


Surveilling masses and unveiling human rights

Uneasy choices for the
Strasbourg Court



Inaugural address delivered by
Prof. dr. Eleni Kosta



Prof. dr. Eleni Kosta is full Professor of Technology Law and Human Rights at the Tilburg Institute for Law, Technology and Society (TILT) of Tilburg University. Eleni obtained her law degree at the University of Athens (Greece) in 2002 and a Masters degree in Public Law at the same University in 2004. In 2005 she completed an LL.M. in legal informatics at the University of Hannover (Germany) and in 2011 she was awarded the title of Doctor of Laws at the KU Leuven (Belgium) with a thesis on consent in data protection that she conducted under the supervision of Prof. Em. Jos Dumortier.

Eleni is conducting research on human rights and the challenges posed by technology. She is an expert in privacy and data protection, specialising in electronic communications and new technologies. Eleni has been publishing extensively in journals and books and participating in international conferences, workshops and roundtables, delivering presentations or joining panel debates. She is member of editorial boards of journals and book series in her field of expertise, and she is regularly invited as Programme Committee Member of European and International Conferences. In addition she functions as external legal expert to numerous organisations, as member of expert groups and as reviewer and evaluator for the European Commission.

She is teaching “Capita Selecta Privacy and Data Protection” at the LLM Law & Technology of the Tilburg Law School, has been regularly giving guest lectures in Universities in the Netherlands and in Europe. She has been involved in numerous EU research projects and in 2014 Eleni was awarded a personal research grant for research on privacy and surveillance by the Dutch Research Organisation (VENI/NWO), which she is currently working on. Eleni also collaborates as associate with timelex (www.timelex.eu).

SURVEILLING MASSES AND UNVEILING HUMAN RIGHTS UNEASY CHOICES FOR THE STRASBOURG COURT

Inaugural Address

delivered in adapted form for the Chair on Technology Law and Human Rights at Tilburg University on 15 December 2017 by Prof. Dr. Eleni Kosta. This chair has been endowed by the Philip Eijlander Diversity Program.

© Eleni Kosta, 2017
ISBN: 978-94-6167-349-7

All rights reserved. This publication is protected by copyright, and permission must be obtained from the publisher prior to any reproduction, storage in a retrieval system, or transmission in any form or by any means, electronic, mechanical, photocopying, recording or otherwise.

www.tilburguniversity.edu

Surveilling masses and unveiling human rights

Uneasy choices for the
Strasbourg Court

1. Introduction

In May 2013 Edward Snowden revealed that UK and US intelligence services were collaborating in the context of surveillance programs involving personal information of individuals in an unprecedented way.¹ Only since then has the general public started realising how far-reaching secret surveillance powers truly are and how dramatically the nature, manner and magnitude of data collection by secret and intelligence authorities have changed in the digital age.

The UK Security Service (commonly known as MI5), the UK Secret Intelligence Service (commonly known as MI6) and the Government Communications Head Quarters (GCHQ) (hereafter jointly referred to as “UK Intelligence agencies”) launched and used a number of surveillance programmes. The Prism and Upstream programmes facilitated the indiscriminate capture of vast quantities of communication data that was obtained by foreign intelligence services and in particular the US National Security Agency (NSA).² The Tempora programme facilitated the “acquisition of worldwide and domestic communications by the GCHQ for use by UK Intelligence Services [...] and other UK and foreign agencies through the interception, under global and rolling warrants, of electronic data transmitted on transatlantic fibre-optic cables.”³ Information on EU citizens was collected thus both by US and UK intelligence services via secret surveillance.

The US legislation discriminates “between the protections afforded by the US constitution to US citizens, and everybody else”⁴, a discrimination that affects the privacy protection of non-US citizens and their data when data are transferred to the US. The transfer of personal data from the EU to the US used to be facili-

¹ Arne Hintz and Lina Dencik, ‘The politics of surveillance policy: UK regulatory dynamics after Snowden’ (2016) 5(3) *Internet Policy Review* < <https://policyreview.info/articles/analysis/politics-surveillance-policy-uk-regulatory-dynamics-after-snowden> > accessed 17 November 2017; Nick Taylor, ‘To find the needle do you need the whole haystack? Global surveillance and principled regulation’ (2014) 18(1) *The International Journal of Human Rights* 45, 49.

² Joint application under Article 34, Big Brother Watch, Open Rights Group, English PEN, Dr Constanze Kurz v. the United Kingdom lodged on 4 September 2013, App. No. 58170/13, 3, < https://www.privacynotprism.org.uk/assets/files/privacynotprism/496577_app_No_58170-13_BBW_ORG_EP_CK_v_UK_Grounds.pdf > accessed 17 November 2017. For a description of the surveillance programmes Prism, and Upstream see: Rachel Levinson-Waldman, ‘NSA surveillance in the war on terror’ in David Gray and Stephen Henderson (eds), *Cambridge Handbook of Surveillance Law* (Cambridge, University Press 2017) 7ff.

³ Joint application under Article 34, Big Brother Watch et al. (ibid); for more information on Tempora, see: Cristina Blasi Casagran, *Global Data Protection in the Field of Law Enforcement: An EU Perspective* (Routledge 2016) 181.

⁴ European Parliament (Report authored by Caspar Bowden), ‘The US surveillance programmes and their impact on EU citizens’ fundamental rights’ (2013), 20.

tated to a large extent by the EU-US safe harbour privacy principles.⁵ Following the Snowden revelations, Maximilian Schrems, an Austrian law student at that time and a Facebook user, launched a complaint with the Irish Data Protection Commissioner requesting him to prohibit Facebook Ireland from transferring Schrems' personal data to the United States. The request was not granted and eventually the Irish High Court sent a request for a preliminary ruling to the Court of Justice of the European Union (CJEU) in relation to the interpretation of the validity of the Commission Decision on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce.⁶

The CJEU in *Schrems* repeated its position that the “protection of the fundamental right to respect for private life at EU level requires derogations and limitations in relation to the protection of personal data to apply only in so far as is strictly necessary”⁷ and clarified that “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.”⁸ The CJEU invalidated the safe harbour Decision. A new self-certification system was adopted in 2016, the Privacy Shield, which introduced a system of checks and balances when transferring data from the EU to the US.⁹ Following *Schrems* a number of additional safeguards were also introduced in the US in relation to the access to personal data by US public authorities for national security purposes.¹⁰

It becomes increasingly and painfully obvious that intelligence authorities and national-security agencies had and continue to have extensive powers to carry out surveillance. These surveillance programs of communications do not constitute *eo ipso* a violation of the right to privacy of citizens. However, they cannot be left unchecked and specific safeguards need to be put in place in order to restrict any and all pockets of governmental impunity. Within this context of the public's awakening to the extent and dangers of government-sanctioned surveillance

⁵ European Commission, 'Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce' [2000] OJ L 215, 7–47.

⁶ Case C-362/14 Maximilian Schrems v Data Protection Commissioner [2015] ECLI:EU:C:2015:650.

⁷ *Idem*, para 92.

⁸ *Idem*, para 94.

⁹ European Commission, 'Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield' [2016] OJ L 207/1.

¹⁰ For instance the Presidential Policy Directive 28 (PPD-28) Signals Intelligence Activities (2014).

programmes, it should come as no surprise that *Schrems* has not been the only example of surveillance programmes being scrutinized. In Europe, in the aftermath of the Snowden revelations, UK surveillance activities have been in the spotlight of privacy and civil rights organisations, as well as of individuals. In 2013, a number of Civil Rights Organisations (incl. Big Brother Watch) filed an application at the European Court of Human Rights (ECtHR or Court) against the GCHQ's secret interception of communications and data claiming a violation of the right to privacy.¹¹ In 2014, a second application was filed by the Bureau of Investigative Journalism, a UK not-for-profit media organisation, against the UK claiming that the generic surveillance carried out by the GCHQ constitutes an interference with their right to privacy and freedom of expression.¹² In these two cases the applicants filed an application directly to the ECtHR, without first filing their case in front of national courts and tribunals, a choice that will be examined in detail in this inaugural address.

Ten human rights organisations¹³ chose a different path and started a legal battle at the national level before turning to the ECtHR. They filed separate applications¹⁴ at the UK Investigatory Powers Tribunal (UK IPT or Tribunal), where their cases were joined. After the publication of the judgment of the UK IPT in 2015, the ten human rights organisations filed an application against the UK at the ECtHR.¹⁵ The main arguments raised by the applicants are that the UK legal framework governing the interception of communications and communications data and the receipt of foreign intercept material is not "in accordance with the law" and thus amounted to an interference with the rights to privacy and freedom of expression.

¹¹ Joint application under Article 34, Big Brother Watch et.al (n 2).

¹² Joint application under Article 34, Bureau of Investigative Journalism and Alice Ross v the United Kingdom lodged on 11 September 2014, App. No. 62322/14

¹³ Amnesty International Limited ("Amnesty International"), Bytes for All ("B4A"), The National Council for Civil Liberties ("Liberty"), Privacy International, The American Civil Liberties Union ("ACLU"), The Canadian Civil Liberties Association ("CCLA"), The Egyptian Initiative for Personal Rights ("EIPR"), The Hungarian Civil Liberties Union ("HCLU"), The Irish Council for Civil Liberties ("ICCL") and The Legal Resources Centre ("LRC").

¹⁴ Case numbers: IPT/13/77/H, IPT/13/92/CH, IPT/13/168-173/H, IPT/13/194/CH, IPT/13/204/CH.

¹⁵ Joint application under Article 34, the 10 human rights organisations (the American Civil Liberties Union, Amnesty International, Bytes for All, the Canadian Civil Liberties Association, the Egyptian Initiative for Personal Rights, the Hungarian Civil Liberties Union, the Irish Council for Civil Liberties, the Legal Resources Centre, Liberty, Privacy International) v UK lodged on 20 May 2015, App. No. 24960/15.

The ECtHR joined the three cases and the hearing took place on 07 November 2017.¹⁶ Although it is not the first time that the ECtHR deals with cases on secret surveillance, the size and intensity of the secret surveillance measures employed in the Prism, Upstream and Tempora programmes, the abundance of personal information collected and processed as well as the interest of the general public vest these cases with a special character. In December 2015 and January 2016 the Court ruled on two seminal cases, *Zakharov v Russia*¹⁷ and *Szabó and Vissy v Hungary*¹⁸ respectively where the Court established more coherent safeguards in relation to secret surveillance that can pave the way for the Court to make bold statements in the pending cases. In *Szabó and Vissy* the Court made concrete reflections on the use of cutting-edge surveillance technologies and the dangers their use entails for the privacy of citizens highlighting that “[t]he guarantees required by the extant Convention case-law on interceptions need to be enhanced so as to address the issue of such surveillance practices.”¹⁹

The terminology relating to surveillance used in the case law of the ECtHR and in the literature varies significantly and so do the definitions of the various terms used in the context of secret surveillance, such as targeted or non-targeted surveillance, strategic monitoring²⁰ or mass surveillance. The European Group on Ethics in Science and New Technologies refers to surveillance as “close observation, especially the act of carefully watching a suspected spy or criminal or a place where an incident may occur.”²¹ Gary Marx provides for a more nuanced definition according to which “[a]t the most general level surveillance of humans (which is often, but need not, be synonymous with human surveillance) can be defined as regard or attendance to a person or to factors presumed to be associated with

¹⁶ The Chamber hearing of 7 November 2017 on the cases *Big Brother Watch and Others v. the United Kingdom* (no. 58170/13), *Bureau of Investigative Journalism and Alice Ross v. the United Kingdom* (no. 62322/14) and *10 Human Rights Organisations and Others v. the United Kingdom* (no. 24960/15) <http://www.echr.coe.int/Pages/home.aspx?p=hearings&w=5817013_07112017&language=en> accessed 17 November 2017.

¹⁷ *Roman Zakharov v Russia* (2015) Application no 47143/06.

¹⁸ *Szabó and Vissy v Hungary* (2016) Application no 37138/14.

¹⁹ *Idem*, para 70.

²⁰ The ECtHR makes commonly use of the term “strategic monitoring”: see for instance: *Weber and Saravia v Germany* 2006-XI Application no 54934/00; *Liberty and Others v United Kingdom* 2008 Application no 58243/00; *Association for European Integration and Human Rights and Ekimdzhev v Bulgaria* (2008) Application no 62540/00; *Szabó and Vissy v Hungary* (2016). The Court referred to “strategic surveillance” in *Szabo*, when referring to report of the Venice Commission (*Szabó and Vissy v Hungary* (2016), para 10).

²¹ European Group on Ethics in Science and New Technologies, ‘Opinion 28 -Ethics of security and surveillance technologies’ (20 May 2014) 14 <<https://publications.europa.eu/en/publication-detail/-/publication/6f1b3ceo-2810-4926-b185-54fc3225c969/language-en>> accessed 17 November 2017.

a person.”²² Surveillance of humans involves non-strategic surveillance, which Marx contrast with strategic surveillance, within which he sees two further types of surveillance: the traditional and the new surveillance ones.

“[Surveillance of humans] can involve *non-strategic surveillance*—the routine, auto-pilot, semi-conscious, often even instinctual awareness in which our sense receptors are at the ready, constantly receiving inputs from whatever is in perceptual range. Smelling smoke or hearing a noise that might or might not be a car’s backfire are examples. This contrasts with *the strategic surveillance* which involves a conscious strategy—often in an adversarial and inquisitorial context to gather information. Within the strategic form we can distinguish traditional from the new surveillance. The latter is at the core of contemporary concerns. *Traditional surveillance* is limited. It relies on the unaided senses and was characteristic of pre-industrial societies—information tended to stay local, compartmentalized, unshared and was often unrecorded, or if kept, difficult to retrieve and analyze in depth. In contrast, **the new surveillance involves scrutiny of individuals, groups and contexts through the use of technical means to extract or create information.** This means the ability to go beyond what is offered to the unaided senses and minds or what is voluntarily reported. The new surveillance is central to the emergence of a surveillance society with its extensive and intensive (and often remote, embedded) data collection, analysis and networks.”²³ (emphasis added)

The surveillance activities of the US and UK secret and intelligence agencies have been systematically referred to as mass surveillance. A definition of the term is attempted by Roger Clarke who defines mass surveillance as “the surveillance of groups of people, usually large groups. In general, the reason for investigation or monitoring is to identify individuals who belong to some particular class of interest to the surveillance organization. It may also, however, be used for its deterrent effects.”²⁴ He further focuses on the term *mass dataveillance*, to which he attributes the following meaning “the systematic use of personal data systems in the investigation or monitoring of the actions or communications of groups of people. In general, the reason for investigation or monitoring is to identify individuals who belong to some particular class of interest to the surveillance

²² Gary T. Marx, *Windows into the Soul: Surveillance and society in an Age of High Technology* (The University of Chicago Press 2016) 15.

²³ Gary T. Marx, “‘Your Papers please’: personal and professional encounters with surveillance, Preface’ in Kirstie Ball, Kevin Haggerty and David Lyon (eds), *Routledge Handbook of Surveillance Studies* (Routledge 2012) xxv.

²⁴ Roger Clarke, *Introduction to Dataveillance and Information Privacy, and Definitions of Terms* (1997, revised 2016), <<http://www.rogerclarke.com/DV/Intro.html>> accessed 17 November 2017.

organization. It may also, however, be used for its deterrent effects.”²⁵ I use the term mass surveillance in this inaugural address under the meaning of Clarke’s notion of mass dataveillance.

In this inaugural address, I discuss the circumstances of the pending cases against the activities of the UK intelligence agencies as an example of the interplay between modern technological surveillance capabilities and the dangers that they bring against human rights, in order to illustrate the crucial need for further research in the area of surveillance and human rights, which I intend to undertake while serving as Chair of Technology Law and Human Rights. For the purposes of this inaugural address and given the current stage of my research, I focus on the analysis of Article 8 of the European Convention on Human Rights (ECHR or Convention) in relation to mass secret surveillance. This choice by no means implies a lesser importance of other human rights relating to secret surveillance measures. Zooming in on the right to privacy in relation to mass surveillance allows me to carry out a thorough analysis and assessment of the literature and case law and identify a number of important issues that require further research, as I will discuss extensively in the last section of this inaugural address. My findings will be the basis for further research on surveillance that I will embark on in the future. It is one of my first aspirations as Professor of Technology Law and Human Rights to complement the research presented in this inaugural address with thorough examination of the interplay between surveillance on the one hand and freedom of expression, the right to non-discrimination and right to effective remedies on the other.

In this inaugural address I will first discuss the procedures in front of the UK IPT in the *10 Human Rights Organisations* case, followed by a short presentation of the applications against actions of UK intelligence agencies in *Big Brother Watch* and in *Bureau of Investigative Journalism* that were directly submitted to the ECtHR. I will then turn to the issue of admissibility in secret surveillance cases, where the victims cannot prove that they have been directly affected by the surveillance measures, and will analyse the protection afforded by the ECtHR in light of its recent case law. After a short presentation of Articles 8 and 10 ECHR this inaugural address will focus on the discussion of the requirements that are established in Article 8(2) ECHR that when satisfied, justify an interference with the right to privacy: legality, legitimacy and necessity. The penultimate section will assess the recent case law of the CJEU in blanket data retention and surveillance cases. Finally I will close this inaugural address with a summary of my main findings and will conclude with thoughts for further research that I intend to undertake in the coming years.

