# Proportionality in EU data protection law

**Preprint** · October 2021

CITATIONS
0

READS
3

**1 author:**

James Camilleri
University of Malta
**12** PUBLICATIONS **0** CITATIONS

SEE PROFILE

There has been significant controversy over the use of surveillance technologies during times of crisis (e.g. terror attacks and other forms of serious crime, COVID-19, etc.) In light of this, critically analyse the principle of proportionality in EU data protection law, and whether and how the principle has a role in contributing to effective data protection.

L-Università ta' Malta
Faculty of Laws

## DECLARATION OF AUTHORSHIP FOR ASSIGNMENTS

I/~~We~~, JAMES CAMILLERI [1], declare that this assignment[2] ECL5043 EU Information Technology Law [3] and the work presented is/are my own personal work.

I confirm that:

- The Word Count of the assignment is 7,973 [4].
- This work was done in partial fulfilment for the master/~~degree~~/~~diploma~~/~~certificate~~ in Master of Laws in European Business Law [5] at the Faculty/~~Institute~~/~~Centre~~ of Laws [6] of the University of Malta.
- Where any part of this assignment has previously been submitted for a degree or any other qualifications at this University or any other institution, this has been clearly stated.
- Where I have consulted the published work of others, this is always clearly attributed.
- Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this assignment is entirely my own work.
- I have acknowledged all sources used for the purpose of this work.
- I have not commissioned this work, whether in whole or in part, to a third party and that this work is my own work.
- I have read the University of Malta's guidelines on plagiarism

Signed: [signature] Date: 27/06/2020

[1] Indicate Name and Surname
[2] Enter study-unit code and title ONLY
[3] Add title and Study unit code of assignment
[4] Indicate word count
[5] Indicate name of degree/masters/diploma course
[6] Indicate the Home Faculty, Institute or Centre applicable

# Table of Contents

# 1. Introduction

The government of any jurisdiction will, sooner or later, be criticised for being ought to have done more in any national or international crisis that occurs. In the aftermath of a crisis, conspiracy theories abound claiming the government could not have possibly been unaware of what was the situation and that any failure to act timely was either intentional or blatant carelessness. The government cannot act irrationally but always needs to make an informed decision. Therefore, conspiracy theories apart, a government's failure to act or to do so in a timely manner may be attributable to the lack of necessary information to be in a proper position to make an informed decision. Governments across the ages and of all shapes and forms have always been information-savvy. What characterises the present scenario under review is that we are witnessing the development of information-savvy governments within an information age context. Governments do not have a monopoly about data collection, and it is a practice done by other large organisations such as religious institutions, large-scale commercial entities, and international bodies. All these different institutions may have varying reasons for wanting to collect data, but the principle is still the same and in times of crisis any one or more of these forms of data collection may be utilized. Therefore, reference in this paper will be made to the use of surveillance technologies by 'data collectors' irrespectively of whether such data collector is a governmental institution or some other form of organisation.

# 2. Big Brother

The use of surveillance technologies during times of crisis is a special niche of the general use of surveillance technologies. Images of George Orwell's *1984* novel and the Big Brother State,[1] have become populist representations of the use of surveillance technologies by data collectors. In George Orwell's modern classic novel, the State, referred to as Big Brother, was constantly monitoring their citizens' every movement not affording them any freedom of thought, let alone action, altogether. The Big Brother State is synthesised in the novel's three axioms:

> War is peace
> Freedom is slavery
> Ignorance is strength

The particularity about the use of surveillance technologies during times of crisis is that it is not as straightforward to dismiss this as an invasion of privacy by data collectors. Even the more hardcore proponents of zero-tolerance surveillance technologies will shy away from arguing that crises such as terror attacks and the present COVID-19 pandemic do not call for any form of surveillance technologies, albeit in an arbitrary manner.

## 2.1. The 1983 Census Act

Hence, there is a consensus that a total ban on the data collectors' practice of using surveillance technologies besides being practically unfeasible, would also not be in the public interest. At this point, it can be claimed that data collectors have a place in society and the argument is not whether they should be permitted to use surveillance technologies but rather to what extent they should be allowed to do so. The process of mass-scale data collection has had a significant presence throughout history – even well before the use of sophisticated devices such as surveillance technologies. The *casus classicus* in this context would be the judgment of the German Federal Constitutional Court

[1] (Secker & Warburg 1949).

delivered on the 15th December 1983.[2] The question before the Constitutional Court was the collection of data as laid out by the 1983 Census Act. Individual citizens of the German Federation availed themselves of their constitutional rights to challenge the 1983 Census Act before the Constitutional Court on the grounds of an invasion of privacy. The court concluded that although the collection of data for census purposes does not constitute an unjustifiable invasion of an individual's privacy, nonetheless certain measures need to be in place to prevent a free-for-all access to personal data by government officials.

