home and not at the sidewalk or the neighbour's home. The placement of a camera within or outside a person's home for surveillance purposes in order to be able to record a criminal action, is subject to an obligatory registration at the Privacy Commission in accordance to the Royal Decree of 2 July 2008 on the registration of the placement and use of surveillance cameras.[270] Whenever the camera is installed within the home of a person for domestic use, this registration will not be necessary.[271]

[267] Art. 10 *Camerawet*; K. CLERIX, "De privacy-lacunes van de camerawet", *Mondiaal Nieuws* 13 maart 2014; P. DE HERT and R. SAELENS, "De camerawet: een zoektocht naar een afweging tussen het recht op privacy en het recht op veiligheid", *T. Strafr*. 2007, 94; W. VERHEYEN, "Onbemande luchtvaartuigen: Vogelvrij of (nu al) gekooid?", *NJW* 2015, 345.

[268] Art. 5 and 6 *Camerawet*; P. DE HERT and R. SAELENS, "De camerawet: een zoektocht naar een afweging tussen het recht op privacy en het recht op veiligheid", *T. Strafr*. 2007, 94; J. MORTELÉ, H. VERMEERSCH, E. DE PAUW, W. HARDYNS and F. DEPRINS, *Cameratoezicht in de openbare ruimte. Ook wie weg is, is gezien?,* Antwerpen, Maklu, 2013, 26.

[269] Article 7, §2 *Camerawet*; Verslag namens de Commissie voor de Binnenlandse Zaken en voor de Administratieve Aangelegenheden uitgebracht door de heer DELPÉRÉE omtrent het wetsvoorstel tot regeling van de plaatsing en het gebruik van bewakingscamera's, *Parl. St.* Senaat, 2006-07, nr. 3-1734/5, 26; P. DE HERT and R. SAELENS, "De camerawet: een zoektocht naar een afweging tussen het recht op privacy en het recht op veiligheid", *T. Strafr*. 2007, 95.

[270] Article 7, §2 *Camerawet*; Koninklijk Besluit van 2 juli 2008 betreffende de aangiften van de plaatsing en het gebruik van bewakingscamera's, *BS* 15 juli 2008; P. DE HERT and R. SAELENS, "De camerawet: een zoektocht naar een afweging tussen het recht op privacy en het recht op veiligheid", *T. Strafr*. 2007, 95.

[271] Article 7, §2 *Camerawet*; P. DE HERT and R. SAELENS, "De camerawet: een zoektocht naar een afweging tussen het recht op privacy en het recht op veiligheid", *T. Strafr*. 2007, 95.

95. MOBILE CAMERA – For mobile cameras, the conditions differ from the previously mentioned provisions for fixed surveillance cameras. Article 7/1 of the *Camerawet* states that police enforcement bodies can make use of mobile surveillance cameras, but only in certain circumstances.[272] The further provisions on mobile surveillance cameras do not mention any use of them in a public place nor in for the public accessible places by any other body, organisation or individual other than police authorities, nor does it mention the use of them in for the public non-accessible places. The Belgian law thus remains silent on whether mobile surveillance systems, such as drones, may be used by civil entities.

3. UK legal framework

96. UK LEGISLATION – Currently, unmanned aircrafts are dealt with under existing legislation covering CCTV surveillance and privacy, namely the Data Protection Act of 1998.[273] Also important regarding surveillance is the CCTV code of practice.

3.1 Data Protection Act 1998

97. DPA '98 – Surveillance by UA devices is covered by the Data Protection Act 1998, which states, in line with the EU Data Protection Directive, that individuals must always be told that a surveillance system is in operation and that they can request copies of the data which the data controller holds about them at all times.[274]

[272] Art. 7/1 *Camerawet*; W. VERHEYEN, "Onbemande luchtvaartuigen: Vogelvrij of (nu al) gekooid?", *NJW* 2015, 345.
[273] I. KROENER, *CCTV: A technology under the radar*?, Surrey, Ashgate Publishing Limited, 2014, 106; C.L. WASHBOURNE and C. NATH, "Civilian drones", *Postnote* 2014, 4; A. ZAVRŠNIK, *Drones and unmanned aerial systems: legal and social implications for security and surveillance*, Heidelberg, Springer, 2016, 112.
[274] R.L. FINN and D. WRIGHT, "Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications", *Computer Law & Security Review* 2012, 193; I. KROENER, *CCTV: A technology under the radar*?, Surrey, Ashgate Publishing Limited, 2014, 106; A. MURRAY, *Information technology law: the law and society*, Oxford, Oxford University Press, 2013, 526; L. SCAIFE, *Handbook of social media and the law*, New York, Informa Law from Routledge, 2015, 243.

In application to drones used for surveillance purposes, it can be said that it may comply with the provisions of the Data Protection Act of 1998 when a clear indication or sign has been put up to inform individuals that they may be filmed by a mobile surveillance system, similar to the obligation for CCTV cameras.[275] However, the Data Protection Act is not applicable when CCTV is used on one's own private property because of the domestic purposes exemption, and thus this obligation must not be complied with, unless footage of individuals outside that private property is captured.[276] Moreover, the Data Protection Act only applies to overt surveillance systems, which includes for example helicopters due to their audibility and visibility and CCTV on the streets.[277] However, this stands in contrast with most UA devices, since one of their known features is that they are silent and can fly at altitudes which makes them practically invisible, which makes it difficult to inform individuals that UA surveillance is taking place.[278] It is thus questionable whether this act is adequate to apply to drones in a domestic surveillance context.

3.2 CCTV Code of Practice

99. CCTV CODE OF PRACTICE – The public in the UK is already used to seeing CCTV cameras on every high street, which do enjoy their general support but nonetheless form an intrusion into the lives of ordinary people in their day-to-day life and may raise wider privacy concerns.[279]

[275] ICO, *CCTV*, https://ico.org.uk; O. RUDGARD, "Should you install CCTV outside your home?", *The Telegraph* 22 May 2015.
[276] S. 36 Data Protection Act 1998; 7th Report of 2014-2015 on the Civilian use of drones in the EU, House of Lords, HL 122, 5 March 2015, 45; ICO, *CCTV*, https://ico.org.uk; E. KOSTA, *Consent in European data protection law*, Leiden, Martinus Nijhoff Publishers, 2013, 71; A. MURRAY, *Information technology law: the law and society*, Oxford, Oxford University Press, 2013, 527.
[277] R.L. FINN and D. WRIGHT, "Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications", *Computer Law & Security Review* 2012, 193; D. KLITOU, *Privacy-invading technologies and privacy by design*, The Hague, Asser Press, 2014, 55.
[278] R.L. FINN and D. WRIGHT, "Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications", *Computer Law & Security Review* 2012, 193; C. SCHLAG, "The new privacy battle: how the expanding use of drones continues to erode our concept of privacy and privacy rights", *Journal of Technology, Law & Policy* 2013, 12.
[279] ICO, *CCTV*, https://ico.org.uk; ICO, *In the picture: A data protection code of practice for surveillance cameras and personal information*, https://ico.org.uk 2015, 15; D. KLITOU, *Privacy-invading technologies and privacy by design*, The Hague, Asser Press, 2014, 142.

Therefor proper safeguards are necessary to ascertain the public that CCTV is used responsibly.[280] The CCTV Code of Practice provides some guidance and advice for CCTV users on how to comply with the Data Protection Act.[281] The CCTV Code has been revised to include a section dealing particularly with UAVs, wherein the ICO stresses that the recording element must be capable of being turned off, since continuous recording is discouraged and highly unlikely to be justifiable.[282] However, this Surveillance Camera Code of Practice is merely voluntary, meaning that its provisions are not binding, which may be seen as a shortcoming.[283]

4. US legal framework

100. US LEGAL FRAMEWORK – Aerial surveillance of drones within the United States raise significant privacy concerns considering they can gather very detailed information on individuals.[284] In the following paragraphs, the current legal framework in the US on video surveillance will be discussed, taking into account the USA Freedom Act and important case law.

