Privacy, surveillance, and the proportionality principle

Milaj, Jonida

Published in:
International Review of Law, Computers & Technology

DOI:
10.1080/13600869.2015.1076993

International Review of Law, Computers & Technology

ISSN: 1360-0869 (Print) 1364-6885 (Online) Journal homepage: https://www.tandfonline.com/loi/cirl20

Privacy, surveillance, and the proportionality principle: The need for a method of assessing privacy implications of technologies used for surveillance

Jonida Milaj

To cite this article: Jonida Milaj (2016) Privacy, surveillance, and the proportionality principle: The need for a method of assessing privacy implications of technologies used for surveillance, International Review of Law, Computers & Technology, 30:3, 115-130, DOI: 10.1080/13600869.2015.1076993

To link to this article: https://doi.org/10.1080/13600869.2015.1076993

International Review of Law, Computers & Technology, 2016
Vol. 30, No. 3, 115–130, http://dx.doi.org/10.1080/13600869.2015.1076993

Routledge
Taylor & Francis Group

Privacy, surveillance, and the proportionality principle: The need for a method of assessing privacy implications of technologies used for surveillance

Jonida Milaj*

Department of European and Economic Law, Faculty of Law, University of Groningen, Groningen 9700 AS, The Netherlands

(*Received 22 April 2015; accepted 23 July 2015*)

Developments in technology have created the possibility for law enforcement authorities to use for surveillance purposes devices that are in the hands or private premises of individuals (e.g. smart phones, GPS devices, smart meters, etc.). The extent to which these devices interfere with an individual's private sphere might differ. In the European Union, surveillance measures are considered lawful if they have been issued in conformity with the legal rules and the proportionality principle. Taking a fundamental rights approach, this paper focuses on the information needed for adopting proportionate decisions when authorizing the use for surveillance of devices that are not built for surveillance purposes. Since existing methods of privacy assessment of technologies do not offer the required information, this paper suggests the need for a new method of assessing privacy implications of technologies and devices which combines an assessment of privacy aspects with the different dimensions of surveillance.

Keywords: privacy; surveillance; proportionality; law enforcement authorities; European Union

1. Introduction

The private life of individuals is protected as a fundamental right in the European Union. While the laws themselves contain limitations of this non-absolute right (Art. 8(2) ECHR; Art. 52 EU Charter of Fundamental Rights; Himma 2007; Kleining et al. 2011, 43), and interferences with the individuals' private life are allowed in specific situations, there is an obligation for national authorities issuing surveillance warrants to take their decisions in conformity with the proportionality principle. This obligation derives from the case law of the European Court of Human Rights[1] (*Rees* §50), the EU Charter of Fundamental Rights (Article 52(1)), and is supported by legal doctrine. Barak (2012, 102), for example, states with regard to the proportionality principle that: ' . . . every limitation of a constitutionally protected right, even if done by law, is to be considered as unconstitutional, unless it is done in conformity with the proportionality principle'.[2] The proportionality of decisions that limit the right to privacy and authorize the use of specific devices for surveillance depends, however, on the knowledge that authorities have on the surveillance potentials and the intrusiveness of these devices. It implies that the national authorities have to assess *ex ante* the interference of the private life that is caused by a particular surveillance measure.

*Email: j.milaj-weishaar@rug.nl

The attentive assessment of a surveillance authorization is especially relevant at a time when technology developments have created the possibility to observe and collect the same information by employing different devices. Information on the location of an individual can be obtained, for example, from direct observation, a GPS device, a mobile phone, the geo location of the computer internet protocol (IP) address when accessing the internet, a radio frequency identifier (RFID) attached on the label of a shirt, etc. While different technologies can be used to attain the same goal, not all technologies have the same effects on privacy.[3] Audio recordings, for example, are considered as more invasive than picture records (Iachello and Abowd 2005), while they may be employed to reach the same result. In this light, the Swedish Data Protection Authority disallowed in-vehicle audio recordings in taxicabs, whereas it permitted the taking of digital pictures of passengers when they entered and left the vehicle (Iachello and Abowd 2005). The scope of the measure was to protect taxi drivers from potential criminal behaviour of their clients and an audio recording was considered as being disproportionate.

The focus of this paper is not to condemn invasions of privacy for law enforcement purposes as such. We would all agree that our basic rights will not be protected in situations in which crime and terror will weaken the State. This paper takes a fundamental rights approach to assess the information that national authorities need for the proper use of the proportionality principle when deciding on surveillance measures that imply the use of technology, especially if this technology is not originally designed for the purpose of surveillance.[4] It therefore does not deal with the *ex post* legal review of surveillance decisions but with the way these decisions are taken *ex ante*. The paper looks at existing methods for privacy assessment of devices and emphasizes the fact that the needed information for the authorities cannot be found in these methods. Therefore, we are in need of a new method for assessing privacy implications of technologies that are used for surveillance.

After this introduction, Section 2 addresses the importance of the proportionality principle when limiting a fundamental right. Subsequently the principle's evaluation in the Council of Europe (Section 2.1) as well as in the European Union (Section 2.2) framework is examined. In Section 3, the information that national authorities need for taking decisions in conformity with the proportionality principle is discussed. Section 4 analyses different methods of assessing privacy and surveillance implications of technologies and devices and emphasizes why the needed information cannot be found in them. Attention is paid in particular to the prior checking method and the data protection impact assessment in the EU (Section 4.1), the privacy impact assessment (Section 4.2), the surveillance impact assessment (Section 4.3), and the model for assessing the privacy 'cost' of a surveillance system proposed by Thommesen and Andersen (2009) (Section 4.4). Section 5 presents a fundamental rights approach to the analysed methods of assessment. Section 6 highlights the main findings and suggests the design of a new method for assessing the privacy implications of surveillance technologies.

2. The proportionality principle

The proportionality principle has a central place in this paper since it strikes a balance between the fundamental right for a protected private life of the individuals and the societal interests for national security, public safety, prevention of disorder or crime, etc. It is therefore the principle that national authorities must follow when deciding on a surveillance measure that interferes *per se* with the fundamental right to privacy.

