UiO : Faculty of Law
University of Oslo

The legitimate scope of surveillance in the jurisprudence of the ECtHR

An evaluation of the balance established by the ECtHR between security and privacy in the context of surveillance

Candidate number: 9011

Submission deadline: 1 December 2017

Number of words: 17 966

Table of contents

1 Introduction

In the words of the European Court Human Rights "a system of secret surveillance designed to protect national security entails the risk of undermining or even destroying democracy on the ground of defending it".[1] This concern dates all the way back to the year 1978, when the Court recognised that the states had to have the ability to counter threats, such as espionage and terrorism, and accepted that some legislation granting powers of secret surveillance could be necessary in a democratic society in the interests of national security and/or the prevention of disorder or crime.[2] However, considering the risks posed by a system of secret surveillance, the states could not adopt whatever measures they deemed appropriate, in the name of that struggle.[3] The ECtHR has maintained this stance up to its latest decision on state surveillance in 2016.[4]

This research is motivated by a concern for the risks involved in a system of secret surveillance. Those risks culminate in the ultimatum pointed out by the ECtHR, the destruction of democracy. A key guardian against those risks is the right to privacy. The role of the right to privacy is clear from the jurisprudence of the ECtHR on surveillance, where the Court essentially attempts to find a balance between the state interest in protecting national security through secret surveillance, and the right to privacy, necessarily restricted by surveillance. The right to privacy not only has value in itself, but it also serves to protect several other rights. Although it is beyond the scope of this paper to map out the several individual and societal interests threatened by state-lead secret surveillance, the potential of a collapse of democracy illustrates, that everything a democratic society values is at stake. Thus, the overarching aim of this paper is to look at the ECtHR jurisprudence on surveillance to examine the current balance established by the Court between the two interests, security and privacy, and whether the scale tips more towards the one or the other.

A series of revelations in 2013 by the former employee of the United States National Security Agency, Edward Snowden, illustrate how the risks involved in the systems of secret surveillance are not only hypothetical, but a reality. The revelations gained considerable attention in the so-called Western liberal democracies, particularly in Europe. The European Parliament concluded in its resolution in 2014 that there was "compelling evidence of the existence of far-reaching, complex and highly technologically advanced systems designed by US and some

[1] *Rotaru v. Romani*a paragraph 59; *Szabó and Vissy v. Hungary* paragraph 57, The same remark is repeated in several other cases concerning surveillance.
[2] *Klass and others v. Germany* paragraphs 48–49.
[3] Ibid.
[4] *Szabó and Vissy v. Hungary* paragraph 57.

Member States' intelligence services to collect, store and analyse communication data, including content data, location data and metadata of all citizens around the world, on an unprecedented scale and in an indiscriminate and non-suspicion-based manner".[5] The scale of the revealed practice was considered so wide as to blur the boundaries between law enforcement and intelligence, leading to every citizen being treated as a suspect and consequently a subject to surveillance.[6] It was also clear that the massive surveillance machinery could be used for other reasons than strictly national security and counter-terrorism.[7] Since surveillance practices are often kept secret, it is not possible to be certain that surveillance mechanisms are not used for reasons such as economic and industrial espionage or profiling on political grounds.

For an assessment of the balance between security and privacy, the central focus of this research is on the scope of surveillance. Logically, the wider the scope of surveillance, the greater the intrusion on the right to privacy, and consequently the higher the risk of negative individual and societal consequences. In the context of surveillance jurisprudence of the ECtHR, the term "scope" refers to the nature of the activities or offences which may give rise to surveillance, and the categories of people monitored.[8] Moreover, one may note that the activities or offences giving rise to surveillance indicate the purposes for which surveillance maybe used. In turn, the persons monitored reveal the scale of surveillance. The relevance of the two components for this research is also clear in light of history. Surveillance of individuals or groups is not a new phenomenon.[9] In liberal democracies surveillance has commonly taken place on the basis of a suspicion that the target person or group of persons has engaged in or is about to engage in criminal activities.[10] Surveillance has been primarily a tool to detect, prevent or investigate crimes. By contrast, in authoritarian regimes surveillance technologies have been used to find the political opponents from the mass of population and to suppress freedom of expression and information.[11] Therefore, "it is precisely the purposes and the scale of surveillance that differentiates democratic regimes from police states".[12]

Although the actual scope of surveillance is in the end always a political decision, one must not undermine the role of the judiciary in restraining instrumentalist objectives. Thus, this research resorts to the judicial concept of legitimacy and assesses the legally permissible scope of sur-

[5] European Parliament, European Parliament resolution on US NSA surveillance programme, surveillance bodies in various Member States and impact on EU citizens' fundamental rights, para. 1.
[6] Ibid., para. G.
[7] Ibid.
[8] *Roman Zakharov v. Russia* paragraph 243.
[9] Bigo et al., 'Mass Surveillance of Personal Data by EU Member States and Its Compatibility with EU Law', 5.
[10] Ibid., 6.
[11] Council of Europe Parliamentary Assembly, 'Council of Europe Resolution 2045(2015) on Mass Surveillance', para. 8.
[12] Bigo et al., 6.