[280] S. 29 Protection of Freedoms Act 2012; ICO, *CCTV*, https://ico.org.uk; D. KLITOU, *Privacy-invading technologies and privacy by design*, The Hague, Asser Press, 2014, 141; T. WESSING, "Drones and data", united-kingdom.taylorwessing.com March 2015.
[281] 7th Report of 2014-2015 on the Civilian use of drones in the EU, House of Lords, HL 122, 5 March 2015, 47; ICO, *CCTV*, https://ico.org.uk; ICO, *In the picture: A data protection code of practice for surveillance cameras and personal information*, https://ico.org.uk 2015, 3; D. KLITOU, *Privacy-invading technologies and privacy by design*, The Hague, Asser Press, 2014, 150; A. MURRAY, *Information technology law: the law and society*, Oxford, Oxford University Press, 2013, 527; T. WESSING, "Drones and data", united-kingdom.taylorwessing.com March 2015.
[282] 7th Report of 2014-2015 on the Civilian use of drones in the EU, House of Lords, HL 122, 5 March 2015, 47; ICO, *In the picture: A data protection code of practice for surveillance cameras and personal information*, https://ico.org.uk 2015, 30; T. WESSING, "Drones and data", united-kingdom.taylorwessing.com March 2015.
[283] S. 33 Protection of Freedoms Act 2012; C. JONES, "Drones: the UK debate and its implications for the EU", *EU Law Analysis* 28 May 2014; A. MURRAY, *Information technology law: the law and society*, Oxford, Oxford University Press, 2013, 530.
[284] X., *Domestic drones*, www.aclu.org; X., *Domestic Unmanned Aerial Vehicles (UAVs) and Drones*, www.epic.org.

4.1 USA Freedom Act

101. USA FREEDOM ACT – In 2015, the US Senate passed the first surveillance reform in a decade, ending the mass collection of American citizens' phone records by the NSA, placing record storage in private companies' hands, creating a public interest advocate for the secret FISA court that oversees surveillance programs, and requiring the Court to notify the Congress when it reinterprets law.[285] Even when this means an increase of US citizens' privacy rights, the Act only concerns surveillance carried out by public authorities, and in particular the NSA.

4.2 Surveillance laws

102. GENERAL SURVEILLANCE LAW – The difficulty in the US is that federal constitutional limitations apply exclusively to governmental bodies, whereas statutes and common law rules may apply to governmental bodies, private persons, or both.[286] When private parties want to use surveillance cameras at home, the law may thus vary from state to state.[287] Generally, following previous case law, if a camera is visible, not recording audio and not invading the privacy of any individuals, it is usually considered to be legal. Furthermore, the Supreme Court decided in *United States v Causby* that an individual's property right extends to the airspace above his private ground.[288] Although it was not made clear to what specific height the property right extends to and thus a lack of clarity exists on this matter, the Supreme Court referred to the airspace as "the immediate reaches above the land, into which intrusions would subtract from the owner's full enjoyment of the property".[289]

---

[285] B.L. NACOS, *Terrorism and counterterrorism*, New York, Routledge, 2016, 26; A. YUHAS, "NSA reform: USA Freedom Act passes first surveillance reform in decade – as it happened", *The Guardian* 2 June 2015.
[286] R. FOGEL, "CCTV and video surveillance laws in US", www.smartsign.com 7 December 2011; S. NOUWT, B.R. DE VRIES and C. PRINS, *Reasonable expectations of privacy? Eleven country reports on camera surveillance and workplace privacy*, Den Haag, TMC Asser Press, 2005, 9.
[287] R. FOGEL, "CCTV and video surveillance laws in US", www.smartsign.com 7 December 2011.
[288] US Supreme Court, 328 U.S. 256 (1946), United States/Causby; K.E. BOON and D.C. LOVELACE JR., *The domestic use of unmanned aerial vehicles*, New York, Oxford University Press, 2014, 243; G. MCNEAL, "Drones and aerial surveillance: considerations for legislators", *Brookings* November 2014, 8.
[289] US Supreme Court, 328 U.S. 256 (1946), United States/Causby; K.E. BOON and D.C. LOVELACE JR., *The domestic use of unmanned aerial vehicles*, New York, Oxford University Press, 2014, 243; G. MCNEAL, "Drones and aerial surveillance: considerations for legislators", *Brookings* November 2014, 9; B. PALMER, "Hey, you! Get off of my cloud! How much of the airspace above your home do you own?", *Slate* 11 July 2013.

It can be said that this may exclude governmental and civilian operated drones above one's private property.[290] This may also lead to the conclusion that the airspace above one's private ground in the US is also part of the individual's property right, thus making it legal for him to operate a drone within that area.

4.2 Case law

103. CASE LAW – The largest privacy concern arising out of civil drone use is its ability to operate as a surveillance tool.[291] The technology that was at issue in *Kyllo* was used to peer through walls by law enforcement bodies and triggered the protection of the Fourth Amendment.[292] However, UAVs may have effects to the same extent, and the problem is that they can be purchased by the general public, which makes it more pervasive than originally believed.[293] When surveillance drones fly in open view or in public airspace, the obtained material containing personal information will not be protected under the Fourth Amendment, because in the *Ciraolo* case the Supreme Court held that there is no reasonable expectation of privacy in these areas.[294]

---

[290] K.E. BOON and D.C. LOVELACE JR., *The domestic use of unmanned aerial vehicles*, New York, Oxford University Press, 2014, 249; G. MCNEAL, "Drones and aerial surveillance: considerations for legislators", *Brookings* November 2014, 9; B. PALMER, "Hey, you! Get off of my cloud! How much of the airspace above your home do you own?", *Slate* 11 July 2013.

[291] K.E. BOON and D.C. LOVELACE JR., *The domestic use of unmanned aerial vehicles*, New York, Oxford University Press, 2014, 227; C. SCHLAG, "The new privacy battle: how the expanding use of drones continues to erode our concept of privacy and privacy rights", *Journal of Technology, Law & Policy* 2013, 15.

[292] *Supra* 52-53, nr. 79; US Supreme Court, 533 U.S. 27 (2001), Kyllo/United States; K.E. BOON and D.C. LOVELACE JR., *The domestic use of unmanned aerial vehicles*, New York, Oxford University Press, 2014, 222; T.N. MCINNIS, *The evolution of the Fourth Amendment*, Plymouth, Lexington Books, 2010, 241; S. NOUWT, B.R. DE VRIES and C. PRINS, *Reasonable expectations of privacy? Eleven country reports on camera surveillance and workplace privacy*, Den Haag, TMC Asser Press, 2005, 35.

[293] S. NOUWT, B.R. DE VRIES and C. PRINS, *Reasonable expectations of privacy? Eleven country reports on camera surveillance and workplace privacy*, Den Haag, TMC Asser Press, 2005, 35; C. SCHLAG, "The new privacy battle: how the expanding use of drones continues to erode our concept of privacy and privacy rights", *Journal of Technology, Law & Policy* 2013, 16.

[294] US Supreme Court, 476 U.S. 207 (1986), California/Ciraolo; K.E. BOON and D.C. LOVELACE JR., *The domestic use of unmanned aerial vehicles*, New York, Oxford University Press, 2014, 223; T.N. MCINNIS, *The evolution of the Fourth Amendment*, Plymouth, Lexington Books, 2010, 233; C. SCHLAG, "The new privacy battle: how the expanding use of drones continues to erode our concept of privacy and privacy rights", *Journal of Technology, Law & Policy* 2013, 16; X., *Domestic Unmanned Aerial Vehicles (UAVs) and Drones*, www.epic.org.

Also, in the *Kyllo* case it was stated that surveillance cameras do not raise privacy concerns when items are in plain view.[295] It may thus be concluded out of previous case law that surveillance by both fixed and mobile cameras, given that the *Ciraolo* case concerned information collected by a helicopter, is allowed.[296] However, these cases only concern the use of surveillance equipment by law enforcement bodies and not by private parties. Though, it may be said that aerial surveillance by private parties is allowed since they do not operate drone vehicles with the same extended capabilities as that of the US government and since anyone can have the ability to observe what can be viewed from the air.[297]

5. Interim-conclusion

104. INTERIM-CONCLUSION – The previous paragraphs have discussed the different surveillance legislations that exist in Europe, Belgium, the United Kingdom and the United States. A general conclusion may be that insufficient attention has gone to the possibility of the use of surveillance cameras by private parties. And when provisions have been foreseen for this issue, it only concerns the use of fixed surveillance cameras such as CCTV, but it doesn't mention mobile surveillance cameras such as drones. It is thus possible to conclude that there is a lack of adequate legislation on the issue of surveillance carried out by private parties. Chapter three will discuss whether the few legal instruments that do exist, usually around CCTV cameras, would be adequate to address the civil use of UAVs for surveillance purposes as well, whether a new legal instrument should see the light, or whether UAVs surveillance carried out by private parties should be prohibited as a whole.

[295] US Supreme Court, 476 U.S. 207 (1986), California/Ciraolo; US Supreme Court, 533 U.S. 27 (2001), Kyllo/United States.
[296] US Supreme Court, 533 U.S. 27 (2001), Kyllo/United States; K.E. BOON and D.C. LOVELACE JR., *The domestic use of unmanned aerial vehicles*, New York, Oxford University Press, 2014, 217.
[297] K.E. BOON and D.C. LOVELACE JR., *The domestic use of unmanned aerial vehicles*, New York, Oxford University Press, 2014, 224; X., *Domestic Unmanned Aerial Vehicles (UAVs) and Drones*, www.epic.org.

