Invalidation of the data retention directive - Extending the proportionality test

Milaj, Jonida

Published in:
Computer Law & Security Review

DOI:
10.1016/j.clsr.2015.07.004

Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Invalidation of the data retention directive – Extending the proportionality test

Jonida Milaj *

Faculty of Law, University of Groningen, The Netherlands

Keywords:
Data retention directive
Non-purpose built devices
Surveillance
Proportionality principle
European Union

A B S T R A C T

The invalidation of the Data Retention Directive is considered as a positive development for the protection of the fundamental rights to privacy and data protection of European citizens and is important for giving an interpretation of these rights in light of the proportionality principle. This paper takes as a starting point the proportionality test as used by the Court of Justice of the EU in its decisions and assesses whether this test is properly defined to accommodate technology developments and the increased surveillance of citizens with devices that are not originally built for the purpose of surveillance (e.g. mobile phones, computers/internet, GPS devices, etc.) and with data that are not originally collected for the purpose of dataveillance. The paper contributes to the existing debates on striking a balance between security and fundamental rights by introducing the so far neglected discussion of the nature of the devices used for surveillance. Due, not only to the level of intrusiveness, but also to the lack of proper legal safeguards for these (non-purpose built but surveillance-ready) devices, it is argued that the proportionality test elaborated by the Court in the Data Retention Directive case is not accurate as long as it does not take the nature of technology used for surveillance into account.

1. Introduction

The Court of Justice of the European Union (the Court) invalidated the Data Retention Directive[1] in its decision of the 8 April 2014.[2] This decision of the Court was the result of its finding that the Directive's interference with the fundamental rights protected by Articles 7 and 8 of the EU Charter of Fundamental Rights (the Charter) was not in conformity with the principle of proportionality (Art. 52(1) of the Charter). This positive development for the protection of the rights to a protected private life and personal data of European citizens signs a culmination[3] but not a conclusion of the debate on data retention for as long as Member States will keep in force national

* Department of European and Economic Law, Faculty of Law, University of Groningen, The Netherlands, Oude Kijk in 't Jatstraat 26, P.O. Box 716, 9700 AS Groningen, The Netherlands. Tel.: +31650222783.
E-mail address: j.milaj-weishaar@rug.nl

[1] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, 13.4.2006, 54–63.

[2] Joint cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and others [2014] nyr.

[3] Kirsten Fiedler, 'European Court overturns EU mass surveillance law' (2014), <http://edri.org/european-court-overturns-eu-mass-surveillance-law/> accessed 22 May 2014; Danny O'Brien, 'Data Retention Directive Invalid, says EU's Highest Court' (2014), <https://www.eff.org/deeplinks/2014/04/data-retention-violates-human-rights-says-eus-highest-court> accessed 22 May 2014.

http://dx.doi.org/10.1016/j.clsr.2015.07.004

legislation to retain personal data for the purpose of law enforcement.[4] While technology is developing by the second and more devices create the possibility for accessing and collecting personal data, it is important to properly use the tools[5] that we have at disposition for the protection of the citizens' rights. This paper will assess if the proportionality principle, as used thus far by the Court for establishing the limits of State interference with the citizens' fundamental rights and key to the invalidation of the Data Retention Directive, is properly addressing the technological advancements to establish the level of interference with individuals' private life and is able to properly protect their rights and freedoms.

The means of electronic communications, mobile phones, smart phones, computers, and internet are part of our daily lives and one could say that the data that are collected via these tools create an accurate map into one's private life.[6] However, communication means are not the only ones able to collect and retain personal data. Development of technology creates more possibilities for data collection and retention from many devices[7] that are part of our daily routine (e.g. smart electricity meters, smart TV, GPS devices). The data collection features of these devices might give the possibility for more control into the life of users from law enforcement authorities. It has to be kept in mind that independent of the nature of the data, being this content data or metadata, the information that can be discovered about the life of an individual via processing and profiling techniques can be quite accurate.[8] We are more and more in possession and are carrying with us devices that are not built for surveillance but that are the best technologies for performing it.

While the decision of the Court of Justice of the EU to invalidate the Data Retention Directive did not come as a surprise but was an expected outcome of the extended debate on the lawfulness of the Directive, the aim of this contribution is to look further. The paper assesses if the proportionality test as used by the Court is able to deal with the problem of the increasing availability and use of devices that are not originally built for the purpose of surveillance but that have a potential to be used for it, and to give suggestions on how to extend the proportionality test to address this issue. The paper adds to the existing debate on the use of the proportionality principle for striking a balance between individuals' rights and security, the discussion on the nature of the technology used for surveillance. It is argued that the proportionality test is not complete without taking into account the nature of the technology used for surveillance.

After these introductory remarks, Section 2 assesses the need for introducing a discussion on the technology used for surveillance. Then the proportionality test as used by the European Court of Justice is discussed in Section 3. The invalidation of the Data Retention Directive was the starting point and the inspiration for writing this paper. Section 4 discusses the proportionality test as used by the Court for the invalidation of the Data Retention Directive and assesses if this test is adequate for dealing with potential surveillance with means not built for that purpose. Suggestions on how to extend the proportionality test for covering surveillance technology and assessing surveillance with non-purpose built technology follow in Section 4.1. The findings of the paper are summarized in Section 5.

2. Surveillance and technology

The aim of this section is to discuss the relevance that the technology used for surveillance has for determining the level of interference with the private life of EU citizens. While the right to a protected private life is not an absolute one and there is the possibility for the State to interfere with it when fulfilling the legality requirements and meeting the set safeguards,

[4] See Article 29 Data Protection Working Party Statement of 1 August 2014 'On the ruling of the Court of Justice of the European Union which invalidates the Data Retention Directive', 14/EN/WP220; Thomas A. Vandamme 'The invalid Directive – The legal authority of a Union act requiring domestic law making' (Europa Law Publishing 2005) 159, as well as the UK new draft law on Data Retention and Investigatory Powers Bill 2014 <https://www.gov.uk/government/publications/the-data-retention-and-investigatory-powers-bill> accessed 10 September 2014; legal analyses from the Danish Ministry of Justice concluding that the Danish retention law is not affected by the CJEU ruling on the Data Retention Directive <http://justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2014/Notat%20om%20logningsdirektivet.pdf> accessed 10 September 2014; reaction from the Dutch government on keeping virtually unchanged national data retention laws <http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2014/11/19/tk-reactie-van-het-kabinet-naar-aanleiding-van-de-ongeldigverklaring-van-de-richtlijn-dataretentie.html> accessed 11 December 2014; Franziska Boehm, Mark D. Cole, 'Data retention after the judgement of the Court of Justice of the European Union' (2014), <https://www.google.nl/?gfe_rd=cr&ei=KRFFVO6OB8nBUOipgvgL&gws_rd=ssl#q=data%20retention%20after%20the%20judgement%20of%20the%20court%20of%20justice%20of%20the%20european%20union> accessed 28 November 2014.

[5] Katja de Vries, Rocco Bellanova, Paul De Hert, and Serge Gutwirth, 'The German Constitutional Court Judgement on data retention: proportionality overrides unlimited surveillance (doesn't it ?)', in Serge Gutwirth, Yves Poullet, Paul De Hert, Ronald Leenes (eds), Privacy and data protection : an element of choice (Springer, 2011) 3–24.

[6] Working document 1, on the US and EU Surveillance programmes and their impact on EU citizens fundamental rights, Committee on Civil Liberties, Justice and Home Affairs, Rapporteur: Claude Moraes, (US and EU Surveillance programmes) <http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/wd_moraes_1012434/wd_moraes_1012434en.pdf> accessed 20 December 2013; Elspeth Guild, Sergio Carrera, 'The political the judicial life of the metadata: Digital Rights Ireland and the trail of the Data Retention Directive' (2014), *CEPS Liberty and Security in Europe* 65; Bert-Jaap Koops, 'On legal boundaries, technologies, and collapsing dimensions of privacy' (2014), *Politica e Società* 2, 247–264.

[7] Francesca Bignami, 'Privacy and law enforcement in the European Union: The Data Retention Directive' (2007), *Chicago Journal of International Law* 8:1, 233–255.

[8] See for an illustration of the data retained from electronic communications the projection of data retention that was done for a Swiss MP <https://www.digitale-gesellschaft.ch/dr.html> accessed 1 June 2014.

surveillance is *par excellence* a way in which the State interferes with the private life of the individuals.