Some authors define proportionality as the set of rules that determines the necessary and sufficient conditions for limiting a protected right (Barak 2012, 3). Others define it as a

principle that restricts the exercise of governmental powers (Jans et al. 2007, 143). The principle therefore fulfils a dual role: it protects fundamental rights and provides a justification for their limitation.

In the presence of the need to limit a fundamental right, the proportionality principle is of particular importance. According to Harbo (2010), the principle can serve as an instrument for balancing conflicting interests in a way that does not give precedence to any of them. There are, however, no rational standards for establishing a balance between two interests of the same level, and the weighting of interests can be sometimes arbitrary or unreflective, according to customary standards or hierarchies (Harbo 2010).

It is important that national authorities adopt proportionate decisions *ex ante* since the *ex post* safeguards will not always be effective for various reasons. First, an *ex post* evaluation of decisions can be complicated by the separation of powers and competences, i.e. 'who should decide whether it [proportionality] has been observed or not?' (Hoffmann 1999). The answer to this question becomes more complicated if we bear in mind that the proportionality principle does not have a normative value as such, and often national authorities have a margin of discretion in deciding. Secondly, another risk that arises in the context of an *ex post* evaluation of proportionality is that the balance might tilt towards allowing the taking of more intrusive measures in the face of more grave offences. We have been experiencing this especially after the September 11 events. In its evaluation, proportionality is, after all, a flexible tool that applies differently in different contexts (Jacobs 1999). Thirdly, in the presence of information asymmetry, it is difficult for national authorities to authorize the least intrusive surveillance measures available. The lack of information might be covered in those cases by the flexibility characteristic that the proportionality principle has.

These concerns highlight the need for a clear guidance for national authorities to aid the proper and well-informed use of the proportionality principle *ex ante*, i.e. when permitting the use of a device for surveillance purposes. Even if we cannot assure that decisions of these authorities will be proportionate, it is important to offer them the necessary tools and information to be able to take proportionate decisions.

For a good understanding of the proportionality principle and its role in balancing conflicting interests, it is important to understand how the principle is being interpreted by the courts (Taylor 2011).[5] In the rest of this section we will discuss the development of the principle first in the context of the Council of Europe and then in the context of the European Union.

2.1. *Development of proportionality in a council of Europe context*

The proportionality principle as such, has not been explicitly mentioned in the European Convention of Human Rights, but according to the European Court of Human Rights (the Court) rulings it is a central feature of human rights (McBride 1999; *Sunday Times* §13). The principle is also used for establishing a balance between the right to a 'protected private life of the individuals' and 'the interest for a safer society and protection of national interests' (Taylor 2003). In order not to unnecessarily restrict the rights of the individuals in return for societal benefits, Arai-Takahashi (2002, 14) argues that a delicate balance must be struck between the employed means and the pursued scope. Following this logic, it is necessary for the authorities to decide upon the appropriate surveillance measures on a case by case basis. Interference with the private sphere of the individuals is allowed only in those situations where there are no other means to safeguard the higher societal interests, in ways that are less intrusive and less restrictive of the rights of the individuals (De Hert 2005).

According to Eissen (1993), the Court first used the principle in the *Handyside* decision. In this case (§49) the Court presented a strict approach for the limitation of a fundamental right that can be brought down to the following four questions: (i) Are we in the presence of a pressing social need for restricting the rights of the Convention? (ii) Does the particular restriction correspond to this need? (iii) Is the restriction a proportionate response to that need? (iv) Are the reasons presented by the authorities, relevant and sufficient?

In other cases, the Court employed more abstract language, referring to proportionality as 'a reasonable relationship between the means and the aim sought to be realized' or 'a fair balance' between the general and individual interests at stake (*Peck* §70). In addition, interferences are considered to be disproportionate if they impair the very essence of the right (*Rees* §50), as well as in situations in which the State has not been making all the necessary positive arrangements to guarantee the effectiveness of the protection of the right (*Marckx* §31; *Gaskin* §42–49).

From the above elaboration it is clear that, even if not codified at Council of Europe level, the proportionality principle is the one that is assessed when national authorities decide on a limitation of a fundamental right. According to some authors, however, the Court has been quite keen in applying the principle and in giving a clear explanation of it. The reason proposed for this is to be found in the intrinsic complexity of the principle itself (De Hert 2012). This is also related to the fact that the Court respects the margin of discretion (Arai-Takahashi 2002, 14) enjoyed by national courts and recognizes that the exclusivity to interpret and apply national law to domestic situations should remain within the domain of national authorities (*Kruslin* §29). This approach becomes even stronger in cases where measures are introduced with the scope of protecting national interests. In such situations the Court reiterated on several occasions that it is for the national authorities to judge what is necessary in order to protect the domestic interests. The attention of the Court in such cases is focused on the analyses of the legal safeguards and guaranties offered to the individuals (*Weber and Saravia* §106; *Klass* §50). This is also related, of course, to the separation of powers. The Court takes only a marginal view of the application of the principle when national authorities have a margin of discretion to decide (Jans et al. 2007, 151). It is difficult for the courts at national or international level to evaluate decisions taken by national authorities to which the legislator, beside the competence for deciding, has also been leaving a margin of discretion. This does not mean, however, that national authorities can adopt their decisions in violation of the proportionality principle.

Having adequate guarantees against abuse by public authorities (*Malone* §81) is a way to secure the protection of the rights of individuals. However, it is clearly more desirable to prevent than to cure. As suggested above, proportionality would be an important guidance for authorities at the moment that they authorize the use of a surveillance measure, and serve therefore better as an *ex ante* guarantee rather than an *ex post* safeguard.

In its case law, the Court held that the object of Article 8 ECHR 'is essentially that of protecting the individual against arbitrary interference by the public authorities' but that 'in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for family life' (*Marckx* §31). In determining whether or not a positive obligation exists, a fair balance must be struck between the general interest of the community and the interest of the individual (*Rees* §35–37; *Cossey* §36–37). In order to avoid having an illusory and merely theoretically protected fundamental right, the State must make all the necessary positive arrangements to guarantee its effectiveness, in particular in relation to interferences by private individuals (*Marckx* §31; *X&Y* §23; *Gaskin* §42–49). If it does not, the State's interference with the private life of the individual is considered as disproportionate. Although the object of Article 8 ECHR is essentially that of

protecting the individual against arbitrary interference by the public administration, it does not merely compel the State to abstain from such interference: in addition to this primarily negative obligation, there must be positive obligations inherent in an effective respect for private or family life (*Airey* §32). They can require positive measures to be taken regarding the sphere of relations between individuals (Eissen 1993). From the elaboration of the proportionality principle at Council of Europe level it is clear that the principle is seen as the one to guide national authorities when deciding on the limitation of the fundamental right.