## 2.2. The EU Charter of Fundamental Rights

A review of surveillance technologies and the principle of proportionality in European Union ('EU') law cannot omit the salient articles in the Charter of Fundamental Rights of the European Union ('CFR').[3] Article 7 CFR 'Respect for private and family life' declares:

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

Article 8 CFR 'Protection of personnel data' declares:

> 1. Everyone has the right to the protection of personal data concerning him or her.
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the persons concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
>
> […]

On the principle of proportionality, Article 52 CFR 'Scope of guaranteed rights' sub-article 1 declares:

> Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those right and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

## 2.3. The Right to Privacy

The concept of what we refer to as privacy can be traced way before the information revolution and the invention of information and communication technology ('ICT') devices such as surveillance technologies. There may be different interpretations of what constitutes the privacy sphere yet every society throughout the ages has had some vestige of this notion. Before the advent of ICT devices someone trying to overhear or see what others said or did within the confines of their private sphere could only do so by being physically present at the scene and in some manner conceal his/her presence. With the industrial revolution came the first telecommunications devices. A pioneering piece of writing on the topic of privacy was written in 1890 by Samuel D. Warren and Louis D. Brandeis in the Harvard Law Review and titled 'The Right to Privacy'.[4] What sort of breaches to one's privacy would Warren and Brandeis have been referring to? In their case it was the introduction of the photographic camera; besides the invention of the telephone as attributed to Alexander Graham

[2] 1 BvR 209, 269, 362, 420, 440, 484/83.
[3] (2012/C 326/02) OJ C326/391.
[4] Vol. IV No. 5.

Bell dated 1876.[5] The safeguarding of privacy requires the use of boundaries but, as the study under review points out, there has to be a sense of proportionality. This principle cuts both ways – too many boundaries would cripple today's information society, and on the other hand, over-surveillance will lead to the infamous Big Brother State. Thus, it is appropriate to have boundaries safeguarding information that is of a sensitive nature but these boundaries should not be such as to forestall the use of social media which, with all its shortcomings, has an important role to play in today's society. The principle of proportionality also offers the flexibility for privacy boundaries to be more easily shifted as core elements of society mutate over time. One of Warren and Brandeis' arguments was to what extent can privacy law be relevant in the face of constantly evolving technologies. There again, from what is being witnessed more so today, one of the determining drivers of privacy boundaries is not merely the dissuasive power of regulatory sanctions but, especially for organisations with a large public following, the reputational shaming that ensues from falling foul to a privacy incident. The academic view of privacy should not be confused with the practical aspect where, as can be seen from the expansion of social media, people in general are freely willing to share their personal information over a public medium. In this respect it is difficult to pin down, but perhaps a safe way of putting it is that people generally enjoy sharing personal information with the public but notwithstanding want to remain in control of which personal information may or may not be shared in public. This may sound as a contradiction and yet that is what is being witnessed as the norm since the advent of social media. The social media phenomenon lends itself well to the study under review, that is the principle of proportionality. In general, people do not seem to treasure the right to be let alone since they would not use social media if they did, however they do not wish to be constantly exposed to public scrutiny.

## 3. The Data Retention Directive

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 communication networks'[6] (the Data Retention Directive, 'DRD') – is a relevant piece of EU legislation for the study under review. As will be discussed further, this directive is no longer in force since the 8th April 2014. The scope of this directive as detailed in Article 1 was:

1. This Directive aims to harmonise Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime […]
2. This Directive shall apply to traffic and location data on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered user. It shall not apply to the content of electronic

[5] 'History of the telephone' (*Wikipedia*) <https://en.wikipedia.org/wiki/History_of_the_telephone#:~:text=Alexander%20Graham%20Bell%20was%20awarded,microphone%20in%20Highland%20Park%2C%20Illinois.&text=Thomas%20Edison%20invented%20the%20carbon%20microphone%20which%20produced%20a%20strong%20telephone%20signal.> accessed 24th June 2020.

[6] And amending Directive 2002/58/EC [2006] OJ L105/54.

> communications, including information consulted using an electronic communications network.

If read carefully, this provision recalls the dreaded Big Brother State. However, it should also be mentioned that public security is a vital element of society and, populist negative sentiments aside, the security system of a state needs to be able to function properly. Once again, the principle of proportionality comes into the scene as a security system inevitably needs to be afforded a certain margin of privilege though when this privilege is used for the wrong reasons it cannot be left unchecked. The DRD raised eyebrows because it applied to citizens across the board whether a citizen was a potential criminal or not at all. The EU legislator possibly justified this because it was the 'traffic and location data' and not 'the content of electronic communications',[7] also known as the 'metadata' or 'data about data'.

### 3.1. *Digital Rights Ireland*

*Digital Rights Ireland and Others* ('*Digital Rights Ireland*') was delivered by the Grand Chamber of the Court of Justice of the European Union ('CJEU') on the 8th April 2014.[8] This judgment cannot pass unmentioned in the study under review because it focuses on two of the prime elements of this study, viz surveillance technologies and the principle of proportionality. Digital Rights Ireland Ltd is an entity concerned with the promotion and protection of civil and human rights.[9] Standing before the High Court of Ireland, Digital Rights Ireland challenged, *inter alia*, the validity of the DRD.[10] During the said proceedings, the High Court considered it in the best interest of the parties to make a preliminary reference to the CJEU.[11] The *Digital Rights Ireland* judgment features two joined cases, the other case involving the Constitutional Court of Austria ('Verfassungsgerichtshof') before which proceedings were brought by the Government of the Province of Carinthia ('Kärntner Landesregierung'), by Mr Michael Seitlinger, Mr Christof Tschohl and 11,128 other applicants.[12] The complaint of the applicants was the transposing into Austrian law of the DRD.[13] During the said proceedings, the Verfassungsgerichtshof considered it in the best interest of the parties to make a preliminary reference to the CJEU.[14] During the proceedings before the Grand Chamber, the Court agreed that in view of, *inter alia*, Articles 7 and 8 of the CFR, the DRD does raise various concerns.[15] In the light of Article 52(1) CFR, the court noted that it is the metadata which is subject to being retained and how the ultimate aim of this exercise is to safeguard public security.[16] However, the targeted public security concerns do not warrant the extent of data retention measures as envisioned by the DRD.[17] According to the court, the DRD did not offer enough safeguards for the retained data to be used solely for the intended purposes.[18] In this respect, the DRD appears too