CHAPTER 3. Civil drones for surveillance purposes?

105. SURVEILLANCE DRONES – Drone technology is new and exciting, and it is even capable of providing benefits for society.[298] However, drones itself will always remain a potential for harm through interference, accidents and violent action, and they will pose problems regarding the right to privacy.[299] Many implemented and proposed methods for dealing with these negative influences of UAVs are not adequate enough to address the problems of necessary controls required to ensure the protection of an individual's privacy rights, especially when the data controllers are civilians themselves and not an organization or the state, since existing data protection regulation is aimed more at the latter.[300] The following paragraphs will discuss how these privacy and data protection risks could be addressed in order to conclude whether civil use of drones for surveillance purposes should be allowed and, if so, under which conditions.

§1 Fixed vs Mobile Cameras

106. SURVEILLANCE LAW – As is discussed before in this master thesis, general privacy and data protection law exists on international and EU level, which of course has an impact on national level, both in the Member States of the EU as in the US.[301]

---

[298] R. CLARKE, "Understanding the drone epidemic", *Computer Law & Security Review* 2014, 230; R. CLARKE and L.B. MOSES, "The regulation of civilian drones' impacts on public safety", *Computer Law & Security Review* 2014, 264; C. SCHLAG, "The new privacy battle: how the expanding use of drones continues to erode our concept of privacy and privacy rights", *Journal of Technology, Law & Policy* 2013, 20; U. VOLOVELSKY, "Civilian uses of unmanned aerial vehicles and the threat to the right to privacy – An Israeli case study", *Computer Law & Security Review* 2014, 310; D. WRIGHT, "Drones: Regulatory challenges to an incipient industry", *Computer Law & Security Review* 2014, 229.

[299] R. CLARKE and L.B. MOSES, "The regulation of civilian drones' impacts on public safety", *Computer Law & Security Review* 2014, 264; U. VOLOVELSKY, "Civilian uses of unmanned aerial vehicles and the threat to the right to privacy – An Israeli case study", *Computer Law & Security Review* 2014, 310; D. WRIGHT, "Drones: Regulatory challenges to an incipient industry", *Computer Law & Security Review* 2014, 229.

[300] B. PALMER, "Hey, you! Get off of my cloud! How much of the airspace above your home do you own?", *Slate* 11 July 2013; C. SCHLAG, "The new privacy battle: how the expanding use of drones continues to erode our concept of privacy and privacy rights", *Journal of Technology, Law & Policy* 2013, 20; B. VAN ALSENOY, "The evolving role of the individual under EU data protection law", *ICRI Working Paper* 23/2015, 12; U. VOLOVELSKY, "Civilian uses of unmanned aerial vehicles and the threat to the right to privacy – An Israeli case study", *Computer Law & Security Review* 2014, 315.

[301] *Supra* 4, nr. 4 etc.

As concerns the use of cameras for surveillance purposes and the privacy and data protection rights related thereto, more attention seems to be paid to the protection of civilians against intrusive investigation powers of law enforcement bodies, rather than surveillance done by civilians themselves.

107. FIXED CAMERAS – Regarding the use of fixed cameras by civilians for surveillance purposes, it can be said that in the US, as well as in the UK, as well as in Belgium, this is allowed when certain conditions are met. These conditions may vary from country to country, and within the US even from state to state.[302] The use of surveillance cameras is generally allowed as long as the placement and use of it is proclaimed at the competent authority, a sign has been put up to warn individuals that they may be filmed and the use of the camera is in accordance to the privacy rules.[303] It has been established throughout the years that CCTV may be used at home in Europe and the US, as long as only an individual's own private property is being filmed and not any public property, nor another individual's private property where an expectation of privacy might exist.[304]

108. MOBILE CAMERAS – Regarding mobile cameras used for surveillance purposes, the law seems to be foreseeing provisions only for law enforcement bodies and public authorities, and not so much for civilians. However, in parallel to the CCTV conditions, it may be suggested that the use of drones for surveillance purposes above one's own private property may be allowed as long as that use is proclaimed for at a competent authority, just as is the case for fixed cameras for home surveillance.[305]

---

[302] R. FOGEL, "CCTV and video surveillance laws in US", www.smartsign.com 7 December 2011.
[303] CJEU 11 December 2014, C-212/13, Ryneš/Office for Personal Data Protection, §16; K.E. BOON and D.C. LOVELACE JR., *The domestic use of unmanned aerial vehicles*, New York, Oxford University Press, 2014, 265; P. DE HERT and R. SAELENS, "De camerawet: een zoektocht naar een afweging tussen het recht op privacy en het recht op veiligheid", *T. Strafr*. 2007, 96; K. CLERIX, "De privacy-lacunes van de camerawet", *Mondiaal Nieuws* 13 maart 2014; R. FOGEL, "CCTV and video surveillance laws in US", www.smartsign.com 7 December 2011; O. RUDGARD, "Should you install CCTV outside your home?", *The Telegraph* 22 May 2015; X., *Aangifte van een bewakingscamera*, www.privacycommission.be.
[304] Fourth Amendment to the United States Constitution; US Supreme Court, 476 U.S. 207 (1986), California/Ciraolo; CJEU 11 December 2014, C-212/13, Ryneš/Office for Personal Data Protection, §33; K.E. BOON and D.C. LOVELACE JR., *The domestic use of unmanned aerial vehicles*, New York, Oxford University Press, 2014, 227; O. RUDGARD, "Should you install CCTV outside your home?", *The Telegraph* 22 May 2015.
[305] *Supra* 71, nr. 107.

This may be the same authority that is competent for the placement of surveillance cameras by civil users, but also a new authority may be established. Also, a sign has to be put up to warn individuals that they are located in an area that is guarded by UAVs, and thus to warn them that they might be filmed.[306] Furthermore, the use of the camera-equipped drones should be in accordance to the privacy rules.[307]

§2 Filling up the gap

109. FILLING THE GAP – As was mentioned before, the current legislation involving mobile cameras for surveillance purposes mainly concerns the use of them by law enforcement bodies and public authorities.[308] The legislation on international, EU and national level remains however quiet about the use of mobile surveillance cameras by private parties. This means that it is not explicitly allowed, but it is not explicitly prohibited by law either. This section will assume that it can be allowed, but that caution should be exercised, and therefor it will suggest some safeguards that may be put into place to assure that an individual's privacy and data protection rights are respected. The usage of drones can be regulated in a number of ways. Firstly, it can be regulated by data protection and aviation laws. However, this thesis has indicated that regulators cannot keep up with the fast advancing technologies and are forced to provide either vague legislation, or legislation which cannot foresee what is yet to come. Legislation thus seems to be inadequate to answer to issues relating fast developing modern technologies infringing on well-established privacy and data protection rights, and therefor it might be necessary to look for solutions somewhere else than on the regulatory level. Therefor, the usage of drones could also be regulated by design, meaning that developers of these technologies have an important role to play.

---

[306] K.E. BOON and D.C. LOVELACE JR., *The domestic use of unmanned aerial vehicles*, New York, Oxford University Press, 2014, 265; ICO, *CCTV*, https://ico.org.uk; O. RUDGARD, "Should you install CCTV outside your home?", *The Telegraph* 22 May 2015; X., *Aangifte van een bewakingscamera*, www.privacycommission.be.

[307] K.E. BOON and D.C. LOVELACE JR., *The domestic use of unmanned aerial vehicles*, New York, Oxford University Press, 2014, 265; CAA, *Droneaware*, http://publicapps.caa.co.uk; K. CLERIX, "De privacy-lacunes van de camerawet", *Mondiaal Nieuws* 13 maart 2014; R. FOGEL, "CCTV and video surveillance laws in US", www.smartsign.com 7 December 2011; X., *Flying drones: guidance on the safety rules that apply when flying unmanned and model aircraft*, http://www.caa.co.uk

[308] *Supra* 70-71, nr. 106.

A. Privacy-enhancing technologies

110. PETs – Privacy-enhancing technologies, or PETs, are technologies which can help to design information and communication services and systems in a way that it minimizes the collection and use of personal data and facilitate compliance with data protection and privacy rules.[309] Technologies can thus be the solution to a problem of drones provoking socially disruptive outcomes by technologically (re)designing them.[310] An example of a PET is the automatic anonymisation after a certain lapse of time, which supports the principle that the processed data should be kept in a form which can identify data subjects for no longer than necessary for the purposes for which the data was originally collected.[311] Privacy by design and privacy by default make use of these PETs in order to take privacy enhancing measures and to minimize data collection to the purposes necessary for the aim of the processing of data. Privacy by design and privacy by default are relatively new concepts, explicitly written down in the current European GDPR.[312] However, it could already be derived from existing law, in particular from article 17 of the European Data Protection Directive, which demands appropriate technical and organisational measures to protect personal data.

