Journal of Politics and Law; Vol. 10, No. 5; 2017
ISSN 1913-9047 E-ISSN 1913-9055
Published by Canadian Center of Science and Education

The Value of Privacy and Surveillance Drones in the Public Domain: Scrutinizing the Dutch Flexible Deployment of Mobile Cameras Act

Gerdo Kuiper[1] & Quirine Eijkman[2]

[1] Lecturer in legal philosophy at the Leiden University of Applied Sciences and a PhD-candidate at the University of Amsterdam (UVA), the Netherlands

[2] PhD. is chair of the Access2Justice Research Group at the Centre for Social Innovation (KSI) Utrecht University of Applied Sciences and *Deputy President* at the National Human Rights Institute of the Netherlands. She contributed to this article in her personal capacity.

Correspondence: Gerdo Kuiper, Lecturer in legal philosophy at the Leiden University of Applied Sciences and a PhD-candidate at the University of Amsterdam (UVA), the Netherlands. E-mail: gerdokuiper@hotmail.com

Received: July 22, 2017 Accepted: August 18, 2017 Online Published: November 29, 2017

doi:10.5539/jpl.v10n5p35 URL: https://doi.org/10.5539/jpl.v10n5p35

Abstract

The flexible deployment of drones in the public domain, is in this article assessed from a legal philosophical perspective. On the basis of theories of Dworkin and Moore the distinction between individual rights and collective security policy goals is discussed. Mobile cameras in the public domain reflect how innovative technological tools challenge public authorities in new ways to balance between privacy and security. Furthermore, the different dimensions of privacy and the distinction between the three types of the value of privacy are reviewed. On the basis of the case study of the Dutch Drones Act, the article concludes that the flexible deployment of mobile cameras in the public domain is not legitimate from a normative perspective. The legal safeguards in the Netherlands are insufficient to protect the value of privacy. Therefore, further restrictions such as prior judicial review should be considered.

Keywords: value of privacy, surveillance, drone, public domain, legitimacy, flexible deployment, prior judicial review, legal philosophy

1. Introduction

Developments in security technology have made the monitoring of the public domain easier and cheaper. Video surveillance, Global-Positioning-Systems, body scanners at airports, and biometric technologies, combined with data mining, provide state agencies with innovative tools to protect public order and national security. The deployment of drones in the public domain is one such new tool. It's use, just like other security and safety measures, requires a balance between privacy and security. Many experts such as Edward Snowden believe we should be worried about our privacy being violated in exchange for security. Their concerns are twofold. On the one hand, the large impact that innovative security technologies may have on our privacy and autonomy and on the other hand, the complexity of ensuring the protection of these values.

This article discusses whether or not the flexible deployment of mobile cameras in the public domain, including drones, is legitimate from the perspective of the value of privacy. In the Netherlands the 2016 Flexible Deployment of Mobile Cameras in the Public Domain Act[1] allows a mayor to designate an area in which drones can be deployed. In times of crises, for example in case of a terrorist threat, but also with a view to dealing with regular crime or the regular maintenance of public order, the privacy of citizens may be restricted. This includes preventive body searches[2], a general duty to provide proof of identity[3] or visual camera surveillance in the public domain[4]. Public surveillance does not have to be overly intrusive to affect someone's life.

Privacy is a human right and a fundamental right. Bloustein (1964: 962) defines the value of privacy as follows:

[1] Flexible Deployment of Mobile Cameras in the Public Domain Act, *Parliamentary Papers II 2014*, 33582, 2.

[2] Preventive body searches Act, *Parliamentary Papers II* 1999, 26865, No. 2.

[3] Compulsory Identification (Extended Scope) Act, *Parliamentary Papers II* 2003, 29218, 2.

[4] CCTV Monitoring in Public Places Act, *Parliamentary Papers II* 2004, 29440, 2.

privacy determines the being of mankind and includes the individual dignity and integrity, the personal autonomy and independence. Privacy is, therefore, essential to the development and growth of each individual. From this perspective, it is evident that this value must be protected against non-necessary restrictions. Whether or not the deployment of drones should (always) be considered a non-necessary restriction is discussed in this article. The aspects which, according to the literature and case law, play a role are: the extent of transparency (visibility and clarity regarding purpose) of the camera surveillance, the kind and extent of intimacy the reasonable expectation of privacy of the people who are monitored, the use of the images and the side-effects (ECtHR, 1992, 2003a/b; HR, 1987a/b, 1995, 2004; Nouwt, de Vries & van der Burgt, 2005).[5] It is of great importance that the legal protection is properly regulated, so that this right to privacy can be protected. Furthermore, this contribution also addresses whether or not these concerns are sufficiently addressed in the Dutch Flexible Deployment of Mobile Cameras in the Public Domain Act and its Explanatory Memorandum.

Henceforth, this publication assesses the legitimacy of the Flexible Deployment of Mobile Cameras in the Public Domain Act (hereinafter the 'Drones Act') from a legal philosophical perspective. Thereby focussing on individual rights versus collective policy goals as well as the moment of review (before, *ex prior*, or after, *ex post*), by whom (judicial review or review by the executive power) and the burden of proof. Because of a 'statistical' form of collective action (Dworkin, 1996: 19-20) and a utilitarian approach by both legislative and executive power on the balance between security versus privacy, it is important for the academic and public debate that the 'rights as trumps' approach of Dworkin (1978) is considered in relation to the flexible deployment of mobile cameras in the public domain. Individual liberty rights can be deployed as trumps in relation to general policy goals in favour of the greater utility or the majority. Furthermore, it is challenging to avail yourself of your right to privacy in the context of such security measures. Therefore a new perspective on the review and the division of the burden of proof in the form of the 'balancing privacy and security while maintaining accountability' theory of Moore (2011, 2016) is worthwhile to consider. According to this theory, prior to the constraint the court conducts a review, *ex ante*, in which the applicant, the government, must demonstrate that there is a probable cause, 'reasonable suspicion', for an infringement of privacy and that the infringing measure is effective.

After a general introduction, this article commences by introducing the Dutch Drones Act and its privacy aspects. Subsequently, a comprehensive conceptual analysis of the concept of privacy is proposed. This includes the dimensions of privacy and the distinction of three types of the 'value of privacy'. Based on a legal classification and the case law of the European Court of Human Rights, the possibilities to protect your right to privacy are summarized. After a brief review of the concept of security, the balance between privacy and security is considered on the basis of theories of legal philosophers Dworkin and Moore. In the conclusion, the legitimacy of the flexible deployment of mobile cameras in the Dutch public domain is discussed.