2.2. *Development of proportionality in a European Union context*

At European Union level, the proportionality principle is contained in Article 52(1) of the Charter of Fundamental Rights, which constitutes a condition to be fulfilled when a necessity/'a need' requires the limitation of non-absolute rights.[6] The principle was, however, fully developed by the European Court of Justice (ECJ) already in the 1970s (Barak 2012, 185), in *Internationale Handelsgesellschaft*. Akin to the German administrative law, also at EU level, the test for establishing the proportionality of a measure is composed of three steps: (i) appropriateness; (ii) necessity; and (iii) proportionality *stricto sensu* (Troncoso Reigada 2012). The measure must be first of all appropriate or suitable to protect the interests that require protection. It must be necessary, meaning that no measure less restrictive must be available to attain the objective pursued. And it must be proportionate *stricto sensu*, meaning that the restriction that it causes must not be disproportionate to the intended objective or result to be achieved (Jans et al. 2007, 149). The ECJ does not always distinguish, however, between the second and the third step of the test.[7]

As a general principle of law, proportionality has been developed by the ECJ primarily with a view of protecting the individual from interference by Union institutions or by Member States. It requires the reaching of a proper balance between the individual's interest and the desired general interests recognized by the Union with the aim of promoting European integration (*Schecke and Eifert* §86; Mifsud Bonnici 2013).

The proportionality principle as applied by the European Court contains a very strong substantial bias (Tridimas 1999; *United Kingdom v. Council* §57; *Hauptzollamt Gronau* §21–24). This is reflected in the different way the ECJ uses the principle when assessing EU or national measures.

When challenging the validity of EU law, the ECJ assesses if the measure is manifestly inappropriate. On the other side, when challenging the validity of a national act, the ECJ applies a stricter test and examines if it would have been possible for the Member State to adopt a less restrictive alternative.[8] According to Jacobs (1999), this might be true in light of the case law (*United Kingdom v. Council* §7; *Hauptzollamt Gronau* §21–24), but perhaps for good reasons: the scrutiny of national measures may need to be more demanding where these are likely to impair the effectiveness of Union measures. Where proportionality is invoked as a ground for review of Union policy measures, the Court is called upon to balance a private against a public interest. The underlying interests that the principle seeks to protect are the rights of the individual but, given the discretion of the legislature, the review of the policy measure is based on the so-called 'manifestly inappropriate' test. When proportionality is invoked to challenge the compatibility of national measures affecting one of the fundamental freedoms with Union law, the Court is called upon to balance a Union interest against a national interest. The proportionality principle is applied in these cases as a market integration mechanism and the intensity of review is much stronger. It is based on necessity exemplified by the 'less restrictive alternative'

test (Tridimas 1999). The alternative method is not required, however, to be the most effective or practical solution.

The reluctance of the Court to use the 'less restrictive alternative' test when judging Union measures was clearly seen in the invalidation of the Data Retention Directive case (*Digital Rights Ireland* §52) where the necessity step of the proportionality test was reduced to a 'limited to what is strictly necessary' analyses (Milaj 2015). Despite these incongruences, it is clear that also at European Union level the proportionality principle is seen as the one to be used by national authorities when deciding on the limitation of a fundamental right.

3. A proportionate decision

In the introduction it was argued that national authorities require information that would enable them to authorize proportionate surveillance measures. Since decisions on surveillance increasingly imply the use of devices not designed for that purpose, the authorities need information and guidance about the technologies they seek to employ in order to enable them to take decisions in conformity with the fundamental right to a protected private life and the principle of proportionality. This section will give a brief overview of this required information.

The information national authorities currently have on technical devices is limited. For this reason De Hert (2005) suggests that a formal approach towards the legality requirement – 'no [use of] technology without law' – would be more in line with the constitutional wisdom. This suggestion derives from the awareness that it is difficult to expect that the assessment of the compatibility of technology with the protection of the individuals' private life will be properly done by national authorities in the absence of clear and specific rules. As a result, De Hert suggests that it is better if national authorities will be able to authorize only the use of those methods of surveillance and devices for which it is explicitly provided in the laws. It is, however, quite impossible and improbable for legislation to keep the same speed as the technology, which develops by the minute. This has created a regulatory disconnection between the legal framework and technology. To mitigate this gap, a clear roadmap for the privacy implications of devices that might be used for surveillance is needed to aid national authorities in taking decisions that are in conformity with the proportionality principle.

Technological development has created the possibility for many devices to be used for surveillance, independent of their original purpose (Mobbs 2003). If we refer again to our example of finding information on the location of an individual, more than one device might be able to provide the same information. The way these devices interfere with the private life of the individual might, however, differ. While the data collected from a GPS device will give information on the geo location of an individual or vehicle in open spaces, a smart phone (which is normally carried close to the body in a pocket or bag) might give more accurate location information, including also in private spaces. Apart from disclosing the location, a smart phone might also be used for intercepting communications, as a portable bug (McCullagh and Broache 2006), for identifying the online behaviour of an individual, etc. Both devices might also collect information from third parties that make use of these devices.[9] The surveillance authorization that a national authority will issue must therefore be proportionate to the identified needs of a specific case and minimize the other possibilities for interfering with the private life of the individuals.

The first information that national authorities must have are details of the alternative devices that might be employed to achieve the same result. The choice of a device to be

used in a specific case must be done after an assessment of the possibilities they offer of interfering with the private lives of the individuals. This attention must be paid, on one hand, to all aspects of privacy and on the other to the dimensions of surveillance.

The private sphere of the individuals consists of a number of aspects that have been identified earlier by Clarke (2006) and further elaborated by other authors (Wright and Raab 2014). These include: (i) privacy of the person; (ii) privacy of personal behaviour; (iii) privacy of personal communication; (iv) privacy of personal data; (v) privacy of location and space; (vi) privacy of thoughts and feelings (Borton 2013; Young 2013);[10] and (vii) privacy of association. The interference of devices with any of these aspects of private life must be taken into account when deciding on the use of a device for surveillance.