veillance established by the ECtHR. The paper builds on the premise that the notion of legitimacy may be understood to comprise of two aspects: "a conformity to the law or rules", as well as an "ability to be defended with logic or justification", referring to an idea of "validity".[13] Here, the latter is understood as the wider meaning of legitimacy, which addresses the exercise of power; it looks at the manner in which the authorities exercise public power and whether it can be considered fair.[14] A focus on the "validity" of a measure, such as secret surveillance, permits to counter "the tyranny of subjective interests and preferences".[15] In turn, the narrower meaning of the notion of legitimacy refers to the legal rules governing a phenomena. This aspect is considered narrower, since the wider assessment of whether the exercise of power may be considered logical, justified, valid or fair, may incorporate an assessment of conformity of the practice in question with law. The narrower understanding of the legitimacy of a measure taken in the exercise of public power, or the legitimacy of a law's restriction on the rights and freedoms, permits to analyse whether the measure or the restriction is sufficiently clear and accessible, and consistent with international law.[16] This aspect of the term also functions to counter subjective assertions with a scrutiny of the laws authorising surveillance by objectively verifiable standards and processes.[17] Where legitimacy in a narrow sense requires the authorities to ground their exercise of power in verifiable standards, the wider understanding of the term demands that the exercise of power must be justified. The former focuses on the conformity with procedural requirements, whereas the latter goes deeper into substantive reasons justifying the measure.

To summarise, this research analyses the case law of the ECtHR on surveillance, with a focus on the key principles established therein. Broadly, it examines the current balance established by the Court between security and privacy, and whether the position of the one or the other is currently stronger. More specifically, the paper examines how the ECtHR has dealt with the scope of surveillance. The two main components of the scope, meaning (1) the purposes, understood as the activities or offences that may give rise to surveillance, and (2) the scale, in the sense of the range of persons that may be subjected to monitoring, will be scrutinised. The principle that grounds this assessment in the legal framework of the ECtHR, is that of legitimacy. The Court in its case law assesses whether an interference with the right to privacy by a system of surveillance may be justified. That assessment is essentially a test for legitimacy of a measure or restriction. It comprises both a test of procedural lawfulness, as well as a more substance oriented test of whether the restriction is necessary, and thereby justified in a democratic society. Thus, this research follows the structure of the ECtHR case law, to illustrate the importance of a careful scrutiny of both of the tests. A thorough legal analysis of the scope of

[13] 'Oxford Dictionaries'.
[14] Tyler, 'Procedural Justice, Legitimacy, and the Effective Rule of Law', 286.
[15] Koskenniemi, 'What Is International Law For?', 41.
[16] Duffy, *The 'War on Terror' and the Framework of International Law*, 1, 66.
[17] Ibid., 1, 66.

surveillance, permits to objectively examine the current situation, and to draw conclusions on the potential impact on the values threatened. It establishes a platform on which democratic decisions on the future of surveillance can be made.

Finally, recent developments point to the urgency of this discussion. Despite the decisions already rendered by the ECtHR and the Court of Justice of the European Union, as well as the concerns voiced, now in 2017 there is no sign the countries would be slowing down their march in the "surveillance arms race", quite the contrary. Particularly in Europe, it seems the revealed large-scale surveillance practices served not as a warning example but as a source of inspiration for the drafting of new surveillance laws.[18] Following a series of terrorist attacks,[19] countries such as Germany, the UK and France have recently enacted laws to authorise the use surveillance on a massive scale.[20] This trend has been followed by several other countries including Italy[21], Austria[22], Poland[23], Norway[24] and Finland[25]. Considering the very real threat to democracy created by these laws, the legitimate scope of surveillance ought to central the discussion. At present, the situation is not sufficiently addressed in academia, let alone in the civil society, which illustrates either a lack of comprehension or awareness of the current development. Therefore, a careful scrutiny of these laws, and the reasons for enacting them, lays down the necessary basis on which a democratic discussion of the validity of these laws can be carried out.

2 Methodology and structure

The main weight of this research is on a legal analysis of the relevant case law of the ECtHR. Also, decisions from other international courts or tribunals may be referred to, where useful to complement the picture. The ECtHR has already rendered a number of decisions dealing with surveillance and there are also several cases pending in front of the Court, expected to clarify the situation regarding the scope of surveillance.[26] Even though the Court does not operate on the basis of a system of binding precedents, it has held that it is "in the interest of legal certainty and foreseeability of rulings not to change its jurisdiction without compelling reasons".[27] Thus,

[18] Lubin, 'A New Era of Mass Surveillance Is Emerging Across Europe'.
[19] Simmons, 'Two Years of Terror'.
[20] Lubin.
[21] Guest author, 'Italy'.
[22] Guest author, 'Austria Creates New Agency with Unprecedented Surveillance Powers'.
[23] The Venice Commission, 'The Venice Commission Opinion No. 839/ 2016 on the Act of 15 January 2016 Amending the Police Act and Certain Other Acts'.
[24] Forsvarsdepartementet, 'Utreder et digitalt grenseforsvar'.
[25] Sisäministeriö, 'Tiedustelulainsäädäntö'.
[26] European Court of Human Rights Press Unit, 'Fact Sheet - Mass Surveillance'.
[27] 'The European Convention on Human Rights - Introduction'.