---

[309] D. KLITOU, *Privacy-invading technologies and privacy by design*, The Hague, Asser Press, 2014, 267; E. MORDINI and P. DE HERT, *Ageing and invisibility*, Amsterdam, IOS Press, 2010, 126-127; D. WRIGHT and P. DE HERT, *Privacy Impact Assessment*, Dordrecht, Springer, 2012, 221; X., *Privacy-enhancing technologies (PETs)*, europa.eu; A. ZAVRŠNIK, *Drones and unmanned aerial systems: legal and social implications for security and surveillance*, Heidelberg, Springer, 2016, 251.

[310] C.J. BENNETT, *The privacy advocates: resisting the spread of surveillance*, Cambridge, The MIT Press, 2008, 84; D. KLITOU, *Privacy-invading technologies and privacy by design*, The Hague, Asser Press, 2014, 267; A. ZAVRŠNIK, *Drones and unmanned aerial systems: legal and social implications for security and surveillance*, Heidelberg, Springer, 2016, 252.

[311] C.J. BENNETT, *The privacy advocates: resisting the spread of surveillance*, Cambridge, The MIT Press, 2008, 84; D. KLITOU, *Privacy-invading technologies and privacy by design*, The Hague, Asser Press, 2014, 279; B. PRENEEL and D. IKONOMOU, *Privacy technologies and policy*, Heidelberg, Springer, 2014, 66; J. STEVOVIC, E. BASSI, A. GIORI, F. CASATI and G. ARMELLIN, "Enabling privacy by design in medical records sharing", in S. GUTWIRTH, R. LEENES and P. DE HERT, *Reforming European data protection law*, Dordrecht, Springer, 2015, 389; X., *Privacy-enhancing technologies (PETs)*, europa.eu; A. ZAVRŠNIK, *Drones and unmanned aerial systems: legal and social implications for security and surveillance*, Heidelberg, Springer, 2016, 252.

[312] Article 23 and Recital 61 GDPR; M. HANSEN, "Data protection by default in identity-related applications", in S. FISCHER-HÜBNER, E. DE LEEUW and C.J. MITCHELL, *Policies and research in identity management*, Heidelberg, Springer, 2013, 4-5; E. LACHAUD, "Could the CE marking be relevant to enforce privacy by design in the Internet of Things", in S. GUTWIRTH, R. LEENES and P. DE HERT, *Data protection on the move: Current developments in ICT and privacy/data protection*, Dordrecht, Springer, 2016, 137; E. MORDINI and P. DE HERT, *Ageing and invisibility*, Amsterdam, IOS Press, 2010, 126; G. SKOUMA and L. LÉONARD, "On-line behavioral tracking: what may change after the legal reform on personal data protection", in S. GUTWIRTH, R. LEENES and P. DE HERT, *Reforming European data protection law*, Dordrecht, Springer, 2015, 36.

B. Privacy by design and privacy by default

1. Privacy by design

1.1 Definition

111. PRIVACY BY DESIGN – Privacy by design is a relatively new concept which introduces the idea of a social and ethical responsibility of engineers and designers when researching, inventing, engineering or designing technologies that may have an effect on society, and more specifically on an individual's right to privacy.[313] The aim of privacy by design is to develop systems or devices which are privacy-aware or privacy-friendly.[314] In other words, privacy by design are practical measures in the form of technological and design-based solutions, aimed at bolstering privacy and data protection laws in order to better ensure compliance and minimize the privacy-intrusive capabilities of technologies.[315] This approach addresses the difficulties that data controllers may face to take relevant privacy and data protection measures after the devices or systems have already been developed and deployed, and places the responsibility at the basis line when those devices or systems are being brought to life.[316]

[313] Article 17 Data Protection Directive 95/46/EC; Privacy Act 1974 Title 5, U.S.C. Part I, Chapter 5, Subchapter II, §552a; D. KLITOU, *Privacy-invading technologies and privacy by design*, The Hague, Asser Press, 2014, 260-261; B. PRENEEL and D. IKONOMOU, *Privacy technologies and policy*, Heidelberg, Springer, 2014, 66; X., *The Privacy Act of 1974*, www.epic.org; A. ZAVRŠNIK, *Drones and unmanned aerial systems: legal and social implications for security and surveillance*, Heidelberg, Springer, 2016, 251.

[314] M. HANSEN, "Data protection by default in identity-related applications", in S. FISCHER-HÜBNER, E. DE LEEUW and C.J. MITCHELL, *Policies and research in identity management*, Heidelberg, Springer, 2013, 4; ICO, *In the picture: A data protection code of practice for surveillance cameras and personal information*, https://ico.org.uk 2015, 31; D. KLITOU, *Privacy-invading technologies and privacy by design*, The Hague, Asser Press, 2014, 262.

[315] M. HANSEN, "Data protection by default in identity-related applications", in S. FISCHER-HÜBNER, E. DE LEEUW and C.J. MITCHELL, *Policies and research in identity management*, Heidelberg, Springer, 2013, 4; D. KLITOU, *Privacy-invading technologies and privacy by design*, The Hague, Asser Press, 2014, 262.

[316] Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, Article 29 Working Party, 02356/09/EN, WP 168, 1 december 2009, 3; D. KLITOU, *Privacy-invading technologies and privacy by design*, The Hague, Asser Press, 2014, 268; E. MORDINI and P. DE HERT, *Ageing and invisibility*, Amsterdam, IOS Press, 2010, 126.

1.2 Application in practice

112. ARTIFICIAL INTELLIGENCE – Applied to CCTV, privacy by design introduces the idea of artificial intelligence or software agents limiting the recording by the cameras to when a certain antisocial act or suspected crime is taking place, hereby diminishing panoptic feelings, undue surveillance and collateral intrusion which people must involuntarily endure by public CCTV cameras.[317] A software algorithm may be used to process images in real-time and distinguish between suspicious or illegal behavior and innocent, ordinary or legal behavior.[318] A parallel line may drawn to the use of drones for surveillance purposes, limiting the actual recording to suspicious or illegal behavior on an individual's private property and processing images in real-time without recording when legal activities are taking place. An example hereof would be the real-time filming of the mailman delivering the post, but the recording of an unknown individual trying to break into the house through the window.

113. GEOFENCING – DJI, a Chinese company specialized in drones, installed a geofencing feature in their devices, which automatically prevents them from entering sensitive airspace like the area around prisons, power plants and airports.[319] This geofencing system works by using a built-in GPS in the drone to compare its location against a map of no-fly zones.[320] If the drone seems to be in or near a restricted no-fly zone, DJI's system will give a warning to the user through its app and will refuse to enter the restricted area.[321]

---

[317] D. KLITOU, *Privacy-invading technologies and privacy by design*, The Hague, Asser Press, 2014, 269; B. PRENEEL and D. IKONOMOU, *Privacy technologies and policy*, Heidelberg, Springer, 2014, 91; D. WRIGHT and P. DE HERT, *Privacy Impact Assessment*, Dordrecht, Springer, 2012, 370.

[318] D. KLITOU, *Privacy-invading technologies and privacy by design*, The Hague, Asser Press, 2014, 269; B. PRENEEL and D. IKONOMOU, *Privacy technologies and policy*, Heidelberg, Springer, 2014, 91; D. WRIGHT and P. DE HERT, *Privacy Impact Assessment*, Dordrecht, Springer, 2012, 370.

[319] S.E. KREPS, *Drones: What everyone needs to know*, New York, Oxford University Press, 2016, 38; K. LESWING, "Why your drone can't fly near airports anymore", *Fortune* 18 November 2015.

[320] 7th Report of 2014-2015 on the Civilian use of drones in the EU*,* House of Lords, HL 122, 5 March 2015, 61; K. LESWING, "Why your drone can't fly near airports anymore", *Fortune* 18 November 2015; A. NAIT-SIDI-MOH, M. BAKHOUYA, J. GABER and M. WACK, *Geopositioning and mobility*, New Jersey, Wiley & Sons Inc., 2013, 158; A. ZAVRŠNIK, *Drones and unmanned aerial systems: legal and social implications for security and surveillance*, Heidelberg, Springer, 2016, 251.

[321] K. LESWING, "Why your drone can't fly near airports anymore", *Fortune* 18 November 2015; X., *6th sense and avoid*, www.dronesense.com; A. NAIT-SIDI-MOH, M. BAKHOUYA, J. GABER and M. WACK, *Geopositioning and mobility*, New Jersey, Wiley & Sons Inc., 2013, 146; P.L. PRATYUSHA, "Geo-fencing for unmanned aerial vehicle", *International Journal of Computer Applications* 2015, 1; A.