[7] Art 1(2) DRD.
[8] Joined Cases C-293/12 and C-594/12 ECLI:EU:C:2014:238.
[9] ibid Opinion of AG Villalón ECLI:EU:C:2013:845, para 10.
[10] *Digital Rights Ireland* (n 8) para 17.
[11] ibid para 18.
[12] ibid para 3.
[13] ibid.
[14] ibid para 21.
[15] ibid paras 25, 28.
[16] ibid paras 39, 41.
[17] ibid para 51.
[18] ibid para 54.

generalised.[19] Neither does the DRD respect the principle of minimisation vis-à-vis the length of data storage.[20] Thus, the conclusion of the Grand Chamber was the invalidity of the DRD.[21]

## 3.2 *Tele2 Sverige*

*Tele2 Sverige* was delivered by the Grand Chamber of the CJEU on the 21st December 2016.[22] It is a judgment relevant to the study under review as a successor to the *Digital Rights Ireland* lawsuit. In fact, following the *Digital Rights Ireland* decision, Tele2 Sverige, a telecom operator established in Sweden, made its intention known to the Swedish Post and Telecom Authority (Post-och telestyrelsen, 'PTS') of discontinuing the retention of data as was required by the invalidated DRD.[23] The National Police Authority of Sweden ('Rikspolissturelsen') complained to the PTS of Tele2 Sverige's action.[24] The Minister for Justice of Sweden ('Justitieminister') concluded the Swedish data retention laws were not incompatible with EU law, including the *Digital Rights Ireland* preliminary ruling.[25] Tele2 Sverige contested this conclusion before the Swedish Administrative Court, Stockholm ('Förvaltningsrätten i Stockholm'), which quoted Article 15(1) of Directive 2002/58.[26] This article provides:

> Member States may adopt legislation measures to restrict the scope of the rights and obligations provided for in […] this Directive when such restrictions constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security […], defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system […]. To this end, Member States may, *inter alia*, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph […]

In appeal before the Swedish Administrative Court of Appeal of Stockholm ('Kammarrätten i Stockholm') confirmation was sought from the CJEU and a request for preliminary ruling was raised.[27] The *Tele2 Sverige* judgment features two joined cases, the other case involving the legality of the Data Retention and Investigatory Powers Act 2014 ('DRIPA') of the United Kingdom ('UK') in light of the *Digital Rights Ireland* preliminary ruling.[28] The High Court of Justice (England & Wales), Queen's Bench Division (Divisional Court) (UK) asked to decide on the matter said section 1 of the DRIPA was at this point not legal any longer.[29] This was appealed by the Secretary of State for the Home Department before the Court of Appeal (England & Wales) (Civil Division) (UK), which then made the request for a preliminary ruling.[30] In the light of Article 15(1) of Directive 2002/58, the Grand

[19] ibid para 57.
[20] ibid para 64.
[21] ibid p 21.
[22] Joined Cases C-203/15 and C-698/15 ECLI:EU:C:2016:970.
[23] ibid.
[24] ibid.
[25] ibid.
[26] 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 (Directive on privacy and electronic communications) [2002] OJ L201/37.
[27] ibid.
[28] ibid.
[29] ibid.
[30] ibid.

Chamber said following the *Digital Rights Ireland* decision the relevant Swedish and UK national legislation does not conform to what is strictly necessary.[31]

## 4. Data Protection vis-à-vis Proportionality

The two preliminary references analysed *supra* present several relevant points to the study under review on surveillance technologies and the principle of proportionality. One of these is the rule of necessity, that is, only data required for the stated purpose may be collected and stored; once the purpose for which the data was gathered has terminated so is the need to store such data. The necessity rule was also incorporated in the General Data Protection Regulation ('GDPR'):[32]

> 1. Personal data shall be:
>
> […]
>
> b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes […] ('purpose limitation');
> c) adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed ('data minimisation');
>
> […]
>
> e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed […] ('storage limitation')[.][33]

### 4.1. *Klass*

From a historical perspective it is enlightening to analyse a judgment of the European Court of Human Rights ('ECtHR'), *Case of Klass and Others v Germany* ('*Klass*') delivered by the Plenary Court on the 6th September 1978.[34] Gerhard Klass *et al* were German nationals opposed to the Federal Republic of Germany's Act of 13th August 1968 on Restrictions on the Secrecy of the Mail, Post and Telecommunications (Gesetz zur Beschränkung des Brief-, Post-, under Fernmellegeheimnisses, 'BBPF').[35] Previously, during proceedings before the German Federal Constitutional Court ('Bundesverfassungsgericht'), it agreed with the applicants that the BBPF was in part invalid where it did not require monitored persons to be made aware of having been subject to state surveillance following the conclusion of the case investigated.[36] Three years after the Bundesverfassungsgericht decision, the BBPF provisions in dispute had not been abrogated.[37] The BBPF allowed a competent authority to overstep the privacy of mail, post and telecommunications in the interest of public security.[38] Only a designated person could make such a surveillance request stating in writing why it was necessary and that no other option was available.[39] Once the specified necessity for the