2. The Dutch Drones Act

The Dutch Drones Act, which amended the existent Municipality Act, allows a mayor of a city or town to temporarily designate an area in which mobile cameras can be deployed.[6] Before CCTV cameras were 'nailed down' and remained in the same place for a considerable long time. For long municipalities advocated the need for a more flexible deployment of surveillance cameras in the public space. This is primarily motivated by the desire to better deal with persisting public nuisances and more effectively by the targeted use of cameras that can be used quickly and flexible for public disorder challenges.[7] There is, however, a difference between the easier movement of cameras on the one hand and the use of drones for public surveillance on the other. Although these 'mobile' cameras such as a trailer with a camera on a tripod or cameras that are easy to mount on lamp posts can be moved easier, they remain visible, and it is also much easier to prove that their placement is an infringement of the right to privacy than in case of drones. When a static camera in the public space is directed at a private home, this is considered to be a clear and objective breach of the requirement of proportionality.[8] In the case of drones, flying around, it is much more challenging to prove that this mobile camera is focused on private homes and subsequently may restrict privacy disproportionately. Another clear difference from traditional visual camera surveillance is that drones are much less visible and audible than video cameras and manned aircraft.

[5] *Parliamentary Papers II* 1996/97, 25403, 3: 26-27 (EM).

[6] *Parliamentary Papers II* 2012/13, 33582, 2.

[7] *Parliamentary Papers II* 2012/13, 33582, 3: 1 (EM).

[8] According to the Dutch Privacy Authority: it is not permitted that from a public area homes, other rooms or private gardens are filmed. Cameras should be aimed in such a manner that they cannot film inside these private areas.

Henceforth, it is remarkable that the word 'drone' does not appear in the Explanatory Memorandum to the act, which explains the legal history of legislation for the flexible deployment of mobile cameras in the Dutch public domain. Only in response to the contribution of the Association of Dutch Municipalities it refers to flying cameras. It states that in general, because of the greater opportunities and the inherent privacy risks, the deployment of mobile and flying cameras can be classified as a more intrusive measure as the deployment of fixed cameras. That is why it is anticipated that in order to satisfy the deployment of moving cameras and, *a fortiori*, flying cameras, the proportionality test will be stricter. [9]

Based on this act the mayor is allowed to deploy mobile cameras to maintain the public order, and there is no requirement for a real disturbance or a specific threat. The mayor's 'maintaining of the public order' also includes the general, prevention of criminal offences that may affect the local society. [10] Representatives of the municipalities suggest that they expect that the proposed changes will contribute to the increase of safety and the security as well the citizens' perception thereof.[11] Ensuring safety and security in the public space is one of the core tasks of the (local) government. Clearly, the act highlights the tension exists between the core task of the government: security on the one hand, and on the other, a different value that the government is required to protect: liberty rights. And, in the case of surveillance drones the right to privacy. In respect of privacy, the Drones Act carries new challenges and may increase existing ones. The Explanatory Memorandum contains a number of proposals including transparency, the proportionality and subsidiarity test and purpose limitation to reduce these risks. However are they sufficient?

2.1 Transparency

Other than the previous arrangement, the current mobile camera legislation requires no specific placement decision, in which the position of each individual camera is recorded. Instead, an area designation will stipulate the area in which mobile cameras may be placed. As a result, people may feel that these cameras are following them: the cameras can be moved swiftly and easily. To reduce this risk, the new act stipulates the requirement of transparency. In any case, citizens must be informed of the fact that they may be captured in images as soon as they enter the area designated for that purpose by the mayor. By placing signs indicating that cameras are deployed in the area in question, the public is alerted to the presence of the cameras. Yet how can this transparency be operationalized in case of 'flying' drones? In comparison to ordinary cameras transparency for drones is more complicated (Oudes & Zwijnenburg, 2011: 28). This because drones are barely visible, audible or identifiable as a police vehicle. Therefore it is unclear to individuals whether they are being observed and if so, by whom and for what purpose. As a result, the recognisability of the monitoring by means of drones is insufficient and this will sooner or later cause a breach of privacy (Schermer & van der Heide, 2013).

2.2 Proportionality and Subsidiarity

Additionally, according to the Explanatory Memorandum to the Drones Act, the criteria of proportionality (a reasonable relationship between the seriousness of the infringement and the gravity of the interest served by the infringement) and subsidiarity (the purpose for which the surveillance is used could not reasonably be achieved by another less adverse means) have to be fulfilled.[12] There is a risk that more and more cameras will be deployed, of which it is not apparent whether they are necessary in the interest of maintaining the public order. Thus, the act obliges the mayor to withdraw the area designation as soon as it is no longer necessary. According to the Dutch Bar Association area designations are rarely challenged. Nonetheless, citizens, deserve a restraint use of the new powers.[13] Firstly, assessing proportionality and subsidiarity is up to the executive power, who often has a utilitarian approach and is guided by a 'statistical' form of collective action (Dworkin, 1996: 19-20), and perhaps are less likely than the judiciary to allow liberty rights to prevail over majority interests in the light of the rule of law. Secondly, when there is a conflict of interests between security and privacy the balance is tested only *ex post*, when the damage has already been done.

2.3 Caution and Purpose Limitation

The flexible and rapid deployment of cameras also involves the risk of inaccuracy.[14] During a routine use of drones in the public space, general public information is collected. In the careful process of 'viewing the images',

[9] *Parliamentary Papers II* 2012/13, 33582, 3: 12 (EM).

[10] *Parliamentary Papers II* 2012/13, 33582, 3: 4 (EM).

[11] *Parliamentary Papers II* 2012/13, 33582, 3: 3 (EM).

[12] *Parliamentary Papers II* 2012/13, 33582, 3: 8 (EM).

[13] *Parliamentary Papers II* 2012/13, 33582, opinion of the Dutch Bar Association.

[14] *Parliamentary Papers II* 2012/13, 33582, 3:7 (EM).

the police have an important task. They must, therefore, be familiar with the rules in relation to the municipal use of CCTV cameras. Here, too, the risk of 'function creep' arises. This suggests that there is a considerable risk that the collected data will be used for other purposes than originally intended.[15] To prevent this, the Explanatory Memorandum explicitly mentions an 'exact definition of the purpose', or purpose limitation of mobile camera deployment in the public space'.[16] But will this work in practice? The Explanatory Memorandum also contains a passage in which the Act is examined in the light of art. 8 of the European Convention of Human Rights (ECHR), art. 10 of the Dutch Constitution, the Data Protection Convention and the Police Data Act.