This is an example of the industry recognizing national security issues with UAVs and trying to resolve them at the basis line instead of waiting for possible draconian legislation.[322] In application to UAVs being used by civilians for surveillance purposes, this system technology may be used to indicate the maximum allowable radius for a drone to travel, which would be the individual's own private property.[323] When it reaches that maximum allowable radius, certain actions may be performed such as an alert, auto landing or return to launch.[324] To prevent possible abuses, it may be advised to have the coordinates of the allowable radius installed in the features of the drone by a certified expert or by the seller of UAVs.

2. Privacy by default

2.1 Definition

114. PRIVACY BY DEFAULT – The exact interpretation of privacy by default is still being debated. However, in the GDPR, privacy by default puts the responsibilities with the data controller, who needs to implement mechanisms to ensure that only those personal data are being processed which are necessary for the specific purpose of the processing and that the data is not collected beyond the minimum necessary for that purpose, both in terms of the amount of the data and the time of their storage.[325] Privacy by default often appears in combination with privacy by design, and thus constitutes a cooperation between engineers and designers of the devices or systems and the data controllers after it has been designed and put on the market.[326]

ZAVRŠNIK, *Drones and unmanned aerial systems: legal and social implications for security and surveillance*, Heidelberg, Springer, 2016, 253.

[322] S.E. KREPS, *Drones: What everyone needs to know*, New York, Oxford University Press, 2016, 38; K. LESWING, "Why your drone can't fly near airports anymore", *Fortune* 18 November 2015.

[323] A.M. ANTONOPOULOS, "Geo-fencing for ArduCopter – Keep your copter fenced in", https://diydrones.com 28 April 2012; N. DEY and A. MUKHERJEE, *Embedded systems and robotics with open source tools*, New York, CRC Press, 2016, 171.

[324] N. DEY and A. MUKHERJEE, *Embedded systems and robotics with open source tools*, New York, CRC Press, 2016, 171; P.L. PRATYUSHA, "Geo-fencing for unmanned aerial vehicle", *International Journal of Computer Applications* 2015, 1.

[325] M. HANSEN, "Data protection by default in identity-related applications", in S. FISCHER-HÜBNER, E. DE LEEUW and C.J. MITCHELL, *Policies and research in identity management*, Heidelberg, Springer, 2013, 5; A. KISS and G.L. SZOKE, "Evolution of revolution? Steps forward to a new generation of data protection regulation", in S. GUTWIRTH, R. LEENES and P. DE HERT, *Reforming European data protection law: Issues in privacy and data protection*, Dordrecht, Springer, 2015, 325; B. PRENEEL and D. IKONOMOU, *Privacy technologies and policy*, Heidelberg, Springer, 2014, 74.

[326] M. HANSEN, "Data protection by default in identity-related applications", in S. FISCHER-HÜBNER, E. DE LEEUW and C.J. MITCHELL, *Policies and research in identity management*, Heidelberg, Springer,

The aim of privacy by default is that the data subject will not have to take any action in order to have their privacy protected but rather that it is built into the system by default, *i.e.* a simple use of the device or the system with least privacy infringement.[327]

2.2 Application in practice

115. CODE OF PRACTICE – In order to have data controllers implement mechanisms to ensure data protection, it might be advised to have a code of practice regarding the use of drones for surveillance purposes.[328] In the UK, a code of practice for the use of CCTV cameras already exists, which lay out the most important principles one should take into account when installing a fixed surveillance camera.[329] Parallel to that code, a similar code of practice may be enacted in every national jurisdiction to administer the use of surveillance drones, setting out the main principles that have to be taken into account specifically with regards to mobile cameras and the use of them for surveillance purposes. A problem would then be the enforcement of the code, however, this can be ensured by connecting infringements to certain penalties, as is the case with the Dronecode in the UK.[330]

2013, 4; B. PRENEEL and D. IKONOMOU, *Privacy technologies and policy*, Heidelberg, Springer, 2014, 99.

[327] A. CAVOUKIAN, "Privacy by design: the 7 foundational principles", https://www.ipc.on.ca 2011; M. HANSEN, "Data protection by default in identity-related applications", in S. FISCHER-HÜBNER, E. DE LEEUW and C.J. MITCHELL, *Policies and research in identity management*, Heidelberg, Springer, 2013, 6; D. KLITOU, *Privacy-invading technologies and privacy by design*, The Hague, Asser Press, 2014, 279; B. PRENEEL and D. IKONOMOU, *Privacy technologies and policy*, Heidelberg, Springer, 2014, 74.

[328] A. MURRAY, *Information technology law: the law and society*, Oxford, Oxford University Press, 2013, 530.

[329] *Supra* 65-66, nr. 99.

[330] *Supra* 50, nr. 75.

Conclusion

116. CONCLUSION – Although more and more regulation is being enacted regarding the use of drones, the use of it by civilians for surveillance purposes still remains an unsearched area of the law. However, it is advised to have some clarification on this subject since drones are becoming increasingly available for the general public at a reasonable and affordable price. As an answer to the question posed by this master thesis, it can be said that the use of mobile cameras, and more specifically drones, by private parties for surveillance purposes is not explicitly prohibited by the law, but it is not explicitly allowed either. Therefor, it is advised to look at already existing surveillance law and apply this in parallel to surveillance drones to the extent that it is possible. First of all, surveillance drones may not film outside the data controller's own private property, this is to respect the reasonable expectation of privacy of individuals on public domain and on their own private domain. Furthermore, data controllers should take appropriate actions to warn individuals of the possibility that they might be filmed by putting up a sign on their private property, which may mitigate the issue of drones being inaudible and invisible. Also a registration at a competent authority of surveillance drones might be made mandatory, as is already the case for CCTV cameras. However, besides the existing surveillance legislation, it is also advised to use modern day privacy-enhancing technologies to its advantage and address the specific issues that arise out of the use of drones for surveillance purposes. Privacy by design developments such as artificial intelligence and geofencing may help legislators to address privacy and data protection issues, and privacy by default developments may help data controllers to stay within the boundaries of the privacy rights of the data subjects, without the latter having to take any action. To conclude, it can be said that surveillance done by private parties using UAVs is possible as long as privacy and data protection rights are respected and the aforementioned safeguards are met.

BIBLIOGRAPHY

LEGISLATION

International

- Universal Declaration of Human Rights, *UNTS* 10 December 1948, 217 A (III);
- International Covenant on Civil and Political Rights, *UNTS* 16 December 1966, No. 14668;
- Convention on International Civil Aviation, *UNTS* 7 December 1944, 15-295;
- OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data;
- Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data of 15 December 2015;
- ICAO Circular 328-AN/190, Unmanned Aircraft Systems (UAS), 38p.

Europe

- European Convention on Human Rights, *ETS* 4 November 1950, 5;
- Convention for the protection of individuals with regard to automatic processing of personal data, *ETS* 28 January 1981, 108;
- Charter of Fundamental Rights of the European Union, *OJEC* 18 December 2000, 364/1;
- 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, *OJEC* 23 November 1995, 281/31;
- Regulation of the European Parliament and of the Council 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, *OJEU* 4 May 2016, 119/1;
- Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 2012/0011 (COD), 15039/15;

- Communication from the Commission to the European Parliament and the Council, "A new era for aviation: opening the aviation market to the civil use of remotely piloted aircraft systems in a safe and sustainable manner", COM(2014) 207, 9 p.;
- Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, Article 29 Working Party, 02356/09/EN, WP 168, 1 december 2009, 28 p.

Belgium

- Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, *BS* 18 maart 1993;
- Wet van 21 maart 2007 tot regeling van de plaatsing en het gebruik van bewakingscamera's, *BS* 31 mei 2007;
- Koninklijk Besluit van 2 juli 2008 betreffende de aangiften van de plaatsing en het gebruik van bewakingscamera's, *BS* 15 juli 2008;
- Koninklijk Besluit van 10 april 2016 met betrekking tot het gebruik van op afstand bestuurde luchtvaartuigen in het Belgisch luchtruim, *BS* 15 april 2016;
- Wetsontwerp houdende wijziging van de wet van 21 maart 2007 tot regeling van de plaatsing en het gebruik van bewakingscamera's, *Parl. St.* Kamer 2008-09, nr. 2076/003, 7 p. ;
- Verslag namens de Commissie voor de Binnenlandse Zaken en voor de Administratieve Aangelegenheden uitgebracht door de heer DELPÉRÉE omtrent het wetsvoorstel tot regeling van de plaatsing en het gebruik van bewakingscamera's, *Parl*. *St*. Senaat, 2006-07, nr. 3-1734/5, 48 p.;
- Principenota van 20 januari 2010 betreffende de wet tot regeling van de plaatsing en het gebruik van bewakingscamera's, nr. 2007.2, 21 p.;
- Aanbeveling nr. 04/2012 van 29 februari 2012 van de Privacycommissie inzake de diverse toepassingsmogelijkheden van camerabewaking, 24 p.