the most recent case law gives an indication of the current situation of surveillance jurisprudence, and will therefore be given particular attention. The two most recent cases are the *Roman Zakharov v. Russia*[28] from December 2015 and the *Szabó and Vissy v. Hungary*[29] decided in June 2016. Notably, the *Roman Zakharov* case was decided by the Grand Chamber of the ECtHR whereas the *Szabó and Vissy* was decided by Section IV Chamber. The Grand Chamber is formed of 17 judges: the Court's President and Vice-Presidents, the Section Presidents and the national judge, together with other judges selected by drawing of lots.[30] The Section IV Chamber in turn consisted of seven judges, including the President and six other judges.[31] Although the Grand Chamber decisions are of equal legitimacy, they are treated by particular scrutiny in the domestic courts, when compared with simple Chamber judgements.[32]

To examine how the scope of surveillance has been dealt with by the ECtHR, the paper follows the steps checked by the Court when assessing an interference with a right enshrined in the European Convention on Human Rights. An interference may be justified only if it (1) serves a legitimate aim, (2) is in accordance with law, and (3) is necessary in a democratic society. The research begins by presenting the context in which the surveillance decisions are given, essentially revolving around the questions concerning the "legitimate aim" of surveillance. The term "context" is understood here as the background, or the framework, in which the Court renders its judgments. It presents the key concepts, surveillance, privacy, security and margin of appreciation, and establishes the basis for a deeper understanding of the decisions made by the Court.

In the second part, aspects of the ECtHR case law, which deal with the scope of surveillance, are analysed within the provision of "in accordance with law". This test of lawfulness deals with the procedural safeguards by addressing the question of legitimacy from a narrower perspective. The two components of the notion "scope" will form the structure of the section: (1) the purpose, in the sense of the activities or offences giving rise to surveillance and (2) the scale, meaning the persons targeted by it. The section demonstrates the complicated task of balancing of the ECtHR, where the Court has to accommodate both the security interest of the state, leaving room for secrecy and vague notions, while at the same time upholding the requirements for foreseeability, in terms of transparency and precision, necessary for safeguarding the right to privacy.

[28] *Roman Zakharov v. Russia*.
[29] *Szabó and Vissy v. Hungary*.
[30] 'European Court of Human Rights Web Page'.
[31] *Szabó and Vissy v. Hungary*.
[32] Council of Europe, 'Annual Report 2016 of the European Court of Human Rights', 20.

Finally, the last section of the research, titled "necessary in a democratic society", examines the rulings of the ECtHR regarding the scope of surveillance, which corresponds to the understanding of the legitimacy principle in its widest form. As explained earlier, the principle of legitimacy deals not only with procedural conformity of a measure or restriction with law, but it also demands the measure or restriction is justified, logical, valid or fair in a society. Therefore, it is within the test of necessity that the Court will address the substance, rather than procedure, oriented arguments that may have a great impact on the permissible scope of surveillance, and consequently, on the values threatened by systems of surveillance.

The said section uses some of the prior work of the author. That work assessed the use of electronic surveillance as a counter-terrorism measure from a human rights perspective. The part in which the paper assessed the "necessity" of electronic surveillance in a democratic society, particularly with respect to establishing a proportionate balance between competing human rights interests, will complement this research.

Lastly, the paper concludes with findings on the balancing task of the ECtHR between privacy and security, the key rivals in the surveillance arms race. An evaluation of the manner in which the ECtHR has dealt with the central questions of the legitimate scope of surveillance, will lay basis for future research and discussion.

3 The context of surveillance jurisprudence

This section presents the key concepts of this research, the notions of surveillance, privacy, security and margin of appreciation. These concepts shed light to the context, the background or the framework, in which the Court renders its decisions on surveillance. Thematically, these concepts revolve around the questions concerning the "legitimate aim" of surveillance. Ultimately, this discussion attempts to establish the basis for a deeper understanding of the decisions made by the Court.

3.1 Surveillance

Surveillance, in the context of security, has been defined as "the targeted or systematic monitoring, by governmental organizations and their partners, of persons, places, items, infrastructures (including means of transport) or flows of information".[33] Surveillance, and the data collected thereof, can be used not only to identify hazards, manage risk, and to enable a preventive,

[33] van Gulijk et al., 'SURVEILLE Deliverable 2.1: Survey of Surveillance Technologies, Including Their Specific Identification for Further Work', 4.

protective or reactive response, but also for preparing such a response in the future.[34] Any technology that makes observation and monitoring more effective and efficient may become a surveillance technology.[35] The "systems of secret surveillance", as referred to by the ECtHR, usually employ a combination of various different surveillance technologies and techniques. Based on the public revelations and an understanding of the methods and devices available, it is possible to presume with a fairly high certainty, what are the main tools used by the authorities. Among such technologies and techniques are tapping fiber-optic cables, circumventing encryption, launching cyber-attacks, gathering data through access to computer and telephone networks and location data, analysis of content and metadata, and many traditional spying methods such as telephone tapping.[36]