The term surveillance derives from the French language and literally refers to a close watch kept over someone or something.[9] In contemporary social and political sciences, surveillance refers to the "*process of watching, monitoring, recording, and processing the behavior of people, objects and events in order to govern activity*".[10] For Wigan and Clarke (2006) the origin of 'surveillance' derives from the times of the French revolution.[11] The term is related with the systematic investigation or monitoring of the actions or communications of one or more persons.[12]

For our study surveillance is considered as an intelligence activity performed by the State and that can be used for meeting different needs of law enforcement authorities, as for example: prevention or detection of crime, identification of the responsible persons, investigation, etc. We distinguish further between traditional surveillance and surveillance with non-purpose built technology. Under the concept of traditional surveillance for this study qualifies not only physical surveillance, as for example when watching someone with the free eye or listening to a conversation through the key hole of a door. Surveillance performed with surveillance technology is also qualified for our study as traditional surveillance. Surveillance technology is defined as devices that are designed and used for the purpose of surveillance as being their first scope as for example bugs, street cameras, wiretapping devices, etc.

Surveillance with non-purpose built technology on the other side is defined for this study as State surveillance via devices that have not been originally built for the purpose of surveillance. To say that a device has not been originally built for the purpose of surveillance might be a bit speculative especially since we do not know that there might be cases in which a certain technology might have been initiated and supported by hidden interests of intelligence service bodies. Devices non-built for the purpose of surveillance for this study are therefore devices that are introduced in the markets mainly for the performance of another activity, as for example: smart phones, GPS navigation systems, smart tv, smart meters, etc. For the purpose of this study it is the combination of the ability and of the official accreditation that determines the qualification of a device as not built for the purpose of surveillance.

Just from the examples of devices mentioned above, it is clear that even if not designed for the purpose of surveillance these devices may have the ability to facilitate different forms of surveillance and interfere with the private life of the individuals in different ways. One way of interference is direct surveillance, i.e. surveillance on the spot or interference by the State on the device or network of a service provider,[13] and the other is dataveillance,[14] i.e. surveillance of the track of data that someone leaves behind. Dataveillance opens the possibility to use for the purpose of surveillance personal data that have been collected by devices and systems for other purposes, as for example for billing transparency. This form of interference with the individuals' lives based on data collected for other purposes is referred in our study as surveillance with non-purpose collected data and is part of the larger category of surveillance with non-purpose built technology. The most obvious example of such a situation is the case of the former Data Retention Directive in the EU.

Technology that has a potential to be used for surveillance creates privacy concerns more directly than any other type of technology since it allows third parties to observe and watch over details from the private life of an individual that are not intended to be observed. Another discussion is the actual use of the devices for such purposes since it is also possible to observe and collect the same information from the individuals, with the use of different devices or systems of surveillance. Information on the location of an individual at a certain moment can be obtained, for example, from direct physical observation, the data of a GPS device, the mobile phone, the geo location of the computer IP when accessing internet, a RFID attached on the label of a shirt, by the data sent by a smart energy meter, etc. Each of these methods and devices presents different levels of intrusion into the private sphere of the individuals. A privacy oriented approach would indicate the use of the less intrusive mean of surveillance for reaching a certain goal.[15]

While the privacy concerns raised by advances in surveillance technologies are widely recognized,[16] recent technology developments have led to a convergence of these technologies with others not designed for the purpose of surveillance. The existence of such devices and technologies challenges the classic understanding of surveillance and, in a way, blurs the distinction between the surveilled and the surveillor, between the state and private parties.[17] As a result, the protection of

[9] As defined by the Merriam-Webster Online Dictionary.

[10] Valerie Jenness, David A. Smith, Judith Stepan-Norris, 'Taking a look at surveillance studies' (2007), *Contemporary sociology: A Journal of Reviews* 36:2, vii–viii.

[11] Marcus Wigan, Roger Clarke, 'Social impacts of transport surveillance'(2006), *Prometheus: Critical studies in Innovation* 24:4, 389–403.

[12] Colin Bennett, 'The public surveillance of personal data: A cross-national analyses', in David Lyon, Elia Zureik (eds.), Computers, surveillance, and privacy (University of Minnesota Press, 1996), 237–259.

[13] Murdoch Vatney 'The justifiability of state surveillance of internet communications as an e-security mechanism' (2006), <http://icsa.cs.up.ac.za/issa/2006/Proceedings/Full/117_Paper.pdf> accessed 17 February 2015.

[14] Roger Clarke 'Dataveillance: Delivering '1984'', in Leila Green, Roger Guinery (eds.), Framing Technology: Society, Choice and Change, (Allen & Unwin, 1994), <www.anu.edu.au/people/Riger.Clarke/DV/PaperPopular.html> accessed 3 February 2015.

[15] The right to privacy in the digital age – Report of the Office of the United Nations High Commissioner for Human Rights, 30 June 2014, para. 25.

[16] Thomas B. Kearns 'Technology and the right to privacy: The convergence of surveillance and information privacy concerns' (1999), *William & Mary Bill of Rights Journal* 7:3, 975–1011.

[17] For example in the Concise Oxford Dictionary surveillance is defined as "*close observation, especially of a suspected person*"; for Gary T. Marx 'What's new about the "New Surveillance"? Classifying for change and continuity' (2002), *Surveillance and Society* 1:1, 9–29, self-monitoring has emerged as an important theme, and is encouraged by the availability of a number of devices (as those that test for alcohol level, etc.) merging the lines between the surveilled and the surveillant.

the right to privacy of European citizens presents new challenges. In the following subsection we will analyze in how far surveillance with non-purpose built devices differs from traditional surveillance on the basis of a number of meta-dimensions.

2.1. *Devices not built for the purpose of surveillance and their effect for the right to privacy*

The proliferation of the means via which the State is able to collect personal information from the citizens, extends the reach of the State and risks the safeguarding of the right to privacy.[18] For assessing if surveillance with devices not built for the purpose of surveillance meets the required safeguards for complying with the right to privacy, it is first important to establish in how far it diverges from traditional surveillance.

In a work of 2002, Gary Marx presents a comparison of 'new surveillance' – named in this way because of the advanced technology used for surveillance that makes it more a scrutinizing rather than an observing activity – as confronted with the 'traditional surveillance' that in his description is linked with physical surveillance and a scarce use of technology. This comparison is based on 26 identified dimensions of surveillance.[19] According to Marx, development of technology has changed the way surveillance is performed at such a level as to fail the current dictionary definitions and understandings of the term. In comparison to 'traditional surveillance', 'new surveillance' is considered to be almost invisible, involuntary and integrated into routine activity, inexpensive, continuous, more intensive and more extensive.

The concept of 'new surveillance' does not overlap completely with our definition of surveillance with non-purpose built technology. The reasons for this non-coincidence are mainly two. Firstly, Marx's 'new surveillance' is not distinguishing between surveillance technology and technology not built for the purpose of surveillance. Secondly, our definition of surveillance with non-purpose built technology is limited to State activities while 'new surveillance' includes also activities of private parties and self-surveillance. Also Marx's definition of 'traditional surveillance' does not fully coincide with ours since we include into this category also all the surveillance performed via surveillance technology being this advanced or not. Despite the non-coincidence in the used definitions, the surveillance dimensions identified by Marx characterize surveillance in general besides any definition boundaries, and they are used also in comparing our separation of traditional surveillance and surveillance with non-purpose built technology.

Below we will make a comparison between the two forms of surveillance. For making this comparison we have grouped the 26 dimensions of surveillance identified by Marx in four meta-dimensions of surveillance that correspond to the following questions: (1) who is the subject (active/passive) of surveillance;[20] (2) how is surveillance performed;[21] (3) what aspects of private life are interfered with;[22] and (4) when is surveillance taking place.[23] This grouping of the dimensions was done for reflecting and focusing better on our aim to compare the two forms of surveillance for identifying the effects that these have for the right to privacy of the individuals. Each of the meta-dimensions is treated in turn highlighting the effects of surveillance with non-purpose built technology for the right to privacy of the citizens.

2.1.1. *Who is the subject of surveillance?*

When looking at the subject of surveillance, one has to keep in mind two aspects. First we will focus on the active subject, the surveillant, and then on the passive subject, the surveilled.

2.1.1.1. The active subject of surveillance. In traditional surveillance, the surveillant is represented by the State and its authorities. Private parties have this role in specific and clearly defined cases, under clear authorization that is in conformity with all the set safeguards (as for example when private parties are authorized to install a CCTV for the scope of protecting their premises).[24] The centralization of surveillance in the hands of the State is mirrored in the exercised control on surveillance as well as in the performance under clear conditions and safeguards.

At the times of technology development and especially of the existence of devices that are non-purpose built for surveillance but have the ability to perform this task, the surveillant cannot be linked anymore exclusively to the State. Devices that might serve for surveillance are available in the hands of the citizens and as we have seen in different examples, most of personal data collected by technology are nowadays available with service providers. As a result, the role of private parties becomes more prominent.