United Kingdom

- Data Protection Act 1998;
- UK Air Navigation Order 2009;
- Protection of Freedoms Act 2012;
- CCTV Code of Practice;
- Dronecode of the UK Civil Aviation Authority;
- 7th Report of 2014-2015 on the Civilian use of drones in the EU, House of Lords, HL 122, 5 March 2015.

United States

- First Amendment to the United States Constitution;
- Fourth Amendment to the United States Constitution;
- Fifth Amendment to the United States Constitution;
- US Privacy Act of 1974;
- FAA Modernization and Reform Act of 2012;
- USA Freedom Act of 2015;
- Drone Aircraft Privacy and Transparency Act of 2015.

CASE LAW

Europe

- CJEU 6 November 2003, C-101/01, Lindqvist;
- CJEU 13 May 2014, C-131/12, Google Spain/Spanish Data Protection Agency (AEPD);
- CJEU 11 December 2014, C-212/13, Ryneš/Office for Personal Data Protection;
- CJEU 6 October 2015, C-362/14, Maximillian Schrems/Data Protection Commissioner;
- ECtHR 28 January 2003, nr. 44647/98, Peck/United Kingdom;
- ECtHR 4 December 2008, nr. 30562/04 and 30566/04, S. and Marper/United Kingdom;
- ECtHR 7 February 2012, nr. 40660/08 and 60641/08, Von Hannover/Germany.

Belgium

- Brussel 9 november 2015, *Computerr.* 2016, 61-67.

United Kingdom

- House of Lords, UKHL 53 (2003), Wainwright/Home Office.

United States

- US Supreme Court, 277 U.S. 438 (1928), Olmstead/United States;
- US Supreme Court, 328 U.S. 256 (1946), United States/Causby;
- US Supreme Court, 389 U.S. 347 (1967), Katz/United States;
- US Supreme Court, 476 U.S. 207 (1986), California/Ciraolo;
- US Supreme Court, 533 U.S. 27 (2001), Kyllo/United States;
- Los Angeles Superior Court, SC 077 257 (2003), Streisand/Adelman.

LEGAL DOCTRINE

Books

- ABEYRATNE, R., *Convention on International Civil Aviation: A commentary*, Cham, Springer, 2014, 737 p.;
- ALEMANNO, A. and SIBONY, A.L., *Nudge and the law: a European perspective*, Oxford, Hart Publishing, 2015, 336 p.;
- BELLABY, R.W., *The ethics of intelligence: A new framework*, New York, Routledge, 2014, 204 p.;
- BENNETT, C.J., *The privacy advocates: resisting the spread of surveillance*, Cambridge, The MIT Press, 2008, 288 p.;
- BOEHM, F., *Information sharing and data protection in the area of freedom, security and justice*, Heidelberg, Springer, 2012, 468 p.;
- BOILLAT, P. and KJAERUM, M., *Handbook on European data protection law*, http://www.echr.coe.int, 2014, 201 p.;
- BOON, K.E. and LOVELACE JR., D.C., *The domestic use of unmanned aerial vehicles*, New York, Oxford University Press, 2014, 326 p.;
- CAREY, P., *E-privacy and online data protection*, Amsterdam, LexisNexis, 2002, 268 p.;

- COLONNA, L., "Europe versus Facebook: an imbroglio of EU data protection issues", in GUTWIRTH, S., LEENES, R. and DE HERT, P., *Data protection on the move: Current developments in ICT and privacy/data protection*, Dordrecht, Springer, 2016, 25-50;
- CUNNINGHAM, D. and NOAKES, J., "What if she's from the FBI? The effects of covert forms of social control on social movements", in M. DEFLEM, *Surveillance and governance: Crime control and beyond*, Bingley, Emerald Group Publishing Limited, 2008, 175-197;
- CUSTERS, B.H.M., OERLEMANS, J.J. en VERGOUW, S.J., *Het gebruik van drones: een verkennend onderzoek naar onbemande luchtvaartuigen*, Meppel, Boom Lemma Uitgevers, 2015, 172 p.;
- DE HERT, P., *Handboek privacy: persoonsgegevens in België*, Brussel, Politeia, 2003, 161 p.;
- DE HERT, P. and GUTWIRTH, S., "Privacy, data protection and law enforcement: opacity of the individual and transparency of the power", in E. CLAES, A. DUFF and S. GUTWIRTH, *Privacy and the criminal law*, Antwerpen, Intersentia, 2006, 61-104;
- DE HERT, P. and GUTWIRTH, S., "Data protection in the case law of Strasbourg and Luxembourg: constitutionalisation in action", in GUTWIRTH, S., POULLET, Y., DE HERT, P., DE TERWANGNE, C. and NOUWT, S., *Reinventing data protection?*, Berlin, Springer, 2009, 3-44;
- FINN. R.L, WRIGHT, D. and FRIEDEWALD, M., "Seven types of privacy", in GUTWIRTH, S., LEENES, R., DE HERT, P. and POULLET, Y., *European data protection: coming of age*, Dordrecht, Springer, 2013, 3-32;
- FRITSCH, C., "Data processing in employment relations; impacts of the European general data protection regulation focusing on the data protection officer at the worksite", in S. GUTWIRTH, R. LEENES and P. DE HERT, *Reforming European data protection law: issues in privacy and data protection*, Dordrecht, Springer, 2015, 147-167;
- GALIANO, D., *The fourth amendment: unreasonable search and seizure*, New York, The Rosen Publishing Group, 2011, 64 p.;

- GOMES DE ANDRADE, N.N., "The right to privacy and the right to identity in the age of ubiquitous computing: friends or foes? A proposal towards a legal articulation", in AKRIVOPOULOU, C. and PSYGKAS, A.E., *Personal data privacy and protection in a surveillance era: technologies and practices*, New York, Information Science Reference 2011, 19-43;
- GOMES DE ANDRADE, N.N. and MONTELEONE, S., "Digital natives and the metamorphosis of the European information society. The emerging behavioral trends regarding privacy and their legal implications", in GUTWIRTH, S., LEENES, R., DE HERT, P. and POULLET, Y., *European data protection: coming of age*, Dordrecht, Springer, 2013, 119-144;
- GONZALEZ FUSTER, G., *The emergence of personal data protection as a fundamental right of the EU*, Dordrecht, Springer, 2014, 274 p.;
- HANSEN, M., "Data protection by default in identity-related applications", in FISCHER-HÜBNER, S., DE LEEUW, E. and MITCHELL, C.J., *Policies and research in identity management*, Heidelberg, Springer, 2013, 4-17;
- HERVEY, T.K. and MCHALE, J.V., *Health law and the European Union*, New York, Cambridge University Press, 2004, 469 p.;
- ICO, *In the picture: A data protection code of practice for surveillance cameras and personal information*, https://ico.org.uk 2015, 45 p.;
- JACOBSEN, A.F., *Human rights monitoring: A field mission manual*, Leiden, Martinus Nijhoff Publishers, 2008, 656 p.;
- KINDT, E.J., *Privacy and data protection issues of biometric applications: a comparative legal analysis*, Dordrecht, Springer, 2013, 975 p.;
- KISS, A. and SZOKE, G.L., "Evolution of revolution? Steps forward to a nw generation of data protection regulation", in GUTWIRTH, S., LEENES, R. and DE HERT, P., *Reforming European data protection law: Issues in privacy and data protection*, Dordrecht, Springer, 2015, 311-332;
- KLITOU, D., *Privacy-invading technologies and privacy by design*, The Hague, Asser Press, 2014, 338 p.;
- KORENHOF, P., AUSLOOS, J. *et al*., "Timing the right to be forgotten: a study into 'time' as a factor in deciding about retention or erasure of data", in GUTWIRTH, S., LEENES, R. and DE HERT, P., *Reforming European data protection law*, Dordrecht, Springer, 2015, 171-201;