²⁵ Ibid.

2. 10 Human Rights Organisations

2.1 The case in front of the UK IP Tribunal

Following the Snowden revelations, 10 human rights organisations claimed that they believed that the content of their communications and their communications data²⁶ could have been intercepted by the UK intelligence services. Their claim was based on the fact that they regularly used means such as email, text messages, phone calls, video calls, social media and instant messaging for their communications and on the sensitivity of the communication with their contacts that range from NGOs and lawyers to victims of human rights abuses and whistle-blowers. In particular the 10 human rights organisations turned against the UK's practice and legal regimes governing the receipt of foreign intercept material collected by the US authorities pursuant to Prism and Upstream programmes and the "bulk" interception of communications pursuant to Tempora and claimed breach of Articles 8 (privacy) and 10 (freedom of expression) ECHR.²⁷ As part of the proceedings, a 'closed' hearing took place where neither the applicants, nor their advocates were allowed to participate. The applicants submitted a renewed request for disclosure of material relating to the internal policies and guidance, especially those concerning the handling of confidential information obtained pursuant to the interception of private communications according to section 8(4) Regulation of Investigatory Powers Act 2000 (RIPA), claiming infringement of their right to privacy.²⁸ More concretely the applicants focused on section 8(4) RIPA that regulated "bulk interception, inspection, retention and disclosure of communications and communications data is not 'in accordance with the law' as required by Article 8(2) ECHR [claiming that] the interception regime under s. 8(4) cannot be characterised as

²⁶ Section 21(4) of the UK Regulation of Investigatory Powers Act 2000 defines "communications data" as "any of the following—

(a) any traffic data comprised in or attached to a communication (whether by the sender or otherwise) for the purposes of any postal service or telecommunication system by means of which it is being or may be transmitted;

(b) any information which includes none of the contents of a communication (apart from any information falling within paragraph (a)) and is about the use made by any person—

(i) of any postal service or telecommunications service; or

(ii) in connection with the provision to or use by any person of any telecommunications service, of any part of a telecommunication system;

(c) any information not falling within paragraph (a) or (b) that is held or obtained, in relation to persons to whom he provides the service, by a person providing a postal service or telecommunications service".

²⁷ Judgment of 05 December 2014, [2014] UKIPTrib 13_77-H, para 3.

²⁸ The 10 Human Rights Organisations, 'Additional submissions on the facts and complaints', para 19 < <https://www.amnesty.org/en/documents/ior60/1415/2015/en/> > accessed 17 November 2017.

either 'necessary in a democratic society' or proportionate under Article 8(2) ECHR' [and finally that the] receipt, inspection and retention of intercepted communications and communications data under Prism and Upstream is not carried out 'in accordance with the law'.²⁹

RIPA allows the interception of internal and external communications, after the issuing of a relevant warrant, containing different provisions for warrants for interception of communications. Warrants for communications that are both transmitted and received within the United Kingdom (internal communications) are regulated in section 8(1) of RIPA and warrants for communications between the United Kingdom and abroad (external communications) are regulated in section 8(4) of RIPA.

Section 8(1) RIPA provides that a warrant must name or describe a person or a set of premises in relation to whom the interception will take place. Section 8(2) RIPA specifies the information of the communications that are to be intercepted. However such information is not necessary, when the interception warrant relates to the interception of external communications in the course of their transmission by means of a telecommunication system. According to section 8(4) RIPA, an interception warrant does not need to specify one person as the interception subject, nor a single set of premises if it relates to the interception of external communications and if the Secretary of State has issued a certificate applicable to the warrant, which explains what is the intercepted material the examination of which he considers necessary. These warrants can be renewed, when they are necessary in the interests of national security³⁰ or for the purpose of safeguarding the economic well-being of the UK³¹ in which case they have a duration of six months each.³² Section 8(4) RIPA may still "authorise the interception of communications that are not external communications insofar as such interception is necessary under section 5(6)(a) [RIPA]³³."³⁴

External communications are defined as communications sent or received outside the British Islands³⁵. The Interception of Communications Code of Practice clarified

²⁹ 10 Human Rights Organisations and Others v UK Application Form to the ECtHR App no 24960/15, 7.

³⁰ RIPA, Section 6(3)(a).

³¹ RIPA, Section 6(3)(c).

³² RIPA, Section 9(6)(b).

³³ Section 5(6) RIPA: "The conduct authorised by an interception warrant shall be taken to include— (a) all such conduct (including the interception of communications not identified by the warrant) as it is necessary to undertake in order to do what is expressly authorised or required by the warrant; [...]"

³⁴ Charles Blandford Farr, Witness Statement on joined cases IPT/13/77/H, IPT/13/92/CH, IPT/13/168-173/H, IPT/13/194/CH, IPT/13/204/CH, 16 May 2014, para 139.

³⁵ RIPA, Section 20.

what should be understood under the concept of external communications, narrowing down its notion:

“External communications are defined by the Act to be those which are sent or received outside the British Islands. They include those which are both sent and received outside the British Islands, whether or not they pass through the British Islands in course of their transit. They do not include communications both sent and received in the British Islands, **even if they pass outside the British islands en route.**”³⁶

The Code as amended in 2016 modified slightly the definition and added an example:

“External communications are defined by RIPA to be those which are sent or received outside the British Islands. They include those which are both sent and received outside the British Islands, whether or not they pass through the British Islands in the course of their transmission. They do not include communications both sent and received in the British Islands, even if they pass outside the British Islands en route. **For example, an email from a person in London to a person in Birmingham will be an internal, not external communication for the purposes of section 20 of RIPA, whether or not it is routed via IP addresses outside the British Islands, because the sender and intended recipient are within the British Islands.**”³⁷ (emphasis added)

The former Director General of the Office for Security and Counter Terrorism (OSCT) at the UK Home Office, Charles Blandford Farr, in his Witness Statement, explained however that in practice UK intelligence services have construed the concept of external communications in a broad way, treating as external, communications that involve web-based platforms.³⁸ He presented as examples a Google search by an individual located in the UK, claiming that it “may well involve a communication from the searcher’s computer to a Google web server, which is received outside the British Islands; and a communication from Google to the searcher’s computer which is sent outside the British Islands. In such a case, the search

³⁶ UK Home Office, Interception of Communications Code of Practice Pursuant to section 71 of the Regulation of Investigatory Powers Act 2000, 2002, para 5.1, <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/513668/interception-comms-code-practice.pdf> accessed 17 November 2017.

³⁷ UK Home Office, Interception of Communications Code of Practice Pursuant to section 71 of the Regulation of Investigatory Powers Act 2000, January 2016, para 6.5 (emphasis added), <<https://www.gov.uk/government/publications/interception-of-communications-code-of-practice-2016>> accessed 17 November 2017.

³⁸ Charles Blandford Farr (n 34), paras 132-138.

would correspondingly involve two “external communications” for the purposes of section 20 of RIPA [...].”³⁹ He presented a similar reasoning in relation to YouTube videos, in which case the location of the web server is the crucial element in order to decide whether the communication is internal or external.⁴⁰ Moreover posts on Facebook or tweets on Twitter are seen as addressing a broad audience and as the data center infrastructures are in most cases based in the United States, the communication will be external.⁴¹

Such a broad interpretation of the concept of external communications under RIPA seems to be contrary to the wishes of the legislator, as clarified in the Interception of Communications Code of Practice. Although further clarification of whether a communication is internal or external in view of the particular characteristics of modern technologies that allows for data packets to travel across the British borders is essential, the current definition of external communication and the diverging opinions on what is covered under the term, especially in relation to web-based platforms and communication that pass outside the British Islands “en route” raise an eyebrow as to the foreseeability of the relevant provisions of RIPA. The Independent Reviewer of Terrorism Legislation, David Anderson, found exactly that the distinction between internal and external communication is not contributing to legal certainty

“In practice [...] s8(1) warrants may target both internal and external communications and s8(4) warrants frequently intercept internal communications (though they may not target them). The distinction between the two categories of warrant [internal and external] is said to be either pointless or misleading, for the following key reasons:

(a) As a starting point, what is classified as an “external communication” is unclear [...]

(b) The distinction is outdated in the context of internet communications that are routed (and intercepted) globally.

(c) It is particularly irrelevant in a situation when it is impossible, in practice, to intercept external communications without intercepting internal ones as well (RIPA ss8(5)(b) and 5(6)(a)).”⁴²

Making the location of the web-based platform the decisive factor in order to characterise a communication as internal or external would lead to different require-

³⁹ Idem, para 134

⁴⁰ Idem, para 135

⁴¹ Idem, paras 136-138.

⁴² David Anderson, A question of trust – Report of the Investigatory Powers Review, 2015, para 12.25, <<https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Web-Accessible1.pdf>> accessed 17 November 2017.

ments for the interception of identical communication between the same parties, that is routed in a different way. Such a legal solution would be contrary to the rule of law and illustrates the fact that the establishment of different requirements for internal and external warrants, based on the current definitions included in RIPA, is obsolete and should be abandoned.⁴³ In its current form the RIPA provisions on internal and external communications do not meet the criterion of foreseeability as specified in the jurisprudence of the European Court of Human Rights, as will be discussed further in detail below.

The UK IP Tribunal published three rulings on the cases initiated by the 10 Human Rights Organisations: one in December 2014, one in February 2015 and in June 2015 its open determination.⁴⁴

2.2 UK IPT judgment of 5 December 2014

In its first judgement, the UK IPT made extensive references to the jurisprudence of the ECtHR in order to reach its conclusion on the case and admitted that activities relating to Prism engage the rights to privacy and freedom of expression, as protected in Articles 8 and 10 ECHR respectively.⁴⁵ The UK IPT examined first the issue concerning the exchange of information, i.e. “accessing or otherwise receiving intercepted communications and communications data from the US Government under the Prism and Upstream programmes (“the Prism issue”)⁴⁶ and second the issue concerning interception of external communication, i.e. “intercepting, inspecting and retaining their communications and their communications data under the Tempora programme (“alleged Tempora interception operation).”⁴⁷ The Tribunal sustained that the system of mass surveillance could be in principle lawful, recognising though that the ECtHR requires a certain degree of accessibility

⁴³ See also UK Intelligence and Security Committee of the UK Parliament Report “Privacy and Security: A modern and transparent legal framework” (12 March 2015) <<http://bit.ly/2yAAie2>> accessed 17 November 2017: “in respect of internet communications, the current system of ‘internal’ and ‘external’ communications is confusing and lacks transparency. The Government must publish an explanation of which internet communications fall under which category, and ensure that this includes a clear and comprehensive list of communications (para 110).

⁴⁴ The functioning of the UK IPT is regulated in sections 65-70 of RIPA and in The Investigatory Powers Tribunal Rules 2000 (IPT Rules 2000), No 2665.

The procedures in the UK IPT different from the procedures valid for ordinary courts, as it is allowed to hold closed sessions without the participation of the applicants to have some parts of the hearing closed and some open and it is not obliged to necessarily provide justifications for its decisions.: David Anderson, ‘A Question of Trust Report of the Investigatory Powers Review’ (Crown Copyright 2015), 122 <https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf> accessed 17 November 2017.

⁴⁵ Judgment of 05 December 2014 [2014] UKIPTrib 13_77-H, para. 36.

⁴⁶ *Idem*, para 5.

⁴⁷ *Ibid.*

and foreseeability of the national legislation regulating secret surveillance,⁴⁸ as will be elaborated below.

The UK IP Tribunal in its 5 December 2014 judgment summarised two requirements for the interference with Article 8 ECHR to be in accordance with the law. The first one required that there should not exist an unfettered discretion for executive action and that there must be controls on the arbitrariness of that action.⁴⁹ According to the second requirement the nature of rules should be clear and their ambit should be in the public domain to the extent that this would be possible, so that the existence of interference with privacy could in general terms be foreseeable.⁵⁰ While the UK IPT concluded that the first requirement was satisfied both before and after the Disclosures made in the UK IPT Judgment, it found that the second one was not satisfied before the public was informed.⁵¹

On the basis on these findings the question remained open whether there was a breach of Articles 8 and 10 ECHR prior to the Disclosure of the intelligence sharing regime, and invited the parties to the case for submissions on the topic,⁵² which became a subject of the second judgement.

2.3 UK IPT judgment of 6 February 2015

Based on the submission of the parties, the UK IPT concluded in February 2015:

“(i) that **prior to the disclosures** made and referred to in the First Judgment [of 5 December 2014] and the Second Judgment [of 6 February 2015], the regime governing the soliciting, receiving, storing and transmitting by UK authorities of private communications of individuals located in the UK, which have been obtained by US authorities pursuant to Prism and/or (on the Claimants’ case) Upstream, **contravened Articles 8 or 10 ECHR**,
(ii) that **it now complies** with the said Articles.”⁵³ (emphasis added)

The disclosures following the Snowden revelations in the UK IPT judgment of 5 December 2014 were considered sufficient by the Tribunal in order to justify the legitimacy of the surveillance regime by the UK intelligence services. In this way the UK IPT considers that the accessibility and foreseeability requirements are satisfied when the public is informed about the circumstances of the surveillance regime, even when such information does not originate for the government or the legislator.

⁴⁸ *Idem*, para 120.

⁴⁹ *Idem*, para 37.

⁵⁰ *Ibid*

⁵¹ Judgment of 6 February 2015, [2015] UKIPTrib 13_77-H, para 22.

⁵² Judgment of 05 December 2014 [2014] UKIPTrib 13_77-H, para 154.

⁵³ Order of 06 February 2015 UKIPTrib 13_77-H.

2.4 UK IPT amended open determination of 22 June 2015

In June 2015 the UK IPT published its amended open determination on the heard cases, addressing two remaining issues.⁵⁴ The Tribunal made determinations in favour of two of the human rights organisations; for the rest, it did not confirm whether their communications had been intercepted. Relating to Egyptian Initiative for Personal Rights, their communications had been intercepted lawfully and proportionately under section 8(4) RIPA, however, the retention time exceeded the one specified in the internal policies of the GCHQ, even though it had not been accessed. The destruction of documents was ordered but no compensation was awarded. In respect to the Legal Resources Centre, the interception was again lawful and proportionate, however, the selection for examination was not done pursuant to the internal procedure. As the material was not used, and no record had been retained, no compensation was awarded.⁵⁵ It is striking that on 1 July 2015 the Tribunal sent a letter to Amnesty International recognising that the open determination should have referred to Amnesty and not the Egyptian Initiative for Personal Rights, wishing to apologise and correct the error.⁵⁶

2.5 Application at the ECtHR

As expected, the 10 human rights organisations that were the claimants in the cases in front of the Tribunal, were not satisfied with the findings of the Tribunal and filed an application against the UK at the ECtHR.⁵⁷ They alleged that the legal framework governing the interception of communications and communications data and the receipt of foreign intercept material is not “in accordance with the law” and thus amounts to an interference with Articles 8 and 10 ECHR. The applicants complained also under Article 6, claiming that the proceedings before the UK IPT infringed their right to a fair trial. Furthermore, relying on Article 14 (prohibition of discrimination) together with Articles 8 and 10, they argued that section 8(4) RIPA is indirectly discriminatory on grounds of nationality and national origin, as section 16 RIPA differentiates between people known to be in the British Islands and abroad, providing additional safeguards only to the former.⁵⁸

⁵⁴ Open determinations of 22 June 2015, amended by 1 July letter (correcting the name of one of the human rights organisations).

⁵⁵ Statement of facts, 10 Human Rights Organisations and Others against the United Kingdom Application no. 24960/15, sec A3(d) <<http://hudoc.echr.coe.int/eng?i=001-159526>> accessed 17 November 2017.

⁵⁶ President of the Investigatory Powers Tribunal, ‘Letter to Amnesty International Ltd and others’ (1.07.2015) <http://www.ipt-uk.com/docs/IPT_to_Liberty_Others.pdf> accessed 17 November 2017.

⁵⁷ Statement of facts, 10 Human Rights Organisations v United Kingdom, app.no. 24960/15.

⁵⁸ Ibid.

3. Applications against actions of UK intelligence services directly submitted at the ECtHR

Two groups of interested applicants followed a different path and turned against the actions of the UK intelligence services directly in front of the ECtHR in Strasbourg.

3.1 Big Brother Watch and Others

The application of Big Brother Watch, Open Rights Group, English PEN and Constanze Kurz, a German internet activist, against the United Kingdom was lodged soon after the Snowden revelations, in September 2013. The ECtHR prioritised the case, but stayed it until the decision of the UK IPT on the *10 Human Rights Organisations v. United Kingdom* case.

The applicants challenge the compatibility with Article 8 ECHR of practices of the UK intelligence services to receive “foreign intercept material relating to their electronic communications”⁵⁹ and seek declarations from the Court that their rights under Article 8 have been violated.⁶⁰

3.2 Bureau of Investigative Journalism and Alice Ross vs United Kingdom

In September 2014, the Bureau of Investigative Journalism (BIJ) and Alice Ross, a reporter with the BIJ, lodged another application against the UK at the ECtHR.⁶¹ Similar to the argumentation in the *Big Brother Watch v. United Kingdom* case, the BIJ and Ms Ross contend that “it is very likely that their communications have come to the attention of the United Kingdom intelligence services via interception powers exercised pursuant to the Regulation of Investigatory Powers Act 2000

(‘RIPA’).”⁶² The applicants in this case did not include in their application a description of the relevant domestic law, but rather they referred to the relevant section of the statement of facts prepared in *Big Brother Watch v. the United Kingdom*.⁶³

The applicants did not only allege a violation of the right to privacy, but they also claimed an interference with the right to freedom of expression, that is protected

⁵⁹ Statement of facts, *Big Brother Watch, Open Rights Group, English PEN, Dr Constanze Kurz v. the United Kingdom*, App. No. 58170/13, 6, <http://hudoc.echr.coe.int/eng?i=001-140713> accessed 17 November 2017.