Because of the ability of technology and its spread it is possible for State surveillance to be performed in a generalized and massive scale without the need to target previously identified individuals. Furthermore, the individuals can themselves collaborate in their own surveillance blurring the distinction between the active and passive subjects of such activity. This is not only for the reason of carrying with them devices that have a potential to be used for surveillance but also for using and feeding with data a number of softwares to organize their activities and even to monitor themselves (as for example

[18] Valsamis Mitsilegas 'The transformation of privacy in the area of pre-emptive surveillance' (2015), *Tilburg Law Review* 20, 35–57.

[19] Gary T. Marx (n 17) see table 1.

[20] Under this question are grouped the surveillance dimensions of: consent, data collector, availability of technology, object of data collection, ratio of self to surveillant knowledge, identifiability of object of surveillance, emphasis on and who collects the data.

[21] Under this question are grouped the surveillance dimensions of: senses, visibility, cost, location of data collector/analyzers, ethos, integration, data resides, comprehensiveness, realism, data analyses, data merging, data communication.

[22] Under this question are grouped the surveillance dimensions of: context, depth and breadth.

[23] Under this question are grouped the surveillance dimensions of: timing, time period and data availability.

[24] Case C-212/13 František Ryneš v Úřad pro ochranu osobních údajů [2014] nyr, paras. 33–34.

keeping online agendas or using an e-health application in smart phones).[25]

2.1.1.2. The passive subject of surveillance. The comparison between traditional surveillance and surveillance with non-purpose built technology has relevance also for the passive subject of surveillance. Traditional surveillance is normally performed toward individuals for whom there is a surveillance mandate. It is quite expensive and inefficient to surveil other individuals in the absence of individual mandates. Mass surveillance of individuals is restricted to clear a precise public spaces, for example the access in airports or being in certain CCTV covered areas. In case non-targeted individuals are incidentally surveilled, it is easy to distinguish them from the targeted subject of surveillance (as for example when incidentally intercepting the phone call of a third person having access to the wiretapped device).

Surveillance with non-purpose built technology creates more possibilities for situations of mass surveillance and incidental surveillance. The introduction of pre-emptive surveillance[26] that aims to detect all situations that might have or not any relation to a possible future criminal activity together with the technology capabilities have increased the use of mass surveillance. This is now not linked anymore with the presence in certain spaces but with the use of certain technology by the citizens. One might be surveilled not only when being in well-defined public spaces, but also when being in the intimacy of one's own private space. In addition it is more difficult to distinguish the cases of incidental surveillance. When analyzing data that have been collected and retained from the use of a device, it is difficult to be certain that the device was used by one person or another (for example another member of the household). Even if surveillance with non-purpose built technology presents itself as more deep than traditional surveillance,[27] incidental involvement of third persons might make this less accurate both in the cases of individual surveillance and in the cases of mass surveillance.

2.1.2. *How is the surveillance performed?*

Also the way surveillance is performed changes in cases of traditional surveillance and surveillance with non-purpose built devices. Traditional surveillance is mainly direct and devices, even the advanced ones, need an activation from the surveillor (as for example when installing a bug or using a terahertz body scanner). Dataveillance[28] is part of traditional surveillance only in specific cases linked with the surveillance technology used (as for example when tracing a CCTV footage).

Surveillance with non-purpose built technology is folded into routine activity and based more on the data collection and retention capability of the devices and systems, therefore has mainly the form of dataveillance. This form of surveillance (due to incidental interception) might create the risk that incorrect or unreliable data are used.[29] Devices and the programmes installed in them would collect data for default and these data, even if non collected for the purpose of surveillance might be further used for this purpose. Non-purpose built technology allows also for direct observation when remotely activating devices and using them for surveillance (as in the case of activating the microphone of a mobile phone and use it as a portable bug or connecting to the satellite to access the location of the navigation system of a car).

2.1.3. *What aspects of private life are interfered with?*

The private sphere of the individuals consists of a number of aspects that have been identified earlier by Clarke (2006)[30] and further elaborated by other authors.[31] These include: (i) privacy of the person concerned with the privacy of an individual's body, (ii) privacy of personal behavior,[32] (iii) privacy of personal communication, (iv) privacy of personal data, (v) privacy of location and space, (vi) privacy of thoughts and feelings,[33] and (vii) privacy of association. The increase of the aspects of privacy that might be interfered by surveillance as well as the separation of subcategories has increased due to the development of technology. For example the privacy of the thoughts and feelings could not be interfered with the traditional ways of surveillance but it is possible now due to the new technology with devices not built for the purpose of surveillance.

Also the level of intrusion into each aspect of privacy diverges in cases of traditional surveillance and surveillance with non-purpose built technology. For example placing a bug inside the home of a citizen for listening to the conversations is intrusive, but remotely activating the microphone of a mobile phone and use it for the same purpose is even more. Someone would carry a mobile phone with himself in most places and therefore be vulnerable to the infringement of the privacy of communications almost everywhere. The same would be when physically following someone on the streets or installing a GPS device in his car, or receiving the same information from the mobile phone GPS. Again in the latter case the coverage and the level of intrusion would be more intensive. Surveilling via the data collected by a smart meter, on the other side, might

---

[25] Jerry Kang, Katie Shilton, Deborah Estrin, Jeff Burke, Mark Hansen 'Self-surveillance privacy' (2012), *Iowa Law Review* 97, 809–847.

[26] Rosamunde van Brakel, Paul De Hert 'Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies' (2011), *Cahiers Politiestudies* 3:20, 163–192.

[27] Gary T. Marx (n 17).

[28] For a definition of dataveillance see Roger Clarke (n 14).

[29] Jannifer Chandler, 'Privacy Versus National Security: Clarifying the Trade-off', in Ian Kerr, Carole Lucock, Valerie Steeves (eds.), Lessons From the Identity Trail: Privacy, Anonymity and Identity in a Networked Society (OUP, 2009), 121–138.

[30] Roger Clarke, 'What's 'Privacy'?' (2006) <http://www.rogerclarke.com/DV/Privacy.html> accessed 10 July 2013.

[31] David Wright, Charles Raab, 'Privacy principles, risks and harms' (2014), *International Review of Law, Computers and Technology* 28:3, 277-298.

[32] Georgios Kalogridis, Stojan Z. Denic, 'Data mining and privacy of personal behavior types in smart grid' (2011), *IEEE*, 636–642.

[33] See for example the newest developments on wireless brain–computer interface in David A. Borton, Ming Yin, Juan Aceros, Arto Nurmikko, 'An implantable wireless neural interface for recording cortical circuit dynamics in moving primates (2013), *Journal of Neural Engineering* 10:2, 16; Susan Young Rojahn, 'A wireless brain–computer interface' (2013), <http://www.technologyreview.com/news/512161/a-wireless-brain-computer-interface/> accessed 24 April 2013.

work as having a continuous physical presence inside a house.[34] From the above examples it is clear that surveillance with non-purpose built technology presents itself as having a higher level of intrusiveness into the private life of the individuals than traditional surveillance.

2.1.4. *When is surveillance taking place?*

Traditional surveillance is mainly taking place simultaneously, at the moment. Surveillance with non-purpose built devices has the possibility also to bring the past into the present and even to predict the future. Retention of personal data, for example, creates the possibility to look back at the past behavior and activities of an individual. As a result, there is the possibility to check the past activities of an individual at a time he was not suspected as related to any criminal activity. It does not go without saying, however that this possibility of surveillance on the bases of retrieving retained data might lead to infringements of other rights of the individuals, as for example their right to due process and the presumption of innocence.[35] Data mining and analyses might also give the possibility for future predictions on the behavior of individuals and serve for fulfilling the scope of preemptive surveillance.

There is a difference also in the timing of surveillance. While traditional surveillance mainly takes place at single or intermittent points of time, surveillance with non-purpose built technology can be continuous and omnipresent. The availability of the surveillance results might present certain time lags for traditional surveillance while it is available in real time for surveillance with non-purpose built technology.

From the above comparison on the bases of the four metadata it is clear that surveillance with non-purpose built technology is more intrusive into the life of the individuals than traditional surveillance. The choice of traditional surveillance or surveillance with non-purpose built technology is of course left with the national authorities responsible for the prevention, investigation, detection and prosecution of criminal activities on the basis of the safeguards offered by the laws and the proportionality principle.