It is beyond the scope of this paper to analyse the different surveillance methods that may or may not be used by national authorities as part of their surveillance strategy. It is also maintained that, in light of the jurisprudence of the ECtHR, this is not absolutely necessary. The Court has repeatedly held in its examination of the laws authorising the various forms of surveillance, that it must be satisfied, irrespective of what kind of a system of surveillance is adopted, that there exist adequate and effective guarantees against abuse.[37] Also the fact that the Court applies the same principles irrespective of the surveillance technology or technique contested, supports the conclusion that the same basic rules apply irrespective. For example, the minimum safeguards the ECtHR consistently refers to in its decisions on surveillance, originate from the *Huvig v. France* case, which concerned the tapping of a telephone conversation.[38] Nevertheless, the Court has repeated those safeguards even in considerably different surveillance cases, such as the latest *Szabó and Vissy* case. It applied the same minimum safeguards to the entire Hungarian system of secret surveillance, which comprised of methods such as the search and keep under surveillance the applicants' homes secretly, the checking of postal mail and parcels, the monitoring of electronic communications and computer data transmissions and the making of recordings of any data acquired through these methods.[39] The Court does acknowledge that the recent technological advances "attract the Convention protection of private life even more acutely" but does not indicate the principles would be considerably changed.[40]

[34] Ibid.
[35] Ibid.
[36] van Gulijk et al., 'SURVEILLE Paper Assessing Surveillance in the Context of Preventing a Terrorist Act', 3; European Parliament, para. 2.
[37] *Klass and others v. Germany* paragraph 50; *Szabó and Vissy v. Hungary* paragraph 57, The same rule is established in several other cases concerning surveillance.
[38] *Huvig v. France* paragraph 34.
[39] *Szabó and Vissy v. Hungary* paragraphs 52, 56.
[40] *Szabó and Vissy v. Hungary* paragraph 53.

Therefore, here it suffices to note that the surveillance measures may locate differently on a spectrum from less intrusive to highly intrusive. On the more intrusive end of the spectrum, there are the measures permitting an untargeted, indiscriminate, strategic surveillance of any person for any purpose, which have surfaced in the surveillance platform more recently. On the other end, there are measures which are targeted only on the persons suspected of planning, committing or having committed an act warranting surveillance, considered as the more traditional methods. As an example, one may consider the tapping of a single telephone connection of a person known by evidence of having committed a serious crime. By contrast, on the more intrusive end of the spectrum, there is for example the tapping of fibre-optic cables in order to identify potential future threats and the people behind them, one of the methods revealed by Edward Snowden in 2013. According to the Guardian, "[e]ach of the cables carries data at a rate of 10 gigabits per second, so the tapped cables had the capacity, in theory, to deliver more than 21 petabytes a day – equivalent to sending all the information in all the books in the British Library 192 times every 24 hours".[41]

Thus, one is to be aware that the technological development now permits authorities to access and process more information, faster and with considerably less chances of being noticed.[42] The process of development is not expected to slow down, quite the contrary. Certainly, the more intrusive the technology or technique available, the more acutely one must safeguard against abuse of that technique or technology. Highly intrusive surveillance methods permit the surveillance of potentially any person and for potentially any purpose, which is why they inherently enable a nearly unlimited scope of surveillance. Consequently, the more intrusive the technology, the wider the scope and the more serious the consequences for the right to privacy and the values protected. However, the basic rules established by the ECtHR, addressing the legitimate scale and purpose of surveillance, have the ability to restrain also this kind of surveillance. The same limitations that demand precision in defining the categories persons or activities monitored, or that require the authorities demonstrate a connection between the activities or offences giving rise to surveillance and the persons or activities actually surveyed, can be applied irrespective of the surveillance methods chosen. Of course, the role of these limitations and requirements becomes even more important, the more intrusive the technology available.

3.2 Interference with the right to privacy

[41] MacAskill et al., 'GCHQ Taps Fibre-Optic Cables for Secret Access to World's Communication'.
[42] van Gulijk et al., 4.

From the perspective of fundamental rights, surveillance by national authorities may interfere with a range of interests protected in a number of human rights treaties; the Universal Declaration on Human Rights ("the UDHR"), the International Covenant on Civil and Political Rights ("the ICCPR"), the Charter of Fundamental Rights of the European Union ("the EU Charter") and the European Convention on Human Rights ("the ECHR"). Surveillance may threaten the very cornerstones of democracy, including "the freedom of expression, of the press, of thought, of conscience, of religion and of association, private life, data protection, as well as the right to an effective remedy, the presumption of innocence and the right to a fair trial and non-discrimination".[43] In its case law concerning surveillance, the European Court of Human Rights has focused on the right to respect for private and family life, home and correspondence ("the right to privacy") as enshrined in article 8(1) of the Convention. The right to privacy is also protected by article 12 of the UDHR, article 17 of the ICCPR and article 7 of the EU Charter.