[31] ibid.
[32] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.
[33] ibid Art 5(1).
[34] App no 5029/71.
[35] ibid para 10.
[36] ibid para 11.
[37] ibid.
[38] ibid paras 16-17.
[39] ibid paras 17-18.

surveillance request had ceased, the overstepping of privacy rights in question had to be stopped at once.[40] Following the said Bundesverfassungsgericht decision, the legislator had amended the relevant provisions is such a way as to notify the person monitored once there was no fear this would compromise in any way the course of the investigation.[41] The whole operation had to be supervised by a qualified official and at its termination the collected information had to be erased.[42] Once a monitored person was informed of having had his/her privacy overstepped, the person could, *inter alia*, file an application for review at an administrative court.[43] During the proceedings in *Klass* reference was made to Article 8 of the European Convention on Human Rights (ECHR):

> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The German government did not deny the BBPF violated Article 8(1) of the ECHR.[44] The ECtHR considered whether the BBPF was justified under Article 8(2) ECHR.[45] The court considered the BBPF was 'in accordance with the law and necessary in a democratic society'.[46] Hence, the BBPF did not breach Article 8 of the ECHR.[47] Thus, the ECtHR gave the greenlight to the BBPF and with hindsight the EU legislators might have benefitted from reading more closely this 1978 judgment before drafting the now invalidated Data Retention Directive.

### 4.2. *Satamedia*

On the other hand, it cannot be imagined the CJEU would have been oblivious of the *Klass* judgment. *Satakunnan Markkinapörssi and Satamedia* (*Satamedia*) is a reference for preliminary ruling of the 16th December 2008.[48] Markkinapörssi is a private entity that was publishing on a newspaper, *Veropörssi*, public data obtained from the Finnish tax authorities.[49] The main purpose of the newspaper is to publish such tax information relating to national persons.[50] Persons objecting to their information being made public on *Veropörssi* may make a request for its removal.[51] Satamedia, a company linked to Markkinapörssi, began offering a service whereby such data as is available on *Veropörssi* would be sent via text message.[52] Such service is against payment and a request may be made for the removal of personnel data.[53] Certain individuals complained about the activities of Markkinapörssi and Satamedia to the Finnish Data Protection Ombudsman ('Tietosuojavaltuutettu')

[40] ibid para 18.
[41] ibid para 19.
[42] ibid para 20.
[43] ibid para 24.
[44] ibid para 41.
[45] ibid para 42.
[46] ibid paras 43, 60.
[47] ibid p 28.
[48] Case C-73/07 ECLI:EU:C:2008:727.
[49] ibid para 25.
[50] ibid para 28.
[51] ibid para 27.
[52] ibid para 29.
[53] ibid.

which requested the Finnish Data Protection Board ('Tietosuojalautakunta') to prevent Markkinapörssi and Satamedia from carrying on such activities.[54] The Tietosuojalautakunta not having consented, the Tietosuojavaltuutettu applied to the Finnish Administrative Court, Helsinki ('Helsingin hallinto-oikeus') and eventually to the Supreme Administrative Court ('Korkein hallinto-oikeus'), which decided to make a request for preliminary ruling.[55] The Grand Chamber of the CJEU clarified the said activities of Markkinapörssi and Satamedia fall under the Data Protection Directive ('DPD'),[56] in force at the time.[57] Secondly, the publication of data within the public domain can be justified as the processing of personal data 'solely for journalistic purposes'[58].[59]

### 4.3. *Schrems*

Under EU law the protection of personal data is a fundamental right as presented by Article 8 of the CFR. The layperson may struggle with the definition of a 'fundamental right', however, even legal professionals who understand the concept may still have a hard time grasping what it means to specifically have a fundamental right such as the protection of personal data. Neither does the legislator attempt to grasp what is a specific fundamental right. If one looks at the provisions of the CFR or the ECHR it is noticeable how most are relatively brief. The legislator is stating the existence of a fundamental right but presumably trusts the judiciary are best suited at expounding a specific fundamental right. The judiciary have certainly done a good job at expounding fundamental rights but, it should be remembered, they often do so on a case by case basis. Moreover, the CJEU does not endorse the doctrine of precedent as do the common law jurisdictions. Going through EU case law to come to terms with the principle of proportionality in the use of surveillance technologies may be enlightening but does it offer a clear understanding of the law and do related cases of the CJEU concur with the fundamental *Digital Rights Ireland* decision?