3. The proportionality test

Some authors define proportionality as the set of rules determining the necessary and sufficient conditions for limiting a protected right.[36] Others define it as a principle that restricts the exercise of government powers.[37] We can say therefore that the proportionality principle fulfils a dual role: it protects fundamental rights and it provides a justification for their limitation.[38] This section will briefly discuss the proportionality test as developed by the Court of Justice of the European Union taking into account its importance in establishing a lawful interference with the fundamental rights of the individuals.[39]

For the European Union (EU) the proportionality principle is introduced in Article 52(1) of the Charter as a condition to be fulfilled when need requires the limitation of certain rights.[40] The principle was however fully developed by the European Court already in 1970,[41] in the *Internationale Handelsgesellschaft* case.[42] Similarly with the German administrative law, the test for establishing the proportionality of a measure is composed of three steps: (i) appropriateness; (ii) necessity; and (iii) proportionality *stricto sensu*.[43] The measure that interferes with fundamental rights must be first of all appropriate or suitable to protect the interests that require protection. Secondly, it must be necessary, meaning that no measure less restrictive must be available to attain the objective pursued.[44] Thirdly, 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.[45] The Court does not always distinguish, however, between the second and the third step of the test.[46]

It is important to note at this point that some authors, when discussing the necessity step of the proportionality test for identifying the least intrusive means of surveillance, refer to it as

[34] Nancy J. King, Pernille W. Jessen 'Smart metering systems and data sharing: why getting a smart meter should also mean getting strong information privacy controls to manage data sharing' (2014), *International Journal of Law and Information Technology*, 1–39.

[35] Jonida Milaj, Jeanne P. Mifsud Bonnici, 'Unwitting subjects of surveillance and the presumption of innocence' (2014), *Computer Law & Security Review* 30:4, 419–428.

[36] Aharon Barak, 'Proportionality – Constitutional Rights and their limitations' (Cambridge University Press 2012), 3.

[37] Jan H. Jans, Roel de Lange, Sacha Prechal, Rob Widdershoven, 'Europeanisation of Public Law' (Europa Law Publishing 2007), 143.

[38] Aharon Barak (n 36) 165; With regard to the USA, since there is general agreement that current privacy theory does not address adequately the societal concerns regarding the use and the protection of information, the idea was thrown to have Privacy 3.0 built upon only one principle – the principle of proportionality, see Andrew B. Serwin, 'Privacy 3.0 – The principle of proportionality' (2009), *University of Michigan Journal of Law Reform* 42:4, 869–890.

[39] Andrew B. Serwin (n 38).

[40] The proportionality principle is central also in the Council Framework Decision 2008/977/JHA (n 29), see for example Article 3.

[41] Aharon Barak (n 36) 185.

[42] Case 11/70 Internationale Handelsgesellschaft v. Einfuhr- und Vorratsstelle Getreide [1970] ECR 1125.

[43] Antonio Troncoso Reigada, 'The principle of proportionality and the fundamental right to personal data protection: The biometric data processing' (2012), *Lex Electronica*, 17:2, 1–44.

[44] Jan H. Jans, 'Proportionality revisited' (2000), *Legal issues of economic integration* 27:3, 239–265; Opinion of the EDPS on the evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC), 31.05.2011; According to Robert Alexy, 'A theory of constitutional rights' (OUP, 2002), 399, necessity is an expression of Pareto optimality: "*Thus the principle of necessity is an expression of the idea of Pareto-optimality as well. Because of the existence of a less intensively interfering and equally suitable means, one position can be improved at no cost to the other.*"

[45] Jan H. Jans, et al. (n 37) 149.

[46] Opinion of AG van Gerven delivered on 11 June 1991, in C-159/90 The Protection of Unborn Children Ireland Ltd v. Stephen Grogan and others [1991] ECR I-04685, para. 27.

the subsidiarity test.[47] The test would rule out the use of more intrusive surveillance when the same result can be achieved with less intrusive means. In this paper we discuss the intrusiveness of surveillance means but we do not use the term subsidiarity and we stay with the larger framework of the proportionality test. This choice is because we would like to avoid the confusion of the terminology from an EU law perspective. In EU law the subsidiarity principle concerns the relationship between the EU and the Member States. Proportionality on the other side has traditionally concerned the relationship between the EU and its economic subjects.[48]

As a general principle of law, proportionality has been developed by the Court primarily with a view to protecting the individual from action by the Union institutions and by the Member States. It has to be kept in mind that proportionality as a general principle of law is different from Article 5 TEU which forms part of a system of provisions whose aim is to control the expansion of the EU legislation.[49] The principle facilitates the establishment of a proper balance between the individual interest and the desired general interests recognized by the EU with the aim of promoting European integration.[50]

The proportionality principle as used by the Court contains a very strong substantial bias.[51] This is reflected in the different ways the Court has been using the principle when judging upon EU or national measures.

When challenging the validity of EU law, the Court looks if the measure is manifestly disproportionate.[52] While when challenging the validity of national measures, the Court applies a stricter test and inquires if there was possible for the Member State to adopt an alternative measure that is less restrictive.[53] According to Jacobs (1999) this bias approach has its good reasons:[54] the scrutiny of national measures may need to be more demanding since these are likely to impair the effectiveness of EU measures.[55]

When proportionality is invoked as a ground of review for policy measures, the Court is called upon to balance a private against a public interest. The underlying interests which the principle seeks to protect are the rights of the individual but, given the discretion of the legislature, review of policy measures is based on the so-called milder 'manifestly disproportionate' test. When proportionality is invoked to challenge the compatibility of EU law of national measures, affecting one of the fundamental freedoms, the Court is called upon to balance an EU interest against a national one. The principle is applied 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.[56] The alternative method is not required, however, to be the most effective or practical solution.[57]

The non-systematic way in which the Court addresses the proportionality test[58] is reflected also in the non-systematic way in which the legislators deal with it. This is a virtuous circle. On one side, for the courts it is difficult to challenge the proportionality and necessity of a legal provision because of the implications that this has with the political considerations of the legislator and their role on the bases of the division of powers between the legislative, judiciary and executive. This argumentation would suggest that it would be better that the proportionality of a legal measure is checked at an earlier stage, by the legislator itself. This is reflected also in a Commission Communication requiring all new legislative and major policy-defining proposals to be checked for compliance with the Charter of Fundamental Rights.[59] On the other side we see in practice that the legislator is not systematically dealing with the proportionality test when adopting new laws.[60] This negligence of the legislator might come as a reflection of the Court failing to convincingly use the proportionality test and to transmit the right message.

[47] Paul De Hert, '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' (2005), *Utrecht Law Review* 1:1, 68–96; Luc Verhey, Mathijs Raijmakers, 'Article 8 of the European Convention on Human Rights – Proportionality and the protection of personal data', in Marjolein van Roosmalen, Ben P. Vermeulen, Fried van Hoof, Marten Oosting (eds), *Fundamental rights and principles* (Intersentia, 2013), 459–479; Antonella Galetta, Paul De Hert 'Complementing the surveillance law principles of the Court of Strasbourg with its environmental law principles. An integrated technology approach to a human rights framework for surveillance' (2014), *Utrecht Law Review* 10:1, 55–75.

[48] Jan H. Jans, et al. (n 37), 150.

[49] Takis Tridimas, 'Proportionality in European Community law: Searching for the appropriate standard of scrutiny', in Evelyn Ellis (eds), *The principle of proportionality in the laws of Europe* (Heart Publishing, 1999), 65–84.

[50] Joined Cases C-92/09 and C-93/09 Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen [2010] ECR I-11063, para. 86; Jeanne P. Mifsud Bonnici, 'Exploring the non-absolute nature of the right to data protection' (2013), *International Review of Law, Computer and Technology* 28:2, 131–143.

[51] Takis Tridimas (n 49); C-84/94 United Kingdom v. Council [1996] ECR I-5755, para. 57; C-265/87 Schraeder HS Kraftfutter GmbH & Co KG v. Hauptzollamt Gronau [1989] ECR 2237, para. 21–24.

[52] Case C-331/88 The Queen v. Minister of Agriculture, Fisheries and Food and Secretary of State for Health, ex parte: Fedesa et al. [1990] ECR I-4023, para. 8; C-491/01 The Queen v. Secretary of State for Health, ex parte British American Tobacco (Investments) Ltd and Imperial Tobacco Ltd [2002] ECR I-11453, para. 123; Joined cases C-453/03, C-11/04, C-12/04 and C-194/04 ABNA Ltd et al. v. Secretary of Health et al. ECR I-10423, paras. 80–84.

[53] Opinion of AG Maduro in Case C-524/06 Heinz Huber v. Bundesrepublik Deutschland [2008] ECR I-09705, para. 16; Case C-210/03 Swedish Match AB and Swedish Match UK Ltd [2004] ECR I-11893, paras. 56–58; Case 120/78 Rewe-Zentral AG v. Bundesmonopolverwaltung für Branntwein [1979] ECR 649; Case 302/86 Commission v. Danmark [1988] ECR 4607, para. 6.

[54] C-84/94 United Kingdom v. Council [1996] ECR I-5755, para. 57; C-265/87 Schraeder HS Kraftfutter GmbH & Co KG v. Hauptzollamt Gronau [1989] ECR 2237, paras. 21–24.

[55] Francis G. Jacobs, 'Recent development in the proportionality principle in European Community law', in Evelyn Ellis (eds), *The principle of proportionality in the laws of Europe* (Heart Publishing 1999), 1–21.

[56] Takis Tridimas (n 49).