Part of the right to privacy is that a citizen has the right to be left alone and be him- or herself uninhibitedly (a clear link to the authenticity and the autonomy of the citizen). A limitation of this right is justified only if the interference is provided for by law. The requirement that the interference is 'provided for by law' means that there should be a legal basis sufficiently accessible for citizens, and foreseeable (ECtHR, 1979, 1984, 1987, 2006, 2008). Because security technology is continuously developing, it is important that, as described above, a precise definition of the purpose and a delimitation of powers exists (ECtHR 1990a/b, 2000, 2006, 2008, 2011, 2015, 2016). In response to the developments in the field of drones, a parliamentary motion was accepted in which the government was requested to carry out research into the use of unmanned aircraft (Custers, Oerlemans & Vergouw, 2015). This report, prepared by the research and documentation centre of the Ministry of Security and Justice (WODC), shows that the legal frameworks offer different legal guarantees for the privacy. Because maintaining privacy sometimes can be very difficult, other privacy guarantees than legal one may be considered. An organizational measure could be the drafting of a policy, showing how the government will use drones within existing policy discretion. On what basis it is concluded that privacy is sufficiently guaranteed?

3. The Importance of Privacy Protection

The Dutch Drones Act raises questions about the protection of privacy in the Netherlands. Yet, why is the protection of this fundamental right so important? What dimensions of privacy are affected by the deployment of drones in the public domain? From the beginning of the concept of privacy, the coherence between liberty and privacy has played a central role in the legal and philosophical debate on privacy. 'The right to be let alone'[17], the first influential formulation of a right to privacy, was already declared an authentic liberal liberty right by Warren & Brandeis (1890; Roessler, 2005). A clear line from general to particular runs from liberty through autonomy and negative liberty to privacy. An essential aspect of the liberal idea of liberty is autonomy. In case of individual autonomy, both positive - and negative liberty play a part.[18] A human being has negative liberty when he is protected from obstacles by, in particular, the state. This concerns an area within which the state should not intervene.

Fundamental constitutional rights, sometimes also called 'negative rights', guarantee negative liberty. The group of negative rights includes multiple rights such as freedom of association, freedom of expression and the right to privacy. But what is the distinctive aspect of privacy in relation to this group of negative rights? Warren & Brandeis (1890) describe it as 'the right to one's personality'. The distinctive element is that privacy is about what we 'hold most dear to our personality' and therefore the other, including the government, does not have the right to know this information (in the broadest sense). In principle, the government has no right to infringe. In short: 'Government, you have no right to interfere in my private life!' This could be considered the intrinsic value of privacy. The government does not have the right to search your house. If it wants to do, it will have to justify why this is legitimized. The same applies to the deployment of a drone flying above your garden.

3.1 The Dimensions of Privacy

Different types or dimensions of privacy can be distinguished. As early as in 1996, Allan (1996) made the distinction between physical -, informational - and decisional[19] privacy. In respect of the relevant dimensions of privacy for drones this article focusses on the physical privacy, which applies to the private and public space ('at home and elsewhere'), and the informational privacy: shielded from unwanted disclosure of information about the privacy. Physical privacy exists when someone claims privacy within the meaning of seclusion and serenity. The protection of physical privacy is very important to us, because the feeling of self as an independent person is

[15] A detailed description of 'function creep' in relation to drones is contained in Custers, Oerlemans & Vergouw (2015: 76).

[16] *Parliamentary Papers II* 2012/13, 33582, 3: 7 (EM).

[17] First used in 1880 in the text of Judge Cooley: *'The right to be let alone*'.

[18] Positive liberty: the 'possibilities' to have a home, food, education will not be further examined, because this is not relevant to privacy.

[19] This article disregards decisional privacy. The dimension of 'decisional privacy' is often listed under the privacy dimensions. Because 'decisional privacy' fully corresponds to autonomy, therefore it does not justify the specific distinction, see also the upper part of the scheme 'freedom from' in typology of Koops, Newell & others. (2017).

constitutive in that we have control over how we can present ourselves (Roessler, 2009). When someone knows that he or she is being observed, he or she will probably behave differently. This, because he or she becomes aware of being observed. If there is structural - or systematic observation[20], it has far-reaching consequences for our autonomy and our authentic presentation. The continuous observation or the possibility of this taking place by, for example, by drones, affects people's behaviour and in doing so it is a serious restriction of our privacy. The protection of the physical privacy is not limited to the home or the garden. Even when the private property has been abandoned, one should be able to enjoy a certain degree of privacy. Although it is likely that cameras will have been mounted in a busy shopping street, that doesn't mean that we are not also entitled to a certain degree of open-mindedness, authenticity and anonymity in the public space (Ippel & Hulsman, 1997).

Informational privacy as repellent against unwanted disclosure of information on the personal lives of people (Warren & Brandeis, 1890). Many authors describe privacy in terms of control over information (Westin, 1967; Fried, 1968; Moore, 2003). The tendency to define privacy in terms of the protection of information on persons really took off in the 1960s, at the time of the emergence of mass media and information technology (Rachels, 1975; Parent, 1983; Etzioni, 1999). This informational privacy can be subdivided into specific information, which in itself is interesting and directly belongs to privacy, and general information, which is often categorized as 'personal data'. The concept of informational privacy is the basis of the European directive and national legislation on the protection of personal data (Blok, 2002). The data generated by the use of drones can be used for big data and data mining. In itself innocent data can be combined to an individual 'portrait'. In this case 'general information' becomes information that belongs to the category of privacy

3.2 Three Types of Value of Privacy

Three types of value of privacy can be derived from the distinctive element of privacy and the different dimensions of privacy. The first value, already mentioned, is the intrinsic value of privacy. When the Government is searching your house - without reasonable suspicion - and, for example, searches your laptop this is an enormous infringement of your privacy. The intrinsic value could be described as 'government, you have no right to interfere with my life'. Additionally, privacy has also an instrumental value. In that case, privacy serves as an instrument to protect another value. This instrumental value can have a direct and an indirect nature. When you are observed, you are likely to change your behaviour. The underlying value which is here at stake is autonomy and to a lesser extent authenticity. One cannot operate fully autonomously or act authentically without privacy. If somebody monitors you by using a drone, you will always take this into account. In a worst case scenario, knowing that you might or could be observed (by drones) leads to self-censorship, which has a chilling effect on autonomy, self-development and human dignity (Goold, 2002; Villasenor, 2013; Volovelsky, 2014; Van der Sloot, 2017). The second value of privacy that is relevant in the drone debate is the direct instrumental value of privacy.