The preliminary ruling of *Maximillian Schrems v Data Protection Commissioner* ('*Schrems*') was delivered on the 6th October 2015.[60] Maximillian Schrems, an Austrian national, complained to the Data Protection Commissioner ('DPC'),[61] that Facebook, a social network, transfers data collected from EU users to computer servers located in the United States of America ('US').[62] Mr Schrems argued the US data protection rules are not sufficiently rigorous.[63] He pointed out the revelations of the American whistle-blower Edward Snowden in regard to various surveillance activities, particularly of the National Security Agency ('NSA').[64] The DPC disagreed with Mr Schrems who then filed an action in the High Court of Ireland – Facebook operates in the EU mainly from its premises in Ireland.[65] The High Court agreed what Snowden revealed was of concern and went against the Irish Constitution's principle of proportionality.[66] Due to the EU law nature of the lawsuit,

[54] ibid para 31.
[55] ibid paras 32, 34.
[56] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.
[57] ibid para 49.
[58] Art 9 DPD.
[59] *Satamedia* (n 48) para 62.
[60] Case C-362/14 ECLI:EU:2015:650.
[61] See Art 28 DPD.
[62] *Schrems*.
[63] ibid.
[64] ibid.
[65] ibid.
[66] ibid.

it was considered necessary to make a reference for preliminary ruling to the CJEU.[67] The Grand Chamber noted Article 25(6) DPD, then in force:

> The [Data Protection] Commission may find […] that a third country ensures an adequate level of protection […], by reason of its domestic law or of the international commitments it has entered into […] for the protection of the private lives and basic freedoms and rights of individuals.

The court went on to examine the duties of the DPC and that it is in line with the scope of the DPC to look at Mr Schrems' complaint.[68] Where the complaint has been rejected, the complainant should have the option to challenge such decision.[69] The point here is that in this preliminary ruling the court seems to add further criteria to the principle of proportionality in comparison to the *Digital Rights Ireland* judgment:[70]

> […] legislation permitting the public authorities to have access *on a generalised basis* to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life[.] (emphasis added)

### 4.4. *Agrana Zucker*

Maintaining a principle of proportionality may be a sensible thing to do but various interpretations of what is proportionately acceptable and what is not may leave suitors feeling frustrated. The idea of a 'test' to try to contain a broad concept is popular in the legal field. The CJEU may not officially declare a judgment is applying a 'test' when formulating a judgment but jurisprudents might afterwards discern a certain logic of the court and create a framework which is then used as a template and labelled a 'test' in that particular context.

The CJEU has had the opportunity to discuss the general principle of proportionality on numerous occasions. In *Agrana Zucker v GmbH v Bundesminister für Land- und Forstwirtschaft, Unwelt und Wasserwirtschaft* ('*Agrana Zucker*'),[71] Agrana Zucker GmbH was allocated by the competent authority a certain quota for the production of sugar but this was restricted by 13.5% due to threshold limits.[72] A production charge was imposed on Agrana Zucker for the entire quota without deducting the 13.5% threshold.[73] The Second Chamber of the CJEU did not consider this contrary to the principle of proportionality for the reasons there expounded.[74] Regarding the principle of proportionality the court reminded that:[75]

- […] acts adopted by institutions of the European Union do not exceed the limits of what is appropriate and necessary in order to attain the legitimate objectives pursued by the legislation in question;
- where there is a choice between several appropriate measures, recourse must be had to the least onerous[;] and

[67] ibid.
[68] ibid.
[69] ibid.
[70] ibid.
[71] Case C-33/08 [2009] ECLI:EU:C:2009:367.
[72] ibid.
[73] ibid.
[74] ibid.
[75] ibid.

- the disadvantages caused must not be disproportionate to the aims pursued […]

## 4.5. *Ruiz Zambrano*

*Ruiz Zambrano*,[76] concerned the refusal by the competent Belgian authority to grant Mr Zambrano, a third-country national, unemployment benefits.[77] Mr Zambrano was living and working in Belgium although he eventually lost his employment but remained living in Belgium. His spouse was also living in Belgium and whilst living there gave birth to two children.[78] Mr Zambrano's request for unemployment benefits to the competent Belgian authority following the loss of his employment was turned down because he was not a Belgian or EU citizen. The Grand Chamber decided that in view of the Zambrano spouses' children having been born in Belgium and acquired Belgian citizenship it was precluded for the competent authority to refuse Mr Zambrano's request for unemployment benefits.[79] What is noteworthy about this decision for the study under review is that Advocate General ('AG') Sharpston,[80] argued the principle of proportionality is to be assessed under both EU and national law.[81]

## 4.6. *ASNEF*

In a nutshell, the principle of proportionality test as developed by the CJEU case law is: i) legitimate objective; ii) appropriateness; iii) necessity; and iv) reasonableness. Breaking down the principle of proportionality into component elements is fine but, there again, what is understood by necessity or reasonableness is still open to debate. In *Asociación National de Establecimientos Financieros de Crédito (ASNEF) / Federación de Comercio Electrónico y Marketing Directo (FECEMD) v Administración del Estado* ('*ASNEF*'),[82] certain provisions of Spanish law about the processing of data without the subject's consent were being contested.[83] The Supreme Court of Spain ('Tribunal Supremo') before which the action was brought, considered Article 7(f) of the DPD then in force:

> Member States shall provide that personal data may be processed only if:
>
> […]
>
> f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party […] to whom the data are disclosed except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject […]

During the reference for a preliminary ruling, the Third Chamber of the CJEU said that adding further criteria to Article 7(f) DPD, as do certain provisions of the contested Spanish law, was to be precluded.