[57] Opinion of AG Maduro in Case C-524/06 Heinz Huber v. Bundesrepublik Deutschland [2008] ECR I-09705, para. 16.

[58] Grainne de Burca, 'The principle of proportionality and its application in EC law' (1993), *Yearbook of European Law* 13:1, 105–150.

[59] COM(2005)172 on compliance with the Charter of Fundamental Rights.

[60] Luc Verhey, Mathijs Raijmakers (n 47).

4. The proportionality test in the Data Retention Directive judgement

After analyzing in general the use of the proportionality principle by the European Court, in this section we will analyze the way it was used for the invalidation of the Data Retention Directive. While the invalidation of the Directive in itself did not came as a surprise,[61] the quick development in technology makes it important to assess if the test used is able to include other situations of interference with the life of the citizens as a result of surveillance with non-purpose built devices.

Before discussing the way the Court used the proportionality test in this case, a few words on the Data Retention Directive are due. The aim of the Directive was to allow the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communication networks for possible use by law enforcement authorities.[62] Essentially, providers of fixed and mobile telephony services and internet service providers were expected to retain records of service users to trace and identify the source, destination, date, time and duration of a communication together with information necessary to identify the type of communication, the equipment used and the geographical location of the user.[63] All this metadata was to be kept according to the time limit set by national law but for no less than six months and no more than two years.[64] The Directive was ensuring that the data retained by the service providers were available for the purpose of investigation, detection and prosecution of serious crime[65] – the latter as defined by each Member State in its national law.[66] The data retention was not undertaken for a specific, limited purpose but was general and continuously covering all electronic communications. The Directive essentially introduced a form of mass surveillance (dataveillance) of citizens at EU level.[67] This was based on the ability of service providers to collect and retain a number of personal data for different purposes (as for example billing details) and then make these data available to law enforcement authorities for other purposes – in our case for mass surveillance of the users of electronic communications.

The Court of Justice of the EU ended the long debate on the validity of the directive finding that its interference with the Articles 7 and 8 of the Charter was exceeding the limits imposed by the principle of proportionality (Art. 52(1) of the Charter). The breach was considered by the Court so severe that, in difference from the opinion of the Advocate General,[68] the Court did not provide for a suspension of the effects of the decision until the Member States would adopt the necessary legal acts required after its invalidation. The effects of the invalidation were immediate and *ab initio*.[69] As a result, the Directive is to be considered today as if it never existed.

In its elaboration the Court first identified the existence of the interference with the protected rights and then elaborated on the possible justifications. The Court distinguishes the right to a protected private life from the right to data protection and considers the directive to interfere with both of them. To interfere with the right to privacy does not necessarily require that the information on the private lives concerned is sensitive but is enough that the individual has been inconvenienced in a certain way.[70] This condition is fulfilled, according to the Court by the retention of the data as well as by the potential access by the national authorities. The processing of the personal data required by the Data Retention Directive brings it automatically to fall also under the data protection regime since data processing is involved. The potential use of the data without informing the person concerned makes this interference particularly serious since "*. . . it is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance*".[71] This argumentation of the Court is related with the fact that this form of data retention turns surveillance for the individuals into a normal situation, a rule. It has to be noted, however, that despite the severe infringement, for the Court the essence of both rights is not considered as adversely affected and the Directive is considered to genuinely satisfy an objective of general interest. In this way, the Court is leaving open the possibility for other legislation on data retention in the EU, provided that it is proportionate.

[61] Already in the case discussing the legal basis of the Directive this conclusion was anticipated. See case C-301/06 Ireland v. European Parliament and Council [2009] ECR I-00593, para. 57 "*. . . it must also be stated that the action brought by Ireland relates solely to the choice of legal basis and not to any possible infringement of fundamental rights arising from interference with the exercise of the right to privacy contained in Directive 2006/24.*"

[62] For a detailed presentation of the reasons for the introduction of the Data Retention Directive please see: Jeanne P. Mifsud Bonnici, 'Recent European Union developments on data protection . . . in the name of Islam or 'Combating terrorism'' (2007), *Information & Communications Technology Law* 16:2, 161–175; Abu Bakar Munir, Siti Hajar Mohd Yasin, 'Retention of communications data: a bumpy road ahead' (2004), *Journal of Computer & Information Law* 22, 731–758; Marie-Helen Maras, 'While the European Union was sleeping, the data retention directive was passed: The political consequences of mandatory data retention' (2011), *Hamburg Review of Social Sciences* 6:2, 1–30; Eleni Kosta, 'The way to Luxemburg: National Court decisions on the compatibility of the data retention directive with the rights to privacy and data protection' (2013), *SCRIPTed* 10:3, 339–363.

[63] Art. 5 Data Retention Directive.

[64] Art. 6 Data Retention Directive.

[65] Joel R. Reidenberg, 'The data surveillance state in the United States and Europe' (2013), Wake Forest Law Review 48, p. 29.

[66] Rec. 21 Data Retention Directive. See also COM(2011) 255 final, Brussels, 18.4.2011, Evaluation Report on the Data Retention Directive.

[67] Hal Roberts, John Palfrey, 'The EU Data Retention Directive in an era of internet surveillance', in Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan Zittrain (eds) *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, (MIT 2010), 35–53; Marie-Helen Maras, 'From targeted to mass surveillance: Is the EU data retention directive a necessary measure or an unjustified threat to privacy', in Benjamin J. Goold, Daniel Neyland, D. (eds.), New directions in surveillance and privacy Routledge (2009), 74–105.

[68] Opinion of AG Cruz Villalon in joint cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and others [2014] nyr.

[69] Joint Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and others [2014] nyr, para. 71.

[70] Joint Cases C-465/00, C-138/01 and C-139/01 Österreichischer Rundfunk and Others [2003] ECR I-04989, para. 75.

[71] Joint Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and others [2014] nyr, para. 37.

After establishing the interference with both fundamental rights, the Court continued by assessing the proportionality of the interference.[72] The Court applied the proportionality test as established in its earlier case law[73] composed of three steps: (i) appropriateness; (ii) necessity; and (iii) proportionality *stricto sensu*.[74] The distinction between the second and the third step of the test, as it is customary also from previous judgments, is not a clear cut.[75] This is not surprising, taking into account that for the Court the necessity test, because of its political implications, remains 'highly fluid and indeterminate'.[76]

In the first step the Court established if the measure was appropriate for attaining the set objectives (para. 49). The focus of the analyses was on the value that the retained data have for national authorities giving them additional opportunities to shed light on serious crime. Data retention methods were, therefore, evaluated as valuable for criminal investigation. What the Court is looking for at this stage is only that the retained data can have a value for law enforcement authorities. For the Court it is not relevant if these data are collected as a result of traditional surveillance or are collected by devices and technology not built for surveillance purposes. As a result, a discussion on the means used for surveillance did not take place.

The Court discussed afterwards the second and the third step of the test (the necessity and the proportionality *stricto sensu* of the measure). In the previous section we saw that when analyzing the proportionality of EU measures the Court looks at their "manifest disproportionality" while for national measures the test is stricter and focuses on the "less restrictive alternative". This biased approach might be justified with the fact that often national measures might be directed to individual cases and this facilitates a proportionality assessment while for EU legislation the separation of powers gives the Court a less prominent role.[77] This biased approach might also stand in the area of market integration[78] but does not have a reason to stand when analyzing the infringement of fundamental rights of the individuals for which a stricter approach is needed.[79]

The Court appeared to be aware of this. If the Court would have been following its established line of reasoning when assessing the proportionality of EU rules, it would have been limiting its reasoning to the "manifestly disproportionate" test. However this was not the case. The Court referred to the *IPI case*[80] and used the formula stating that ". . . *derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary*". The Court used therefore a third test that has an *ex post* approach, focusing on the existence of clear and precise rules to govern the scope and application of the interfering measure and the existing minimum safeguards introduced against the risk of unlawful access and use of personal data. This test does not give the Court the possibility to discuss the technology used for surveillance. This will be discussed in more detail in the following sub-section.

4.1. *Extending the proportionality test*

This sub-section will reflect on how to extend the proportionality test for including also an assessment of the technology used for surveillance. As already explained, the technology used for surveillance will influence the amount of the data and the level of the interference with the private life of the individual. It is important to note at this point that a discussion on the means of surveillance in the Data Retention Directive it is not just introduced by us. The Court by itself in discussing the proportionality of the Directive (para. 57) declares that its provisions are referring in a generalized manner to "all persons", "*all means (of surveillance)*" and "all data". In continuing the discussion however the Court elaborates on "all persons" (para. 58) and "all data" (para. 59) without referring anymore to "all means". This is first of all related with the Court limiting its attention to an *ex post* rectification of the effects approach without paying attention to the technology used. Secondly this is related also with the Court making use of the "limited to what is strictly necessary" test. This test is used rarely and, as discussed earlier, when EU law is contrasted to individual rights the Court is normally focusing its attention on the "manifestly disproportionate" nature of the measure. In our case the Court found the measure to be appropriate, but since

[72] See the legal analyses from the Danish Ministry of Justice (n 4); Xavier Tracol, 'Legislative genesis and judicial death of a directive: The European Court of Justice invalidated the data retention directive (2006/24/EC) thereby creating a sustained period of legal uncertainty about the validity of national laws which enacted it' (2014), *Computer Law & Security Review* 30, 736–746.