Apart from identifying the way in which the private sphere of the individual is being intruded upon, it is important also to evaluate the level of intrusiveness of the method of surveillance and the devices that can be used. For this evaluation, the dimensions of surveillance need to be assessed. Marx (2002) has identified 26 dimensions of surveillance, starting with the way the senses are aided by the devices, to the possibilities for analysing, merging and communicating the information. The level of intrusiveness into the private life of the targeted individuals as well as the potential intrusion into the private life of third parties must be carefully assessed by the authorities that decide upon the surveillance measure.

Knowledge of the aspects of privacy interfered with, the level of interference and the involvement of third parties will give national authorities the possibility to take an informed decision that complies with the fundamental rights of the individuals as well as with the principle of proportionality. The assessment will guide authorities to select the less intrusive method and device. This evaluation is independent of what is the most practical or effective solution in a specific case. Interferences with the private spheres of individuals will be considered as proportionate in those situations in which the prevailing societal interest that requires the interference cannot be safeguarded by measures that are less intrusive and less restrictive of the rights of the individuals (De Hert 2005).

4. Privacy assessment methods

This part of the paper focuses on existing methods for assessing the privacy implications of devices and analyses why national authorities cannot find in them the information they need for taking proportionate surveillance authorizations. As already discussed, national authorities are the ones who decide upon the use of a particular surveillance method and device. These authorities also have the duty to refrain from abusing with their authorization the intrusions into the private spheres of individuals, since such protection is a fundamental right in the European Union.

These existing methods are in reality not targeting law enforcement bodies, but technology designers and the private sector. The aim is to increase awareness and so introduce protection of the private lives of citizens as one of the characteristics of their devices. From a parsimony and efficiency point of view it is desirable, however, to be able to use the existing methods of providing the needed information to national authorities before starting to design a new method.

After discussing the prior checking and data protection impact assessment (Section 4.1) in the framework of the European Union, this section discusses other methods that are being considered for introduction in the EU, such as: the privacy impact assessment method (Section 4.2), the surveillance impact assessment method (Section 4.3) and and a model proposed by Thommesen and Andersen (2009) for assessing the privacy 'cost' of a surveillance system (Section 4.4). Privacy auditing and compliance reviews (De Hert 2012) are not

considered since they have a narrow focus on compliance with applicable privacy laws, regulations or other rules to which a data user is subject (Waters 2012). Their scope is to present a legality check of a device. These methods, consequently, do not pay attention to any technical features of devices that impact the privacy of individuals.

4.1. *Prior checking in the EU and the data protection impact assessment*

Security and surveillance-related matters lack a common regulatory framework in the European Union.[11] Until the entry into force of the Lisbon Treaty in 2009, the field of 'police and judicial cooperation in criminal matters' was part of the third pillar. In this pillar, the Union had only limited competences that were exercised in an intergovernmental way. With the entry into force of the Lisbon Treaty, the legal possibilities to intervene in the area of data protection, privacy and surveillance are changed. This is not only due to the elimination of the pillar structure, but also because of the entry into force of the Charter of Fundamental Rights that recognizes both the right to privacy and the right to data protection, as well as the introduction of a new legal base for the adoption of legislative acts in the area of processing personal data in Article 16 TFEU. The focus of the EU secondary legislation thus far is however on data protection and not on privacy. This limited approach of the European legislator leaves other aspects of the private sphere of the individuals uncovered and is considered as regressive by Wright and Raab (2014). It looks almost as if the legislator wrongly believes that regulating data protection issues would by itself solve the problems faced by the right to privacy.

Article 20 of the Data Protection Directive (Directive 95/46/EC) provides for a prior checking examination. This method provides that Member States shall determine processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined before they start. Prior checking serves to determine if processing of personal data will be done in compliance with the laws, or whether the system needs to be improved from a data protection perspective. Almost all the Member States have been implementing the provision in their national legislation. The operations that would fall under this provision, however, differ. Prior checking is limited to sensitive data in Estonia and Greece, to certain risks in the Czech Republic, Ireland, Italy, the UK and Malta, and to certain cases in Lithuania (Le Grand and Barrau 2012).[12] The scope of the application of prior checking is not extended, however, to law enforcement activities.

The proposal for a Data Protection Regulation to substitute the existing Data Protection Directive was published by the European Commission in January 2012.[13] Article 33 of this proposal provides for a data protection impact assessment (DPIA): 'where those processing operations are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes'. The draft Regulation has not yet been adopted by the European Parliament and the Council and it is not clear what the extent of such data protection impact assessment will be. For some authors it would not be more than a compliance check (De Hert 2012) while for others the formulation of the provision certainly gives a wrong and limiting message to the industry since it does not include any reference to the different aspects of privacy but only to data protection (Wright 2012). Even when adopted, the Regulation will not apply to the processing of personal data for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

The draft Directive[14] proposed by the Commission to replace Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police

and judicial cooperation in criminal matters, does not include a data protection or privacy impact assessment. In the current form of Article 45 it only includes a duty for supervisory authorities to monitor relevant developments of information and communication technologies. Since the formulations of the Directive are not yet final, it is too early to discuss in which ways this provision, if adopted, will apply.

Both prior checking as well as the proposed data protection impact assessment give limited information on surveillance possibilities related to technical features of the devices. They have a limited scope of application, focusing only on data protection and covering only one of the aspects of privacy, namely data protection, and they are not part of the legislation covering police and judicial cooperation in criminal matters. These are the reasons why the information that results from these methods does not satisfy the needs of national authorities in light of the proper use of the proportionality principle.

4.2. *Privacy impact assessment*

Another method used in a number of States and proposed to be introduced at European Union level is the Privacy Impact Assessment (PIA). It is considered as an important tool for assessing privacy implications of different devices. PIAs can be defined as: 'a methodology for assessing the impacts on privacy of a project, policy, programme, service, product, or other initiative and, in consultation with stakeholders, for taking remedial actions that are necessary to avoid or minimize negative impacts' (Wright 2012). PIAs are seen as an early warning system, to identify possible privacy implications of new devices, preferably at a stage that still permits the intervention in the project in order to amend them. PIAs are regarded as helping to ensure that privacy is designed as a characteristic of the new devices (Waters 2012).