- KOSTA, E., *Consent in European data protection law*, Leiden, Martinus Nijhoff Publishers, 2013, 462 p.;
- KOSTA, V., *Fundamental rights in EU internal market legislation*, Oxford, Hart Publishing, 2015, 336 p.;
- KREPS, S.E., *Drones: What everyone needs to know*, New York, Oxford University Press, 2016, 240 p.;
- KROENER, I., *CCTV: A technology under the radar*?, Surrey, Ashgate Publishing Limited, 2014, 162 p.;
- LACHAUD, E., "Could the CE marking be relevant to enforce privacy by design in the Internet of Things", in GUTWIRTH, S., LEENES, R. and DE HERT, P., *Data protection on the move: Current developments in ICT and privacy/data protection*, Dordrecht, Springer, 2016, 135-162;
- LYON, D., *Surveillance studies: An overview*, Cambridge, Polity Press, 2007, 243 p.;
- MACKENZIE, D., *ICAO: A history of the International Civil Aviation Organization*, Toronto, University of Toronto Press Incorporated, 2010, 560 p.;
- MARCELLA JR., A.J. and STUCKI, C., *Privacy handbook: guidelines, exposures, policy implementation and international issues*, New Jersey, John Wiley & Sons Inc., 2003, 384 p.;
- MCINNIS, T.N., *The evolution of the Fourth Amendment*, Plymouth, Lexington Books, 2010, 334 p.;
- MORDINI, E. and DE HERT, P., *Ageing and invisibility*, Amsterdam, IOS Press, 2010, 222 p.;
- MORTELÉ, J., VERMEERSCH, H., DE PAUW, E., HARDYNS, W. and DEPRINS, F., *Cameratoezicht in de openbare ruimte. Ook wie weg is, is gezien?,* Antwerpen, Maklu, 2013, 196 p.;
- MURRAY, A., *Information technology law: the law and society*, Oxford, Oxford University Press, 2013, 602 p.;
- NACOS, B.L., *Terrorism and counterterrorism*, New York, Routledge, 2016, 500 p.;
- NAIT-SIDI-MOH, A., BAKHOUYA, M., GABER, J. and WACK, M., *Geopositioning and mobility*, New Jersey, Wiley & Sons Inc., 2013, 264 p.;

- NOUWT, S., DE VRIES, B.R. and PRINS, C., *Reasonable expectations of privacy? Elevent country reports on camera surveillance and workplace privacy*, The Hague, TMC Asser Press, 2005, 363 p.;
- ODUNTAN, G., *Sovereignty and jurisdiction in the airspace and outer space: legal criteria for spatial delimitation*, Oxon, Routledge, 2012, 408 p.;
- OXLEY, A., *Security risks in social media technologies*, Oxford, Chandos Publishing, 2013, 292 p.;
- PEERS, S., HERVEY, T., KENNER, J. and WARD, A., *The EU charter of fundamental rights: A commentary*, Oxford, Hart Publishing, 2014, 1865 p.;
- PRENEEL, B. and IKONOMOU, D., *Privacy technologies and policy*, Heidelberg, Springer, 2014, 215 p.;
- RALLO, A. and MARTINEZ, R., "Data protection, social networks and online mass media", in GUTWIRTH, S., LEENES, R., DE HERT, P. and POULLET, Y., *European data protection: coming of age*, Dordrecht, Springer, 2013, 407-430;
- RENGEL, A., *Privacy in the 21st century*, Leiden, Martinus Nijhoff Publishers, 2013, 280 p.;
- RICHARDSON, M., BRYAN, M., VRANKEN, M. And BARNETT, K., *Breach of confidence: social origins and modern developments*, Cheltenham, Edward Elgar Publishing Limited, 2012, 192 p.;
- SCAIFE, L., *Handbook of social media and the law*, New York, Informa Law from Routledge, 2015, 444 p.;
- SKOUMA, G. and LÉONARD, L., "On-line behavioral tracking: what may change after the legal reform on personal data protection", in GUTWIRTH, S., LEENES, R. and DE HERT, P., *Reforming European data protection law*, Dordrecht, Springer, 2015, 35-60;
- SOLOVE, D.J., *Understanding privacy*, Cambridge, Harvard University Press, 2008, 272 p.;
- STEVOVIC, J., BASSI, E., GIORI, A., CASATI, F. and ARMELLIN, G., "Enabling privacy by design in medical records sharing", in S. GUTWIRTH, R. LEENES and P. DE HERT, *Reforming European data protection law*, Dordrecht, Springer, 2015, 385-406;

- STYLIANOU, K.K., "Hasta la vista privacy, or how technology terminated privacy", in AKRIVOPOULOU, C. and PSYGKAS, A.E., *Personal data privacy and protection in a surveillance era: technologies and practices*, New York, Information Science Reference 2011, 44-58;
- TERSTEGGE, J., "Privacy in the law", in PETKOVIĆ, M. and JONKER, W., *Security, privacy, and trust in modern data management*, Berlin, Springer, 2007, 11-20;
- VAN LIESHOUT, M., "Privacy and innovation: from disruption to opportunities", in GUTWIRTH, S., LEENES, R. and DE HERT, P., *Data protection on the move: Current developments in ICT and privacy/data protection*, Dordrecht, Springer, 2016, 195-212;
- WADHAM, J., HARRIS, K. and PERETZ, G., *Blackstone's guide to the Freedom of Information Act 2000*, Oxford, Oxford University Press, 2011, 284 p.;
- WALDO, J., LIN, H.S. and MILLETT, L.I., *Engaging privacy and information technology in a digital age*, Washington, The National Academies Press, 2007, 452 p.;
- WITZLEB, N., LINDSAY, D., PATERSON, M. and RODRICK, S., *Emerging challenges in privacy law: comparative perspectives*, Cambridge, Cambridge University Press, 2014, 470 p.;
- WRIGHT, D. and DE HERT, P., *Privacy Impact Assessment*, Dordrecht, Springer, 2012, 523 p.;
- ZAVRŠNIK, A., *Drones and unmanned aerial systems: legal and social implications for security and surveillance*, Heidelberg, Springer, 2016, 275 p.;
- ZIEGLER, K.S., *Human rights and private law: Privacy as autonomy*, Oregon, Hart Publishing, 2007, 242 p.

Articles

- ANTONOPOULOS, A.M., "Geo-fencing for ArduCopter – Keep your copter fenced in", https://diydrones.com 28 April 2012;
- ATWILL, N., "Online Privacy Law: France", https://www.loc.gov 2012;
- AVERETT, N., "Drones take off as wildlife conservation tool", www.audubon.org 2014;

- BANISAR, D. and DAVIES, S., "Privacy and human rights: an international survey of privacy laws and practice", gilc.org;
- BRUGGEMAN, F., "Wettelijke regeling voor drones is klaar", *De Redactie* 31 maart 2015;
- BUTLER, D., "The dawn of the age of the drones – an Australian privacy law perspective", *UNSW Law Journal* 2014, 434-470;
- CALO, M.R., "The drone as privacy catalyst", *Stanford Law Review Online* 12 December 2011;
- CAVOUKIAN, A., "Privacy by design: the 7 foundational principles", https://www.ipc.on.ca 2011;
- CHANG, L., "How easy is it to hijack a drone?", *Digital Trends* 2 March 2016;
- CLARKE, R., "Understanding the drone epidemic", *Computer Law & Security Review* 2014, 230-246;
- CLARKE, R., "What drones inherit from their ancestors", *Computer Law & Security Review* 2014, 247-262;
- CLARKE, R. AND MOSES, L.B., "The regulation of civilian drones' impacts on public safety", *Computer Law & Security Review* 2014, 263-285;
- CLARKE, R., "The regulation of civilian drones' impacts on behavioural privacy", *Computer Law & Security Review* 2014, 286-305;
- CROPPER, L., "GDPR gets the final seal of approval", privacylawblog.fieldfisher.com 15 April 2016;
- CURTIS, S., "Drone laws in the UK – what are the rules?", *The Guardian* 18 April 2016;
- DE BOT, D., "Eye in the sky – Het gebruik van drones en privacy", *Rechtskundig Weekblad* 2014-2015, 1362;
- DE HERT, P. and PAPAKONSTANTINOU, V., "The Council of Europe data protection convention reform: analysis of the new text and critical comment on its global ambition", *Computer Law & Security Review* 2014, 633-642;
- DE HERT, P. and SAELENS, R., "De camerawet: een zoektocht naar een afweging tussen het recht op privacy en het recht op veiligheid", *T. Strafr*. 2007, 93-100;
- DE LOOPER, C., "License plates for drones will make drone operators accountable for their actions", *Tech Times* 22 August 2015;

- DUNLAP, T., "We've got our eyes on you: When surveillance by unmanned aircraft systems constitutes a Fourth amendment search", *South Texas Law Review* 2009, 173-204;
- FÄRBER, H.B., "Eyes in the sky & privacy concerns on the ground", *Scitech Lawyer* 2015, 6-9;
- FINN, R.L. and WRIGHT, D., "Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications", *Computer Law and Security Review* 2012, 184-194;
- FINN, R.L., WRIGHT, D., JACQUES, L. and DE HERT, P., "Study on privacy, data protection and ethical risks in civil Remotely Piloted Aircraft Systems operations – final report", http://ec.europa.eu 2014, 413 p.;
- FOGEL, R., "CCTV and video surveillance laws in US", www.smartsign.com 7 December 2011;
- FRANTZIOU, E., "Further developments in the right to be forgotten: The European Court of Justice's judgment in case C-131/12, Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de datos", *Human Rights Law Review* 2014, 761-777;
- GLANCY, D.J., "The invention of the right to privacy", *Arizona Law Review* 1979, 1-39;
- GOOLD, B.J., "Surveillance and the political value of privacy", *Amsterdam Law Forum* 2009, 1-6;
- GREENLEAF, G., "The influence of European data privacy standards outside Europe: Implications for globalisation of Convention 108?", *International Data Privacy Law* 2012, 1-34;
- GUTWIRTH, S., "Short statement about the role of consent in the European data protection directive", http://works.bepress.com/serge_gutwirth 2012, 1-3;
- HERN, A., "Skateboards, drones and your brain: everything got hacked", *The Guardian* 11 August 2015;
- HUSTINX, P., "EU data protection law: the review of Directive 95/46/EC and the proposed general data protection regulation", https://secure.edps.europa.eu 2013, 1-52;
- JONES, C., "Drones: the UK debate and its implications for the EU", *EU Law Analysis* 28 May 2014;