[73] Case 11/70 Internationale Handelsgesellschaft v. Einfuhr- und Vorratsstelle Getreide [1970] ECR1125.

[74] Antonio Troncoso Reigada (n 43).

[75] Opinion of AG van Gerven delivered on 11 June 1991, in C-159/90 The Protection of Unborn Children Ireland Ltd v. Stephen Grogan and others [1991] ECR I-04685, para. 27; for a clarification of the necessity and proportionality stricto sensu steps of the proportionality test see Julian Rivers, 'A theory of Constitutional rights and the British Constitution', A translator's introduction in Robert Alexy, *A theory of constitutional rights*, (OUP, 2002), xxxi: "*Necessity asks whether any less intrusive means would achieve the same end, which is essentially an empirical question of prognosis and causation, and proportionality asks whether the end is worth pursuing, given what it necessary costs. It is important to see that necessity and proportionality (in the narrow sense) are different tests: a measure may be the least intrusive means to achieve a certain end, and yet even the least intrusion necessary may be too high a price to pay in terms of the interference with other legally recognized interests.*"

[76] Antonella Galetta, Paul De Hert (n 47); Steven Greer, 'The exceptions to Articles 8 to 11 of the European Convention of Human Rights' (1997), *Human Rights Files*, no. 15, (Council of Europe Publishing).

[77] However, the Court often goes against the wording of a provision and the intention of the legislator in its judgements and extends the scope of application of EU law. See for example case C-617/10 Aklagaren v. Hans Akerberg Fransson [2013] ECR nyr, were the Court gave an extended interpretation of the wording "*implementation of EU law*".

[78] Tor-Inge Harbo, 'The function of the proportionality principle in EU law' (2010), *European Law Journal*, 16:2, 158–185.

[79] Case C-112/00 Eugene Schmidberger, Internationale Transporte und Planzuge v. Austria [2003] ECR I-5659, para. 74; Case C–73/07 Satakunnan Markkinapörssi and Satamedia [2008] ECR I–9831, para. 56, and Joined Cases C–92/09 and C–93/09 Volker und Markus Schecke and Eifert [2010] ECR I–11063, paras. 77 and 86.

[80] Case C-473/12 Institut professionnel des agents immobiliers (IPI) v. Geoffrey Engelbert, Immo 9 SPRL, Gregory Francotte [2013] nyr, para. 39.

fundamental rights of the individuals are concerned and their limitation has to be interpreted in a strict way the Court reasons that the interference with the rights introduced by the EU legislator must apply only in so far as "strictly necessary".[81]

This reasoning from the Court for invalidating the Data Retention Directive is plausible. It is to be kept in mind that mass data retention affects primarily individuals that do not have any past, present or even future relation to a criminal activity.[82] As a result high safeguards as well as a strict proportionality test has to take place for non-compromising their fundamental rights. When defending mass surveillance of citizens it is normally said that if one has nothing to hide then he has nothing to fear.[83] But in situations of untargeted surveillance a reasonable question would be: "If one has nothing to hide than why does the State look into one's private life?" At present it is continuous surveillance that one is experiencing and rightfully fearing.

Coming back to our discussion of the technology used for surveillance, we have already seen that the level of intrusion and awareness is different when using means that have been designed for the purpose of surveillance and when using non-purpose built technology. The level of intrusion with one's private life is different when looking at his behavior by CCTV with all the warning signs or with a personal computer camera, freely used and moved in private spaces without any intimation or warning.[84]

In the Data Retention Directive case the Court is limiting the necessity step of the proportionality test to the "limited to what it is strictly necessary" analyses. The Court has however failed so far to clearly determine what is covered under the definition of necessity in a democratic society. Since in the case of the data retention the Court is assessing fundamental rights against EU public interests and the rights of millions of innocent people are interfered, less restrictive alternatives should have been taken into account.[85] The proportionality test used by the Court, even if plausible, should have been going further, as to include the "less restrictive alternative" analyses including an evaluation of the technology used for surveillance.[86] Even if the Charter of Fundamental Rights of the EU is hierarchically at the same level as the EU treaties,[87] it is not disputable that fundamental rights of EU citizens would rank higher than market integration instruments.[88] The use of the "less restrictive alternative" criteria will give the Court the possibility to properly use the proportionality principle for the protection of the fundamental rights of the individuals and to effectively limit the interference of these rights to what is strictly necessary.

The "limited to what is strictly necessary" test does not open the doors for an assessment of the means used for surveillance since its aim is different. In the way this test has been used so far by the Court,[89] it does not assess the form of surveillance and the way it is done but aims to limit the impact of the interference with the life of the individual by evaluating the existing safeguarding measures. In comparison, the "less restrictive alternative" criteria, as the name suggests, aims to show that the desired result cannot be achieved with other means that would interfere less with the rights of the individual. In our case the application of this test might have as a result the limitation in the use for surveillance of non-purpose built means that collect data. Since surveillance is related with a limitation of fundamental rights of the citizens, we would suggest that the Court uses the "less restrictive alternative" test when assessing the proportionality of European measures in this regard. The need for identifying the less intrusive alternative mean is suggested also by the European Court of Human Rights in the *Uzun* case where the use of a GPS device for controlling the car movements of the claimant was considered as a proportionate measure given that the less restrictive alternatives were provided not to be successful.[90] One has to keep in mind that Mr. Uzun faced targeted surveillance and the use of the less restrictive alternative is even more important when interfering with the rights of innocent citizens in cases of mass surveillance. The use of these criteria as part of the proportionality test will also give the possibility to assess the use of non-purpose built devices for surveillance and better safeguard the rights of the citizens.

5. Concluding remarks

While the Data Retention Directive is invalidated by the Court of Justice of the EU, data retention laws are still in force and operational in the Member States of the EU. New data retention provisions or other mass surveillance programmes might also be adopted in the future by the European or the national

[81] Clare Ovey, Robin White, 'European Convention on Human Rights', (OUP 3rd ed. 2002), 257.

[82] Ian Brown, Douwe Korff, 'Terrorism and the proportionality of internet surveillance' (2009), *European Journal of Criminology* 6:2, 119–134.

[83] Daniel Solove, 'Nothing to Hide: The False Tradeoff Between Privacy and Security' (Yale University Press, 2011), 1.

[84] Spencer Ackerman, James Ball, 'Optic Nerve: millions of Yahoo webcam images intercepted by GCHQ' (2014), *The Guardian*, <http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo> accessed 11 December 2014.

[85] Lukas Feiler, 'The legality of the Data Retention Directive in light of the fundamental rights to privacy and data protection' (2010), *European Journal of Law and Technology* 1:3, 25; Christopher Docksey, 'The European Court of Justice and the decade of surveillance', in Hielke Hijmans, Herke Kranenborg, (eds) *Data protection anno 2014: How to restore trust?* (Intersentia, 2014), 97–111.

[86] The "less intrusive alternative" is proposed also in UN General Assembly Report of the Special Rapporteur Ben Emmerson on the Promotion and protection of human rights and fundamental freedoms while countering terrorism, A/69/397, 23 September 2014, paras. 51–52.

[87] Article 6 Treaty of the EU.

[88] See Case C-301/06 Ireland v. Parliament and Council [2009] ECR I-00593 and Art. 6 Treaty of the EU.

[89] Case C-473/12 Institut professionnel des agents immobiliers (IPI) v. Geoffrey Engelbert, Immo 9 SPRL, Gregory Francotte [2013] nyr, para. 39.

[90] Uzun v. Germany, ECHR application no. 35623/05, 2 September 2010, para. 78.

legislators.[91] A discussion on the use of the proportionality test in these cases for the best protection of the rights of the individuals is therefore not superfluous. Development of technology creates more and more possibility for data retention and surveillance of citizens with devices not designed for the purpose of surveillance. These present a higher level of intrusion into the private life of the citizens and less legal safeguards than in the case of surveillance technologies. Since the proportionality test is the tool for ensuring the protection of the rights of the citizens it is therefore important to extend it to cover also the technologies that are used for surveillance – being these built for that purpose or not. It is needless to say that if the proportionality test is properly used by the courts, this would also give the right message to the legislator when discussing the proportionality of the measures they want to introduce at an early stage.