⁶⁰ Joint application under Article 34, *Big Brother Watch et al. (n 2)*, paras 6.1-6.3.

⁶¹ *Bureau of Investigative Journalism and Alice Ross vs. the United Kingdom*, App. No. 62322/14.

⁶² Statement of Facts, *Bureau of Investigative Journalism and Alice Ross vs. the United Kingdom*, App. No. 62322/14, 2 < <http://hudoc.echr.coe.int/eng?i=001-150946> > accessed 17 November 2017.

⁶³ *Ibid.*

under Article 10 of the Convention, as freedom of expression is a cornerstone right for journalists. The applicants in this case contested the argument -broadly supported by both the UK and the US governments- that the collection of metadata is not infringing the confidentiality of communications and does not pose a threat to fundamental rights. They alleged that the collection of metadata can be a threat to confidentiality of communications, which is essential for the work of journalists, and to the freedom of expression.⁶⁴

4. Admissibility Following Article 34 ECHR, “[t]he Court may receive applications from any person, non-governmental organisation or group of individuals claiming to be the victim of a violation”⁶⁵ of right(s) protected by the Convention. The ECtHR as a principle does not consider it its task to review laws and practices *in abstracto*, “but to determine whether the manner in which they were applied to, or affected the applicant gave rise to a violation of the Convention.”⁶⁶ However, occasionally the Court has allowed the submission of cases where the applicants suspect interference of their rights that are protected under the Convention, even when they cannot prove it, especially in relation to secret surveillance.⁶⁷

In the recent cases *Zakharov* and *Szabó and Vissy*, the Court made concrete reflections on admissibility in surveillance cases. The Court accepted that “the secret nature of surveillance measures would deprive individuals of access to effective review [seeing] the mere existence of surveillance laws as a threat”⁶⁸ and explicitly

⁶⁴ *Idem* 2-3.

⁶⁵ Article 34 ECHR.

⁶⁶ *Roman Zakharov v Russia* (2015) Application no 47143/06, para 164 citing *N.C. v Italy* (2002) Application no 24952/94, para 56; *Krone Verlag GmbH & Co. KG v Austria* (no. 4) (2006) Application no 72331/01, para 26; and *Centre for Legal Resources on behalf of Valentin Câmpeanu v Romania* (2014) Application no 47848/08, para 101.

⁶⁷ For more about (in)admissibility of ‘in abstracto claims’ and their differentiation from claims in which the Court recognized ‘hypothetical harm’ as sufficient for granting applicants the victim status see, for instance, Bart van der Sloot, ‘Is the Human Rights Framework Still Fit for the Big Data Era? A Discussion of the ECtHR’s Case Law on Privacy Violations Arising from Surveillance Activities’ in Serge Gutwirth, Ronald Leenes, Paul de Hert (eds), *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection* (Springer 2016), 419-422 and 426-429.

⁶⁸ Mark Cole and Annelies Vandendriessche, ‘From Digital Rights Ireland and Schrems in Luxembourg to *Zakharov* and *Szabó/Vissy* in Strasbourg: What the ECtHR made of the deep pass by the CJEU in the recent cases on mass surveillance’ (2016) 1EDPL 121,129.

stated that it accepts *in abstracto* claims.⁶⁹ The Court elaborated on Kennedy⁷⁰ and established a harmonised approach, laying down concrete conditions for admissibility in cases of secret surveillance, bringing an end to the ambiguity regarding *in abstracto* considerations by the Court:

“(…) the Court accepts that an applicant can claim to be the victim of a violation occasioned by the **mere existence** of secret surveillance measures, or legislation permitting secret surveillance measures, if the following conditions are satisfied. Firstly, the Court will take into account the **scope of the legislation** permitting secret surveillance measures by examining whether the applicant can possibly be affected by it, either because he or she belongs to a group of persons targeted by the contested legislation or because the legislation directly affects all users of communication services by instituting a system where any person can have his or her communications intercepted. Secondly, the Court will take into account the **availability of remedies** at the national level and will adjust the degree of scrutiny depending on the effectiveness of such remedies.”⁷¹ (emphasis added)

Judge Dedov in his concurring opinion in *Zakharov* questioned the Court’s competence to examine the domestic law *in abstracto*.⁷² He referred to *Klass*⁷³ and *Kennedy* where the Court examined *in abstracto* the national law is Germany and the United Kingdom respectively. He recognised though that both countries⁷⁴ were involved directly or indirectly in the mass surveillance scandals revealed by Edward Snowden, claiming that “[t]his indicates that something was wrong with the Court’s approach from the very outset”.⁷⁵ Nevertheless, the Grand Chamber implicitly acknowledged that the technological developments that facilitate secret surveillance allow for and actually dictate a change in the position of the Court in order for it to accept *in abstracto* examination of domestic laws in cases of secret

⁶⁹ Roman Zakharov v Russia (2015), para 178. For some further thoughts on the fact that the Court accepts *in abstracto* claims, see: Bart van der Sloot, ‘Editorial’ (2016) 1 EDPL 1.

⁷⁰ Kennedy v United Kingdom (2010) Application no 26839/05, para 119, further citing established case law in *Klass and Others v Germany* (1978) Series A no 28 Application no 5029/71 and *Malone v United Kingdom* (1984) Series A no 82 Application no 8691/79 para 64.

⁷¹ Roman Zakharov v Russia (2015), para 171.

⁷² Roman Zakharov v Russia (2015), Concurring opinion of Judge Dedov.

⁷³ *Klass and Others v Germany* (1978), para 34.

⁷⁴ In this context Judge Dedov recalled that “the mobile telephone conversations of the Federal Chancellor of Germany were unlawfully intercepted by the national secret service; and secondly, the UK authorities provided a US secret service with access to and information about the former State’s entire communication database” (Roman Zakharov v Russia (2015), Concurring opinion of Judge Dedov).

⁷⁵ Roman Zakharov v Russia (2015), Concurring opinion of Judge Dedov.

surveillance, something that was clearly stated in *Szabó and Vissy*.⁷⁶ In addition, of great importance to the pending UK cases, but also in general to the examination of admissibility is the fact that, despite his reservations, Judge Dedov voted for the admission of the case seeing the judgement of the Grand Chamber as an opportunity to reinforce the role of courts in society:

“This judgment could serve as a basis for improving the legislation in the sphere of operational and search activities and for establishing an **effective system of public control** over surveillance. Moreover, this judgment demonstrates that if widespread suspicion exists in society, and if there is no other possibility for society to lift this suspicion without a social contract and appropriate changes in national law and practice, then where the problem is not identified by the other branches of power, the **judiciary must be active** in order to facilitate those changes.”⁷⁷ (emphasis added)

Judge Dedov saw, thus the Grand Chamber’s judgment in *Zakharov*, as an opportunity to stress the important role of the judiciary in the interplay of separation of powers in the context of secret surveillance. When the legislative is not providing for sufficient and effective guarantees against abuse and the executive is taking advantage of the legal regime in order to carry out secret surveillance overstepping its powers, then it is a responsibility of the judiciary to intervene and contribute in a twofold way: establish the safeguards that need to be put in place in order to ensure that the legal framework in question is compatible with the human rights framework and ensure effective protection of the individuals, while at the same time, limit the powers of the executive.

In cases of secret surveillance, the Court will examine whether the two aforementioned conditions – the scope of legislation and the availability of remedies - are fulfilled in order to recognise the applicants as victims. In this way it brought the two main admissibility issues under one umbrella: the discussion on general challenges and the effectiveness of national remedies.

With regard to domestic remedies, Article 35(1) ECHR requires that “[t]he Court may only deal with the matter after all domestic remedies have been

⁷⁶ *Szabó and Vissy v Hungary* (2016), para 32: “in recognition of the particular features of secret surveillance measures and the importance of ensuring effective control and supervision of them, the Court has accepted that, under certain circumstances, an individual may claim to be a victim on account of the mere existence of legislation permitting secret surveillance, even if he cannot point to any concrete measures specifically affecting him.”

⁷⁷ *Roman Zakharov v Russia* (2015), Concurring opinion of Judge Dedov.

exhausted.”⁷⁸ The Court has been traditionally examining the issue of notification of interception of communications, which it finds to be “inextricably linked to the effectiveness of remedies before the courts.”⁷⁹

The national legislation in the UK does not allow complaints on human rights against the UK Intelligence agencies to be heard by the UK High Court. Such complaints are under the exclusive jurisdiction of the UK IPT.⁸⁰ The Court examined in *Kennedy* domestic remedies in the UK and the role of the UK IPT in the context of interception of internal communications. The Court concluded in relation to the admissibility requirement of exhaustion of internal remedies that:

“The Court takes note of the Government’s argument that Article 35 § 1 [ECHR] has a special significance in the context of secret surveillance given the extensive powers of the IPT to investigate complaints before it and to access confidential information. While the extensive powers of the IPT are relevant where the tribunal is examining a specific complaint of interception in an individual case and it is necessary to investigate the factual background, their relevance to a legal complaint regarding the operation of the legislative regime is less clear. In keeping with its obligations under RIPA and the Rules [...], the IPT is not able to disclose information to an extent, or in a manner, contrary to the public interest or prejudicial to national security or the prevention or detection of serious crime. Accordingly, it is unlikely that any further elucidation of the general operation of the interception regime and applicable safeguards, such as would assist the Court in its consideration of the compliance with the regime with the Convention, would result from a general challenge before the IPT.”⁸¹

In *Zakharov* the Court recognised the importance of having clearly specified in the national legislation the period after which an interception authorisation expires.⁸²

In light of the recent case law of the Court the national UK legislation seems to fulfil the two admissibility requirements established in *Zakharov*. On the one hand RIPA “directly affects all users of communication services by instituting a system where any person can have his or her communications intercepted.”⁸³ On the other hand

⁷⁸ Article 35(1) ECHR

⁷⁹ *Klass and Others v Germany* (1978), para 57; *Weber and Saravia v Germany* (2006), para 135; *Roman Zakharov v Russia* (2015), para 286.

⁸⁰ Adam Tomkins ‘Justice and security in the United Kingdom’ (2014) 47 (3) *Israel Law Review* 4.

⁸¹ *Kennedy v United Kingdom* (2010), para 110.

⁸² *Roman Zakharov v Russia* (2015), para 251.

⁸³ *Idem* 171.

it allows for interception warrants to be renewed on a rolling basis.⁸⁴ Therefore it seems plausible that the UK legislation in question will not be able to fulfil the foreseeability requirement. Based on *Zakharov* and on *Kennedy*, the applicants do not have any effective remedy for the complaints they want to raise against the UK intelligence services and are therefore allowed to file an application directly with the ECtHR.

De Hert and Cristobal Bocos acknowledge that the examination of the criteria set by the Court follow the example set by the CJEU in *Schrems*. They identify thus a trend for courts to “analyse the whole surveillance system of a country”,⁸⁵ making it difficult for any mass surveillance law to pass and declaring that “[t]he hunting has started.”⁸⁶ Soon after *Zakharov* the Court took a more nuanced approach in *Szabó and Vissy* and it is actually expected to see the sequel to this hunting in the pending cases against the activities of the UK intelligence agencies.

5. Interference with Articles 8 and 10 ECHR

In the cases against the actions of the UK intelligence agencies, the applicants claim interference with Articles 8 and 10 ECHR, namely with the right to privacy and to

freedom of expression. A short discussion of the main provisions of these Articles is essential in order to follow the discussion of this inaugural address.

Article 8 ECHR safeguards the right to respect for private and family life, home and correspondence and is commonly referred to as protecting the right to privacy:

Right to respect for private and family life

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 demo-

⁸⁴ See e.g. Equality and Human Rights Commission, ‘Response of the Equality and Human Rights Commission to the Consultation: Investigatory Powers Review – Call for Evidence’ (October 2014), para 30, <https://www.equalityhumanrights.com/en/file/6016> accessed 17 November 2017.

⁸⁵ Paul de Hert and Pedro Cristobal Bocos, ‘Case of Roman Zakharov v. Russia: The Strasbourg follow up to the Luxembourg Court’s *Schrems* judgment’, 23.12.2015, <<https://strasbourgeoiservers.com/2015/12/23/case-of-roman-zakharov-v-russia-the-strasbourg-follow-up-to-the-luxembourg-courts-schrems-judgment/>> accessed 17 November 2017.

⁸⁶ Paul de Hert and Pedro Cristobal Bocos, ‘Case of Roman Zakharov v. Russia: The Strasbourg follow up to the Luxembourg Court’s *Schrems* judgment’, 23.12.2015, <<https://strasbourgeoiservers.com/2015/12/23/case-of-roman-zakharov-v-russia-the-strasbourg-follow-up-to-the-luxembourg-courts-schrems-judgment/>> accessed 17 November 2017.

cratic 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.

In the recent *Szabó and Vissy* case the Court stressed the importance to protect the right to privacy in light of technological developments: “Given the technological advances since the *Klass and Others* case, the potential interferences with email, mobile phone and Internet services as well as those of mass surveillance attract the Convention protection of private life even more acutely.”⁸⁷ The Court has been traditionally evolving the protection under Article 8 in order to meet technological developments under its approach that the Convention is a “living instrument.”⁸⁸

Article 10 ECHR protects the right to freedom of expression:

Freedom of expression

1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.
2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

Both the right to privacy and the right to freedom of expression are not absolute rights but interferences with them can be justified only if they fulfil the requirements mentioned in the second paragraph of Articles 8 and 10 respectively. The limitations to the rights to privacy and freedom of expression are not identical, but they are similar enough, introducing a three-part test and allowing for a joint analysis.⁸⁹ First, the limitation should be “in accordance with the law” or ‘prescribed by

⁸⁷ *Szabó and Vissy v Hungary* (2016), para 53.

⁸⁸ George Letsas, ‘The ECHR as a Living Instrument: Its Meaning and its Legitimacy’ in Andreas Føllesdal, Birgit Peters and Geir Ulfstein (eds), *Constituting Europe - The European Court of Human Rights in a National, European and Global Context* (Cambridge University Press 2013) 106 ff.

⁸⁹ Bernadette Rainey, Elizabeth Wicks, and Clare Ovey, *Jacobs, White and Ovey: The European Convention of Human Rights* (5th edn, OUP 2010) 308-309.

law”. Second, that the limitation is “legitimate”⁹⁰ serving the interests mentioned in each of the Articles, such as national security or prevention of disorder or crime, and third that it is necessary in a democratic society.

6. Legality requirement An interference with the rights to privacy and freedom of expression can be justified when it is based in national law. This requirement is known as the legality requirement and is common in the second paragraph of Articles 8 to 11 ECHR.⁹¹ The legality test was initially discussed in *Sunday Times*⁹² in the context of examining interference with the right to freedom of expression:

“... the following are two of the requirements that flow from the expression “prescribed by law”. Firstly, the law must be adequately **accessible**: the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case. Secondly, a norm cannot be regarded as a “law” unless it is formulated with sufficient precision to enable the citizen to regulate his conduct: he must be able - if need be with appropriate advice - to **foresee**, to a degree that is reasonable in the circumstances, the consequences which a given action may entail.”⁹³ (emphasis added)

In *Silver*⁹⁴ the Court extended this interpretation to the limitations of the right to privacy.⁹⁵ Since then, the Court has repeatedly held the position that interferences shall fulfil the requirements of accessibility, of foreseeability and be compatible with the rule of law in its Article 8 case law.⁹⁶ Nardell summarised the legality requirement as essentially meaning that “the citizen with whose rights the State

⁹⁰ *Idem* 311.

⁹¹ Stefan Sottiaux, *Terrorism and the Limitations of Rights: the ECHR and the US Constitution* (HART Publishing 2008) 41.

⁹² *The Sunday Times v United Kingdom* (1979) Series A no 30 Application no 6538/74.

⁹³ *Idem*, para 49.

⁹⁴ *Silver and Others v United Kingdom* (1983) Series A no 61 Application no 5947/72 et al., paras 85-88.

⁹⁵ *Idem*, paras 86-89.