According to Clarke (2009), the concept of PIAs started to emerge and mature in the period 1995–2005. In the EU, as already seen above, the Data Protection Directive does not make direct reference to PIAs, but only to a prior checking (Le Grand and Barrau 2012).[15] The introduction of a PIA in the EU was suggested by the European Commission in 2009 in a recommendation on radio frequency identifiers (RFIDs). This was followed in 2011 by an act of the Article 29 Working Party approving a PIA framework and was further developed by an industry group for RFIDs.[16] As for the Member States, the United Kingdom is the most active one and, in 2007, introduced the *PIA Handbook*, commissioned by the UK Information Commissioner's Office. Finland and Ireland also appear to be moving in the direction of PIAs (Clarke 2009).

A benefit of the PIAs is that they focus on the devices themselves. According to some authors, however, existing models focus almost entirely on data protection, not covering the other aspects of privacy already identified (Wright et al. 2010). This is also reflected in the current draft of the data protection regulation that limits itself to a data protection impact assessment. Since PIAs are designed to be conducted at a very early stage of a project and because of their nature and aim, it is not clear how they would operate when new privacy implications of a device are identified at an advanced stage, especially when the devices are already in the hands of the users. From comparative analyses of PIAs in Australia, New Zealand, Canada, the USA, Ireland and the UK with the aim of making the best suggestions for designing a European method, it is suggested that a PIA will be most beneficial if it is considered as an ongoing process that should continue until and even after deployment of the project (Wright, Finn, and Rodrigues 2013). Thus far, PIAs are supposed to be undertaken by the project developers with the result that the authority or company selected to perform this will have an influence on and interest in the outcome. In addition,

the making public or not of the results of a PIA is still under discussion (Wright and De Hert 2012). The publication of the results of a PIA will influence the awareness of the individuals on the fundamental rights implications of the devices they have in their hands. The currently proposed design of PIAs is thus of limited help for authorities that need the results of the assessment for the proper use of the proportionality principle.

4.3. *Surveillance impact assessment*

A surveillance impact assessment (SIA) was first suggested in a report for the British Information Commissioner by the Surveillance Studies Network. The idea for this new method came from the identified necessity: 'to encompass the potential harmful effects of surveillance on a wider basis than that of protecting privacy'.[17] SIA was suggested to assess the impacts of surveillance on a range of values that may include, but also transcend, privacy itself. For this it was suggested to develop PIA tools beyond their existing configuration. The 29 questions drafted by Marx (1998) for determining the ethics of surveillance were suggested as a starting point for designing a SIA.

The SIA method was further developed in 2012 by Wright and Raab. Contrary to what its name would suggest, a SIA does not focus on the impact on surveillance of a new project or device, but makes a social, economic, financial, political, legal, ethical and psychological impact of surveillance on individuals or society as a whole.[18] A SIA therefore has a focus not on the devices, but on the subjects of surveillance, being individuals or entire groups of population.

The methodology of SIA was further developed in the SAPIENT project, where its purpose is presented as: 'to assess the risks that a surveillance related project, policy, programme, service, product or other initiative poses for privacy, as well as for other human rights and ethical values' (Wright et al. 2014). The method is proposed to be used when a new surveillance project is contemplated or an existing surveillance system is to be modified or expanded. Its focus is therefore on surveillance technologies, systems and applications and not on other devices that are not built for the purpose of surveillance.

As briefly described above, the method is principally directed towards identifying the impact of surveillance projects on individuals or society as a whole, not the surveillance capabilities of devices (Wright and Raab 2012). In addition, it appears that the definition 'surveillance projects' is limited to projects designed for the purpose of surveillance and is not extended to devices we use daily, which are not designed for the purpose of surveillance but can be used for such purposes. This conclusion also derives from the fact that those that are required to undertake a SIA are identified as: developers of surveillance systems, the ones who commission the design of surveillance systems, and regulators that want to assess surveillance systems proposals. This method is therefore only of limited value for guiding the proper use of the proportionality principle by national authorities.

4.4. *A model for assessing the privacy 'cost' of a surveillance system*

A model for assessing the privacy 'cost' of a surveillance system was elaborated by Thommesen and Andersen (2009). The model comes closer to our idea of a method for identifying the needed information for national authorities that issue surveillance authorizations. The model offers a matrix for establishing the intrusiveness of different surveillance systems. The authors start by listing the dimensions of privacy: (i) privacy of personal behaviour; (ii) privacy of location and space; (iii) privacy of the person; (iv) privacy of personal data, and (v) privacy of personal communication. It is to be noticed that 'privacy of

location and space' was not included in the work on the types of privacy by Clarke (2006). Due to technology advances, however, other authors consider the division of Clarke as insufficient and propose to add three more types of privacy to his original list: 'privacy of location and space', 'privacy of thoughts and feelings' and 'privacy of association (including group privacy)' (Wright and Raab 2014). Only the first type is considered in the matrix designed by Thommesen and Andersen. This is why we consider it as not covering all the aspects of the protected private life of the individuals.

The authors then identify the ways privacy can be invaded and distinguish three types of invasion: physical intrusion, observation and, acquisition of personal information from others. The degree of intrusiveness of different surveillance methods is then established as the outcome of seven different dimensions of surveillance. The nature of the observer, then the degree of personal identification, the place where surveillance is performed, the sensitivity of the collected information, its degree of accuracy, the purpose of surveillance and last, the awareness of the observed subject, are assessed. The authors stress the possibility that the method might be useful for the analyses of ethical aspects of surveillance systems and might aid in foreseeing problems and reactions that may not be identified before the system has been implemented.

The matrix created has the benefit of covering more aspects of privacy than the other methods discussed so far. But it does not cover them all. This is, however, not the only complaint about the designed matrix. When dealing with the dimensions of surveillance, it only covers seven such dimensions while other authors, for example Marx (2002), have identified 26. The matrix does not offer the possibility of comparing alternative surveillance devices and the effects that a surveillance system might have on the invasion of privacy of third parties. The matrix also does not offer the possibility of assessing possible linkages of collected data with other systems that will make the information that results from the combination more intrusive and dangerous in terms of the violation of the right to privacy. The guidance that this model of privacy assessment gives to national authorities is limited and does not solve the existing problem that they face when assessing the proportionality of their decisions.