This paper gave an overview of the proportionality test as applied by the Court in general and in the case of the invalidation of the Data Retention Directive. It was found that the test currently lacks the possibility to assess the nature of the technologies used for surveillance. The line of reasoning of the Court focusing on the "limited to what is strictly necessary" test does not aim to assess the nature of the technology used for surveillance but tries to reduce the effects of the interference with citizens' fundamental rights by evaluating the existence of legal safeguards.

We propose that the "less restrictive alternative" test that the Court uses when analyzing the proportionality of national rules against EU rules must apply also when testing EU rules against citizens' fundamental rights. In this way, the proportionality test will be extended to cover also an assessment of the technologies used for surveillance. These would give the possibility, especially in cases of mass surveillance when interference with the rights of millions of innocent people takes place, to better use the proportionality principle for protecting the rights of the citizens. A lawful interference with the private lives and personal data of European citizens must take into account the different levels of intrusion that traditional and non-purpose built surveillance technology presents. The proper use of the proportionality principle in the presence of ever-growing devices that have a potential to be used for surveillance will serve for better protecting the rights of the individuals. The proper use of the proportionality principle by the Court should also give the right message to the legislators at European and national level to assess the intrusiveness of the means they propose to be used for surveillance in legislative initiatives so as to protect the rights of the European citizens.

[91] National legislation in this field has to comply with Art. 15 of Directive 2002/58/EC which provides among other that such legislation must constitute a necessary, appropriate and proportionate measure within a democratic society in compliance with the Charter of Fundamental Rights and general principles of Union law.

6. Sources

(1) Abu Bakar Munir, Siti Hajar Mohd Yasin, 'Retention of communications data: a bumpy road ahead' (2004), *Journal of Computer & Information Law* 22, 731–758.

(2) Aharon Barak, 'Proportionality – Constitutional Rights and their limitations' (Cambridge University Press, 2012).

(3) Andrew B. Serwin, 'Privacy 3.0 – The principle of proportionality' (2009), *University of Michigan Journal of Law Reform* 42:4, 869–890.

(4) Antonella Galetta, Paul De Hert 'Complementing the surveillance law principles of the Court of Strasbourg with its environmental law principles. An integrated technology approach to a human rights framework for surveillance' (2014), *Utrecht Law Review* 10:1, 55–75.

(5) Antonio Troncoso Reigada, 'The principle of proportionality and the fundamental right to personal data protection: The biometric data processing' (2012), *Lex Electronica*, 17:2, 1–44.

(6) Article 29 Data Protection Working Party Statement of 1 August 2014 "On the ruling of the Court of Justice of the European Union which invalidates the Data Retention Directive, 14/EN/WP220.

(7) Article 29 Data Protection Working Party, Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes, 10 April 2014, 819/14/EN/WP215.

(8) Article 29 Data Protection Working Party, Opinion 8/2014 on the recent developments on the internet of things, 16 September 2014, 14/EN/WP223.

(9) Bert-Jaap Koops, 'On legal boundaries, technologies, and collapsing dimensions of privacy' (2014), *Politica e Società* 2, 247–264.

(10) Christopher Docksey, 'The European Court of Justice and the decade of surveillance', in Hielke Hijmans, Herke Kranenborg, (eds) *Data protection anno 2014: How to restore trust?* (Intersentia, 2014), 97–111.

(11) Clare Ovey, Robin White, 'European Convention on Human Rights', (OUP 3rd ed. 2002), 257.

(12) Colin Bennett, 'The public surveillance of personal data: A cross-national analyses', in David Lyon, Elia Zureik (eds.), Computers, surveillance, and privacy (University of Minnesota Press, 1996), 237–259.

(13) COM(2005)172 on compliance with the Charter of Fundamental Rights.

(14) COM(2011) 255 final, Brussels, 18.4.2011, Evaluation Report on the Data Retention Directive.

(15) 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, 60–71.

(16) Daniel Solove, 'Nothing to Hide: The False Tradeoff Between Privacy and Security' (Yale University Press, 2011).

(17) Danish Ministry of Justice legal analyses on the Danish data retention law after the CJEU ruling on the Data Retention Directive <http://justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2014/Notat%20om%20logningsdirektivet.pdf> accessed 10 September 2014.

(18) David A. Borton, Ming Yin, Juan Aceros, Arto Nurmikko, 'An implantable wireless neural interface for recording cortical circuit dynamics in moving primates (2013), *Journal of Neural Engineering* 10:2, 16.
(19) David Lyon, 'Surveillance studies: An overview' (Polity Press, 2007), 111–112; Zygmunt Bauman, David Lyon, 'Liquid surveillance: A conversation', (Polity Press, 2013), pp. 2–3.
(20) David Wright, Charles Raab, 'Privacy principles, risks and harms' (2014), *International Review of Law, Computers and Technology* 28:3, 277-298.
(21) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201, 31.07.2002, 37–47.
(22) Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, 13.4.2006, 54–63.
(23) 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, 23.11.1995, 31–50
(24) Dutch government reaction on national data retention laws after the CJEU ruling on the Data Retention Directive <http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2014/11/19/tk-reactie-van-het-kabinet-naar-aanleiding-van-de-ongeldigverklaring-van-de-richtlijn-dataretentie.html> accessed 11 December 2014.
(25) EDPS Opinion on the evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC), 31.05.2011 Robert Alexy, 'A theory of constitutional rights' (OUP 2002).
(26) Eleni Kosta, 'The way to Luxemburg: National Court decisions on the compatibility of the data retention directive with the rights to privacy and data protection' (2013), *SCRIPTed* 10:3, 339–363.
(27) Elspeth Guild, Sergio Carrera, 'The political the judicial life of the metadata: Digital Rights Ireland and the trail of the Data Retention Directive'(2014), *CEPS Liberty and Security in Europe* 65.
(28) Francesca Bignami, 'Privacy and law enforcement in the European Union: The Data Retention Directive' (2007), *Chicago Journal of International Law* 8:1, 233–255.
(29) Francis G. Jacobs, 'Recent development in the proportionality principle in European Community law', in Evelyn Ellis (eds), *The principle of proportionality in the laws of Europe* (Heart Publishing 1999), 1–21.
(30) Franziska Boehm, Mark D. Cole, 'Data retention after the judgement of the Court of Justice of the European Union' (2014), <https://www.google.nl/?gfe_rd=cr&ei=KRFFVO6OB8nBUOipgvgL&gws_rd=ssl#q=data%20retention%20after%20the%20judgement%20of%20the%20court%20of%20justice%20of%20the%20european%20union> accessed 28 November 2014.
(31) Gary T. Marx, 'What's new about the "New Surveillance"? Classifying for change and continuity' (2002), *Surveillance and Society* 1:1, 9–29.
(32) Georgios Kalogridis, Stojan Z. Denic, 'Data mining and privacy of personal behavior types in smart grid' (2011), *IEEE*, 636–642.
(33) Grainne de Burca, 'The principle of proportionality and its application in EC law' (1993), *Yearbook of European Law* 13:1, 105–150.
(34) Hal Roberts, John Palfrey, 'The EU Data Retention Directive in an era of internet surveillance', in Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan Zittrain (eds), Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace (MIT, 2010), 35–53.
(35) Ian Brown, Douwe Korff, 'Terrorism and the proportionality of internet surveillance' (2009), *European Journal of Criminology* 6:2, 119–134.
(36) Jan H. Jans, 'Proportionality revisited' (2000), *Legal issues of economic integration* 27:3, 239–265.
(37) Jan H. Jans, Roel de Lange, Sacha Prechal, Rob Widdershoven, 'Europeanisation of Public Law' (Europa Law Publishing, 2007).
(38) Jannifer Chandler, 'Privacy Versus National Security: Clarifying the Trade-off', in Ian Kerr, Carole Lucock, Valerie Steeves (eds.), Lessons From the Identity Trail: Privacy, Anonymity and Identity in a Networked Society (OUP, 2009), 121–138.
(39) Jeanne P. Mifsud Bonnici, 'Exploring the non-absolute nature of the right to data protection' (2013), *International Review of Law, Computer and Technology* 28:2, 131–143.
(40) Jeanne P. Mifsud Bonnici, 'Recent European Union developments on data protection . . . in the name of Islam or 'Combating terrorism'' (2007), *Information & Communications Technology Law* 16:2, 161–175.
(41) Jerry Kang, Katie Shilton, Deborah Estrin, Jeff Burke, Mark Hansen, 'Self-surveillance privacy' (2012), *Iowa Law Review* 97, 809–847.
(42) Joel R. Reidenberg, 'The data surveillance state in the United States and Europe' (2013), Wake Forest Law Review 48, p. 29.
(43) Jonida Milaj, Jeanne P. Mifsud Bonnici, 'Unwitting subjects of surveillance and the presumption of innocence' (2014), *Computer Law & Security Review* 30:4, 419–428.
(44) Julian Rivers, 'A theory of Constitutional rights and the British Constitution', A translator's introduction in Robert Alexy, *A theory of constitutional rights* (OUP, 2002),
(45) Katja de Vries, Rocco Bellanova, Paul De Hert, and Serge Gutwirth, 'The German Constitutional Court Judgement on data retention: proportionality overrides unlimited surveillance (doesn't it ?)', in Serge Gutwirth, Yves Poullet, Paul De Hert, Ronald Leenes (eds), Privacy and data protection : an element of choice (Springer, 2011) 3–24.
(46) Kirsten Fiedler, 'European Court overturns EU mass surveillance law' (2014), <http://edri.org/european-court-overturns-eu-mass-surveillance-law/> accessed 22 May 2014; Danny O'Brien, 'Data Retention Directive Invalid, says EU's Highest Court'(2014), <https://www.eff.org/deeplinks/2014/04/data-retention-violates-human-rights-says-eus-highest-court> accessed 22 May 2014.