⁹⁶ Ilina Georgieva, ‘The Right to Privacy under Fire – Foreign Surveillance under the NSA and the GCHQ and Its Compatibility with Art. 17 ICCPR and Art. 8 ECHR’ (2015) 31 *Utrecht Journal of International and European Law* 118. See also *Leander v Sweden* (1987) Series A no 116 Application no 9248/81; *Kruslin v France* (1990) Series A no 176-A Application no 11801/85; *Kopp v Switzerland* (1998) Reports 1998-II Application no 23224/94; *Lambert v France* (1998) Reports 1998-V Application no 23618/94; *Amann v Switzerland* 2000-II Application no 27798/95; *Khan v United Kingdom* 2000-V Application no 35394/97; *Perry v United Kingdom* 2003-IX Application no 63737/00; *Weber and Saravia v Germany* (2006); *Liberty and Others v United Kingdom* (2008); *Kennedy v United Kingdom* (2010); *Shimovolos v Russia* 2011 Application no 30194/09.

interferes is entitled to ask: ‘why me?’.”⁹⁷

The requirement of legality requires the law to be in the public domain in some way. The legal basis can be given by statute law, but also by provisions with lower than legal rank, case-law and rules of public international law incorporated in the domestic legal system.⁹⁸ By taking this position, the Court preserves the essence of the common law legal systems and allows the “law” to adapt to the continuous technological development through judicial decisions.⁹⁹ The ECtHR considers that a law is adequately accessible when: “the citizen must be able to have an indication that is adequate, in the circumstances, of the legal rules applicable to a given case.”¹⁰⁰ The requirement of foreseeability means that a citizen “must be able – if need be with appropriate advice - to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail.”¹⁰¹ The Court recognised that in some cases, the legislation cannot avoid using vague terms, the “interpretation and application [of which] are questions of practice.”¹⁰²

The Court has admitted that increasing terrorist threats affecting democratic societies justify the undertaking of secret surveillance measures to effectively counter such threats.¹⁰³ To avoid the authorities abusing the power provided modern surveillance technologies, the ECtHR requires its systems to “afford adequate safeguards against various possible abuses.”¹⁰⁴ In *Zakharov* the Court clearly recognised that “the risk of abuse [...] is inherent in any system of secret surveillance, and [...] is particularly high in a system where the secret services and the police have direct access, by technical means, to all mobile telephone communications.”¹⁰⁵ In this way the Court acknowledges that the mere existence of a secret surveillance system amounts to an interference with the rights to privacy and “may undermine or even destroy democracy under the cloak of defending it”,¹⁰⁶ therefore requiring effective and appropriate guarantees against abuse.

⁹⁷ Gordon Nardell, ‘Levelling up: Data Privacy and the European Court of Human Rights’ in Serge Gutwirth et al. (eds), *Data Protection in a Profiled World*, (Springer 2010) 46.

⁹⁸ *The Sunday Times v United Kingdom* (1979), para 87; *Kruslin v France* (1990), para 29; *Huvig v France* (1990) Series A no 176-B Application no 11105/84, para 28; *Kopp v Switzerland* (1998), para 60; *Weber and Saravia v Germany* (2006), para 87, etc.

⁹⁹ Paul de Hert ‘A human rights perspective on privacy and data protection impact assessments’ in Paul de Hert and David Wright (eds), *Privacy Impact Assessment* (Springer Netherlands 2012) 46.

¹⁰⁰ *The Sunday Times v United Kingdom* (1979), para 87.

¹⁰¹ *Idem*, para 49.

¹⁰² *Ibid.*

¹⁰³ *Klass and Others v Germany* (1978), para 48.

¹⁰⁴ *Huvig v France* (1990), para 34 and *Kruslin v France* (1990), para 35.

¹⁰⁵ *Roman Zakharov v Russia* (2015), para 302.

¹⁰⁶ *Idem*, para 232.

Ni Loidean recognises a twofold relevance of the requirement of foreseeability in secret surveillance cases: “[f]irstly it acknowledges the inherent risks of arbitrariness involved in this area and secondly, it demands a level of transparency in the otherwise secret exercise of this power by public authorities.”¹⁰⁷ Requiring full foreseeability in regards to secret surveillance measures would impede their effectiveness and undermine their ability to effectively counter terrorist threats. Nonetheless, the Court set minimum admissible standards of foreseeability: “the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence.”¹⁰⁸

The first judgements detailing the safeguards to be included in legislations regulating secret surveillance of communications were *Huvig*¹⁰⁹ and *Kruslin*.¹¹⁰ The *Huvig* and *Kruslin* judgments concerned telephone tapping and the Court used identical wording in order to specify adequate safeguards that would legitimise the interference:

- the categories of people liable to have their telephones tapped
- the nature of the offences which may give rise to such an interception order
- limits on the duration of telephone tapping
- the procedure for drawing up the summary reports containing intercepted conversations
- the precautions to be taken in order to communicate the recordings intact and in their entirety for possible inspection by the judge
- the circumstances in which recordings may or must be erased or the tapes be destroyed, in particular where an accused has been discharged by an investigating judge or acquitted by a court.¹¹¹

The list of safeguards in *Huvig* and *Kruslin* was not exhaustive and the Court presented them as examples of safeguards. The Court repeated these safeguards in other cases that dealt with interception of communications,¹¹² which were eventually listed in *Weber and Saravia* as minimum safeguards that have to be included in

¹⁰⁷ Nora Ni Loideain, ‘Surveillance of Communications Data and Article 8 of the European Convention on Human Rights’ in: Serge Gutwirth, Ronald Leenes, Paul de Hert(eds) *Reloading Data Protection* (Springer 2014) 189.

¹⁰⁸ *Malone v United Kingdom* (1984), para 67.

¹⁰⁹ *Huvig v France* (1990), para 34.

¹¹⁰ *Kruslin v France* (1990), para 35.

¹¹¹ *Huvig v France* (1990), para 34.

¹¹² See, among others, *Valenzuela Contreras v Spain* (1998) Reports 1998-V Application no 27671/95, para 46 part (iv) and *Amann v Switzerland* (2000), para 76.

statute law¹¹³.

The development of new surveillance technologies led the Court to adapt its requirements to new surveillance modalities. In *Uzun* the Court found that GPS tracking constitutes a lesser interference with the right to privacy compared to other methods of visual or acoustical surveillance.¹¹⁴ Following *Uzun* the established safeguards in the cases of telephone tapping do not apply to all types of surveillance measures, but only to those that have similar level of interference. When the interference is substantially different, as the Court found in the specific case of GPS tracking in *Uzun*, then the safeguards are adapted to the level of interference¹¹⁵ and consequently the legality test is modified in the sense that the national law does not need to meet all six safeguards codified in *Weber and Saravia*. This will be a demanding but valuable exercise from the Court that will undoubtedly have to focus not on the type of the surveillance means but on the surveillance potential these means have. Especially in cases of mass surveillance that is based on the analysis of metadata or other indirect measures of surveillance, which – especially when combined – can lead to severe interferences with Article 8 ECHR the Court will have to justify extensively deviations from the safeguards established in *Weber and Saravia*.

When the Court finds an interference that does not fulfil the legality requirement, it does not continue in examining the rest of the requirements,¹¹⁶ which also explains the richness of case law regarding surveillance measures decided on the legality requirement. This approach of the Court, not to examine all three requirements of the three-step test, has been criticised as limiting the Court from making a full assessment of the measures in discussion.¹¹⁷ De Hert and Gutwirth “regret, but understand” the Court’s choice to examine each requirement separately, but they criticise the focus that the Court pays in its case law on the legality requirement and “and its disregard of the formal status of the legal basis that is used by the

¹¹³ *Weber and Saravia v Germany* (2006), para 95.

¹¹⁴ *Uzun v Germany* 2010 Application no 35623/05, para 52.

¹¹⁵ Antonella Galetta and Paul de Hert, *Complementing the Surveillance Law Principles of the ECtHR with its Environmental Law Principles: An Integrated Technology Approach to a Human Rights Framework for Surveillance* (2014) 10(1) *Utrecht Law Review*, 60.

¹¹⁶ Marie Helen Murphy, ‘The relationship between the European Court of Human Rights and National Legislative Bodies: Considering the Merits and the Risks of the Approach of the Court in Surveillance Cases’ (2013) 3(2) *Irish Journal of Legal Studies*, 75.

¹¹⁷ *Idem* 76, with further references to *Malone v United Kingdom* (1984), Concurring Opinion of Judge Pettiti; Paul de Hert, Serge Gutwirth, ‘Privacy, data protection and law enforcement. Opacity of the individual and transparency of power’ in Erik Claes, Antony Duff, Serge Gutwirth (eds), *Privacy and the Criminal Law* (Intersentia 2006) 63.

Member States to justify certain privacy limitations.”¹¹⁸

However, in *S. and Marper* the Court assessed whether the national legislation establishing a DNA database provided sufficient level of accessibility and foreseeability. The Court acknowledged that “[the questions are] closely related to the broader issue of whether the interference was necessary in a democratic society”¹¹⁹ and analysed them in relation to its proportionality and whether or not they strike a fair balance between the competing public and private interests.¹²⁰ In this way, the Court actually assessed the need and adequacy of the measures in a democratic society and blurred the limits in what elements of the relevant national legislation on the surveillance measure fall under each of the two requirements. Murphy welcomed this “joint consideration approach” as the Court is carrying out a full analysis of the case in question,¹²¹ while de Hert found this an intelligent manoeuvre:

“Politically speaking, it is less painful to tell a Member State that it has violated the Convention because of a problem with its legal basis than to pass the message that an initiative favoured by a Member State or accepted by a Member State is, in fact, not necessary in a democratic society.”¹²²

De Hert observed that when a case satisfies the qualitative requirements of the legality test, including the necessary safeguards, then the sufficiency of the legal safeguards is assessed again as part of the proportionality check.¹²³

Zakharov seems to bring an end to this debate, as the Court considered jointly elements from the legality and elements from the necessity test. In particular, the Court stated that it needed to ascertain “whether the domestic law is accessible and contains adequate and effective safeguards and guarantees to meet the requirements of ‘foreseeability’ and ‘necessity in a democratic society’”¹²⁴ and examined the following elements (a) the accessibility of the domestic law, (b) the scope and duration of the secret surveillance measures, (c) the procedures to be followed for storing, accessing, examining, using, communicating and destroying the intercepted data, (d) the authorisation procedures, (e) the arrangements for supervising the implementation of secret surveillance measures, and (f) any notification mechanisms and the remedies provided for by national law. This is an important development in the case law of the Court, which established a set of

¹¹⁸ Paul de Hert, Serge Gutwirth (idem) 87.

¹¹⁹ *S. and Marper v United Kingdom* 2008 Application no 30562/04 et al., para 99.

¹²⁰ *Idem*, para 118.

¹²¹ Marie Helen Murphy (n 116) 86.

¹²² Paul de Hert (n 99) 47.

¹²³ *Idem* 59.

¹²⁴ *Roman Zakharov v Russia* (2015), para 237.

minimum safeguards that need to be ensured in cases of mass surveillance. The examination of all these aspects of the national legislation in question seems to follow the example set by the CJEU in *Schrems*,¹²⁵ where the CJEU examined closely numerous aspects of the legislation in question, even if they did not seem directly related to the case in question.

The combined approach promoted in *Zakharov* allows room for detailed analysis and balancing of all the circumstances of the case when taking into account the need of the discussed surveillance measures and the level of interference that they invoke, than confining their analysis as part of the legality test. It remains to be seen whether the Court will continue using this approach in cases of secret surveillance and the pending cases are the ideal situation for the Court to prove its will to move beyond the artificial border of the requirements of the three-step test and carry out effective and strict judicial control in cases of mass surveillance.

It is an essential task of the ECtHR to find its position in the interplay of the separation of powers. Although in cases of mass surveillance and measures for national security the scope of the executive is broader, the rule of law requires effective safeguards against arbitrary interferences by the State and by intelligence services.¹²⁶ The Court recognised in its case law the need for control over the executive power and promoted as solution on the one hand the judicial control and on the other hand the strict delineation from the legislative¹²⁷: the development of a list of concrete elements in *Zakharov* that allow for thorough examination of the adequacy and the effectiveness of existing safeguards and guarantees to meet the foreseeability and necessity requirements is a clear indication of how the legislator should provide limits to the executive. As already discussed above, Judge Dedov in his concurring opinion highlighted the importance of *Zakharov* exactly in relation to the important role of the judiciary in the interplay of separation of powers in the context of secret surveillance.

The UK IPT in *10 Human Rights Organisations* examined so-called “below the water-line” arrangements that regulated the activities of the UK Intelligence Services.¹²⁸ To the extent that rules or arrangement are not disclosed, the Tribunal found that

¹²⁵ C-362/14 Maximilian Schrems v Data Protection Commissioner (2015).

¹²⁶ 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) 1(1) Utrecht Law Review, 68, 77.

¹²⁷ For a detailed analysis of the separation of powers in the case law of the ECtHR see Aikaterini Tsampi, ‘Le principe de séparation des pouvoirs dans la jurisprudence de la Cour européenne des droits de l’homme’ in A. Pedone (ed), Series : Fondation Marangopoulos pour les droits de l’Homme, (Paris 2018) [forthcoming].

¹²⁸ Judgment of 05 December 2014, [2014]UKIPTrib 13_77-H, para. 55.

“what is required is a sufficient signposting of the rules or arrangements”¹²⁹ and considered it sufficient, in the field of intelligence sharing, when “[a]ppropriate rules or arrangements exist and are publicly known and confirmed to exist, with their content sufficiently signposted, such as to give an adequate indication of it.”¹³⁰

A major challenge in the case of surveillance legislation is exactly the degree of information that needs to be publicly available in order for the accessibility and foreseeability requirements to be fulfilled. The UK IPT considered sufficient the reference in the law that further arrangements are in place regulating the specific surveillance activities, responding in this way to one of the main arguments of the applicants in *10 Human Rights Organisations* and allocated crucial importance to the element of signposting. The “signposting” element was sufficient for the UK IPT to recite in their declaration that “‘prior to the disclosures made and referred to in the Tribunal’s Judgment of 5 December 2014 and this judgment’ the Prism and/or Upstream arrangements contravened Articles 8 or 10 ECHR, but now comply.”¹³¹ The UK IPT relies on a coincidental event, the Disclosures made during the hearings of the cases following the Snowden revelations, in order to reach a dubious conclusion: the same arrangements were not justified before the Disclosures, while they are justified after them. Such an interpretation does not serve the rule of law and does not safeguard legal security, as it makes the assessment of foreseeability and accessibility dependent on random events and not on the established legal framework that regulates the activities of the intelligence services.

Despite the exerted criticism, Bernal highlighted the importance of the position of the UK IPT in *10 Human Rights Organisations*, pointing out that the UK IPT for the first time in its history upheld a complaint against the UK intelligence agencies, and that the February 2015 judgment, which was more favourable to the applicants, “should be seen as part of a much bigger trend in surveillance law – a trend that requires more transparency, more clarity, more emphasis on compliance with human rights, and an understanding of the implications of the new forms of communication and of surveillance.”¹³²

The Strasbourg Court in line with its case law, is not expected to follow this reasoning of the UK IPT. In *Liberty* the Court evaluated the provision of the UK legislation that the Secretary of State in cases of issuing a warrant for the interception of external communications was asked to “make such arrangements as he consid-

¹²⁹ *Idem*, para 41.

¹³⁰ *Ibid.*

¹³¹ Judgment of 6 February 2015, [2015] UKIPTrib 13_77-H, para. 32.

¹³² Paul Bernal, ‘Liberty and others vs. GCHQ and others’ JusletterIT, 11, <<https://ueaeprints.uea.ac.uk/60576/>> accessed 10 October 2017.

er[ed] necessary.”¹³³ As these arrangements were not contained in UK legislation, nor were they made available to the public in any other way, the Court concluded that the accessibility requirement was not met, as the domestic law did not “set out in a form accessible to the public any indication of the procedure to be followed for selecting for examination, sharing, storing and destroying intercepted material.”¹³⁴ The mere reference in a law that further arrangements will be specified in order to regulate surveillance activities can be used as a Trojan Horse to evade the scrutiny of the ECtHR on the legality requirement. At the same time, focusing on the “signposting” of such activities would water down the protection offered by the ECtHR, which has been trying, in its case law, to establish an objective set of criteria that can be used for the assessment of the accessibility and foreseeability requirements.

7. Legitimacy requirement According to Article 8(2) ECHR, lawful interferences with the right to privacy must serve one of the following legitimate purposes: national security, public safety, economic wellbeing of the country, prevention of disorder or crime, protection of health or morals, protection of the rights and freedoms of others. In the text of the Convention the legitimate aims are expressed broadly, and the Court has accepted a very broad range of legitimate purposes without requiring any additional specific terms,¹³⁵ such that the requirement has almost been converted into a mere formality and the Court examines the legitimacy of the purposes as part of the necessity test.¹³⁶ However the Court has been using the legitimacy principle “to fix the acceptability threshold of new technologies in our everyday life and to find out whether their deployment is truly against Article 8 ECHR.”¹³⁷

When assessing the interference of surveillance systems with the right to privacy, the most used legitimate aims are prevention of disorder or crime¹³⁸ and national

¹³³ *Liberty and Others v United Kingdom* (2008), para 66.

¹³⁴ *Idem*, para 69.

¹³⁵ See, among others, *Lambert v France* (1998), para 28; *Weber-Saravia v Germany* (2006), para 106; *Segerstedt-Wiberg and Others v Sweden* 2006-VII ECtHR Application no 62332/00, para 87; *S. and Marper v UK* (2008), para 100; *Kvasnica v Slovakia* 2009 ECtHR Application no 72094/01, para 82.

¹³⁶ Ian Cameron, ‘National Security and the European Convention on Human Rights’ (Kluwer Law International 2000) 35.

¹³⁷ Antonella Galetta and Paul de Hert (n 115) 71 with further reference to Thérèse Murphy and Gearóid Ó Cuinn, ‘Works in Progress: New Technologies and the European Court of Human Rights’ (2000) 10(4) *Human Rights Law Review* 618.