## 4.7. *Volker*

In *Volker and Markus Schecke GbR / Hartmut Eifert v Land Hessen* ('*Volker*'),[84] Volker und Markus Schecke GbR is an agricultural business concern and Hartmut Eifert a farmer. The two applicants

[76] Case C-34/09 [2011] ECLI:EU:C:2011:124.
[77] ibid para 2.
[78] ibid para 19.
[79] ibid p 1253.
[80] ibid Opinion of AG ECLI:EU:C:2010:560.
[81] ibid para 111.
[82] Joined Cases C-468/10 and C-469/10 [2011] ECLI:EU:C:2011:777.
[83] ibid.
[84] Joined Cases C-92/09 and C-93/09 [2010] ECLI:EU:C:2010:662.

were approved to receive funds from the European Agricultural Guarantee Fund ('EAGF') and the European Agricultural Fund for Development ('EAFRD').[85] This was published on the website of Federal Office for Agriculture and Food (Bundesanstalt für Landwirtschaft und Ernährung ('the Bundesanstalt') by the Land of Hesse ('Land Hesse') where the website makes public the beneficiaries of the EAGF and the EAFRD, including the amounts received.[86] The applicants disagreed with the publication of their personal details and brought court proceedings to that effect.[87] The Administrative Court of Wiesbaden ('Verwaltungsgericht') made a request for preliminary ruling.[88] The Grand Chamber said there ought to be a balance between the need for transparency and the protection of data.[89] The court found in the case at hand that the right to data protection was jeopardised for the sake of transparency.[90]

### 4.8. *Szabó*

The *Case of Szabó and Vissy v Hungary* ('*Szabó*') is a judgment of the ECtHR.[91] The applicants, Mr Máte Szabó and Ms Beatrix Vissy, were employees of a non-governmental organisation ('NGO'), Eotvos Károby Kozpolitikai ('EKKI').[92] They brought proceedings in the Hungarian Constitutional Court because of privacy concerns in the surveillance measures of the country's Anti-terrorism Task Force ('TEK').[93] The applicants' action was mainly dismissed by the Constitutional Court.[94] The applicants then brought proceedings before the ECtHR claiming a violation to their privacy under Article 8 of the ECHR because the surveillance measures of the TEK did not include appropriate safeguards with respect to potential abuse.[95] The ECtHR noted that a violation of sub-article 8(1) of the ECHR is only permitted in accordance to sub-article 8(2).[96] It is agreed the purpose of TEK is to act in the public interest of safety and security.[97] What was being questioned in the proceedings is whether the said objectives respect certain parameters of democracy.[98] In paragraph 56 of the judgment the court declares it,

> has developed the following minimum safeguards that should be set out in law in order to avoid abuses of power: the nature of offences which may give rise to an interception order; the definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or destroyed[.]

The court found an interference of sub-article 8(1) ECHR by the institution of TEK and proceeded to examine whether this was justified under sub-article 8(2).[99] It was noted that secret surveillance

[85] ibid.
[86] ibid.
[87] ibid.
[88] ibid.
[89] ibid.
[90] ibid.
[91] App no 37138/14 (12th January 2016).
[92] ibid paras 1, 7.
[93] ibid paras 8, 13.
[94] ibid para 14.
[95] ibid para 37.
[96] ibid para 54.
[97] ibid para 55.
[98] ibid.
[99] ibid para 58.

measures afford certain specific characteristics.[100] However, it would be contrary to the rule of law if secret surveillance authorities were granted unchecked discretion.[101] For example, the court pointed out the fact the TEK could perform secret surveillance on practically any person residing in Hungary and that state surveillance technologies had reached impressive levels of sophistication.[102] In light of this, the court remarked it would be ironic for a state to use secret surveillance technologies to eradicate the threat of terrorism only to then create the concept of a Big Brother State.[103] It said the use of secret surveillance technologies is only permissible where this is strictly necessary.[104] In line with the rule of law secret surveillance authorities should be, at least at the final stage of the approval, subject to judicial control, although it is also understood that in exceptional circumstances, such as an imminent terrorist attack, state surveillance authorities would have to be allowed to act with emergency.[105] Another lacuna is the unsatisfactory option for a citizen to lodge a complaint about any TEK activities, should he or she feel compelled to do so.[106] Having taken these and other factors into consideration the ECtHR came to the conclusion the TEK institution is in violation of Article 8 ECHR because it does not offer adequate secret state surveillance countermeasures.[107] Like in *Digital Rights Ireland*, the *Szabó* judgment is clear that the fight against terrorism and criminality requires some form of secret surveillance. The CJEU's and ECtHR's explanations of how state surveillance authorities are to go about doing their business whilst respecting citizens' right to privacy although extensive is still not sufficiently clear.

### 4.9. *Zakharov*

The *Case of Roman Zakharov v Russia* ('*Zakharov*') was delivered by the Grand Chamber of the ECtHR on the 4th December 2015.[108] The applicant, Mr Roman Andreyevich Zakharov, is a Russian national.[109] The nature of Mr Zakharov's complaint was that the Russian state's secret surveillance practices of public ICT networks was a violation of his right to private life, as enshrined in Article 8 of the ECHR.[110] The applicant first brought proceedings before the Vasileostrovskiy District Court of St Petersburg that rejected his complaint because it claimed he could not prove he had been subject on any occasion to secret state surveillance.[111] On appeal the St Petersburg City Court confirmed that Mr Zakharov had failed to prove he was subject to any form of public ICT network surveillance.[112] During the ECtHR proceedings, the Russian Government said there were judicial remedies at national law – a request to the Constitutional Court could be made to review secret surveillance operations, and requests for redress could be made to the civil courts.[113] It also said there were sufficient counterchecks to prevent abuse of the public ICT network secret surveillance.[114] The ECtHR, however, agreed with the applicant that the existence of a secret state surveillance framework and the potential of subjecting any citizen to surveillance measures constituted *locus standi* to challenge