5. A fundamental rights approach of privacy assessment methods

In the previous section we discussed a number of privacy assessment methods that are adopted (like prior checking), or are proposed to be adopted in the European Union. In this section we will argue why none of these methods satisfies the identified need of the authorities for information on the surveillance abilities of the devices.

The private life of the individual is protected as a fundamental right in the European Union. Even if the legal provisions allow a limitation of this right by State authorities, it is important that any limitation of the right is done lawfully. The proportionality principle is the one indicated by the laws, courts' decisions and doctrine to guide national authorities when adopting a decision for limiting a fundamental right.

Since the proportionality principle does not have a normative value, it is important that national authorities have *ex ante* all the required information for adopting proportionate decisions at their disposal. In Section 2, it was argued that it is difficult to apply the legal safeguards for the proportionality principle properly *ex post* because of the implications that derive from the flexibility of the principle and the margin of discretion that national authorities enjoy.

From a fundamental rights perspective it is clear that lawful interferences with the private spheres of individuals are to be done in the way that restricts and interferes the

least with the individuals' rights. Considerations of efficiency are to be less of a concern in such decisions. For complying with such a requirement, national authorities must be aware first of all of the alternative devices that can be used to reach the same goal and so select among them the one that interferes the least with the rights of the individuals. It is important to identify the aspects of the private life with which devices used for surveillance will interfere. In addition, for establishing their level of intrusiveness, an evaluation of the dimensions of surveillance with which these devices have an impact needs to take place. The effects of the surveillance measure for third parties also need to be identified.

Regarding the aspects of privacy, it was seen that, thus far, the existing and proposed assessment methods do not cover all these aspects. Prior checking, DPIA and PIA focus mainly on data protection aspects of the devices and not on privacy as such. As mentioned earlier, it almost looks like the European legislator wants to equalize the right to data protection with the right to privacy. This is quite surprising, not only because privacy and data protection are presented as two separate rights in the European Charter of Fundamental Rights (articles 7–8) but also because of their different scopes. The right to privacy aims to protect the private life of individuals from arbitrary interferences of State actors, while the right to data protection focuses on the fair and legitimate collection and processing of personal data (Mitsilegas 2015). It is true that in certain situations the two rights might overlap, but even in such situations the right to privacy would focus on the aspects of the private life that have been interfered with and the way this is done while the right to data protection would focus on the way the personal data are treated. The SIA method on the other hand does not focus on devices as such, but on the subjects of surveillance and on the effects the surveillance activity has on them. Also, the fact that its methodology points to the fact that the method is designed to focus on surveillance-related projects or products, excludes from its scope of application devices not built for the purpose of surveillance. The model for assessing the privacy 'costs' of a surveillance system also has its deficits in this regards. It focuses only on limited aspects of privacy and not on all the aspects identified thus far.

Regarding the dimensions of surveillance, we have seen that prior checking, DPIA and PIA are not directed at law enforcement authorities. As a result, they also do not focus on the dimensions of surveillance. SIA focuses on the ethics of surveillance and aims to present a social, economic, financial, political, legal, ethical and psychological impact of surveillance for individuals or society as a whole. However, since it does not focus on devices, it is not clear if it is able to establish in this way the intrusiveness level of the different devices into the life of the individuals. The model for assessing the privacy 'costs' of a surveillance system on the other hand, covers only seven dimensions of surveillance, while some authors identify 26 such dimensions.

The interference that devices not built for surveillance have with the private lives of individuals that are not the target of the surveillance authorization, is not considered in any of the explored methods. From the above elaboration it can be said that the existing methods of privacy assessment of devices, from a fundamental rights point of view, do not satisfy the need of national authorities for information that would enable them to adopt proportionate decisions.

6. Concluding remarks

This paper has focused on the importance of the proportionality principle when national authorities decide on the limitations of the fundamental right to a protected private life by authorizing surveillance measures. It was argued that for the proper use of the principle,

the authorities need to have information on the surveillance possibilities and on the interference with the private lives of the individuals that will result from the surveillance measures and devices the authorities authorize to be used.

The existing methods for assessing privacy implications of devices are not able to provide the necessary information to national authorities. None of the methods discussed in this paper is able to give enough information to identify which alternative devices can be used to reach the same outcome, nor to give information of the incidental interference the devices might have with the lives of third parties. Almost all of these methods focus on data protection instead of privacy aspects. The method designed by Thommesen and Andersen makes an exception. It covers more aspects of privacy, although not all of them. Regarding the dimensions of surveillance, the methods are again lacking in their assessment. For these reasons a new method, to guide national authorities on the surveillance properties and privacy implications of the devices that they authorize for use in specific situations, was identified as needed.

This method must first of all be able to identify all alternative devices that might be used to achieve the same result. The alternative devices must be assessed in light of the different privacy aspects, and to establish the aspects of the private lives of the individuals with which they interfere. They must also be assessed in light of the dimensions of surveillance in order to compare their level of intrusiveness into the individuals' private lives. The method has to take into account possible data combinations as well as interferences with the private lives of third parties. To complete the theoretical framework of this assessment method, however, further research is needed. Only when national authorities have the required information on the technologies they authorize to be used to limit the rights of individuals, can we expect that the fundamental right to privacy will be safeguarded in conformity with the proportionality principle.

Conflict of Interest Disclosure

No potential conflict of interest was reported by the authors.

Notes

1. On the basis of the case law from the European Court of Human Rights, any interference from the State with the rights of the individuals must not exceed the necessary minimum.
2. For earlier works on proportionality see Van Gerven (1999) and Tridimas (1999).
3. In *Uzun* (§68–69), for example, the European Court of Human Rights considered the use of a GPS device for location tracking in public areas as a less intrusive measure than interception of personal communications.
4. For this study, surveillance with technology not originally built for the purpose of surveillance is understood to be devices that are introduced in the markets for the performance of other activities but that have a potential to be used for surveillance. Some examples of these devices would be: mobile phones, computers, smart electricity meters, GPS devices, etc. These devices offer possibilities for direct surveillance, for gathering personal information, location data, behaviour patternss, etc.
5. According to Taylor (2011) the proportionality principle plays a role in establishing a balance between the nature and the extent of the interference and the reasons for interfering.
6. The proportionality principle is central in the Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, *Official Journal* L 350, 30/12/2008, see for example Article 3.
7. The proportionality principle is central in the Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and

judicial cooperation in criminal matters, *Official Journal* L 350, 30/12/2008, see for example Article 3.