¹³⁸ See, among others, *Lambert v France* (1998), para 28; *S. and Marper v UK* (2008), para 100; *Kvasnica v Slovakia* (2009), para 82.

security,¹³⁹ with the latter aim being the one mostly used in cases of untargeted and mass surveillance. The broad terms in which the legitimate aims contained in Article 8(2) are expressed do not facilitate the definition of the purposes that can fall under this concept.¹⁴⁰ Furthermore, the Court never defined the scope of the term national security either and actually does not require such a definition. In *Esbester* the European Commission for Human Rights (ECmHR) stated that “the term ‘national security’ is not amenable to exhaustive definition and [considers it satisfactory when] sufficient indication is given of the scope and manner of exercise of the functions of the Security Service. (...)”¹⁴¹ In *Liberty*¹⁴² the Court relied on the definition of national security given by the British Commissioner designated under the British Interception of Communications Act of 1985.¹⁴³ In his report of 1986 the Commissioner defined threats to national security as activities: “which threaten the safety or well-being of the State, and which are intended to undermine or overthrow Parliamentary democracy by political, industrial or violent means.”¹⁴⁴ Later on, the Court again mentioned this definition in *Kennedy*¹⁴⁵ when indicating how to apply the term regarding secret surveillance activities in the UK. Under the current UK legislation, RIPA does not contain a definition of national security. However the notion of national security is found to have an expansive definition spanning from “the classic concept of direct threats (whether internal or external) to the safety of the realm but also indirect ones.”¹⁴⁶ In the pending cases the Court will analyse the concept of national security in the national context and will likely accept the activities of the UK Intelligence services as serving the purpose of national security.

8. Necessity requirement The ECHR introduces in the second paragraph of articles 8 to 11 a democratic necessity test.¹⁴⁷ The notion of “democratic society” and that of “necessity” are intrinsic elements to the test, which is

¹³⁹ See, among others, *Segerstedt-Wiberg v Sweden* (2006), para 87 and *Weber-Saravia v Germany* (2006), para 106.

¹⁴⁰ *Ian Cameron* (n 136) 36.

¹⁴¹ *Esbester v United Kingdom* (1993) Application no 18601/91.

¹⁴² *Liberty and Others v United Kingdom* (2008), para 20.

¹⁴³ The British Interception of Communications Act of 1985 was the predecessor of UK RIPA 2000.

¹⁴⁴ British Commissioner designated under the British Interception of Communications Act of 1985, Report of the UK Commissioner of 1986 under reference of *Liberty and Others v United Kingdom* 2008 Application no 58243/00, para 20.

¹⁴⁵ *Kennedy v United Kingdom* (2010), para 159.

¹⁴⁶ Eric Metcalfe, ‘Terror, reason and rights’ in Esther D. Reed et al. (eds), *Civil Liberties, National Security and Prospects for Consensus: Legal, Philosophical and Religious Perspectives* (Cambridge University Press 2012) 155.

¹⁴⁷ *Stefan Sottiaux* (n 91) 44.

satisfied when the right limitation corresponds to a pressing social need and it is proportionate to the legitimate aim pursued.¹⁴⁸ The interference will be considered lawful when it contributes to make the social interest prevail over the interests of individuals. Moreover, the interference cannot go beyond what is necessary in democratic society.¹⁴⁹ However, as was pointed out before, the Court has been reluctant in discussing what constitutes a democratic society in the context of surveillance cases.¹⁵⁰

The Court discussed extensively the necessity test in the context of *Handyside*, which dealt with the right to freedom of expression. On the use of the adjective ‘necessary’ in the French law in question, the Court found that “the adjective ‘necessary’ [...], is not synonymous with ‘indispensable’ [...], the words ‘absolutely necessary’ and ‘strictly necessary’ and [...], the phrase ‘to the extent strictly required by the exigencies of the situation’, neither has it the flexibility of such expressions as ‘admissible’, ‘ordinary’ [...], ‘useful’ [...], ‘reasonable’ [...] or ‘desirable’.”¹⁵¹ Proportionality is essential part of the necessity test. In the same case the Court clearly stated however that “it is for the national authorities to make the initial assessment of the reality of the pressing social need implied by the notion of ‘necessity’ in this context.”¹⁵²

The reasoning that the Court expressed in *Handyside*, can be found in only a few Article 8 cases. De Hert and Gutwirth acknowledge that such an interpretation of the adjective “necessary” would be “too far reaching for the European judges as regards privacy” that links necessity to proportionality.¹⁵³ They claim the Court first analysed the notion of necessity in a democratic society in relation to Article 8 in *Peck*¹⁵⁴ examining “whether, in the light of the case as a whole, the reasons adduced to justify the disclosure were ‘relevant and sufficient’ and whether the measures were proportionate to the legitimate aims pursued.”¹⁵⁵

The Court has explicitly purported that “the notion of necessity implies that the interference corresponds to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued; in determining whether an interference

¹⁴⁸ *Gillow v United Kingdom* (1986) Series A no 109 Application no 9063/80, para 55 under reference of *Leander v Sweden* (1987), para 58.

¹⁴⁹ Bernadette Rainey, Elizabeth Wicks, and Clare Ovey (n 89) 311.

¹⁵⁰ Paul de Hert, Serge Gutwirth (n 117) 92-93.

¹⁵¹ *Handyside v United Kingdom* (1976) Series A no 24 Application no 5493/72, para 48.

¹⁵² *Idem*, para 49.

¹⁵³ Paul de Hert, Serge Gutwirth (n 117) 92.

¹⁵⁴ *Ibid.*

¹⁵⁵ *Peck v United Kingdom* 2003-I Application no 44647/98, para 76 and *Silver and Others v United Kingdom* (1983) under deference of Stefan Sottiaux (n 91) 271.

is ‘necessary in a democratic society’, the Court will take into account that a margin of appreciation is left to the Contracting States [...].”¹⁵⁶ The margin of appreciation “refers to the latitude a government enjoys in valuating factual situations and in applying the provisions enumerated in the international human rights treaties.”¹⁵⁷

In *Uzun*, the Court found that “the safeguards in place to prevent a person’s total surveillance, including the principle of proportionality, were sufficient to prevent abuse.”¹⁵⁸ Murphy concludes that the Court hesitated to find unjustified interferences with Article 8 when assessing national surveillance legislation and in particular when such legislation relates to terrorist actions.¹⁵⁹ Indeed in cases of secret surveillance the Court justified an interference only when “strictly necessary” safeguards were in place:

“(...) for safeguarding democratic institutions. In practice, this means that there must be adequate and effective guarantees against abuse. The assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law.”¹⁶⁰

In *Marper* the Court made a balancing exercise between public and private interests, as part of the necessity test in order to come to the conclusion that

“(...) the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences, [...] fails to strike a fair balance between the competing public and private interests and that the respondent State has overstepped any acceptable margin of appreciation in this regard. Accordingly, the retention at issue constitutes a disproportionate interference with the applicants’ right to respect for private life and cannot be regarded as necessary in a democratic society.”¹⁶¹ (emphasis added)

Nardell commented that the Court moved beyond the examination of the legality requirements and examined the issues at stake as part of a broader issue focusing

¹⁵⁶ *Olsson v Sweden* (1988) Series A no 130 Application no 10465/83, para 67.

¹⁵⁷ Yutaka Arai-Takahashi, ‘The Margin of appreciation doctrine and the principle of proportionality in the jurisprudence of the ECHR’ (Intersentia 2002) 2.

¹⁵⁸ *Uzun v Germany* (2010), para 73.

¹⁵⁹ Maria Helen Murphy, ‘Investigative use of GPS Tracking Devices and the European Court of Human Rights’ (2012) 22(1) *Irish Criminal Law Journal*, 11.

¹⁶⁰ *Kennedy v United Kingdom* (2010), para 153.

¹⁶¹ *S. and Marper v United Kingdom* (2008), para 125.

on the assessment of the interference against the democratic society requirement, which allowed the Court to focus on sufficient evidence and find an interference with Article 8 ECHR.¹⁶² Murphy saw the Court's focus on the necessity test and the detailed approach taken by the Court in assessing the necessity requirement – examining the risks for individuals and the potential benefits of the DNA database system, taking into account societal interests and evaluating the existence of remedies - as a potential model for the assessment of surveillance cases by the Court when examining interferences with Article 8 ECHR.¹⁶³ As already discussed above, the Court in *Zakharov* actually developed and operationalized an approach in examining interferences with Article 8 in secret surveillance cases relying not only on legality, but expanding on the examination of issues pertaining to the necessity requirement.

The doctrine of the margin of appreciation, which is essential in the exercise of the democratic necessity test, indicates the level of discretion a State has in relation to the protection of the rights that are safeguarded in the ECHR. The margin of appreciation doctrine is justified as due to “their direct and continuous contact with the vital forces of their countries, State authorities are in principle in a better position than the international judge” to decide on the democratic necessity test.¹⁶⁴ According to the Court “[t]his margin is given both to the domestic legislator (“prescribed by law”) and to the bodies, judicial amongst others, that are called upon to interpret and apply the laws in force [...]”.¹⁶⁵ The application of the margin of appreciation is difficult to foresee. It changes according to the context of each case and its elements - summarized in *Silver*¹⁶⁶ - are addressed inconsistently by the jurisprudence of Court.¹⁶⁷ Given the broadness of the margin of appreciation, Galletta and de Hert nicely compare the unclear position of the Court in relation to the margin of appreciation in the context of Article 8 ECHR with “a squeeze-box device to which the proportionality principle adapts accordingly.”¹⁶⁸

The breadth of the margin of appreciation nevertheless follows some general patterns. States have a narrow margin of interest when particularly important existence or identity aspects of an individual are involved. Some examples found in case law involve the right of physical integrity, sexual freedom or the

¹⁶² Gordon Nardell (n 97) 49-50.

¹⁶³ Marie Helen Murphy (n 116) 87-88.

¹⁶⁴ David Harris, Michael O'Boyle, Edward Bates, and Carla Buckley, *Law of the European Convention on Human Rights* (3rd edn OUP 2014) 670.

¹⁶⁵ *Handyside v United Kingdom* (1976), para 48.

¹⁶⁶ *Silver and Others v United Kingdom* (1983), para 97.

¹⁶⁷ Bernadette Rainey, Elizabeth Wicks, and Clare Ovey (n 89) 326.

¹⁶⁸ Antonella Galletta and Paul de Hert (n 115) 71.

disclosure of sensitive personal data.¹⁶⁹ To the contrary, states have a wide margin of appreciation in areas where States have no common standards in respect to certain issues. This happens for instance in cases involving morals, since there is no uniform conception of morality amid the contracting states. Moreover, a wide margin of appreciation is found when it is necessary to strike a balance between public and private interests or rights contained in the ECHR,¹⁷⁰ or when national security is the issue at stake.¹⁷¹

In the area of surveillance, directed by the need of the States to safeguard public order, the legislative powers of States are not scrutinised in a strict way, enjoying a broad margin of appreciation.¹⁷² Despite the recognition of a broad margin of appreciation to the States in surveillance cases, the Court has recognised that “the risk that a system of secret surveillance in the struggle against terrorism, espionage and for the protection of national security may undermine or even destroy democracy under the cloak of defending it. Therefore the Court must be satisfied that there exist adequate and effective guarantees against abuse.”¹⁷³ In any case, “the Court dislikes “blanket” measures that apply indiscriminately to a large class of people, since these prevent a case-by-case assessment of the need for an interference: a one-size-fits-all approach to human rights needs compelling justification.”¹⁷⁴ This approach was reinforced in *Zakharov* where the Court clearly recognised that “the risk of abuse [...] is inherent in any system of secret surveillance, and [...] is particularly high in a system where the secret services and the police have direct access, by technical means, to all mobile telephone communications.”¹⁷⁵

¹⁶⁹ *X and Y v Netherlands* (1985) Reports 1997-II Application no 21830/93 and *Z v Finland* (1998) Reports 1997-I Application no 22009/93 under reference of Bernadette Raaney, Elizabeth Wicks, and Clare Ovey (n 89) 326.

¹⁷⁰ *Taşkin and Others v Turkey* (2004) Reports 2004-X Application no 46117/99, para 119; *Giacomelli v Italy* (2006) Reports 2006-XII Application no 59909/00, para 83; *Hardy and Maile v United Kingdom* 2012 Application no 31965/07, para 221 under reference of Antonella Galetta and Paul de Hert (n 115) 71.

¹⁷¹ *Weber and Saravia v Germany* (2006), para 104.

¹⁷² Elisabet Fura and Mark Klamberg, ‘The Chilling Effect of Counter-Terrorism Measures: A Comparative Analysis of Electronic Surveillance Laws in Europe and the USA’ in Josep Casadevall, Egbert Myjer, Michael O’Boyle (eds), *Freedom of Expression – Essays in honour of Nicolas Bratza – President of the European Court of Human Rights* (Wolf Legal Publishers 2012) 472 and Paul de Hert (n 126) 72 citing: *Klass and Others v Germany* (1978), para 59; *Leander v Sweden* (1987), para 59; *L. v. Norway* (1990) Application No. 13564/88; *Esbester v United Kingdom* (1993); *Christie v United Kingdom* (1994) Application no 21482/93.

¹⁷³ *Elisabet Fura and Mark Klamberg (idem)* 472-473, with reference to *Klass and others v Germany* (1978) paras 49-50; *Leander v Sweden* (1987) para 60; *Weber-Saravia v Germany* (2006), paras 106 and 116-118.

¹⁷⁴ *Gordon Nardell* (n 97) with further references to, among others, *Handyside v United Kingdom* (1976); *Hirst v United Kingdom (No. 2)* (2005) Reports 2005-IX Application No. 74025/01.

¹⁷⁵ *Roman Zakharov v Russia* (2015), para 302.

In *Szabó and Vissy* the Court elaborated on the democratic necessity test taking into account the use of modern technological developments and provided a detailed interpretation that will play a crucial role in the future case law of the Court:

“(…) given the particular character of the interference in question and the potential of cutting-edge surveillance technologies to invade citizens’ privacy, the Court considers that the requirement “necessary in a democratic society” must be interpreted in this context as requiring “strict necessity” in two aspects. A measure of secret surveillance can be found as being in compliance with the Convention only if it is strictly necessary, **as a general consideration**, for the safeguarding the democratic institutions and, moreover, if it is strictly necessary, **as a particular consideration**, for the obtaining of **vital intelligence in an individual operation**.”¹⁷⁶ (emphasis added)

This new criterion will raise a barrier to common practices of law enforcement authorities and intelligence services to group people, as they are now clearly required to examine the conditions for interception of communications on a case by case basis, which in the eyes of the Court “is only in this way that the need for safeguards to ensure that emergency measures are used sparingly and only in duly justified cases can be satisfied.”¹⁷⁷ This requirement that secret surveillance measures should be strictly necessary in order to collect “vital” intelligence in a specific operation will most likely render incompatible with Article 8 standard operations of surveillance authorities and will be practically impossible to be complied with in cases of algorithmic surveillance.

As already discussed above, in *Zakharov* the Court made a combined examination of elements pertaining to the legality and the necessity requirements, establishing a list of six elements that are crucial for the assessment of measures of secret surveillance in view of the fact that “a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it.”¹⁷⁸

The oversight of surveillance measures is an essential element in the exercise of the proportionality test in the context of the democratic necessity requirement when balancing the rights of the individual and the needs of a democratic society.¹⁷⁹ The ECtHR has dealt with the issue of oversight in the context of surveillance activities in various countries and in the UK in particular, identifying three stages during surveillance activities, when “review and supervision of secret surveillance

¹⁷⁶ *Szabó and Vissy v Hungary* (2016), para 73.

¹⁷⁷ *Ibid*, citing *Roman Zakharov v Russia* (2015), para 266.

¹⁷⁸ *Roman Zakharov v Russia* (2015), para 232.

¹⁷⁹ *Klass and Others v Germany* (1978), para 59.

measures may come into place”¹⁸⁰: (a) when the surveillance is first ordered, (b) while it is being carried out, or (c) after it has been terminated. The issues of oversight in relation to these three stages are comprehensively discussed in *Zakharov*:

“As regards the first two stages, the very nature and logic of secret surveillance dictate that not only the surveillance itself but also the accompanying review should be effected without the individual’s knowledge. Consequently, since the individual will necessarily be prevented from seeking an effective remedy of his or her own accord or from taking a direct part in any review proceedings, it is essential that **the procedures established should themselves provide adequate and equivalent guarantees safeguarding his or her rights**. In addition, the values of a democratic society must be followed as faithfully as possible in the supervisory procedures if the bounds of necessity, within the meaning of Article 8 § 2, are not to be exceeded. In a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge, judicial control offering the best guarantees of independence, impartiality and a proper procedure [...]. As regards the third stage, **after the surveillance has been terminated**, the question of **subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies** before the courts and hence to the existence of effective safeguards against the abuse of monitoring powers. There is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively [...] or, in the alternative, unless any person who suspects that his or her communications are being or have been intercepted can apply to courts, so that the courts’ jurisdiction does not depend on notification to the interception subject that there has been an interception of his communications (...).”¹⁸¹ (emphasis added)

It has been thus established case law of the ECtHR that the notification of interception of communications is “inextricably linked to the effectiveness of remedies before the courts”¹⁸² and that the persons concerned should be informed “[a]s soon as notification can be carried out without jeopardising the purpose of the restriction after the termination of the surveillance measure.”¹⁸³ In *Telegraaf Media v. The Netherlands* the Court clearly established the requirement for prior over-

¹⁸⁰ Roman Zakharov v Russia (2015), para 233.