It is also possible that the observation will not only affect a person directly but also indirectly. Once the state collects personal data and data mining may lead to an indirect restriction. It could lead to a restriction to fly to a certain country of fly back to your home country. This example appears a little exaggerated, but actually these kinds of things happen in real life. For example, the Malaysian Rahinah Ibrahim, who was not allowed to fly back from Malaysia to the United States of America, her country of residence, because the CIA had mixed up some information. The name of her voluntary organisation was similar to a terrorist cell (Tokmetzis, 2013). The 'mass data' collected by, for instance, a drone, may not directly affect your autonomy, but at a later stage it indirectly' affect a person's autonomy. This is a clear example of the third, the indirect instrumental value of privacy that must be protected. In many cases this comes up in the protection of personal data. As described above, drones can be used to obtain similar 'general' information and this could play an important part in the legislation on drones.[21]

4. Privacy Protected as a Human Right?

The legal protection as proposed in the Dutch Drones Act appears to provide insufficient protection for individual people. For, instance, if a drone flies above your garden and you feel your privacy has been violated; there are few opportunities to file a complaint? As argued Privacybarometer, a website that collects statistics about the parliamentary votes about Acts that threaten privacy, the person concerned cannot file a complaint (Privacybarometer, 2013). As the mayor does not take a formal decision those affected are not able to submit a

[20] Described in Zamyatin's; We and in Orwell's: 1984: Winston at the beginning of ' 1984' only put his 'authentic' thoughts on paper, when he considers himself unobserved.

[21] See also the opinion of ARTICLE 29 DATA PROTECTION WORKING PARTY: Opinion 01/2015 on Privacy and Data Protection Issues relating to the utilisation or Drones, 16 July 2015.

written objection and/or request a judicial review of this decision on the basis of the General Administrative Law Act.

Furthermore, the current protection of the right to privacy, which in the Netherlands primary follows from Article 8 ECHR, increasingly is at risk to lose its relevance, in particular the informational privacy discussed above. The classification of privacy as a subjective and a personal human right implies that only the recipient can appeal to it. Only an individual, a natural person, can file a complaint to protect his or her individual interests, if he or she can demonstrate that he or she has suffered personal injury as a result of intervention by the authorities. This appeal to the protection of privacy also depends upon whether or not the alleged violation occurs in a situation in which the citizen normally may reasonably expect that he or she can uninhibitedly be him- or herself (HR, 2004). In this criterion the Dutch Drones Act carries an important risk: to the extent that more surveillance is carried out, the reasonable expectation of privacy that people will have is affected. There is an inherent risk that the privacy will continue to erode (Schermer & van der Heide, 2013).

Where by far the protection caused the most problems, is in respect of the indirect instrumental value of privacy. What is the individual interest? What is the personal injury somebody may suffer? The practice as reflected in the judgement of the European Court of Human Rights (ECtHR) in respect of the handling of complaints concerning privacy violations in principle is focused on the complaints of natural persons who can prove an individual interest (art. 34 ECHR). There needs to be a reasonable chance that the applicant has been harmed: the reasonable likelihood criterion (ECtHR 1978, 2010).[22] Primarily the Court feels that an individual interest and personal injury must be shown by the complainant, so that in principle, legal persons cannot invoke a right to privacy, or can only do so to a limited extent (ECtHR, 1985). The result of the emphasis on the individual interest and personal injury claims is that '*in abstracto*' claims, in which complaints are made about a law or practice as such, without it having been applied or otherwise having had an impact on the complainant him- or herself, are declared inadmissible (ECtHR. 1995, 1998).[23]

At the same time, this applies to the '*actio popularis*', in which a person, group or civil-society appeals against a law or practice, not from a personal point of view, but in the interest of society (ECtHR 1999). And this applies to alleged complaints and 'a priori' claims (ECtHR 1976, 1995, 2012) concerning a possible and future infringement by the state (Van der Sloot, 2014, 2017). This makes the road to ensure the protection of privacy for individual person challenging. In many cases, the issue of admissibility in a court case about the use of drones for public surveillance will be a serious problem, even before the substantive proportionality and subsidiarity tests can be considered.

5. Security as a Right and Security as Policy

The previous section suggests that the violation of privacy should always be weighed against the public interest. One of these interests frequently placed opposite privacy is safety or security. There is a lot of talk about 'the' threat to security while it completely remains unclear whether it concerns physical, social in the context of a national security or public order (Muller, Kummeling & Bron, 2007; Powell, 2008; author, 2017). Security is understood to means something inherently so important that if threatened, the use of 'exceptional' means are permissible to restore it, or to protect it (Brainich von Brainich Felth, 2004). Security traditionally is the state's domain. The state should protect its citizens against foreign threats, external security. But it should also protect the life, freedom, physical integrity and ownership of its people, the internal security. As the relationship between citizens and the state became more of a social contract, the internal security is twofold. Not only does it relate to the protection against 'other' forces but also against the state itself (Locke, 2003; Muller, Kummeling & Bron, 2007; Lazarus, 2012;). This perspective of security as a social contract implies that the natural liberty of citizens is at stake, but in anchoring the security, a part of the liberty of citizens is being anchored, too.[24] Therefore, citizens, need to be protected against the power of the state too. Henceforth, security can be considered an individual right that is protected by the social contract with the state.

This social contract line of thought allows for two different viewpoints regarding the balance between security and liberty rights. Hobbes argued that 'security' was about securing basic individual rights, including the right to life. According to Hobbes, this social contract is based on individual rational self-interest - and as such not

[22] Concerning the 'reasonable likelihood' criterion, the court appears to interpret this criterion somewhat more widely, especially in the recent cases of *Zakharov v. Russia* 2015 and *Szabó en Vissy v. Hungary* 2016 (ECtHR, 1978, 2015, 2016)

[23] There are some exceptions, especially in the recent cases of *Zakharov v. Russia* 2015 and *Szabó en Vissy v. Hungary* 2016 (ECtHR, 1978,1984, 2006, 2007, 2008, 2009, 2010, 2015, 2016).

[24] Obviously there is a distinction based on the severity of protecting fundamental rights of citizens. A threat to one's life is more important than the degradation of property and therefore justifies a heavier state intervention.

consequentialistic. Hobbes argued that in relation to the government, hardly any fundamental individual liberty remain for the citizens, because otherwise destructive forces would likely have a free reign. This is a proportionality consideration regarding the relation between liberty (privacy) and security, currently considered unbalanced on empirical grounds, but in case of war, or the current war on terrorism, citizens might again be swayed by this vision of Hobbes (1998). Locke (2003) interpreted security in the same way, but considered it less endangered than Hobbes, leaving more scope for fundamental - but not absolute - rights of liberty. Security in the liberal sense therefore has a much more specific content than in the current populist appeal to the subjective fears of the people. In the liberal view it can be translated into rights.