8. See Opinion of AG Maduro in Case 524/06 Heinz Huber v. Bundesrepublik Deutschland, para. 16.
9. 'Collateral intrusion' is defined in the UK in a guiding document to the application of RIPA as interference with the privacy of persons, other than the subject of the surveillance.
10. See for example the newest developments on wireless brain–computer interfaces in Borton (2013).
11. The lack of a common framework does not mean however that sector specific laws dealing with privacy and surveillance have not been adopted. See, for example, the Schengen agreements, creation of Europol and Eurojust, etc.
12. These authors present a detailed analyses of the implementation of Article 20 of the Data Protection Directive.
13. See the 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, Brussels, 25.1.2012, COM(2012) 11 final, 2012/0011 (COD) – art. 33, rec. 74.
14. Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the movement of such data, Brussels, 25.1.2012, COM(2012) 10 final, 2012/0010 (COD).
15. See Article 20 of the Data Protection Directive.
16. Please note that, in April 2013, the Article 29 Working Party released an opinion that was very critical and did not approve a PIA framework proposed for smart electricity meters.
17. See: 'A Report on the Surveillance Society for the information Commissioner', prepared by the Surveillance Studies Network in September 2006.
18. See comment by the authors themselves in Footnote 4 of Wright and Raab (2012).

References

Arai-Takahashi, Y. 2002. *The Margin of Appreciation Doctrine and the Principle of Proportionality in the Jurisprudence of the ECHR*. Antwerpen: Intersentia.

A report on the Surveillance Society for the Information Commissioner by the Surveillance Studies Network, September 2006. Accessed June 17, 2015. http://www.surveillance-studies.net/?page_id=3

Article 29 Working Party Opinion on a PIA framework proposed for the smart electricity meters. Accessed June 17, 2015. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp205_en.pdf

Barak, A. 2012. *Proportionality – Constitutional Rights and their Limitations*. Cambridge: Cambridge University Press.

Borton, D. A. 2013. "An Implantable Wireless Neural Interface for Recording Cortical Circuit Dynamics in Moving Primates." *Journal of Neural Engineering* 10 (2). doi:10.1088/1741-2560/10/2/026010.

Clarke, R. 2006. What's 'Privacy'? Accessed June 17, 2015. http://www.rogerclarke.com/DV/Privacy.html

Clarke, R. 2009. "Privacy Impact Assessment: Its Origins and Development." *Computer Law and Security Review* 25: 123–135.

Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. OJ L 350, 30 December 2008.

De Hert, P. 2005. "Balancing Security and Liberty within the European Human Rights Framework. A Critical Reading of the Court's Case Law in the Light of Surveillance and Criminal Law Enforcement Strategies After 9/11." *Utrecht Law Review* 1 (1): 68–96.

De Hert, P. 2012. "A Human Rights Perspective on Privacy and Data Protection Impact Assessment." In *Privacy Impact Assessment*, edited by Wright and De Hert, 33–76. Dordrecht: Springer.

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, OJ L 281, 23 November 1995.

Eissen, M. 1993. "The Proportionality Principle in the Case Law of the European Court of Human Rights." In *The European System for the Protection of Human Rights*, edited by R. St. J. Macdonald, F. Matscher, and H. Petzold, 125–137. Alphen aan Den Rijn: Kluwer.

Harbo, T. 2010. "The Function of the Proportionality Principle in EU Law." *European Law Journal* 16 (2): 158–185.

Himma, K. E. 2007. "Privacy vs. Security: Why Privacy is not an Absolute Value or Right." *San Diego Law Review* 44: 859–922.

Hoffmann, L. 1999. "The Influence of the European Principle of Proportionality Upon UK Law." In *The Principle of Proportionality in the Laws of Europe*, edited by E. Ellis, 107–115. Oxford: Hart Publishing.

Iachello, G., and G. D. Abowd. 2005. Privacy and Proportionality: Adapting Legal Evaluation Techniques to Inform Design in Ubiquitous Computing, *CHI 2005*. Accessed June 15. http://sociotech.pbworks.com/f/Iachello-Privacy_and_Proportionality-ACM.pdf

Jacobs, F. G. 1999. "Recent Development in the Proportionality Principle in European Community Law." In *The Principle of Proportionality in the Laws of Europe*, edited by E. Ellis, 1–21. Oxford: Hart Publishing.

Jans, J. H., R. de Lange, S. Prechal, and R. Widdershoven. 2007. *Europeanisation of Public Law*. Groningen: Europa Law Publishing.

Kleining, P., P. Mameli, S. Miller, D. Salane, and A. Schwartz. 2011. *Security and Privacy: Global Standards for Ethical Identity Management in Contemporary Liberal Democratic States*. Canberra: ANU E Press.

Le Grand, G., and E. Barrau. 2012. "Prior Checking, a Forerunner to Privacy Impact Assessments." In *Privacy Impact Assessment*, edited by Wright and De Hert, Dordrecht: Springer, 97–116.

Marx, G. T. 1998. "Ethics for the New Surveillance." *The information society: An International Journal* 14 (3): 171–185.

Marx, G. T. 2002. "What is New About 'New Surveillance'? Classifying for Change and Continuity." *Surveillance and Society* 1 (1): 9–29.

McBride, J. 1999. "Proportionality and the European Court of Human Rights." In *The Principle of Proportionality in the Laws of Europe*, edited by E. Ellis, 23–36. Oxford: Hart Publishing.

McCullagh, D., and A. Broache. 2006. FBI Taps Cell Phone Mic as Eavesdropping Tool, *CNet News*. Accessed June 16, 2015. http://news.cnet.com/2100-1029-6140191.html

Mifsud Bonnici, J. P. 2013. "Exploring the Non-Absolute Nature of the Right to Data Protection." *International Review of Law, Computer and Technology* 28 (2): 131–143.