¹⁸¹ Idem, paras 233-234.

¹⁸² See among others Roman Zakharov v Russia (2015), para 234.

¹⁸³ Idem, para 287 with reference to *Klass and Others v Germany* (1978), para 58 and *Weber and Saravia v Germany* (2006), para 135. Similar reflections were made by the Court in *Szabó and Vissy v Hungary* (2016), para 86.

sight, as a rule.¹⁸⁴

The ECtHR has taken the position that the oversight of surveillance authorities should in principle be entrusted to a judge. However in *Klass* recognised that sufficient guarantees existed in the oversight scheme, even if there was no judicial control in place, paying special attention to the independence of the supervisory authorities.¹⁸⁵ When the ECtHR examined the same legislation in the context of *Weber and Saravia*, it found that the supervision system, which had remained unchanged in the legislation, was “such as to keep the interference resulting from the contested legislation to what was “necessary in a democratic society”.”¹⁸⁶ In *Zakharov* the Court summarised its established case law on the issue of independence of the supervisory authorities:

“As to the independence requirement, in previous cases the Court has taken into account the manner of appointment and the legal status of the members of the supervisory body. In particular, it found sufficiently independent the bodies composed of members of parliament of both the majority and the opposition, or of persons qualified to hold judicial office, appointed either by parliament or by the Prime Minister (...). In contrast, a Minister of Internal Affairs – who not only was a political appointee and a member of the executive, but was directly involved in the commissioning of special means of surveillance – was found to be insufficiently independent (...). Similarly, a Prosecutor General and competent lower-level prosecutors were also found to be insufficiently independent (...).”¹⁸⁷

Of particular importance for the pending cases in front of the Court, is the analysis of the UK oversight regime in *Kennedy*. The Court found that the oversight exercised by the Interception of Communications Commissioner for the interception of internal communications, along with the scrutiny of the UK IPT provide sufficient safeguards against abuse, although there was no supervisory control by a judge:

“(...) it is in principle desirable to entrust supervisory control to a judge (...). In the present case, the Court highlights the **extensive jurisdiction of the IPT** to examine any complaint of unlawful interception. Unlike in many other domestic systems (...) any person who suspects that his communications have been or are being intercepted may apply to the IPT (...). The **jurisdiction of the IPT does not, therefore, depend on notification** to the interception subject that

¹⁸⁴ *Telegraaf Media Nederland Landelijke Media B.V. and Others v the Netherlands* (2013) Application no 39315/06, paras 100-101.

¹⁸⁵ *Klass and Others v Germany* (1978), para 56.

¹⁸⁶ *Weber and Saravia v Germany* (2006), para 117.

¹⁸⁷ *Roman Zakharov v Russia* (2015), para 278.

there has been an interception of his communications. The Court emphasises that the IPT is an independent and impartial body, which has adopted its own rules of procedure. The members of the tribunal must hold or have held high judicial office or be experienced lawyers (...). In undertaking its examination of complaints by individuals, the IPT has access to closed material and has the power to require the Commissioner to provide it with any assistance it thinks fit and the power to order disclosure by those involved in the authorisation and execution of a warrant of all documents it considers relevant (...). In the event that the IPT finds in the applicant's favour, it can, *inter alia*, quash any interception order, require destruction of intercept material and order compensation to be paid (...). The publication of the IPT's legal rulings further enhances the level of scrutiny afforded to secret surveillance activities in the United Kingdom (...)."¹⁸⁸ (emphasis added)

In addition to the UK IPT, the oversight in the UK is realised via the Interception of Communications Commissioner. The Commissioner has the task to oversee the general functioning of the surveillance regime and the authorisation of interception warrants in specific cases in the UK. With regard to the role and responsibilities of the Interception of Communications Commissioner the Court made specific statements to support its position that the oversight system was in accordance with Article 8 ECHR:

"The Court notes that the Commissioner is **independent of the executive and the legislature and is a person who holds or has held high judicial office** [...]. He **reports annually** to the Prime Minister and his report is a public document (subject to the non-disclosure of confidential annexes, which is laid before Parliament [...]. In undertaking his review of surveillance practices, he has **access to all relevant documents**, including closed materials and all those involved in interception activities have a duty to disclose to him any material he requires [...]. The obligation on intercepting agencies to keep records ensures that the Commissioner has effective access to details of surveillance activities undertaken. The Court further notes that, in practice, the Commissioner reviews, provides advice on and approves the section 15 arrangements [...]. The Court considers that the Commissioner's role in ensuring that the provisions of RIPA and the Code are observed and applied correctly is of particular value and his biannual review of a random selection of specific cases in which interception has been authorised provides an important control of the activities of the intercepting agencies and of the Secretary of State himself."¹⁸⁹ (emphasis added)

¹⁸⁸ Kennedy v United Kingdom (2010), para 167.

¹⁸⁹ Idem 166.

However, in light of the establishment of strict requirements in relation to oversight in *Zakharov* it is questionable whether the Court will repeat the position it took in *Kennedy*. In *Zakharov* the Court established a requirement that sufficient information should be kept about the surveillance measures taken in order for the supervising authorities to be able to assess their legitimacy.¹⁹⁰ Moreover in *Zakharov* the ECtHR reiterated its position in previous cases on “whether the supervisory body’s activities are open to public scrutiny”,¹⁹¹ which is an essential feature to guarantee independent and effective supervision. The Court further examined in detail the competences and powers vested to the prosecutor, who according to the Russian legislation is may exercise supervision over operational-search activities. The ECtHR repeated his position that “it is essential that the supervisory body has access to all relevant documents, including closed materials and that all those involved in interception activities have a duty to disclose to it any material it required”¹⁹². The Court came to the conclusion that the scope of supervision of the Russian prosecutors was limited due to the fact that “information about the security services’ undercover agents, and about the tactics, methods and means used by them, [was] outside the scope of prosecutors’ supervision. (...) Moreover, surveillance measures related to counter-intelligence de facto escape supervision by prosecutors.”¹⁹³

One month after *Zakharov*, the Court in *Szabó and Vissy* repeated that “control by an independent body, normally a judge with special expertise, should be the rule and substitute solutions the exception, warranting close scrutiny”¹⁹⁴ and criticised oversight systems that are not entrusted in the hands of a judge, declaring in the specific case that “supervision by a politically responsible member of the executive, such as the Minister of Justice, does not provide the necessary guarantees.”¹⁹⁵ The Court in *Szabó and Vissy* seems to be taking a stricter approach on what should be considered as effective oversight systems, as it seems to imply that an “official qualified for judicial office”¹⁹⁶ should be involved. Malgieri and De Hert concluded that the clear preferences of Court in *Szabó and Vissy* towards a judicial oversight system, should in any case be supplemented with a reality check.¹⁹⁷

¹⁹⁰ Roman Zakharov v Russia (2015), para 272.

¹⁹¹ Idem, para 283.

¹⁹² Idem, para 281, citing Kennedy v United Kingdom (2010), para 166.

¹⁹³ Ibid.

¹⁹⁴ Szabó and Vissy v Hungary (2016), para 77.

¹⁹⁵ Ibid.

¹⁹⁶ Idem, para 85.

¹⁹⁷ Gianclaudio Malgieri and Paul De Hert, ‘European Human Rights, Criminal Surveillance, and Intelligence Surveillance: Towards ‘Good Enough’ Oversight, Preferably But Not Necessarily by Judges’ in David Gray and Stephen Henderson (eds), Cambridge Handbook of Surveillance Law (Cambridge University Press 2017), 528.

A crucial issue that will be examined by the ECtHR in the pending cases is the issue of effective oversight of the activities of the UK intelligence agencies and whether the system already in place in the UK is adequate to ensure the safeguarding of the human rights of individuals. Despite the Court's ruling in *Kennedy*, in light of the detailed requirements relating to oversight in *Zakharov*, I expect the Court to find

the oversight regime of the UK in the pending cases as not solid and not meeting the necessity requirement, especially as the Interception of Communications Commissioner has no power to prohibit or quash an interception warrant¹⁹⁸. Georgieva claims that the Snowden revelations undoubtedly illustrate that the UK oversight regime was not able to “check the growth of NSA or GCHQ employees and contractors who use the monitoring systems to spy on and control their own personal affairs” and therefore it does not provide for “real safeguards against abuse.”¹⁹⁹ This reality check can be an additional ground for the Court to find that the UK oversight regime does not pass the democratic necessity test.

9. A tale of two courts revisited While the Strasbourg Court has been developing its case law on secret surveillance, especially in *Zakharov* and *Szabó and Vissy*, the CJEU has been also active in dealing with cases relating to surveillance and data retention, delivering seminal cases that establish strong safeguards for the protection of privacy and personal data of individuals. In *Digital Rights Ireland* the CJEU found that several provisions of the Data Retention Directive were not respecting the proportionality principle, in light of Articles 7 (right to respect for private and family life), 8 (right to protection of personal data) and 52(1) of the Charter of Fundamental Rights of the European Union (CFR)²⁰⁰.²⁰¹ Two years later the CJEU dealt again with data retention in *Tele2/Watson*,

¹⁹⁸ RIPA does not provide the Interception of Communications Commissioner with any power to quash an interception warrant. See on this issue a.o. Bingham Centre for the Rule of Law, ‘The Investigatory Powers Review by the Independent Reviewer of Terrorism Legislation’ (November 2014), 22 < https://www.biicl.org/documents/399_bingham_centre_submission_to_investigatory_powers_review_final_2014-11-19.pdf?showdocument=1 > accessed 18 November 2017.

¹⁹⁹ Iliana Georgieva (n 96) 118.

²⁰⁰ Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, p. 391–407. The CFR recognises two distinct rights, the right to respect for private and family life (commonly referred to as the right to privacy) in Article 7 and the right to protection of personal data in Article 8.

²⁰¹ Case C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and others* [2014] *Digital Rights Ireland and Seitlinger and others* ECLI:EU:C:2014:238, para 69.

examining Article 15(1) of the ePrivacy Directive²⁰² that facilitates the retention of data under specific conditions, and the choices of the national legislators in the UK and Sweden. In this judgment, the CJEU stayed close to *Digital Rights Ireland* and established safeguards for the protection and security of traffic and location data. In both *Digital Rights Ireland* and in *Tele2/Watson* the CJEU, criticised the retention of and access to retained data of individuals for whom there is “no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious criminal offences”²⁰³, as well as the lack of “any relationship between the data whose retention is provided for and a threat to public security.”²⁰⁴ In *Digital Rights Ireland*, and similarly later in *Tele2/Watson* the CJEU relied on the principle of proportionality in order to examine the limitations that can be posed on the rights to privacy and data protection.²⁰⁵

In 2015 the CJEU delivered one more seminal judgment in the *Schrems* case. In *Schrems*²⁰⁶ the CJEU was asked to interpret some of the provisions of the Data Protection Directive regarding the transfers of data to third countries and to examine the validity of the Commission Decision on the Safe Harbour Principles.²⁰⁷ In *Schrems* the CJEU went beyond *Digital Rights Ireland* and condemned “legislation permitting the public authorities to have access on a generalised basis to the

²⁰² Article 15(1) of Directive 2002/58, as amended, reads as follows: “Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. 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. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union”: European Parliament and the Council of the European Union, Directive 2002/58/EC 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 (31.07.2002).

²⁰³ C-203/15 and C-698/15 *Tele2/Watson* (2016) ECLI:EU:C:2016:970, para 105, referring also to C-293/12 and C-594/12 *Digital Rights Ireland* (2014), paras 57-58.

²⁰⁴ C-293/12 and C-594/12 *Digital Rights Ireland* (2014), para 59; C-203/15 and C-698/15 *Tele2/Watson* (2016), para 106.

²⁰⁵ C-293/12 and C-594/12 *Digital Rights Ireland* (2014), paras 45 and 69; C-203/15 and C-698/15 *Tele2/Watson* (2016), para 94.

²⁰⁶ C-362/14 *Maximilian Schrems* (2015).

²⁰⁷ Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46 on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (OJ 2000 L 215, p. 7)

content of electronic communications [...] as compromising the **essence** of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter” (emphasis added).²⁰⁸ The CJEU criticised also the lack of effective remedies as not respecting the **essence** of the right to effective judicial review, which is intrinsically linked to the rule of law.²⁰⁹

Since the CJEU started dealing with human rights cases, it has traditionally been referring to the case law of the ECtHR.²¹⁰ The CJEU in its judgments made extensive reference to the established Article 8 case law of the ECtHR, recognising that the access of competent national authorities to data constitute an interference with the fundamental right to privacy²¹¹, which can be justified depending on the particular circumstances. However, the European legislation should put in place minimum safeguards to guarantee effective protection against the risk of abuse and unlawful access and use of data.²¹² The CJEU has recognised a greater need to establish such safeguards when the processing of data is subjected to automatic processing, a statement with great importance in mass surveillance cases²¹³, where data processing is relying highly on processing based on sophisticated automatic means.

In the recent cases relating to surveillance and national security the CJEU and the ECtHR have been looking closer at each others judgments making cross references in crucial points. In particular in relation to oversight for accessing data, the CJEU in *Tele2/Watson* referred to the safeguards established in *Szabó and Vissy*.²¹⁴ In *Zakharov* the ECtHR required that courts should have the possibility to verify “the existence of a reasonable suspicion against the person concerned, in particular, whether there are factual indications for suspecting that person of planning, committing or having committed criminal acts or other acts that may give rise to secret surveillance measures, such as, for example, acts endangering national security.”²¹⁵ The CJEU relied on this reasoning and made analogous reflections in the context of data retention.

However, the positions of the two Courts have not been completely aligned at all

²⁰⁸ C-362/14 Maximilian Schrems (2015), para 94.

²⁰⁹ *Idem*, para 95.

²¹⁰ Sionaidh Douglas-Scott, ‘A Tale of Two Courts: Luxembourg, Strasbourg and the Growing European Human Rights Acquis’ (2006)43 *Common Market Law Review* 629 ff.

²¹¹ C-293/12 and C-594/12 *Digital Rights Ireland* (2014), para 35.

²¹² *Idem*, para 54; C-362/14 Maximilian Schrems (2015), para 91.

²¹³ C-293/12 and C-594/12 *Digital Rights Ireland* (2014), para 55; C-362/14 Maximilian Schrems (2015), para 91.

²¹⁴ C-203/15 and C-698/15 *Tele2/Watson* (2016), para 120.

²¹⁵ *Roman Zakharov v Russia* (2015), para 260.

points. In *Tele2/Watson* the CJEU found that general access to all retained data goes beyond what is strictly necessary and recognised that access to retained data can “as a general rule, be granted, in relation to the objective of fighting crime, only to the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime”,²¹⁶ citing *Zakharov*. Nevertheless the CJEU recognised that terrorist threats may justify deviations from this rule and authorise access to data of persons for which there is no direct link to a (prospective or committed) crime “where there is objective evidence from which it can be deduced that that data might, in a specific case, make an effective contribution to combating such activities.”²¹⁷ The exception, thus, established by the CJEU has a limited nature and is applicable under specific circumstances. In *Szabó and Vissy* the Court did not require such reasonable suspicion to exist, but rather referred to individual suspicion, an issue that was criticised by Judge Pinto de Albuquerque in his concurring opinion.²¹⁸ The approach of both the ECtHR and the CJEU seems to suggest that bulk surveillance is not compliant with the existing safeguards and activities such as the ones under examination in the three ECtHR pending cases against the UK will not meet the requirements of the Courts.

The issue of notification of the affected individuals was crucial in *Tele2/Watson* and the CJEU stated that “the competent national authorities to whom access to the retained data has been granted must notify the persons affected, under the applicable national procedures, as soon as that notification is no longer liable to jeopardise the investigations being undertaken by those authorities.”²¹⁹

In October 2017 the UK IPT in the context of *Privacy International v Secretary of State for Foreign and Commonwealth Affairs*²²⁰, which deals with the acquisition and use of bulk communications data by the UK intelligence agencies, sent a request for a preliminary ruling to the CJEU.²²¹ In its September 2017 judgment²²² the UK IPT acknowledged the notification requirement established in *Tele2/Watson*, finding it however to “be very damaging to national security.”²²³ The UK IPT recognised that the notification requirements would be difficult to enforce in relation to bulk

²¹⁶ C-203/15 and C-698/15 *Tele2/Watson* (2016), para 119.

²¹⁷ *Ibid.*

²¹⁸ *Szabó and Vissy v Hungary* (2016), Concurring Opinion Judge Pinto de Albuquerque, para 20.

²¹⁹ C-203/15 and C-698/15 *Tele2/Watson* (2016), para 121.

²²⁰ Case [2016-2017] UKIPTrib IPT_15_110_CH

²²¹ Order for reference to the Court of Justice of the European Union issued in case [2017] UKIPTrib IPT_15_110_CH <<http://www.ipt-uk.com/docs/IPT%20BULK%20DATA%20ORDER%20FOR%20REFERENCE%20TO%20CJEU.pdf>> accessed 18 November 2017.

²²² Judgment of 8 September 2017 [2017] UKIPTrib IPT_15_110_CH.