[100] ibid para 62.
[101] ibid para 65.
[102] ibid para 66, 68.
[103] ibid para 68.
[104] ibid para 73.
[105] ibid para 77, 80.
[106] ibid para 83.
[107] ibid para 89.
[108] App no 47143/06.
[109] ibid para 1.
[110] ibid para 3.
[111] ibid para 11.
[112] ibid para 13.
[113] ibid para 156.
[114] ibid para 157.

the contested measures.[115] The court confirmed the use of public ICT networks was an integral part of a person's private life.[116] The court did not agree with the Russian Government that satisfactory judicial remedies are available.[117] The applicant lamented the discretion of the state to order secret surveillance operations.[118] In paragraph 183 of the *Zakharov* judgment the Russian Government,

> […] submitted that interception of communications might be conducted only following the receipt of information that a criminal offence had been committed, was being committed or was being plotted; about persons conspiring to commit, or committing, or having committed a criminal offence; or about events or activities endangering the national, military, economic or ecological security […]

The applicant's legal counsel argued about the lack of a 'reasonable suspicion' as a criterion to roll out a secret state surveillance operation.[119] The Russian Government reiterated a state authority's public ICT network secret surveillance request had to be made before a court and it was only in case of an emergency that the judicial approval could be omitted.[120] It went on to add that secret surveillance operations were adequately supervised by the highest state offices.[121] Following the conclusion of the investigative operation, a monitored person could request to see the data collected.[122] It was submitted, however, that a monitored subject was not bound to be informed of the secret surveillance operation in which he or she was involved.[123] The court observed the discretion with which secret surveillance operations could be rolled out was contrary to the rule of law.[124] The court examined the submissions of both parties to the lawsuit under the following titles:

- Accessibility of the domestic law[125]
- Scope of application of secret surveillance measures[126]
- The duration of secret surveillance measures[127]
- Procedures to be followed for storing, accessing, examining, using, communicating and destroying the intercepted data[128]
- Authorisation of interceptions[129]
- Supervision of the implementation of secret surveillance measures[130]
- Notification of interception of communications and available remedies[131]

The ECtHR's decision was that the Russian Government's public ICT network secret surveillance measures do meet the required fundamental human rights criteria.

---

[115] ibid para 167.
[116] ibid para 174.
[117] ibid para 175.
[118] ibid para 176.
[119] ibid para 192.
[120] ibid para 198, 201.
[121] ibid para 208.
[122] ibid para 214.
[123] ibid para 213.
[124] ibid para 230.
[125] ibid p 60.
[126] ibid p 61.
[127] ibid p 63.
[128] ibid.
[129] ibid p 65.
[130] ibid p 69.
[131] ibid p 73.

## 5. Final Considerations

Following the terrorist attacks in the US on the 11th September 2001 and other attacks in Europe, states increased the use of surveillance technologies in the fight against terrorism and crime. The terrorist attacks in Europe were one of the motors for the drafting of the Data Retention Directive. In *Digital Rights Ireland* the court acknowledged there is a legitimate objective in the use of surveillance technologies to monitor terrorist and criminal activities, but scope of surveillance should be strictly for the purpose indicated. However, the Big Brother State is undesirable for the concern of having individuals living in the constant fear that their actions may be subject to monitoring and scrutiny. Nonetheless, the fight of state against terrorist organisations and criminality continues. Although the invalidation of the DRD in the EU has obliged governments to be more selective in the way surveillance technologies are implemented there is undoubtedly going to remain a sustained use of state surveillance technologies so long as there is a fight against terrorism and crime. Perhaps the Grand Chamber in the *Digital Rights Ireland* and *Tele2 Sverige* rulings could have shed more light on how the state surveillance authorities may go about their business of countering terrorism and crime whilst at the same time ensuring they do not overstep the right of data protection. The right to data protection of a known suspect can be waived because it is necessary to monitor him/her in the interest of public security. However, as any state surveillance authority will confirm limiting the fight against terrorism and crime simply to known or even possible suspects will not go far enough. It may be the case, as does in actual fact happen, that a terrorist organisation may seek to engage less suspectable individuals, such as, women, youngsters and people not culturally or personally associated to any extremist cause, to perpetrate certain key duties. Also, a serious crime may be perpetrated by an individual with no previous infringements of the law and having been raised and brought up in a social background that would least indicate any form of criminal activity from the individual. History is laden with horrible crimes perpetrated by the least suspectable of individuals. Therefore, not necessarily by people raised in dubious conditions who have been arrested by the police countless number of times, but perhaps by a respectable family man with a well-to-do occupation, or by a seemingly charming woman. Youngsters coming from decent families have been known to join extremist organisations for no apparent reason. News broadcasts are replete with reports of neighbours being interviewed on the spot by journalists seeking their reaction following some atrocity perpetrated by someone in their neighbourhood: 'He seemed such a nice person,' they will say; 'She kept herself occupied'; or 'I had no suspicion whatsoever.' Mention can also be made of certain white-collar crimes, which go beyond the petty theft, by employees one would have described as a diligent, trustworthy person.