Privacy as a notion is not clearly defined or delineated. Four of the most common ways in which the concept is approached relate privacy to non-interference, degree of access to a person, informational control, and intimate or sensitive information.[44] Privacy may also be understood not as an end in itself, but as an instrument to attain other goals.[45] This functional approach highlights the importance of privacy protection for a number of individual and societal values.[46] Just to note a few, the individual values served may include individuality, autonomy, dignity and integrity, whereas civility, stability, pluralism and democracy are considered as the core societal values in this regard.[47] Also from the rights perspective, privacy is deemed both a fundamental right in its own value as well as a "human right that supports other human rights".[48] It may be considered as the very basis upon which democratic societies are founded.[49]

The fact that privacy has no clear and specific meaning is not problematic, but a common nature of value notions.[50] An understanding of the concept of privacy is constantly evolving and subject to change.[51] This has an impact on what is considered as an intrusion, what should be protected against it and to what extent. In this regard, the European Convention on Human Rights permits an evolutive interpretation of the rights enshrined, taking into account recent developments, present-day conditions and commonly accepted standards.[52]

---

[43] European Parliament, para. T.
[44] Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits*, 128–29.
[45] Ibid., 125.
[46] Ibid., 125–35.
[47] Koops and Leenes, '"Code" and the Slow Erosion of Privacy', 135–36.
[48] UN Special Rapporteur, 'Report of the Right to Privacy A/HRC/13/37', 6.
[49] Ibid., 6.
[50] Koops and Leenes, 123.
[51] Ibid., 132.
[52] *Tyrer v. The United Kingdom* paragraph 31.

With respect to the ambit of article 8, the ECtHR has ruled that telephone, facsimile, e-mail and other confidential communications as well as personal internet usage are covered by the notions of "private life" and "correspondence" within the meaning of the article.[53] Both content and metadata fall within the scope.[54] Also the secret search and surveillance of homes, the checking of postal mail and parcels, the monitoring of electronic communications and computer data transmissions and the making of recordings of any data acquired through these methods can be examined in the context of "private life" and "correspondence".[55]

Generally, in cases concerning covert or non-consensual surveillance, the existence of an interference with the rights under article 8(1) is not contested.[56] For example, the mere collecting and storing of information relating to an individual's private life by national authorities constitutes an interference, irrespective of subsequent use.[57] Interestingly, the ECtHR has also considered that "the mere existence of secret measures or of legislation permitting secret measures" as part of government surveillance may constitute an interference with the right to respect for private and family life and for correspondence.[58] In the absence of national laws explicitly authorising surveillance, applicants have been required to demonstrate a "reasonable likelihood" the surveillance practices falling within the scope of article 8 have been applied to them.[59] In turn, where a claim has been based on the mere existence of a law permitting secret surveillance, the ECtHR has qualified the admissibility requirements in its later case law. The Court will first look at the scope of the legislation to examine the possibility the applicant will be affected by it.[60] This can be either because the applicant belongs to a group of persons targeted by it or because the system may intercept the communications of any person and therefore all users of communication services are directly affected by the legislation.[61] Second, the Court will consider the availability of remedies at national level; the less effective the remedies, the closer the scrutiny of the Court.[62] Notably, where there exists no effective domestic remedies, the applicant need not demonstrate any risk of being subjected to surveillance.[63] Whereas if effective remedies are in place, the applicant is to show that him or her is potentially at risk of being subjected to such measures.[64]

---

[53] *Copland v. the United Kingdom* paragraph 42; *Klass and others v. Germany* paragraph 40; *Liberty and Others v. the United Kingdom* paragraph 56.
[54] *Malone v. the United Kingdom* paragraph 83; *Weber and Saravia v. Germany* paragraph 76.
[55] *Szabó and Vissy v. Hungary* paragraph 52.
[56] Research Division of the European Court of Human Rights, 'Sécurité Nationale et Jurisprudence de La Cour Européenne Des Droits de l'homme', 8.
[57] *Amann v. Switzerland* paragraph 70.
[58] *Klass and others v. Germany* paragraph 34.
[59] *Halford v. the United Kingdom* paragraph 57.
[60] *Kennedy v. the United Kingdom* paragraph 124; *Roman Zakharov v. Russia* paragraphs 170–172.
[61] *Roman Zakharov v. Russia* paragraph 171.
[62] *Kennedy v. the United Kingdom* paragraph 124; *Roman Zakharov v. Russia* at 170–72.
[63] *Roman Zakharov v. Russia* paragraph 171.
[64] Ibid.

This means the ECtHR has relaxed the victim requirement contained in article 34 of the Convention and may consider cases *in abstracto*.[65] Normally, the Court examines whether the manner in which the laws and practices were applied to or affected the applicant constitutes a violation of the Convention, and does not deal with cases *in abstracto*.[66] The main reason why the Court is ready to derogate from its earlier practice is mainly related to the secret nature of many of the government surveillance practices. An individual may not be aware of being monitored and thus would also not be aware of any potential violation of his or her right guaranteed in article 8.[67] Therefore, the surveillance would be unchallengeable and article 8 could be deprived of its protective purpose in this respect.[68] Additionally, the fact that surveillance activities may interfere with the rights of vast amounts of people, potentially everyone living within a specific regime must have had an impact on the stance taken by the Court.[69]

Arguably, in these *in abstracto* cases concerning secret surveillance, the Court essentially addresses the issue of abuse of power by national authorities.[70] This can be seen as "a societal interest, related to the legitimacy and legality of a state".[71] How this may affect the rulings of the Court will be discussed later.