²²³ *Idem*, para 63.

data and wondered on its practical implantation.²²⁴ The UK IPT has sent a request for preliminary ruling to the CJEU in the context of the case in question and therefore the CJEU will have to clarify its position on the limits, if any, of the notification requirement. The CJEU will have to provide an answer with regard to the notification requirement in relation to bulk data and provide further guidance compared to the jurisprudence of the ECtHR on notification, which requires that “[a]s soon as notification can be carried out without jeopardising the purpose of the restriction after the termination of the surveillance measure, information should be provided to the persons concerned.”²²⁵

In this case, the CJEU will have the opportunity to discuss the application of the requirements it developed in *Telet/Watson* and the safeguards established by the ECtHR and to reflect on the upcoming judgment of the ECtHR on the secret surveillance activities of the UK intelligence agencies. The CJEU is explicitly requested to answer the question “how and to what extent do those requirements apply, taking into account the essential necessity of the SIAs [Security and Intelligence Agencies] to use bulk acquisition and automated processing techniques to protect national security and the extent to which such capabilities, if otherwise compliant with the ECHR, may be critically impeded by the imposition of such requirements.”²²⁶ In essence, this request for a preliminary ruling raises a challenge for the CJEU that will have to clearly take a position towards the stance of the ECtHR in surveillance cases. Will the two Courts align their positions in the UK bulk surveillance cases or will they establish each their own system of requirements? The cross-references between the case law of the two Courts in the last cases relating to secret surveillance allows me to hope that the two Courts will join their forces and will deliver coherent judgments that will establish a robust system of checks and balances in cases of secret surveillance. It should be borne in mind that Article 52(3) CFR requires that “In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection.”²²⁷ This provision facilitates the CJEU to interpret the relevant European legislation in line with the case law of

²²⁴ *Idem*, para 64.

²²⁵ *Roman Zakharov v Russia* (2015), para 287, with reference to *Klass and Others v Germany* (1978), para 58 and *Weber and Saravia v Germany* (2006), para 135. Similar reflections were made by the Court in *Szabó and Vissy v Hungary* (2016), para 86.

²²⁶ Order for reference to the Court of Justice of the European Union issued in case [2017] UKIPTrib IPT_15_110_CH, 22.

²²⁷ Article 52(3) EU Charter of Fundamental Rights.

the ECtHR and could be the basis for judicial cross-fertilisation.²²⁸

10. Conclusions and further research Secret and intelligence authorities have powers to carry out surveillance and one cannot but recognise the important role they play in safeguarding national security and fighting serious crime and terrorism. The employment of secret surveillance measures by these authorities is essential for their activities in collecting intelligence and protecting national security. As often recognised by the ECtHR the executive has broad powers in the context of secret surveillance exactly due to the nature of their operations and the states enjoy a wide margin of appreciation when national security is the issue at stake.²²⁹

Despite the fact that states have a broad margin of appreciation in surveillance cases and that secret surveillance programmes do not constitute a violation of the right to privacy of citizens in and of themselves, it goes without saying that they should abide by a strict system of checks and balances. The legislator provides for specific requirements in secret surveillance legislation, and the judiciary is called to assess the compliance of these requirements with the legitimacy, legality and necessity requirements, as stipulated in Article 8(2) ECHR.

Lest we were lulled into a false sense of security with respect to the protection of right to privacy, the Court felt it imperative to underline that secret surveillance measures entail a risk and “may undermine or even destroy democracy under the cloak of defending it”,²³⁰ which was reinforced recently with the crystal clear message that “the risk of abuse [...] is inherent in any system of secret surveillance, and [...] is particularly high in a system where the secret services and the police have direct access, by technical means, to all mobile telephone communications”²³¹. In addition, the Court underscored the dangers that the use of cutting-edge surveillance technologies entails for the privacy of citizens.

The Court has been reluctant to accept *in abstracto* claims. However, *Zakharov* marks a turning point in the case law of the Court in this respect, as the Court decided to examine the domestic legislation *in abstracto* and make a thorough analysis.

²²⁸ “These provisions may constitute a sound basis to interpret EU law in accordance with the model of protection underlying the ECHR”: Oreste Pollicino and Marco Bassini ‘Bridge is down, data truck cannot get through...-A critical view of the Schrems judgment in the context of European constitutionalism’ in Giuliana Ziccardi Capaldo (ed), *The global community - Yearbook of International Law and Jurisprudence* (Oxford University Press 2016) 260.

²²⁹ *Weber and Saravia v Germany* (2006), para 104.

²³⁰ *Elisabet Fura and Mark Klamberg* (n 172) 472-473.

²³¹ *Roman Zakharov v Russia* (2015), para 302.

Judge Dedov in his concurring opinion characterised this choice of the Court as an issue that raises questions as to the separation of powers between the legislature, executed by the Parliamentary Assembly of the Council of Europe and the judiciary, represented by the Court.²³² Judge Dedov stated that “the examination of a case *in abstracto* is similar to an expert report, but not to a judgment.”²³³ Nevertheless, he voted for the admissibility of the case, seeing the judgement of the Grand Chamber as an opportunity to reinforce the role of courts in society. When the legislative is not providing sufficient and effective guarantees against abuse and the executive is taking advantage of the legal regime in order to carry out secret surveillance overstepping its powers, then it is a responsibility of the judiciary to intervene and contribute in a twofold way: by establishing the safeguards that need to be put in place in order to ensure that the legal framework in question is compatible with the human rights framework and ensuring effective protection of the individuals, while at the same time limiting the powers of the executive. The new role vested in the Court, by opening up the examination of domestic legislation relating to secret surveillance *in abstracto*, as carried out in both *Zakharov* and *Szabó and Vissy* brings in its reasoning terms and approaches that are similar to the ones employed by a constitutional court.

The three pending cases on mass secret surveillance conducted by the UK intelligence agencies, which have been central to in this inaugural address, are an example of the interplay between modern technological surveillance capabilities and the excessive dangers that they bring against the protection of human rights and in particular of the right to privacy. These dangers are accentuated by the extensive use of big data analytics and modern surveillance techniques, which provide intelligence and surveillance authorities the capabilities to use sophisticated surveillance techniques. Algorithms offer security and intelligence services the possibility to collect and process vast amounts of data, facilitating new ways of surveillance. The above described situation has generated a great interest in these cases on the part of the public, a fact illustrated not only by the extensive coverage in the press, but also by the high number of organisation to which the Court granted leave to intervene in the written proceedings as third parties.

The galloping developments in the technical capabilities of carrying out surveillance are bound to have a reflective impact on the protection of human rights. Does it suffice to refine the existing guarantees in order to meet the challenges brought by technological developments, such as algorithmic surveillance, or should we completely rethink the system of checks and balances that guarantees the protection of human rights?

²³² The issue of separation of powers within the Council of Europe and the role of the Court in this context is an important one, albeit it falls outside the scope of this inaugural address.

²³³ *Roman Zakharov v Russia* (2015), Concurring opinion of Judge Dedov.

The ECtHR in *Szabó and Vissy* acknowledged that the possibility of governments “to acquire a detailed profile [...] of the most intimate aspects of citizens’ lives may result in particularly invasive interferences with private life. [...] This threat to privacy must be subjected to very close scrutiny both on the domestic level and under the Convention. The guarantees required by the extant Convention case-law on interceptions need to be enhanced so as to address the issue of such surveillance practices.”²³⁴ The Court in *Szabó and Vissy* did not have to carry out such scrutiny, as the guarantees of the Hungarian legislation in question failed to meet the established criteria of the ECtHR. However, the Court highlighted the need for further enhancement of the established safeguards given the technological possibilities that facilitate surveillance. Algorithmic surveillance facilitates the aggregation of data, as well as the creation of detailed profiles and expands the surveillance assemblage.²³⁵

The ECtHR in its case law has traditionally linked the principle of foreseeability to clear information in the interception warrant, which would be reviewed by an oversight authority, in principle entrusted to a judge. For example in *Weber*, the use of catchwords was extensively discussed as a monitoring method that was foreseen in the German law²³⁶. However, algorithmic surveillance, surveillance that relies on the use of algorithms and employs machine-learning techniques, does not allow either the law itself or a warrant stipulating the surveillance to specify the surveillance methods in detail. Especially in relation to mass surveillance measures the patterns are not predetermined, but they are technologically inferred during the processing. Modern surveillance techniques are often not focusing on one individual, but are interested in groups of individuals, categorised on the basis of various criteria. It is therefore a great challenge for the Court to reassess its views on foreseeability so that the requirement adapts to the technological developments and balance the needs of security and intelligence services against the protection of human rights of individuals.

Algorithmic surveillance gives rise to one additional challenge to the Court, as it creates groups, whose rights need to be protected. Traditionally the Court required reasonable likelihood for an individual to claim the status of a victim. In *Zakharov* the Court adopted a broad interpretation of the admissibility criteria. It discussed the issue of effective remedies, which has traditionally been examined under the auspices of admissibility in its case law, as an issue pertaining actually to the merits of the case, making it difficult for mass surveillance cases to be rendered inad-

²³⁴ *Szabó and Vissy v Hungary* (2016), para 70.

²³⁵ Maria Helen Murphy, ‘Algorithmic surveillance: the collection conundrum’ (2017) 31 *Int’l Rev L Computers & Tech* 225

²³⁶ *Weber and Saravia v Germany* (2006), para 32.

missible.²³⁷ Nevertheless the nature of mass algorithmic surveillance is such that opens a number of questions in relation to the protection of groups that are generated based on the algorithmic computations. Will the focus of protection remain with the individual or will new approaches be developed in the regulation of human rights protecting groups of people?

Building on its recent case law and on the case law of the CJEU on blanket retention and surveillance cases, the ECtHR is presented with a unique opportunity to make a thorough assessment not only of the legality requirement, but also to carry out an extensive scrutiny of the necessity requirement and provide detailed guidance on the exercise balancing the various interests at stake and applying the proportionality principle. In *Szabó and Vissy* the Court established a double necessity standard for secret surveillances measures, both as a general consideration for the safeguarding of democratic institutions and as a particular consideration, for the obtaining of vital intelligence in an individual operation.²³⁸ It will be almost impossible for surveillance authorities to meet these strict necessity criteria especially in cases of algorithmic surveillance, a challenge that the ECtHR will need to tackle. The Court is confronted with a big dilemma: how to protect human rights in an era when secret surveillance capabilities are expanding through technological developments, facilitating new and invasive surveillance methods? Will the Court remain close to the strict necessity criterion of *Szabó and Vissy* rendering algorithmic surveillance as violating human rights *per se*?

Before *Zakharov*, van der Sloot was pessimistic as to the admissibility and the outcome of the Big Brother Watch and others.²³⁹ The Court's recent case law makes me more optimistic that it will uphold its role as the guardian of human rights in Europe and will adjudge and declare that the interference with Article 8 is not justified, while at the same time providing sufficient arguments both in relation to the legality, as well as to the necessity requirement.

The thorough analysis of the case law of the ECtHR illustrated that in cases with relevance to national security, as are surveillance cases, the standards for the examination of the accessibility and foreseeability of the relevant law are different compared to situations where national security is not at stake. The challenge for the Strasbourg Court is to elaborate on the building blocks it has already devised in surveillance cases and to tackle the perils of modern surveillance technologies in order to consolidate a solid framework based on which it assesses the accessibility and foreseeability of secret surveillance regimes. In this respect *Zakharov* "set

²³⁷ Lorna Woods, 'Introductory note to *Zakharov v Russia* (Eur.CT.H.R.)' (2016) 55 ILM 208.

²³⁸ *Szabó and Vissy v Hungary* (2016), para 73.

²³⁹ Bart van der Sloot, 'Privacy in the Post-NSA Era: Time for a Fundamental Revision?' (2014) 5 JIP-ITEC, 9-10.

the European standard on mass surveillance for intelligence and national security purposes.”²⁴⁰

This inaugural address focused on the analysis of the right to privacy and its justified limitations, as stipulated in Article 8 ECHR and as interpreted in the case law of the Court, in relation to secret surveillance. I discussed the circumstances of the pending cases against the activities of the UK intelligence agencies as an example of the interplay between modern technological surveillance capabilities and the dangers that they bring against human rights, in order to illustrate the crucial need for further research in the area of surveillance and human rights, which I intend to undertake in my role as Chair of Technology Law and Human Rights. For the purposes of this inaugural address and given the current stage of my research, I focused on the analysis of Article 8 ECHR in relation to mass secret surveillance. In order to build a comprehensive framework of checks and balances for human rights in the era of mass secret surveillance, however, I intend to study further the right to freedom of expression, the right to non-discrimination and right to effective remedies.

Despite the perils that model techniques of secret surveillance bring for human rights, it is not all bleak. The rising awareness of the public and the legislative and judicial reactions both at the domestic and at the international level to the Snowden revelations fill me with a degree of optimism and a sense of duty to contribute in my own humble way and in my role as Chair of Technology Law and Human Rights in the safeguarding of human rights and the right of privacy in the digital era.

²⁴⁰ Szabó and Vissy v Hungary (2016), Concurring Opinion Judge Pinto de Albuquerque, para 1.

Acknowledgments

Acknowledgments Most of the people that know me have probably heard me say at some point that my life is a path full of amazing coincidences and marvellous people. From this podium I would like to thank some of these people, apologising in advance to anyone that I unintentionally fail to include. I owe my interest in law and technology to Prof. Lilian Mitrou, who –a century ago- made our evening classes in the old building on Asklipiou Street brighter with her lectures. Thank you, Lilian, for stimulating me to continue my studies abroad. My path then led me to Hannover, where I met Prof. Nikolaus Forgó, who never ceased to amaze me when teaching us about law and technology. Thank you, Nikolaus, for opening a great window of knowledge for me. Then my path brought me to Leuven, where I spent seven years close to Prof. Em. Jos Dumortier, who became also my “Doctorvater” –the Germans have a great term for everything, as Maša keeps reminding me. Jos, thank you for teaching me the value of leading and the importance of supporting. In Leuven there was one person that believed in me from the outset: Prof. Peggy Valcke. Thank you Peggy for being there for me all the way.

The latest turn of the path brought me in Tilburg, my academic home. I can never thank enough Prof. Ronald Leenes for giving me the opportunity to join TILT. Ronald, thank you for believing in me, supporting me, challenging me and motivating me to keep improving. You are a wonderful leader and a great colleague. Special thanks are due to Prof. Corien Prins. Corien, thank you for offering me a warm welcome to Tilburg Law School, for sharing freely your knowledge and your experiences and for always having a kind smile and a warm word. TILT is a very special place and Prof. Bert-Jaap Koops is one of its special assets. Bert-Jaap, thank you for always making time to discuss and for the meticulous and detailed feedback in everything I ask. And then there is Prof. Paul de Hert. Paul you are a moving library and a continuous source of mental inspiration. Thank you for all the interesting discussions, the insightful feedback and the life lessons you offer wholeheartedly.

Both in Leuven and in Tilburg, I was so lucky to have magnificent colleagues. I would not dare to name all of you, but I cherish the support and friendship of each one of you.

I cannot thank enough my wonderful doctoral students –Damian Clifford, Dimitra Stefanatou, Irene Kamara, Jef Ausloos, Milda Macenaite, Maša Galič, Lorenzo Dalla Corte and Sascha van Schendel- for the countless discussions and the stimulating debates. I am very proud for every single one of you. A special “thank you” goes also to Magda Brewczyńska for her endless motivation and her great support in the preparation of this inaugural address.

My gratitude goes to the Executive Board of the University, the Board of the Law Faculty, the former and current Rector Magnificus and Dean of the Law Faculty for endorsing and supporting this Chair on Technology Law and Human Rights under the Philip Eijlander Diversity Programme.

The ancient Greek philosopher Anacharsis stated that it is better to have one friend of great value, than many friends who are good for nothing. I have been lucky to have the best friends one can possibly meet in their life. Their support, love and care mean everything to me. First and foremost, I would like to thank Eleni Papanikolaou, who has been a guardian angel in all the steps of my personal life and academic career. Eleni, I do not know what is next to come, but I know you will be there. Thank you! Panos Merkouris, my dear old friend, we follow parallel paths for twenty years now and life brought us both in the Netherlands. It cannot be a coincidence. Thank you for everything –you know. My sweet and loving Federica Lucivero, Tilburg will always be linked to you no matter where you are. Thank you for everything we have been going through together and for teaching me that people can actually talk for two hours without taking a breath. I miss you a lot!

I would not be standing on the podium today, if it was not for my wonderful parents, who have been an inspiration in all my life, supporting me in every step of my professional and personal life. Thank you for believing in me, even when I did not. Life is a wonderful journey, but sailing alone is not fun. I was blessed to meet my amazing husband, Georgios Orfanos, and sail through life together. Giorgo, thank you for all your love and support! I cannot end this inaugural address without thanking the wonderful miracle of my life, my little prince, Yiannis, the creature that taught me that no matter how much work there is, there is always time for a hug and a kiss. And peekaboo... :)

I have spoken.