There are different interpretations of this right to security. There is this social contract minimalistic approach of the right to security in the line of Locke and Lazarus where the core is that on one hand security is a huge value in securing fundamental rights as life, limb and liberty but on the other hand that there should be explicit limits to the power of the government to realize this security (Locke, 2003; Lazarus, 2007). And there is the approach where the right to security should be interpreted much broader (Shue, 1996; Fredman, 2007). Shue identified security as a basic right. For Shue (1996: 67), security is therefore a right of utmost importance, a meta-right which acts as a precondition to the enjoyment of all other rights. Lazarus (2012: 100) replies that these claims regarding a broad and meta-right to security can be reformulated as follows: the right to security gives rise to correlative duties for states to create the conditions in which objective risks of future threats which might reasonably cause subjective feelings of apprehension or insecurity, are minimized to a degree that allows the enjoyment of other rights. In the line of Locke and Lazarus the State's political and moral duty to secure individuals must always be clearly constrained. If there is a right to security correlative upon the State's broader duty of security, it must be balanced with liberty, dignity and equality (Lazarus, 2015: 434). The broad interpretation is sometimes quite vague and there is not a clear indication that results from a conceptual analysis. The implementation and prioritization of this broader approach are often determined by political policy decisions. Powell (2008) calls this the 'politics of security'.

So there should be a distinction between 'security as a right'[25] and 'security as policy'? Security as a policy is not related to this social contract interpretation and timeless but this is related to short term policy based on majority interests by government of that moment. When there is a swing to a more security conscious government there will be probably more support for repressive measures including broader surveillance powers. This type of surveillance is considered security as policy instead of security as a right. The deployment of drones could also be considered as such a measure.

6. Dworkin and Moore on the Balance of Security and Privacy

In accordance with the legal theory of Dworkin (1986) the right to privacy is interpreted as a 'trump'. The judge and the legislature must provide additional protection to such individual rights against general interest policy purposes in consequentialist terms. The right to privacy then will take precedence *prima facie*, unless the government can prove that the importance of surveillance by drones from the perspective of the general social interest or security is so important that the right to privacy must yield. Security (as a right) can also be interpreted in terms of individual rights such as the right to physical integrity. Privacy is of course therefore no absolute right also. But the Dutch Drones Act does not principally concern an individual right to security, but aims to prevent potential crime or disorder, so mainly for 'policy' purposes. The government, the legislature and the courts must have to balance: under which conditions and according to which criteria a legitimate infringement can be made on the right to privacy taking into account security (as a right and policy) considerations?

When we look at the security and privacy discussion, we see a wide spectrum ranging from 'in praise of Big Brother' (Taylor, 2005) and 'security trumps', where security interests intrinsically outweigh privacy interests (Himma, 2007) to 'balancing privacy and security while maintaining accountability' (Moore, 2011, 2016) and even 'rights (privacy) as trumps' (Dworkin, 1979), cited by Waldron (2003) 'Security and liberty; the image of a balance' with emphasis on the priority of individual rights in respect of policies in the interest of general well-being: 'rights as trumps'. Subsequently, the question then becomes: how to protect the right to privacy against the not necessary or disproportionate use of drones? Henceforth, in this section the consequentialist - and Dworkin's deontological rights based approach are reviewed before providing a liberal perspective on balancing security and privacy: Moore's (2011, 2016) prior judicial review.

[25] And even a distinction between the traditional fundamental rights and the social fundamental rights.

6.1 The Consequentialist Approach versus Dworkin's Deontological Approach

Consequentialists consider the effects for the larger group to morally justify the choices made in the deployment of the privacy restricting measures (Taylor, 2005). These consequentialists may argue that man has a natural desire to survive, and thus a vast majority will have a strong preference for survival. Security and safety measures, including monitoring by drones, can protect people from life-threatening situations such as terrorist attacks. Although a part of the population also values privacy, they will make that subordinate to survival. This justifies the deployment of drones from a consequentialist point of view. From a liberal-deontological perspective, the fundamental weakness of this argument is the crucial importance of actual preferences. This could easily result in the individual being sacrificed to the majority interests. An additional argument against the consequentialist approach is that it offers a criterion for a fair distribution containing an incoherent perversion of its own starting point. The principle of the (consequentialist) utilitarianism is that everyone's interests are equally taken into account, in contrast to the previous perfectionistic theories of justice. But the interests of citizens might clash. According to Bentham (2005), the solution to this problem could be found in a quantified utilitarian calculation: the greatest happiness of the greatest number of people would prevail. Critics point out that this is contrary to the original intention, because this way, the individual's interest is sacrificed to the majority interest. Considering the original principle, this would be particularly unfair.

This criticism was, among others, expressed by Dworkin (1986) by analogy with his criticism of the democratic majority rule. Democracy presumes that you must be prepared to accept each political opinion as equally valid and to leave the legislation of the state to the political opinion of the majority. Dworkin (1986) calls this the 'majority interpretation of democracy'. Whether something is democratic, is not determined by the substantive outcome of the democratic process, but by the way in which the content is created. Dworkin's perspective is that this majority view shows a 'statistical' form of collective action. According to the majority interpretation, political decisions must be taken in accordance with the majority of all those individuals who may be involved in the decision making process for a law. Statistically, the influence of any one person is as great as that of any other. Dworkin (1994) puts the 'communal interpretation' opposite the 'majority interpretation'.

According to Dworkin (1994), in the existing democracies the prevailing view rarely is that the majority is the decisive factor. Many democracies have constitutions and individual rights. In recognizing this, those rights are withdrawn from ordinary majorities. Constitutional democracies admit that majorities sometimes do not take the interests of individuals and minorities sufficiently into account. To avoid a 'majority dictatorship', fundamental individual rights that ordinary majorities cannot detract from are included and protected. The community view of democracy advocated by Dworkin (1978) does not centre on the 'majority', but on 'equality'. Law requires everyone to be treated as equals, i.e. with equal concern and respect. Dworkin - in accordance with Locke - argues that 'original' rights are not lost when closing a 'social contract', as the 'statistical' understanding of democracy is maintained. Justice is a matter of individual rights, and not an independent general interest issue.

This way, Dworkin (1978) comes up with an alternative to the consequentialist majority view: individual rights as trumps in relation to policy based on general interest. He attaches a special value to individual rights in relation to policies in favour of the majority. To explain these concepts of rights and policies Dworkin makes an important distinction, which he associates with the distinction between principles and goals. Goals are "that kind of standard that sets out a goal to be reached, generally an improvement in some economic, political or social feature of the community" (Dworkin, 1978: 22). Principles are described by Dworkin (1978: 22) as "a standard to be observed, not because it will advance or secure an economic, political, or social situation, but because it is a requirement of justice or fairness or some other dimension of morality." Principles are therefore propositions of political morality that confirm the existence of individual rights. The judiciary may not support their decisions in principle on the basis of this distinction on policy arguments, but only on individual (liberty) rights and the principles that support these rights. Dworkin embeds his individual (liberty) rights as 'trump cards, enabling the citizen to 'play' them at any time against the government or others, in case of infringements. The judicial review should be taken on the basis of fundamental considerations and has a certain gravity that reaches beyond the specific case. Because of this necessary fundamental dimension of case law, a constitutional review, in particular, may offer protection against government infringements of liberty and privacy. Judiciary thus represents the 'forum of principles'; a bastion of individual rights (Adams, 2003).