(47) Luc Verhey, Mathijs Raijmakers, 'Article 8 of the European Convention on Human Rights – Proportionality and the protection of personal data', in Marjolein van Roosmalen, Ben P. Vermeulen, Fried van Hoof, Marten Oosting (eds), *Fundamental rights and principles* (Intersentia 2013), 459–479.
(48) Lukas Feiler, 'The legality of the Data Retention Directive in light of the fundamental rights to privacy and data protection' (2010), *European Journal of Law and Technology* 1:3, 25.
(49) Marcus Wigan, Roger Clarke, 'Social impacts of transport surveillance' (2006), *Prometheus: Critical studies in Innovation* 24:4, 389–403.
(50) Marie-Helen Maras, 'From targeted to mass surveillance: Is the EU data retention directive a necessary measure or an unjustified threat to privacy', in Benjamin J. Goold, Daniel Neyland, D. (eds.), New directions in surveillance and privacy (Routledge, 2009), 74–105.
(51) Marie-Helen Maras, 'While the European Union was sleeping, the data retention directive was passed: The political consequences of mandatory data retention' (2011), *Hamburg Review of Social Sciences* 6:2, 1–30.
(52) Nancy J. King, Pernille W. Jessen 'Smart metering systems and data sharing: why getting a smart meter should also mean getting strong information privacy controls to manage data sharing' (2014), *International Journal of Law and Information Technology*, 1–39.
(53) Noam Cohen, 'It's tracking your every move and you may not even know' (2011), *The New York Times*, <http://www.nytimes.com/2011/03/26/business/media/26privacy.html?_r=0> accessed 22.5.2014.
(54) Nora Ni Loideain, 'Surveillance of Communications data and Article 8 of the European Convention of Human Rights', in Serge Gutwirth, Ronald Leens, Paul de Hert (eds), *Reloading data protection* (Springer, 2014), 183–209.
(55) Paul De Hert, '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' (2005), *Utrecht Law Review* 1:1, 68–96.
(56) Projection of data retention traces done for a Swiss MP <https://www.digitale-gesellschaft.ch/dr.html> accessed 1 June 2014.
(57) Rec(95)4 of the Council of Europe on the protection of personal data in the area of telecommunication services, with particular reference to telephone services.
(58) Roger Clarke, 'Dataveillance: Delivering '1984'', in Leila Green, Roger Guinery (eds.), Framing Technology: Society, Choice and Change (Allen & Unwin, 1994), 496–522.
(59) Roger Clarke, 'What's 'Privacy'?' (2006) <http://www.rogerclarke.com/DV/Privacy.html> accessed 10 July 2013.
(60) Spencer Ackerman, James Ball, 'Optic Nerve: millions of Yahoo webcam images intercepted by GCHQ' (2014), *The Guardian*, <http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo> accessed 11 December 2014.
(61) Steven Greer, 'The exceptions to Articles 8 to 11 of the European Convention of Human Rights' (1997), *Human Rights Files*, no. 15 (Council of Europe Publishing).
(62) Susan Young Rojahn, 'A wireless brain-computer interface' (2013), <http://www.technologyreview.com/news/512161/a-wireless-brain-computer-interface/> accessed 24 April 2013.
(63) Takis Tridimas, 'Proportionality in European Community law: Searching for the appropriate standard of scrutiny', in Evelyn Ellis (eds), *The principle of proportionality in the laws of Europe* (Heart Publishing 1999), 65–84.
(64) Thomas A. Vandamme 'The invalid Directive – The legal authority of a Union act requiring domestic law making' (Europa Law Publishing, 2005), 159.
(65) Tor-Inge Harbo, 'The function of the proportionality principle in EU law' (2010), *European Law Journal*, 16:2, 158–185.
(66) UK new draft law on Data Retention and Investigatory Powers Bill 2014 <https://www.gov.uk/government/publications/the-data-retention-and-investigatory-powers-bill> accessed 10 September 2014.
(67) UN General Assembly Report of the Special Rapporteur Ben Emmerson on the Promotion and protection of human rights and fundamental freedoms while countering terrorism, A/69/397, 23 September 2014.
(68) UN General Assembly Report of the Special Rapporteur Ben Emmerson on the Promotion and protection of human rights and fundamental freedoms while countering terrorism, A/69/397, 23 September 2014, paras. 51–52.
(69) Valerie Jenness, David A. Smith, Judith Stepan-Norris, 'Taking a look at surveillance studies' (2007), *Contemporary sociology: A Journal of Reviews* 36:2, vii–viii.
(70) Valsamis Mitsilegas, 'The transformation of privacy in the area of pre-emptive surveillance' (2015), *Tilburg Law Review* 20, 35–57.
(71) Working document 1, on the US and EU Surveillance programmes and their impact on EU citizens fundamental rights, Committee on Civil Liberties, Justice and Home Affairs, Rapporteur: Claude Moraes, <http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/wd_moraes_1012434/wd_moraes_1012434en.pdf> accessed 20 December 2013.
(72) Xavier Tracol, 'Legislative genesis and judicial death of a directive: The European Court of Justice invalidated the data retention directive (2006/24/EC) thereby creating a sustained period of legal uncertainty about the validity of national laws which enacted it' (2014), *Computer Law & Security Review* 30, 736–746.

7. Case law

(1) C-112/00 Eugene Schmidberger, Internationale Transporte und Planzuge v. Austria [2003] ECR I-5659.
(2) C-210/03 Swedish Match AB and Swedish Match UK Ltd [2004] ECR I-11893.
(3) C-212/13 František Ryneš v Úřad pro ochranu osobních údajů [2014] nyr.
(4) C-265/87 Schraeder HS Kraftfutter GmbH & Co KG v. Hauptzollamt Gronau [1989] ECR 2237.
(5) C-301/06 Ireland v. Parliament and Council [2009] ECR I-00593.

(6) C-331/88 The Queen v. Minister of Agriculture, Fisheries and Food and Secretary of State for Health, ex parte: Fedesa et al. [1990] ECR I-4023.
(7) C-473/12 Institut professionnel des agents immobiliers (IPI) v. Geoffrey Engelbert, Immo 9 SPRL, Gregory Francotte [2013] nyr.
(8) C-491/01 The Queen v. Secretary of State for Health, ex parte British American Tobacco (Investments) Ltd and Imperial Tobacco Ltd [2002] ECR I-11453.
(9) C-617/10 Aklagaren v. Hans Akerberg Fransson [2013] ECR nyr.
(10) C-73/07 Satakunnan Markkinapörssi and Satamedia [2008] ECR I–9831.
(11) C-84/94 United Kingdom v. Council [1996] ECR I-5755.
(12) Case 11/70 Internationale Handelsgesellschaft v. Einfuhr- und Vorratsstelle Getreide [1970] ECR1125.
(13) Case 120/78 Rewe-Zentral AG v. Bundesmonopolverwaltung für Branntwein [1979] ECR 649.
(14) Case 302/86 Commission v. Danmark [1988] ECR 4607.
(15) Joined cases C-453/03, C-11/04, C-12/04 and C-194/04 ABNA Ltd et al. v. Secretary of Health et al. ECR I-10423.
(16) Joined cases C-92/09 and C-93/09 Volker und Markus Schecke and Eifert [2010] ECR I–11063.
(17) Joint cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and others [2014] nyr.
(18) Joint cases C-465/00, C-138/01 and C-139/01 Österreichischer Rundfunk and Others [2003] ECR I-04989.
(19) Opinion of AG Cruz Villalon in joint cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and others [2014] nyr.
(20) Opinion of AG Maduro in Case C-524/06 Heinz Huber v. Bundesrepublik Deutschland [2008] ECR I-09705.
(21) Opinion of AG van Gerven delivered on 11 June 1991, in C-159/90 The Protection of Unborn Children Ireland Ltd v. Stephen Grogan and others [1991] ECR I-04685.
(22) Uzun v. Germany, ECHR application no. 35623/05, 2 September 2010.