Bibliography

Bibliography

Anderson A, *A question of trust – Report of the Investigatory Powers Review*, 2015, <<https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Web-Accessible1.pdf>> accessed 17 November 2017

Arai-Takahashi Y, 'The Margin of appreciation doctrine and the principle of proportionality in the jurisprudence of the ECHR' (Intersentia 2002)

Bernal P, '*Liberty and others vs. GCHQ and others*' *JusletterIT*, 2015, <<https://ueaeprints.uea.ac.uk/60576/>> accessed 10 October 2017

Bingham Centre for the Rule of Law, 'The Investigatory Powers Review by the Independent Reviewer of Terrorism legislation' (November 2014), <https://www.biicl.org/documents/399_bingham_centre_submission_to_investigatory_powers_review_final__2014-11-19.pdf?showdocument=1> accessed 18 November 2017.

Blasi Casagran C, *Global Data Protection in the Field of Law Enforcement: An EU Perspective* (Routledge 2016)

Cameron I, *National Security and the European Convention on Human Rights* (Kluwer Law International 2000)

Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, 391–407

Clarke R, *Introduction to Dataveillance and Information Privacy, and Definitions of Terms* (1997, revised 2016), <<http://www.rogerclarke.com/DV/Intro.html>> accessed 17 November 2017

Cole M and Vandendriessche A, 'From *Digital Rights Ireland* and *Schrems* in Luxembourg to *Zakharov* and *Szabó/Vissy* in Strasbourg: What the ECtHR made of the deep pass by the CJEU in the recent cases on mass surveillance' (2016) 1 EDPL 121

De Hert P and Bocos P, 'Case of Roman Zakharov v. Russia: The Strasbourg follow up to the Luxembourg Court's *Schrems* judgment', (23.12.2015) <<https://strasbourgobservers.com/2015/12/23/case-of-roman-zakharov-v-russia-the-strasbourg-follow-up-to-the-luxembourg-courts-schrems-judgment/>> accessed 17 November 2017.

De Hert P and Gutwirth S, 'Data protection in the case law of Strasbourg and Luxembourg: constitutionalisation in action' in Serge Gutwirth et al. (eds), *Reinventing data protection?* (Springer 2009) 3

De Hert P and Gutwirth S, 'Privacy, data protection and law enforcement. Opacity of the individual and transparency of power' in Erik Claes, Antony Duff, Serge Gutwirth (eds), *Privacy and the Criminal Law* (Intersentia 2006) 61

De Hert P, 'A human rights perspective on privacy and data protection impact assessments' in Paul de Hert and David Wright (eds), *Privacy Impact Assessment* (Springer Netherlands 2012) 33

De Hert P, '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) 1(1) *Utrecht Law Review* 68

Douglas-Scott S, 'A Tale of Two Courts: Luxembourg, Strasbourg and the Growing European Human Rights Acquis' 43 *Common Market Law Review* (2006) 629

Equality and Human Rights Commission, 'Response of the Equality and Human Rights Commission to the Consultation: Investigatory Powers Review – Call for Evidence' (October 2014), <<https://www.equalityhumanrights.com/en/file/6016>> accessed 17 November 2017

European Commission, Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46 on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce [2000] OJ L215/7

European Commission, 'Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield' [2016] OJ L 207/1

European Court for Human Rights, Press release (7 November 2017) <http://hudoc.echr.coe.int/eng-press?i=003-5907256-7537826> accessed 18 November 2017.

European Group on Ethics in Science and New Technologies, 'Opinion 28 -Ethics of security and surveillance technologies' (20 May 2014) <<https://publications.europa.eu/en/publication-detail/-/publication/6f1b3ceo-2810-4926-b185-54fc3225c969/language-en>> accessed 17 November 2017.

European Parliament (Report authored by Caspar Bowden), 'The US surveillance programmes and their impact on EU citizens' fundamental rights' (2013) <http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/briefingnote_/briefingnote_en.pdf> accessed 17 November 2017.

European Parliament and the Council of the European Union, Directive 2002/58/EC 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

Fura E and Klamberg M, 'The Chilling Effect of Counter-Terrorism Measures: A Comparative Analysis of Electronic Surveillance Laws in Europe and the USA' in Josep Casadevall, Egbert Myjer, Michael O'Boyle (eds), *Freedom of Expression – Essays in honour of Nicolas Bratza – President of the European Court of Human Rights* (Wolf Legal Publishers 2012) 463

Galetta A and de Hert P, 'Complementing the Surveillance Law Principles of the ECtHR with its Environmental Law Principles: An Integrated Technology Approach to a Human Rights Framework for Surveillance' (2014) 10(1) *Utrecht Law Review*, 55

Georgieva I, 'The Right to Privacy under Fire – Foreign Surveillance under the NSA and the GCHQ and Its Compatibility with Art. 17 ICCPR and Art. 8 ECHR' (2015) 31 *Utrecht Journal of International and European Law* 104

Harris D, O'Boyle M, Bates E and Buckley C, *Law of the European Convention on Human Rights* (3rd ed OUP 2014)

Hintz A and Dencik L, 'The politics of surveillance policy: UK regulatory dynamics after Snowden' (2016) 5(3) *Internet Policy Review* 1

Letsas G, 'The ECHR as a Living Instrument: Its Meaning and its Legitimacy' in Andreas Føllesdal, Birgit Peters and Geir Ulfstein (eds), *Constituting Europe - The European Court of Human Rights in a National, European and Global Context* (Cambridge University Press 2013) 106

Levinson-Waldman R, 'NSA surveillance in the war on terror' in David Gray and Stephen Henderson (eds), *Cambridge Handbook of Surveillance Law* (Cambridge, University Press 2017) 7

Malgieri G and de Hert P, 'European Human Rights, Criminal Surveillance, and Intelligence Surveillance: Towards 'Good Enough' Oversight, Preferably But Not Necessarily by Judges' in David Gray and Stephen Henderson (eds), *Cambridge*

Handbook of Surveillance Law (Cambridge University Press 2017) 509

Marx G, “Your Papers please”: personal and professional encounters with surveillance, Preface’ in Kirstie Ball, Kevin Haggerty and David Lyon (eds), *Routledge Handbook of Surveillance Studies* (Routledge 2012) xx

Marx G, *Windows into the Soul: Surveillance and society in an Age of High Technology* (The University of Chicago Press 2016)

Metcalf E, ‘Terror, reason and rights’ in Esther D. Reed et al. (eds), *Civil Liberties, National Security and Prospects for Consensus: Legal, Philosophical and Religious Perspectives* (Cambridge University Press 2012) 152

Murphy M H, ‘Algorithmic surveillance: the collection conundrum’ (2017) 31 *Int’l Rev L Computers & Tech* 225

Murphy M H, ‘Investigative use of GPS Tracking Devices and the European Court of Human Rights’(2012) 22(1) *Irish Criminal Law Journal*, 8

Murphy M H, ‘The relationship between the European Court of Human Rights and National Legislative Bodies: Considering the Merits and the Risks of the Approach of the Court in Surveillance Cases’ (2013) 3(2) *Irish Journal of Legal Studies* 65

Nardell G, ‘Levelling up: Data Privacy and the European Court of Human Rights’ in Serge Gutwirth et al. (eds), *Data Protection in a Profiled World*, (Springer 2010) 43

Ni Loideain N, ‘Surveillance of Communications Data and Article 8 of the European Convention on Human Rights’ in: Serge Gutwirth, Ronald Leenes, Paul de Hert(eds) *Reloading Data Protection* (Springer 2014) 183

Nyst C, ‘The European Court of Human Rights Constrains Mass Surveillance (Again)’ [2016] *Just Security*’ J <<https://www.justsecurity.org/28939/ecthr-constrains-mass-surveillance/>> accessed 18 November 2017

Pollicino O and Bassini M, ‘Bridges are down, data trucks cannot get through...-A critical view of the Schrems judgment in the context of European constitutionalism’ in Giuliana Ziccardi Capaldo (ed), *The global community - Yearbook of International Law and Jurisprudence* (Oxford University Press 2016) 245

Presidential Policy Directive 28 (PPD-28) Signals Intelligence Activities (2014)

Reid K, *A practitioner's guide to the European Convention of Human Rights* (Sweet & Maxwell 2011)

Sottiaux S, *Terrorism and the Limitations of Rights: the ECHR and the US Constitution* (HART Publishing 2008)

Taylor N, 'To find the needle do you need the whole haystack? Global surveillance and principled regulation' (2014) 18(1) *The International Journal of Human Rights* 45

UK Investigatory Powers Tribunal Rules 2000 No 2665 (IPT Rules 2000)

Tomkins A, 'Justice and security in the United Kingdom' (2014) 47 (3) *Israel Law Review* 305

Tsampi A, *Le principe de séparation des pouvoirs dans la jurisprudence de la Cour européenne des droits de l'homme* in A.Pedone (ed), Series : Fondation Marangopoulos pour les droits de l'Homme, (Paris 2018) [forthcoming].

UK Home Office, *Interception of Communications Code of Practice Pursuant to section 71 of the Regulation of Investigatory Powers Act 2000, 2002*, paras 5.1; 6.5 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/513668/interception-comms-code-practice.pdf> accessed 17 November 2017.

UK Intelligence and Security Committee of the UK Parliament, Report "Privacy and Security: A modern and transparent legal framework" (12 March 2015), para 110 <<http://bit.ly/2yAAie2>> accessed 17 November 2017

UK Regulation of Investigatory Powers Act 2000

Van der Sloot B 'Privacy in the Post-NSA Era: Time for a Fundamental Revision?' (2014) 5 *JIPITEC* 2

Van der Sloot B, 'Editorial' (2016) 1 *EDPL* 1

Van der Sloot B, 'Is the Human Rights Framework Still Fit for the Big Data Era? A Discussion of the ECtHR's Case Law on Privacy Violations Arising from Surveillance Activities' in Serge Gutwirth, Ronald Leenes, Paul de Hert (eds), *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection* (Springer 2016), 411

White Robin, Clare Ovey, *Jacobs, White and Ovey: The European Convention on Human Rights* (5th edn, Oxford University Press [2010])
Woods L, 'Introductory note to *Zakharov v Russia* (Eur.CT.H.R)' (2016) 55 ILM 207

Case law

Amann v Switzerland 2000-II ECtHR Application no 27798/95

Association for European Integration and Human Rights and Ekimdzhev v Bulgaria (2008) ECtHR Application no 62540/00

Big Brother Watch, Open Rights Group, English PEN, Dr Constanze Kurz v. the United Kingdom

- Joint application under Article 34, *Big Brother Watch, Open Rights Group, English PEN, Dr Constanze Kurz v. the United Kingdom*, App. No. 58170/13, lodged on 4 September 2013
- Statement of facts, *Big Brother Watch, Open Rights Group, English PEN, Dr Constanze Kurz v. the United Kingdom*, Application No. 58170/13, 6 <<http://hudoc.echr.coe.int/eng?i=001-140713>> accessed 17 November 2017.

Bureau of Investigative Journalism and Alice Ross v the United Kingdom

- Joint application under Article 34, *Bureau of Investigative Journalism and Alice Ross v the United Kingdom*, App. Nr. 62322/14, lodged on 11 September 2014
- *Bureau of Investigative Journalism and Alice Ross vs. the United Kingdom*, App. No. 62322/14, lodged on 11 September 2014, Statement of Facts communicated on 05 January 2015, <<http://hudoc.echr.coe.int/eng?i=001-150946>> accessed 17 November 2017.

Centre for Legal Resources on behalf of Valentin Câmpeanu v Romania (2014) ECtHR Application no 47848/08

Christie v United Kingdom (1994) inadmissible ECtHR Application no 21482/93

Esbester v United Kingdom (1993) ECtHR Application no 18601/91

Gillow v United Kingdom (1986) Series A no 109 ECtHR Application no 9063/80

Halford v United Kingdom (1997) Reports 1997-III ECtHR Application no 20605/92

Handyside v United Kingdom (1976) Series A no 24 ECtHR Application no 5493/72

Huvig v France (1990) Series A no 176-B ECtHR Application no 11105/84

Kennedy v United Kingdom (2010) ECtHR Application no 26839/05

Khan v United Kingdom 2000-V ECtHR Application no 35394/97

Klass and Others v Germany (1978) Series A no 28 ECtHR Application no 5029/71

Kopp v Switzerland (1998) Reports 1998-II ECtHR Application no 23224/94

Krone Verlag GmbH & Co. KG v Austria (no. 4) (2006) ECtHR Application no 72331/01

Kruslin v France (1990) Series A no 176-A ECtHR Application no 11801/85

Kvasnica v Slovakia 2009 ECtHR Application no 72094/01

Lambert v France (1998) Reports 1998-V ECtHR Application no 23618/94

Leander v Sweden (1987) Series A no 116 ECtHR Application no 9248/81

Liberty and Others v United Kingdom 2008 ECtHR Application no 58243/00

Malone v United Kingdom (1984) Series A no 82 ECtHR Application no 8691/79

N.C. v Italy (2002) ECtHR Application no 24952/94

Olsson v Sweden (1988) Series A no 130 ECtHR Application no 10465/83

Perry v United Kingdom 2003-IX ECtHR Application no 63737/00

Peck v United Kingdom 2003-I Application no 44647/98

Roman Zakharov v Russia

- Roman Zakharov v Russia (2015) ECtHR Application no 47143/06
- Roman Zakharov v Russia (2015) Application no 47143/06, Concurring opinion of Judge Dedov

S. and Marper v United Kingdom 2008 ECtHR Application no 30562/04 et al

Segerstedt-Wiberg and Others v Sweden 2006-VII ECtHR Application no 62332/00

Shimovolos v Russia 2011 ECtHR Application no 30194/09

Szabó and Vissy v Hungary

- Szabó and Vissy v Hungary (2016) ECtHR Application no 37138/14
- Szabó and Vissy v Hungary (2016) Application no 37138/14, Concurring Opinion Judge Pinto de Albuquerque

Telegraaf Media Nederland Landelijke Media B.V. and Others v the Netherlands (2013) ECtHR Application no 39315/06

The Sunday Times v United Kingdom (1979) Series A no 30 ECtHR Application no 6538/74

The 10 human rights organisations (the American Civil Liberties Union, Amnesty International, Bytes for All, the Canadian Civil Liberties Association, the Egyptian Initiative for Personal Rights, the Hungarian Civil Liberties Union, the Irish Council for Civil Liberties, the Legal Resources Centre, Liberty, Privacy International) v the United Kingdom

- Joint application under Article 34, The 10 human rights organisations (the American Civil Liberties Union, Amnesty International, Bytes for All, the Canadian Civil Liberties Association, the Egyptian Initiative for Personal Rights, the Hungarian Civil Liberties Union, the Irish Council for Civil Liberties, the Legal Resources Centre, Liberty, Privacy International) v the United Kingdom, App. No. 24960/15, lodged on 20 May 2015
- Statement of facts, 10 Human Rights Organisations and Others against the United Kingdom Application No. 24960/15, sec A3(d) <<http://hudoc.echr.coe.int/eng?i=001-159526>> accessed 17 November 2017
- The 10 Human Rights Organisations, 'Additional submissions on the facts and complaints', para 19 <<https://www.amnesty.org/en/documents/ior60/1415/2015/en/>> accessed 17 November 2017.

Uzun v Germany 2010 ECtHR Application no 35623/05

Valenzuela Contreras v Spain (1998) Reports 1998-V ECtHR Application no 27671/95

Weber and Saravia v Germany 2006-XI ECtHR Application no 54934/00

X and Y v Netherlands (1985) Series A no 91 ECtHR Application no 8978/80

Z v Finland (1998) Reports 1997-I Application no 22009/93

Case C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and others [2014] ECLI:EU:C:2014:238

Case C-362/14 Maximilian Schrems v Data Protection Commissioner [2015] ECLI:EU:C:2015:650

Case C- C-203/15 and C-698/15 Tele2/Watson [2016] ECLI:EU:C:2016:970

UK IPT, Liberty and Others v GCHQ and Others

- Judgment of 5 December 2014 [2014] UKIPTrib 13_77-H
- Judgment of 06 February 2015 [2015] UKIPTrib 13_77-H
- Order of 06 February 2015 UKIPTrib 13_77-H
- Open determinations of 22 June 2015, amended by 1 July letter (correcting the name of one of the human rights organisations).
- Farr Ch, Witness Statement on joined cases IPT/13/77/H, IPT/13/92/CH, IPT/13/168-173/H, IPT/13/194/CH, IPT/13/204/CH, 16 May 2014 < https://www.privacyinternational.org/sites/default/files/Witness%20st%20of%20Charles%20Blandford%20Farr_o.pdf> accessed 17 November 2017
- President of the Investigatory Powers Tribunal, 'Letter to Amnesty International Ltd and others' (1.07.2015) <http://www.ipt-uk.com/docs/IPT_to_Liberty_Others.pdf> accessed 17 November 2017.

UK ITP, Privacy International v Secretary of State for Foreign and Commonwealth Affairs & Others

- UK IPT, Case [2016-2017] UKIPTrib IPT_15_110_CH
- UK IPT, Order for reference to the Court of Justice of the European Union issued in case [2017] UKIPTrib IPT_15_110_CH <<http://www.ipt-uk.com/docs/IPT%20BULK%20DATA%20ORDER%20FOR%20REFERENCE%20TO%20CJEU.pdf>> accessed 18 November 2017.

United States v. Maynard, 615 F.3d 544 (D.C.Cir. 2010)

Colofon

vormgeving

Beelenkamp Ontwerpers, Tilburg

fotografie omslag

Maurice van den Bosch

opmaak en druk

PrismaPrint, Tilburg University