In the light of this article, it should be added that security or public order are not only considered as policy, but also as important individual rights (see the distinction in security as a right and as a policy in section 5). Many consider the right to life and, as a consequence, the right to security of this right to life, one of the most important individual rights. In this case, security also enjoys the protection of the trump card. This does not mean that Dworkin (1978) maintains that there can never be an infringement of individual rights, but this may only occur

in special cases. The extent to which such considerations of public interest are able to outdo the effect of a right depends on the gravity to which the law in question is entitled. In any case, any right ought to be able to act to some degree as a trump card against policy considerations, and a marginal social benefit may never be a good enough reason for the infringement of a right. Thus, an infringement of individual rights demands a much stronger substantiation than an infringement of a general interest. Thus Dworkin (1986) is one of the most vocal supporters of the system of constitutional review (*ex post*), in which the highest court is competent to decide whether legislation sufficiently respects the constitutional rights of individual citizens.

6.2 A Liberal Perspective on Security, Privacy: Moore's Prior Judicial Review

If security may be qualified as an individual right, there are multiple trump cards in play. Opposing points of view with different emphases on security and privacy exist among the deontological liberals. Moore (2011) outlines four scenarios of security and privacy, in which he criticizes Himma (2007) within the 'Security Trumps' scenario. Himma does not focus primarily on the consequences, but maintains that the intrinsic value of security outweighs privacy interests. Moore criticizes the Himma view and positions himself as an advocate of privacy. He argues that individuals have moral privacy rights, which may limit the surveillance activities of governments (Moore, 2010). Although, according to Moore, these rights are not absolute, but they do protect the individual against the prying eyes and ears of neighbours, businesses and the government.

According to his 'Balancing Privacy and Security While Maintaining Accountability' theory, the court only can issue a warrant for security measures, for which the applicant (the government) must show that reasonable suspicion, probable cause, exists for an infringement of privacy. However, Moore (2011) believes that there are situations in which the judicial review does not need to be waited for. Where Dworkin mentions a subsequent judicial review afterward, *ex post*, Moore (2011) explores the possibilities prior to the constraint: judicial oversight e*x ante*, thus ensuring public accountability at each step. The legislation must contain a sunset clause and adequate procedural guarantees should be in place, such as the principle of public oversight. The requirement of the reasonable suspicion puts the burden of proof in principle in the right place: the applicant, the government must demonstrate why the infringement of privacy is justified.[26] The Government should at least prove that the privacy infringing security measure is effective and necessary.

So in the case of drones when the executive power wants to deploy them the government needs to substantiate why this is legitimate. Moore (2011) also emphasizes that government officials should not make this consideration themselves, but that this must be a judicial decision. Moore maintains this in his criticism of the scenario: 'Just trust us' in which the consideration and the balance of privacy and supervision is left to the ruler. The numbers of people who believe that the public authorities put their interests first, is high. But what is the basis for this trust in the state? Looking at Snowden's -revelations and those of Assange with Wikileaks, one could expect certain distrust towards state authorities. It is also evident that state considers large scale preventive monitoring of citizens acceptable, but as soon as state officials are the object of such attentions, they perceive this as signs of unfounded mistrust and unacceptable behaviour (ANP/Novum, 2013). If information management results in power, and if the idea that the government should know everything would expand that power radically, the risk of an abuse of power by the government offers a good reason to question the exchange of privacy for security (Moore, 2011). What can protect the citizens from an ever-increasing development towards a surveillance state? In any case, without sufficient protection the deployment of drones in the public domain may bring us one step closer.

7. Reflection

One can question whether or not the act that legalizes the flexible deployment of mobile cameras in the Netherlands is legitimate from the perspective of the value of privacy. Especially, since this act has only modest consideration for the side-effects of the use of surveillance drones in the public domain. There is an enormous difference between mobile cameras like a tripod on a trailer or a special camera which could easily be mounted at lamp posts and drones. Basically, the Explanatory Memorandum to the act does not discuss drones specifically. Henceforth, it is no coincidence that Members of the Dutch parliament requested a special study on the use of drones (Custers, Oerlemans & Vergouw 2015). Although the report frequently mentions concerns for the protection of privacy, it does not challenge the use of drones in the public domain as such.

For the use of drones in the public domain, however, the eroding value of privacy has to be taken into account. The value of privacy is very important and it contains not only the intrinsic value: 'government you have no right to intervene in my private space', but also the instrumental value, where privacy is an instrument to protect other

[26] Moore provides a table containing a guideline to properly consider the balance of security and privacy (Moore, 2011).

values like autonomy and authenticity. This instrumental value of privacy could consist of a direct way or an indirect way. From this perspective the individual protection of privacy is important and people need a manner to protect it. Nonetheless, even before their individual right is taken into consideration, the substantive proportionality and subsidiarity test should be applied and the issue of admissibility be raised.

In many instances, it can be expected that executive authorities when deciding upon the use of drones in the public domain will reason from a utilitarian or majority point of view. Thereby following what will result in the greatest utility and what the majority of the population probably desires: more security in the broad perspective. Dworkin criticism: 'rights as trumps' reflects this position. The decision to deploy drones in the public domain should not only be based on the greatest utility or what the ‘majority’ would like, but on ‘equality’ before the law and respect for minorities should prevail. The rule of law should be taken into consideration, which is why it is so important that an extra value (trump) is granted to individual rights.

When balancing public policies and individual liberties, such as privacy, the right to privacy should lend more weight. A judicial review afterwards, *ex post*, of the principles and the constitution will consider not only the short term policy but the long term rule of law and its fundamental (liberty) rights. Because in that case not only the majority rules (statistical democracy), but equality, respect and principles (rule of law) will also have to be taken into account, and probably, individual liberties such as privacy are considered as well. Nonetheless Dworkin’s theory is not sufficient in taking into consideration the challenges of the infringement that already took place. Therefore we should not focus on judicial review afterwards, but we should explore prior judicial review. Moore explores the possibilities prior to the infringement. A court could issue a warrant for security measures like the use of drones in the public domain, for which the applicant (the government) must demonstrate that reasonable suspicion, ‘probable cause’, exists that justifies an infringement of privacy. The requirement of the 'probable cause' puts the burden of proof in principle where it should be: the applicant, the government must demonstrate why the infringement of privacy is justified. The Government should at least prove that the privacy infringing security measure is effective and necessary.

Henceforth, when Dworkin’s and Moore’s theories are both taken into consideration there should be prior judicial review where the executive power needs to make the case why the invasion of privacy is necessary as a measure to protect the right to security. Not security as (short term) policy because that will be overruled by the individual (liberty) rights. The executive power needs to demonstrate that ‘reasonable suspicion’, ‘probable cause’, exists and therefore the infringement of the right to privacy is legitimate. Not the potential victims, the citizens, the media or scholars but the executive power needs to substantiate why the infringement is legitimate.