3.3 National security as a legitimate aim

The right to privacy is not an absolute right.[72] It is important for the framework of human rights law to apply at all times, particularly in times of national or international tension, and therefore it must permit a degree of flexibility.[73] The law must accommodate exceptional circumstances and be responsive to new developments.[74] This flexibility may be seen as inherent in human rights law, where the question of a violation of a right will depend on all circumstances of a particular case or situation.[75] It is visible not only in situations of 'public emergency' and an armed conflict, but also when certain rights are restricted to facilitate other fundamental rights or interests, often those of the 'common good'.[76]

---

[65] Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, Article 34 stipulates that: 'The Court may receive applications from any person, non- governmental organisation or group of individuals claiming to be the victim of a violation by one of the High Contracting Parties of the rights set forth in the Convention or the Protocols thereto'.
[66] *Szabó and Vissy v. Hungary* paragraph 32.
[67] *Klass and others v. Germany* paragraph 36.
[68] Ibid., paragraph 36.
[69] Ibid., paragraphs 37, 41.
[70] Sloot, 'Is the Human Rights Framework Still Fit for the Big Data Era?', 20.
[71] Ibid.
[72] Koops and Leenes, 127.
[73] Duffy, 475.
[74] Ibid.
[75] Ibid.
[76] Ibid.

With respect to the right to privacy, article 8 paragraph 2 lays down the following:

"There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.".

From this it may be inferred that limitations to the right to privacy are permissible if the restriction (1) is in accordance with law, (2) serves one of the legitimate aims mentioned and (3) is necessary in a democratic society. In cases concerning government surveillance, national security is often invoked as the legitimate aim justifying an interference with article 8(1). This is one of the factors that complicate the matter of establishing the legitimate scope of surveillance. Although it might turn out to be impossible to draw a comprehensive outline of the notion of national security, the jurisprudence of the ECtHR permits to examine the contents of and complications involved in the concept.[77]

First of all, it is to be noted that with respect to fundamental rights, the state has a double burden; it has to take steps to protect the rights of those within its jurisdiction, that is, to ensure the rights are not violated by others, while at the same time the state may not violate those rights itself.[78] In other words, the state is at the same time required to both respect rights and ensure rights.[79] This is expressly stipulated in article 2 of the ICCPR, which requires the states "to respect and to ensure" to all individuals under its jurisdiction the rights recognised by the Covenant.[80] Similarly, the ECHR article 1 mentions both an "Obligation to respect Human Rights" as well as that the parties to the convention "shall secure to everyone within their jurisdiction the rights and freedoms".

The state obligation to respect rights is understood as requiring abstention or negative action, whereas the obligation to ensure/secure rights is seen to demand positive action from the state.[81] In the present context, the state has a duty to, on the one hand, take active measures to ensure the life and safety of those under its jurisdiction, as enshrined in articles 2 and 5 of the ECHR as well as articles 6 and 9 of the ICCPR. To this end, the state maintains and develops a national

[77] Research Division of the European Court of Human Rights, 5.
[78] Bennoune, 'Terror/Torture', 10.
[79] Ibid.
[80] International Covenant on Civil and Political Rights, Article 2(1) lays down: 'Each State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant, without distinction of any kind'".
[81] Rodley, 'International Human Rights Law', 792.

security strategy. On the other hand, the state must at the same time respect the article 8 ECHR and article 17 ICCPR right to privacy. This means it must abstain from excessive intrusion with the said right.

In the same vain as a failure to respect a fundamental right may constitute a violation thereof, it is possible that a failure to ensure a fundamental right could in certain circumstances constitute a violation by the state of the right concerned.[82] This would for example be the case if the state was "permitting or failing to take appropriate measures or to exercise due diligence to prevent, punish, investigate or redress the harm caused by such acts by private persons or entities".[83] More explicitly, in its examination of an alleged violation of the positive obligation to secure rights, the ECtHR requires that "the authorities knew or ought to have known at the time of the existence of a real and immediate risk □of a violation of a right□ of an identified individual or individuals from the criminal acts of a third party and that they failed to take measures within the scope of their powers which, judged reasonably, might have been expected to avoid that risk".[84]

It can be considered implicit in the said obligation that the state needs to ensure it is aware of risks and has the capacity to prevent them.[85] It ought to take active measures and make reasonable enquiries to have sufficient knowledge about risks, as well as to ensure it has effective systems in place to identify and manage those risks.[86] Moreover, where dangerous activities are concerned, the state has an obligation to provide timely information, as part of the duty to protect.[87]

In light of the foregoing, it is understandable the state invokes the national security paradigm to justify measures such as electronic surveillance, which is tailored to produce information about risks and ultimately to protect the life and security of those under the jurisdiction of a state. Incorporation of such measures in the national security strategy may not be an option as much it is a legal obligation for the state.[88]

Also, as pointed out in the introduction, the ECtHR has explicitly acknowledged the need of the states to enact laws, which authorise the authorities to collect and store in non-public registers information on persons, and to conduct secret surveillance.[89] Already in 1978 the Court

[82] Human Rights Committee, 'General Comment No. 31: Nature of the General Legal Obligation Imposed on States Parties to the Covenant', para. 8.
[83] Ibid.
[84] *Osman v. the United* Kingdom paragraph 115.
[85] Duffy, 490.
[86] Ibid.
[87] *Öneryildiz v. Turkey* paragraph 90.
[88] See similarly in: Duffy, *The 'War on Terror' and the Framework of International Law*, 495.
[89] *Leander v. Sweden* paragraph 59; *Klass and others v. Germany* paragraph 48.