- KILKELLY, U., "The right to respect for private and family life: A guide to the implementation of Article 8 of the European Convention on Human Rights", http://www.coe.int 2001, 1-66;
- CLERIX, K., "De privacy-lacunes van de camerawet", *Mondiaal Nieuws* 13 maart 2014;
- KOKOTT, J. and SOBOTTA, C., "The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR", *International Data Privacy Law* 2013, 222-228;
- KUIJER, M., "Effective remedies as a fundamental right", www.ejtn.eu 28 april 2014, 20 p.;
- KUNER, C., CATE, F.H. *et al*., "The data protection credibility crisis", *International Data Privacy Law* 2015, 161-162;
- LESWING, K., "Why your drone can't fly near airports anymore", *Fortune* 18 November 2015;
- LEWIS, P., "CCTV in the sky: Police plan to use military-style spy drones", *The Guardian* 23 January 2010;
- LUYCKX, J., "Sleutelgaten en drones", *Limburgs Rechtsleven* 2015, 253-254;
- LYON, D., "Facing the future: Seeking ethics for everyday surveillance", *Ethics and Information Technology* 2001, 171-181;
- MCBRIDE, P., "Beyond Orwell: The application of unmanned aircraft systems in domestic surveillance operations", *Journal of Air Law and Commerce* 2009, 627-662;
- MCNEAL, G., "Drones and aerial surveillance: considerations for legislators", *Brookings* November 2014, 1-34;
- PALMER, E., "Online Privacy Law: Germany", https://www.loc.gov 2012;
- PRATYUSHA, P.L., "Geo-fencing for unmanned aerial vehicle", *International Journal of Computer Applications* 2015, 1-7;
- PRENEEL, B., ROGAWAY, P., RYAN, M.D. and RYAN, P.Y.A., "Privacy and security in an age of surveillance", drops.dagstuhl.de 2014, 107-123;
- ROBBEN, F., "De wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens: toepassingsgebied en begripsdefinities", *www.frankrobben.be* 1994, 1-24;

- RUDGARD, O., "Should you install CCTV outside your home?", *The Telegraph* 22 May 2015;
- SCHERMER, B., "An eye in the sky: privacy aspects of drones", *Criminal Law and Criminology* 20 June 2013;
- SCHLAG, C., "The new privacy battle: how the expanding use of drones continues to erode our concept of privacy and privacy rights", *Journal of Technology, Law & Policy* 2013, 1-22;
- SIDDIQUE, H., "Home surveillance CCTV images may breach data protection laws, ECJ rules", *The Guardian* 11 December 2014;
- SIMONITE, T., "Drones could make rogue operators accountable", *MIT Technology Review* 18 August 2015;
- ULDALL, R., "Data protection reform – Parliament approves new rules fit for the digital era", http://www.europarl.europa.eu 2016;
- VACEK, J., "Big Brother will soon be watching – or will he? Constitutional, regulatory, and operational issues surrounding the use of unmanned arial vehicles in law enforcement", *North Dakota Law Review* 2009, 674-692;
- VAN ALSENOY, B., "The evolving role of the individual under EU data protection law", *ICRI Working Paper* 23/2015, 1-35;
- VERHEYEN, W., "Commercieel gebruik van drones: bedreig(en)de vogels?", *De Juristenkrant* 2014, 20;
- VERHEYEN, W., "Onbemande luchtvaartuigen: Vogelvrij of (nu al) gekooid?", *NJW* 2015, 338-347;
- VOLOVELSKY, U., "Civilian uses of unmanned aerial vehicles and the threat to the right to privacy – An Israeli case study", *Computer Law & Security Review* 2014, 306-320;
- WARREN, S.D. and BRANDEIS L.D., "The right to privacy", *Harvard Law Review* 15 December 1890;
- WASHBOURNE, C.L. and NATH, C., "Civilian drones", *Postnote* 2014, 1-5;
- WESSING, T., "Drones and data", united-kingdom.taylorwessing.com March 2015;
- WHITEHEAD, J.W., "Drones over America: Tyranny at home", *The Rutherford Institute* 28 June 2010;

- WRIGHT, D., "Drones: Regulatory challenges to an incipient industry", *Computer Law & Security Review* 2014, 226-229;
- X., "Drone over Heathrow was 'wingspan away' from collision with jet", *The Guardian* 26 February 2016;
- X. "Tina Turner's wedding photographed by drones", *The Huffington Post* 8 February 2013;
- X., "Lufthansa jumbo reports near miss with drone over Los Angeles", *The Guardian* 21 March 2016;
- YUHAS, A., "NSA reform: USA Freedom Act passes first surveillance reform in decade – as it happened", *The Guardian* 2 June 2015.

Other

- Opinion 04/2004 on the processing of personal data by means of video surveillance, Article 29 Data Protection Working Party, 11750/02/EN, WP 89, 11 February 2004, 26 p.;
- Opinion 08/2015 on applicable law, Article 29 Data Protection Working Party, 0836-02/10/EN, WP 179, 16 December 2010, 34 p.;
- Opinion 15/2011 on the definition of consent, Article 29 Data Protection Working Party, 01197/11/EN, WP 187, 13 July 2011, 38 p.;
- Opinion 01/2015 on privacy and data protection issues relating to the utilisation of drones, Article 29 Data Protection Working Party, 01673/15/EN, WP 231, 16 June 2015, 21 p.;
- Policy department C: citizens' rights and constitutional affairs, "Privacy and data protection implications of the civil use of drones: in-depth analysis for the LIBE Committee", PE.519.221, www.europarl.europa.eu, June 2015, 30 p.

INTERNET LINKS

- CAA, *Air navigation: The order and regulations*, https://publicapps.caa.co.uk;
- CAA, *Droneaware*, http://publicapps.caa.co.uk;
- ICO, *Drones*, https://ico.org.uk;
- ICO, *CCTV*, https://ico.org.uk;
- X., *Aangifte van een bewakingscamera*, www.privacycommission.be;
- X., *Article 29 Working Party*, http://ec.europa.eu;
- X., *Article 29 Working Party*, https://secure.edps.europa.eu;
- X., *Article 34 ECHR – admissibility of individual applications*, echr-online.info;
- X., *Common law right to privacy*, privacy.uslegal.com;
- X., *Domestic drones*, www.aclu.org;
- X., *Domestic Unmanned Aerial Vehicles (UAVs) and Drones*, www.epic.org;
- X., *Data protection legislation*, https://secure.edps.europa.eu;
- X., *6th sense and avoid*, www.dronesense.com;
- X., *European Union Directives*, eur-lex.europa.eu;
- X., *Flying drones: guidance on the safety rules that apply when flying unmanned and model aircraft*, http://www.caa.co.uk;
- X., *Het Belgisch Koninklijk Besluit werd zopas gepubliceerd!*, www.drone-kopen.be;
- X., *Het vonnis in de zaak Facebook*, www.privacycommission.be;
- X., *Is de camerawet van toepassing op drones?*, www.startpuntveiligheid.be;
- X., *Is de Privacywet van toepassing op de informatie die drones verwerken?*, www.privacycommission.be;
- X., *Legal matters and obtaining consent*, www.andfestival.org.uk;
- X., *Minister Galant heeft aangepast KB Drones rond*, www.drone-kopen.be;
- X., *OECD Guidelines on the protection of privacy and transborder flows of personal data*, http://www.oecd.org;
- X., *Overzicht van de drone wetgeving in België*, www.droneblog.be;
- X., *Privacy-enhancing technologies (PETs)*, europa.eu;
- X., *Questions and answers*, www.echr.coe.int;
- X., *Reform of EU data protection rules*, ec.europa.eu;

- X., *The general data protection regulation*, www.consolium.europa.eu;
- X., *The personal data act*, http://www.datainspektionen.se;
- X., *The Privacy Act of 1974*, www.epic.org;
- X., *Wat is een bewakingscamera?,* www.privacycommission.be;
- X., *Wat met hacking van drones?,* www.privacycommission.be;
- X., *What do I need to know about the right to privacy?*, http://findlaw.co.uk.