Considering the various possibilities of the deployment of drones in the public domain, we propose that prior judicial review would be most desirable, in particular with regard to the preventive deployment of drones. Special prior requests may result in allocation, for instance during a football game in a stadium (a clearly defined area, and no impact on a residential area). Also the proportionality and subsidiarity requirements should be taken into account. In a defined area such as a stadium, outside the residential area, a proportional commitment of drones is much more likely. In case of festivities in a park, or even in an entire city, the court should determine whether the deployment of these measures is sufficiently proportional. This also matters in case of the routine deployment in the public space. If this public space is defined to exclude residential areas, the question is whether this monitoring cannot be effectuated with ‘normal’ mobile cameras or policemen (the subsidiarity principle should be assessed). It is, after all, much easier to avoid static cameras and not feel permanently observed. Subsequently a person’s autonomy will not be affected. In routine deployments the definition of the purpose of the deployment of drones should also be considered explicitly. This definition must be detailed and should not lead to 'function creep'.

In conclusion, considering all the arguments based on theories of both Dworkin and Moore the Dutch Drones Act is not legitimate from a normative perspective. The legal safeguards for the flexible deployment of mobile cameras in the public domain appear to be insufficient.

Acknowledgments

This article is based on a paper presented at the Amsterdam Privacy Conference (APC) 2015 and the Washington Privacy and Security Forum 2016. Both authors would like to thank Prof. C. Maris, J. van der Vliet and Prof. A. Moore for their feedback on earlier versions.

References

Adams, M. (2003). Vrijheid en Gelijkheid bij Ronald Dworkin. In J. Velaers (Ed.), *Vrijheid en Gelijkheid: De horizontale werking van het discriminatieverbod in de antidiscriminatiewet, enkele constitutionele beschouwingen* (pp. 115-146). Antwerpen: Maklu.

Allen, A. L. (1996). Constitutional Law and Privacy. In D. M. Patterson (Ed.), *A Companion to Philosophy of Law and Legal Theory* (pp. 145-159). Cambridge, MA: Blackwell.

ANP/NOVUM. (2013). The NSA has eavesdropped on thirty heads of state after an American official had passed them their data. 22 October 2013.

Bentham, J. (2005). *An Introduction to the Principles of Morals and Legislation* (1789). Whitefish, Montana: Kessinger Publishing.

Blok, P. (2002). *Het Recht op Privacy: Een onderzoek naar de betekenis van het begrip 'privacy' in het Nederlandse en Amerikaanse recht*. Den Haag: Boom Juridische Uitgevers.

Bloustein, E. J. (1964). *Privacy as an Aspect of Human Dignity: An answer to Dean Prosser*. New York: New York University, School of Law.

Brainich von Brainich Felth, E. T. (2004). *Het Systeem van Crisisbeheersing: Bevoegdheden en verplichtingen bij de voorbereiding op en het optreden tijdens crises*. Amsterdam: Boom Uitgeverij.

Corstens, G. J. M. (2005). Dijkdoorbraken in de Strafrechtspleging. *Nederlands Juristen Blad* (NJB), *6*, 289.

Custers, B. H. M., Oerlemans, J. J., & Vergouw, S. J. (2015). *Het Gebruik van Drones: Een verkennend onderzoek naar onbemande luchtvaartuigen*. Meppel: Boom.

Dworkin, R. M. (1977). *The Philosophy of Law*. Oxford: University Press Oxford.

Dworkin, R. M. (1978). *Taking Rights Seriously*. Cambridge: Harvard University Press.

Dworkin, R. M. (1986). *Law's Empire*. London: Fontana Press.

Dworkin, R. M. (1994). *Life's Dominion: An argument about abortion, euthanasia, and individual freedom*. New York: Alfred A. Knopf.

Dworkin, R. M. (1996). *Freedom's Law: The Moral Reading of the American Constitution.* Oxford University Press.

Eijkman, Q. (2017). Indiscriminate Bulk Data Interception and Group Privacy: Civil Society Payback through Strategic Litigation? In L. Taylor, B. van der Sloot, & L. Floridi (Eds.), *Group Privacy: Challenges of data technologies* (pp. 123-138). Springer: Dordrecht.

Etzioni, A. (1999). *The Limits of Privacy*. New York: Basic Books.

Fredman, S. (2007). The Positive Right to Security. In B. J. Goold & L. Lazarus (Eds.), *Security and Human Rights* (pp. 307-324). Oxford: Hart Publishing.

Fried, C. (1968). Privacy: A moral analysis. *Yale Law Journal*, *77*(1), 475-493. https://doi.org/10.2307/794941

Goold, B. J. (2002). Privacy Rights and Public Spaces: CCTV and the problem of the unobservable observer. *Criminal Justice Ethics*, *21*(1), 21-27. https://doi.org/10.1080/0731129X.2002.9992113

Himma, K. E. (2007). Privacy Versus Security: Why privacy is not an absolute value or right. *San Diego Law. Review*, *44*(4), 859-919.

Hobbes, T. (1988). *The Leviathan* (1651). New York: Prometheus Books.

Ippel, P. C., & Hulsman, B. J. P. (1997). Privacy in Publieke Ruimtes: Een zorg voor zonderlingen? *NJCM-bulletin: Nederlands tijdschrift voor de mensenrechten*, *8*, 964-978.

Koops, B. J., Newel, B., Timan, T., Skorvánek, I., Chokrevski, T. & Galič, M. (2017). A Typology of Privacy. *of Pennsylvania Journal of International Law*, *38*(2), 483-575.

Lazarus, L. (2007). Mapping the Right to Security. In B. J. Goold, & L. Lazarus (Eds.), *Security and Human Rights.* Oxford: Hart Publishing.

Lazarus, L. (2012). The Right to Security: Securing rights or securitizing rights. In R. Dickenson (Ed.), *Examining Critical Perspectives on Human Rights*. Cambridge: Cambridge University Press. https://doi.org/10.1017/CBO9781139026291.007

Lazarus, L. (2015). The Right to Security. In R. Cruft, & S. M. Liao. (Eds.), *Philosophical Foundations of Human Rights*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199688623.003.0024

Locke, J. (2003). *Two Treatises of Government* (1690) *and a Letter Concerning Toleration* (1689). New Haven: Yale University Press.

Moore, A. D. (2003). Privacy: Its meaning and value. *American Philosophical Quarterly*, *40*(3), 215-227.

Moore, A. D. (2010). *Privacy rights: Moral and legal foundations*. Pennsylvania State University Press.