took note of the technical advances made in the means of espionage and of surveillance; as well as of the development of terrorism in Europe.[90] It found democratic societies threatened by highly sophisticated forms of espionage and by terrorism, threats which the state had to be able to effectively counter, and therefore had to conduct secret surveillance of "subversive elements operating within its jurisdiction".[91] The Court concluded that some legislation authorising surveillance was, under exceptional conditions, necessary in a democratic society in the interests of national security and/or for the prevention of disorder or crime.[92]

Applied in the present-day conditions, the ever-increasing pace of technical development, as well as the heightened risk of terrorist attacks, it is certain the aim of ensuring national security by measures such as secret surveillance and information gathering will not be disputed. However, it is also notable that the Court in its most recent decision on secret surveillance places the weight not on the increased risk of threats of terrorism and espionage, but on the threats created by the recent technical advances in state surveillance, the potential interferences and mass surveillance, which warrant the Convention protection "even more acutely".[93] Whether the balance tips on one way or the other in the future will remain to be seen.

As a final remark, it is also interesting to note how the Court has opened up the possibility to monitor "subversive elements" within the jurisdiction of a state, also in the interest of "prevention of disorder or crime". These are very broad notions potentially permitting the states to target surveillance on activities or persons that pose no real security threat but are rather linked to a political, economic or social activity in which the state may have an interest. This again relates to the scope of surveillance, particularly the purpose for which surveillance may be employed, discussed more in detail in the next chapter.

To conclude, the state has an obligation to simultaneously respect the right to privacy remains intact. Although the aim of defending national security may be considered legitimate, and usually is not contested in the cases concerning government surveillance in front of the ECtHR, the state may not do whatever it wishes to.[94] A balance must be established between the state interest in protecting its national security and the seriousness of interference with the right to respect for privacy.[95] The state has a certain discretion in conducting its matters in the field but that discretion is not unlimited. This will be discussed in the following section.

[90] *Klass and others v. Germany* paragraph 48.
[91] Ibid.
[92] Ibid.
[93] *Szabó and Vissy v. Hungary* paragraph 53.
[94] Research Division of the European Court of Human Rights, 5.
[95] *Leander v. Sweden* paragraph 59.

3.4 Margin of appreciation

Finally, it is necessary to scrutinise the judge-made doctrine of margin of appreciation, in order to fully understand the context in the present issue regarding the legitimate scope of surveillance. This section permits to examine the framework of national security more in depth as well as to reflect on the relationship between the ECtHR and the state parties to the European Convention on Human Rights.

As a preliminary remark, it is to be recognised that the notion of national security is not defined, and therefore it necessarily implies there is a degree of flexibility and elasticity inherent in the concept.[96] The margin of appreciation then reflects the flexibility granted to the states when dealing with matters in the sphere of national security.[97]

Reasons why the ECtHR has resorted to the concept revolve around the issue of the role of the Court vis-á-vis the state parties to the ECHR. First of all, the Court does not consider itself well positioned to challenge national decisions concerning national security.[98] A central rationale for this is that national interests are considered to form the core of state sovereignty and the Court is not to substitute the states in defining their interests.[99] Moreover, the Court has noted that the states have the primary role in safeguarding human rights, so that the machinery of protection established by the Convention is merely subsidiary to the national systems.[100]

By recognising that the laws expressing the requirements of morals vary from time to time and place to place, the Court concludes that "by reason of 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 in determining the exact content of the requirements of morals as well as on the "necessity" of a "restriction" or "penalty" intended to meet them".[101] Consequently, the states are left with a margin of appreciation to interpret and apply the laws in force.[102]

This margin reflects the relationship between the ECtHR and the state parties to the Convention. The Court is a supranational body whose task is "to ensure the observance of the engagements undertaken by the High Contracting Parties".[103] Its decisions are binding on the parties to a

[96] Research Division of the European Court of Human Rights, 5.
[97] Ibid.
[98] *Janowiec and others v. Russia* paragraph 213.
[99] *Bucur et Toma c. Roumanie* paragraph 110.
[100] *Handyside v. the United Kingdom* paragraph 48.
[101] Ibid.
[102] Ibid.
[103] Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, Article 19.

case, and will have effects extending beyond the confines of a particular case.[104] The judgments rendered by the Court not only settle the individual cases brought before it but, more generally, they "elucidate, safeguard and develop the rules instituted by the Convention, thereby contributing to the observance by the States of the engagements undertaken by them as Contracting Parties".[105] It may well be that the most important role of the ECtHR is, next to the scrutiny of allegations of human rights violations, to identify the "constitutional limits" on the exercise of government power.[106]

At least, it is clear the decisions of the Strasbourg Court on surveillance can significantly influence the protection of human rights at the national level.[107] This of course requires a willingness of the states to give effect to the decisions of the Court and thereby to exercise their sovereign power within the confinements of the Convention, as interpreted by the ECtHR. In the absence of enforcement power, the Court needs to be mindful of maintaining its ability to influence national practices, especially since "a careless approach could result in pushback from the national governments and hinder the influence of the Court at the domestic level".[108]

In this respect, cases dealing with government surveillance, which is a measure enacted for the purpose of national security, which in turn forms the essence of state sovereignty, are particularly sensitive. The ECtHR may well have the key role in defining the future of surveillance, also with regards to the legitimate scope of it. However, due to its lack of enforcement power and the sensitivity of matters concerning national security, much will depend on the relationship between the states and the Court. It remains to be seen whether the ECtHR will have the authority it needs to influence the states in this matter.