Milaj, J. 2015. "Invalidation of the Data Retention Directive – Extending the Proportionality Test." *The Computer Law and Security Review* 31 (5). doi:10.1016/j.clsr.2015.07.004.

Mitsilegas, V. 2015. "The Transformation of Privacy in an Era of Pre-emptive Surveillance." *Tilburg Law Review* 20: 35–57.

Mobbs, P. 2003. Privacy and Surveillance: How and When Organisations and the State Can Monitor Your Actions, *GreenNet CSIR*, no. 3. Accessed June 17, 2015. http://www.internetrights.org.uk/briefings/irtb05-rev1-draft.pdf

Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the movement of such data, Brussels, 25.1.2012, COM(2012) 10 final, 2012/0010 (COD)

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, Brussels, 25.1.2012, COM(2012) 11 final, 2012/0011 (COD)

Raab, C. D., and D. Wright. 2012. "Surveillance: Extending the Limits of Privacy Impact Assessment." In *Privacy Impact Assessment*, edited by Wright and De Hert, 363–383. Dordrecht: Springer.

Taylor, N. 2003. "Policing, Privacy and Proportionality." *European Human Rights Law Review, Supp (Special issue: privacy 2003)*, 86–100.

Taylor, N. 2011. "A Conceptual Legal Framework for Privacy, Accountability and Transparency in Visual Surveillance Systems." *Surveillance and Society* 8 (4): 455–470.

Thommesen, J., and H. B. Andersen. 2009. Privacy Implications of Surveillance Systems. Accessed May 6, 2013. http://orbit.dtu.dk/fedora/objects/orbit:56150/datastreams/file_4010841/content

Tridimas, T. 1999. “Proportionality in European Community Law: Searching for the Appropriate Standard of Scrutiny.” In *The Principle of Proportionality in the Laws of Europe*, edited by E. Ellis, 65–84. Oxford: Hart Publishing.
Troncoso Reigada, A. 2012. “The Principle of Proportionality and the Fundamental Right to Personal Data Protection: The Biometric Data Processing.” *Lex Electronica* 17 (2): 1–44.
Van Gerven, W. 1999. “The Effect of Proportionality on the Actions of Member States of the European Community: National Viewpoints from Continental Europe.” In *The Principle of Proportionality in the Laws of Europe*, edited by E. Ellis, 37–63. Oxford: Hart Publishing.
Waters, N. 2012. “Privacy Impact Assessment – Great Potential Not Often Realized.” In *Privacy Impact Assessment*, edited by Wright and De Hert, 149–160. Dordrecht: Springer.
Wright, D. 2012. “The State of Art in Privacy Impact Assessment.” *Computer Law and Security Review* 28: 54–61.
Wright, D., and P. De Hert. 2012. “Introduction to Privacy Impact Assessment.” In *Privacy Impact Assessment*, edited by Wright and De Hert, 3–32. Dordrecht: Springer.
Wright, D., M. Friedewald, S. Gutwirth, M. Langheinrich, E. Mordini, R. Bellanova, P. de Hert, K. Wadhwa, D. Bigo. 2010. “Sorting Out Smart Surveillance.” *Computer law & Security Review* 26: 343–354.
Wright, D., I. Kroener, M. Lagazio, M. Friedewald, D. Hallinan, M. Langheinrich, R. Gellert, S. Gutwirth. 2014. SAPIENT Deliverable 4.4: A Guide to Surveillance Impact Assessment – How to Identify and Prioritise Risks Arising from Surveillance Systems. Accessed June 11, 2015. http://www.sapientproject.eu/D4.4%20-%20SIA%20Manual%20(submitted%2001%20August%202014).pdf
Wright, D., Finn, R., and R. Rodrigues. 2013. “A Comparative Analysis of Privacy Impact Assessment in Six Countries.” *Journal of Contemporary European Research* 9 (1): 160–180.
Wright, D., and C. D. Raab. 2012. “Constructing a Surveillance Impact Assessment.” *Computer Law and Security Review* 28: 613–626.
Wright, D., and C. D. Raab. 2014. “Privacy Principles, Risks and Harms.” *International Review of Law, Computers and Technology* 28 (3): 277–298.
Young, S. 2013. A Wireless Brain-Computer Interface. Accessed March 30, 2015. http://www.technologyreview.com/news/512161/a-wireless-brain-computer-interface/

Case law from the European Court of Human Rights

Airey v. Ireland, ECHR application no. 6289/73, 9 October 1979
Cossey v. The United Kingdom, ECHR application no. 10843/84, 27 September 1990
Gaskin v. The United Kingdom, ECHR application no. 10454/83, 7 July 1989
Handyside v. The United Kingdom, ECHR application no. 5493/72, 7 December 1976
Klass v. Germany, ECHR application no. 5029/71, 6 September 1978
Kruslin v. France, ECHR application no. 11801/85, 24 April 1990
Malone v. The United Kingdom, ECHR application no. 8691/79, 2 August 1984
Marckx v. Belgium, ECHR application no. 6833/74, 13 June 1979
Peck v. The United Kingdom, ECHR application no. 44647/98, 28 January 2003
Rees v. The United Kingdom, ECHR application no. 9532/81, 17 October 1986
Sunday Times v. The United Kingdom, ECHR application no. 6538/74, 26 April 1979
Uzun v. Germany, ECHR application no. 35623/05, 2 September 2010
Weber and Saravia v. Germany, ECHR application no. 54934/00, 29 June 2006
X & Y v. The Netherlands, ECHR application no. 8978/80, 26 March 1985

Case law from the Court of Justice of the EU

C-265/87 Schraeder HS Kraftfutter GmbH & Co KG v. Hauptzollamt Gronau [1989] ECR 2237
C-84/94 United Kingdom v. Council [1996] ECR I-5755
Case 11/70 Internationale Handelsgesellschaft v. Einfuhr- und Vorratsstelle Getreide [1970] ECR1125
Joined Cases C-92/09 and C-93/09 Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen [2010] ECR I-11063
Joint cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and others [2014] nyr
Opinion of AG Maduro in Case 524/06 Heinz Huber v. Bundesrepublik Deutschland