Moore, A. D. (2011). Privacy, Security, and Government Surveillance: Wikileaks and the new accountability. *Public Affairs Quarterly*, *25*(2), 141-156.

Moore, A. D. (2016). *Privacy, Security and Accountability*. London: Rowman & Littlefield International.

Muller, E. R., Kummeling, H., & Bron, R. P. (2007). *Veiligheid en Privacy: Een zoektocht naar een nieuwe balans*. Amsterdam: Boom Juridische Uitgevers.

Nouwt, S., Vries, B. R., de & Burgt, D. van der. (2005). Camera Surveillance in the Netherlands. In S. Nouwt, B.R. de Vries & C. Prins, (Eds.), *Reasonable Expectations of Privacy?* (pp. 115-139). Cambridge: Cambridge University Press.

Oudes, C., & Zwijnenburg, W. (2011). *Onbemand Maakt Onbemind?: Een verkenning van het debat over drones en robots in oorlogsvoering*. IKV Pax Christi, 28.

Parent, W. A. (1983). Privacy, Morality, and the Law. *Philosophy & Public Affairs*, *12*(4), 69-288.

Powell, R. (2008). *The Relational Concept of Security*. DPhil dissertation, University of Oxford.

Privacybarometer. (2013). *Wetsvoorstel Flexibel Cameratoezicht, inclusief Drones.* Retrieved from https://www.privacybarometer.nl/nieuws/12148/Wetsvoorstel_flexibel_cameratoezicht_incl_drones_onnodig

Rachels, J. (1975). Why Privacy is Important. *Philosophy & Public Affairs*, *4*(4), 323-333.

Roessler, B. (2005). *The Value of Privacy*. Cambridge: Polity.

Roessler, B. (2009). De Glazen Samenleving en de Waarde van Privacy. *Filosofie & Praktijk*, *30*(5), 20-29.

Schermer, B. W., & Heide, M., van der. (2013). Privacyrechtelijke Aspecten van Drones. *Nederlands Juristen Blad*, *27*, 1773-1799.

Schoeman, F. D. (1984). *Philosophical Dimensions of Privacy: An anthology*. Cambridge University Press. https://doi.org/10.1017/CBO9780511625138

Shue, H. (1996). *Basic Rights: Subsistence, Affluence and US Foreign Policy*. Princeton University Press.

Sloot, B., van der. (2014). Privacy in het Post-NSA-tijdperk: Tijd voor een fundamentele herziening? *Nederlands Juristen Blad*, *17*, 1172-1179.

Sloot, B., van der. (2017). *Privacy as Virtue: Moving beyond the individual in the age of Big Data*. Antwerpen / Cambridge: School of Human Rights Research, Intersentia.

Solove, D. J. (2011). *Nothing to Hide: The false tradeoff between privacy and security.* New Haven, CT: Yale University Press.

Taylor, J. S. (2005). In Praise of Big Brother: Why we should learn to stop worrying and love government surveillance. *Public Affairs Quarterly*, *19*(3), 227-246.

Tokmetzis, D. (2013). U Bent Nu een Terreurverdachte (en we zeggen niet waarom). *De Correspondent*, December 10, 2013.

Verhey, L. F. M. (1992). *Horizontale Werking van Grondrechten, in het Bijzonder van het Recht op Privacy*. Zwolle: W.E.J. Tjeenk Willink.

Villasenor, J. (2013). Observations from Above: Unmanned aircraft systems and privacy. *Harvard Journal Law & Public Policy*, *457*(36), 458-493.

Volovelsky, U. (2014). Civilian Uses of Unmanned Aerial Vehicles and the Threat to the Right to Privacy - An Israeli case study. *Computer Law & Security Review*, *30*(3), 306-320. https://doi.org/10.1016/j.clsr.2014.03.008

Waldron, J. (2003). Security and Liberty: The image of balance. *Journal of Political Philosophy*, *11*(2), 191-210. https://doi.org/10.1111/1467-9760.00174

Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Rev., 5*, 193-220.

Westin, A. F. (1967). *Privacy and Freedom*. New York: Atheneum. https://doi.org/10.2307/1321160

Cases

European Commission of Human Rights (ECmHR) 10 May 1985, 10439/83, 10440/83, 10441/83, 10452/83, 10512/83, 10513/83 (*Mersch and others v. Luxembourg*)

European Court of Human Rights (ECtHR) 18 May 1976, 6825/74 (*X. v. Iceland*)

ECtHR 6 September 1978, 5029/71 (*Klass and others v. Germany*)

ECtHR 26 April 1979, 6537/74 (*Sunday Times v. United Kingdom*)

ECtHR 2 August 1984, 8691/79 (*Malone v. United Kingdom*)

ECtHR 14 July 1988, 12763/87 (*Lawlor v. United Kingdom*)

ECtHR 24 April 1990(a), 11105/84 (*Huvig v. France*)

ECtHR 24 April 1990(b), 11801/85 (*Kruslin v. France*)

ECtHR 15 June 1992, 12433/86 (*Lüdi v. Switzerland*)

ECtHR 4 December 1995, NJ 28204, No.95 (*Tauira and others vs. France*)

ECtHR 29 June 1999, 29121/95 (*Asselbourg and 78 others and Greenpeace Association-Luxembourg v. Luxembourg*)

ECtHR 15 February 2000, 27798/95 (*Amman vs. Switzerland*)

ECtHR 28 January 2003(a), 44647/98 (*Peck v. United Kingdom*)

ECtHR 17 July 2003(b), 44647/98 (*Perry v. United Kingdom)*

ECtHR 29 June 2006, 54934/00 (*Weber and Saravia v. Germany*)

ECtHR 28 June 2007, 62540/00 (*Association for European Integration and Human Rights and Ekimdzhiev v. Bulgary*)

ECtHR 1 July 2008, 58243/00 (*Liberty and others v. United Kingdom*)

ECtHR 10 February 2009, 25198/02 (*Iordachi and others v. Moldavia*)

ECtHR 18 May 2010, 26839/05 (*Kennedy v. United Kingdom*)

ECtHR 21 June 2011, No. 30194/09 (*Shimovoloz v. Russia*)

ECtHR: 15 May 2012, 49458/06 (*Colon v. Netherlands)*

ECtHR 4 December 2015, 47143/06 (*Roman Zakharov v. Russia*)

ECtHR 12 January 2016, 37138/14 *(Szabó en Vissy v. Hungary*)

Dutch Supreme Court (HR) 9 January 1987(a), ECLI:NL:HR:1987:AG5500

HR 16 October 1987(b), ECLI:NL:HR:1987:AC9997

HR 7 February 1995, ECLI:NL:HR:1995:ZC9948

HR 20 April 2004, ECLI:NL:HR:2004:AL8449

Copyrights