The legal counsel of the applicant in *Zakharov* spoke about the legitimacy of surveillance technologies where there is a 'reasonable suspicion'. From a human rights perspective it is befitting secret surveillance should be something associated with the infringement of the law. The fear of the Big Brother State concept militates against the situation where anyone can be subject to secret surveillance. The invisible line between individuals labelled as 'criminal' and those seen as conforming to the law is considered sacrosanct in the eyes of many. This may have its perils as those labelled as criminal are perceived as sub-human. Ironically, this would defy the fundamental principle of human rights where everyone is deemed to be entitled to the respect of his/her rights irrespectively of any form of discrimination. The potential use of secret surveillance technologies on any resident of the state gives the impression of an erosion of the boundary between those labelled criminals, and those considered 'God-fearing' citizens. The vision of this imaginary line may benefit the state as a person aware of the stigma associated with being labelled a criminal would be conditioned to abide by the law. Thus, God-fearing citizens may find peace of mind in abiding by the law and feeling confident the ill-treatment reserved to criminals would not apply to them. The

principle of proportionality comes into play because although it is granted everybody should be treated with respect for their fundamental human rights, there are those individuals in a society who acting as criminals must be treated differently. According to this line of thought, it is proportionately acceptable to use surveillance technologies to, say, monitor and stop in their tracks a group of terrorists planning to slip a large amount of explosives into a crowded area to cause as much harm as possible. A group of terrorists would not perform their preparatory acts in broad daylight, therefore if one is to apply the reasonable suspicion theory there has to be a point in which the law and order authorities become aware of their deviant plans. This touches upon certain well-established notions of criminal law but the argument here is not strictly one of criminal law but that, put simply, surveillance technologies are effective tools in the fight against terrorism and criminality. The terrorist attack on the Twin Towers in the US ('the 9/11 attacks') has already been introduced in the study under review. In these attacks, terrorists hijacked several airline planes and diverted them against buildings, amongst these the two skyscrapers forming the Twin Towers. Harsh criticism was levelled against the American intelligence agencies, notably the Federal Bureau of Investigation ('the FBI') and the Central Intelligence Agency ('the CIA'). To this day, there are conspiracy theories that these intelligence agencies could not have been in the obscure of what was being concerted and in one way or another were conspirators to the attacks. The 9/11 attacks took place in 2001. A few years later terrorist attacks, not on the same scale, also took place in Europe. Before the 9/11 attacks occurred, surveillance technologies would not have been as sophisticated as today's because technology has advanced since then and because secret state surveillance, although prevalent, was on a considerably lower scale. The 9/11 attacks changed this and the terrorist attacks in Europe confirmed terrorist and criminal perpetrators could be smarter than one imagined. In fact, criminals are colloquially claimed to be always ahead of the law and order authorities. In fact, the technologies at the time had aided the perpetrators of the 9/11 attacks in their intent. By way of the Snowden revelations it is possible to imagine that in the years following the 9th September 2001, governments, not only in the US but also in other jurisdictions, invested heavily in secret surveillance with surveillance technologies being the most effective method of implementation. According to Snowden the US Government, and those following in its steps, took it too far making the breach of data protection privacy the norm. The case law examined in the study under review concurs with the Snowden train of thought. The courts acknowledge the necessity of secret state surveillance in combatting terrorism and criminality. The principle of proportionality justifies the breach by the state of an individual's right to privacy and the protection of data in the interest of public safety and security, such as in a conspiracy to carry out a terrorist attack. However, the courts propound criteria, as has been discussed in the study under review, that nail the use of secret surveillance technologies only if these are used proportionately to what is their purpose and the fundamental rights of citizens.

## 6. Conclusion

To conclude, this may be a case of going in through the window instead of through the door. There are valid reasons to assume that following the 9/11 attacks in 2001 the use of surveillance technologies has increased exponentially lead by the desire of stakeholders, such as the US Government, to benefit from it and fuelled by the advances in technology being witnessed to the present day. No one would deny the use of surveillance technologies to fight terrorism and criminality is a good thing since no one would want to be the victim of a terrorist attack. Whether the use of surveillance technologies is leading towards the Orwellian Big Brother State is a discussion that has been going on since the book was first published in 1949. It is not the purpose of the study under review to agree or disagree with that discussion, but it is safe to say the use of surveillance

technologies has not diminished since its rise in 2001. The Snowden revelations and the invalidation of the DRD have not slowed down appetite for surveillance technologies. The DRD was shot down because not in conformity with the principle of proportionality. This is not to say that data retention practices are not being exercised – they simply are not being done with the benediction of the law and in a transparent way.

Are the courts right in insisting the use of surveillance technologies should follow the principle of proportionality? The answer is 'without a doubt'. Just as no one wants to be the victim of a terrorist attack, no one want to live in a Big Brother State. The courts have not been clear enough how secret surveillance agencies are to go about doing their business without treading on the feet of privacy and data protection. The principle of proportionality criteria presented by the courts may look good on paper and the legislator will certainly take them into account before drafting anything similar to the DRD. However, the secret surveillance agencies may not know what to make of them – their job is to monitor, and breaking privacy and data protection rights comes with the job. Perhaps, it is to be hoped the teachings of the courts will permeate through the legislator into the corridors of the secret surveillance agencies. The ball, at this point, is in the legislator's court (no pun intended!).