The margin of appreciation then serves as a method for the Court to show it acknowledges the role of the states in human rights protection and the importance of local conditions, thereby respecting the principle of subsidiarity.[109] The scope of the margin may vary depending on the nature of the aim pursued as well as of the interference involved.[110] Generally, in matters concerning national security it could be regarded as wide,[111] although the two most recent cases, *Szabó and Vissy v. Hungary* and *Roman Zakharov v. Russia*, mention only a "certain margin of appreciation".[112] The ECtHR has repeatedly stated the domestic power of appreciation is not

[104] Ibid., Article 46; *Marckx v. Belgium* paragraph 58.
[105] *Ireland v. the United Kingdom* paragraph 154.
[106] Greer, *The European Convention on Human Rights*, 170–71.
[107] 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', 69.
[108] Ibid.
[109] Ibid., 70.
[110] *Leander v. Sweden* paragraph 59.
[111] Ibid.
[112] *Roman Zakharov v. Russia* paragraph 232; *Szabó and Vissy v. Hungary* paragraph 57.

unlimited but goes hand in hand with a European supervision: the responsibility of the Court to ensure the observance of the States' engagements (Article 19) grants it he power to give the final ruling on whether a "restriction" or "penalty" is reconcilable with a right protected by the Convention.[113] With respect to secret surveillance, the states do not enjoy an unlimited discretion to subject persons within their jurisdiction to secret monitoring.[114] The Court, "being aware of the danger such a law poses of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate".

The reason for which the ECtHR steps in even where national security is at stake is that, from the perspective of the concepts of lawfulness and the rule of law in a democratic society, the reasons for the decision and the relevant evidence to undertake measures affecting fundamental human rights must be subject to review in adversarial proceedings before a competent, independent body.[115] If it was not possible to effectively challenge the executive's assertion that national security was at stake, "the State authorities would be able to encroach arbitrarily on rights protected by the Convention".[116]

Therefore, the Court will review the domestic decisions taken within the discretionary powers.[117] The state's margin of appreciation applies throughout the process: to the aim of the measure challenged,[118] to the requirements of foreseeability as part of the "in accordance with law" test,[119] and to the to the assessment of "necessary in a legitimate society", which comprises an analysis of a pressing social need, the choice of means for achieving the legitimate aim and the necessity of the measure to that end.[120] Thus, the supervision covers the same aspects, both the basic legislation and the decision applying it,[121] as well as the reasons stated for the decision and the relevant evidence presented for its support.[122]

To conclude, this section concerning the "context" of surveillance, the basic concepts that form the framework in which the Court renders decisions, indicates the importance of finding a balance between the right to privacy and the right to security. At the same time, the discussion on the doctrine of margin of appreciation points to the difficult position of the Court in establishing

[113] *Handyside v. the United Kingdom* paragraph 49.
[114] *Klass and others v. Germany* paragraph 49.
[115] *Janowiec and others v. Russia* paragraph 213.
[116] Ibid.
[117] *Bucur et Toma c. Roumanie* paragraph 110.
[118] *Handyside v. the United Kingdom* paragraph 49.
[119] *Roman Zakharov v. Russia* paragraphs 228–230.
[120] *Handyside v. the United Kingdom* paragraph 49; *Leander v. Sweden* paragraph 59.
[121] *Handyside v. the United Kingdom* paragraph 49.
[122] *Janowiec and others v. Russia* paragraph 213.

this balance. In the coming chapter, the paper turns to a closer scrutiny of how the ECtHR has dealt with the more concrete questions relating to the scope of surveillance.

4 In accordance with law

This section examines the legitimate scope, the scale and purpose, of surveillance by focusing on the understanding of legitimacy in a narrow sense, that is, the objectively verifiable standards established in the framework of the ECtHR. Keeping in mind the risks involved in the systems of secret surveillance, one may note that the vaguer the procedural requirements, the more there is discretion for the national authorities and thus, the more likely it is the scope of surveillance will be extended. This, in turn, would mean a more severe intrusion on the right to privacy, and consequently, on the values protected by it. Therefore, the analysis here focuses to uncover the strength of the procedural limitations imposed by the ECtHR on the scale and purpose of surveillance. Only those aspects of ECtHR jurisprudence that deal with the scope of surveillance under the "in accordance with law" test will be looked at.

As to the expression of "in accordance with law", it entails that the impugned measure ought to (1) have some basis in law and (2) be compatible with the rule of law, meaning it must satisfy requirements for the quality of law: the law must be (a) accessible to the person concerned, (b) foreseeable as to its effects and (c) necessary in a democratic society.[123] The main weight here is on the foreseeability requirement, which deals with the aspects relevant for an analysis of the scope of surveillance.

4.1 The foreseeability requirement

Essentially, the foreseeability requirement means that the law must enable the applicant to foresee its consequences to him or her.[124] The Court has more thoroughly clarified the notion in its jurisprudence on surveillance, by applying the same understanding of the concept in the different cases.[125] The Court has reiterated that foreseeability, in the special context of secret measures of surveillance, cannot mean that an individual should be able to foresee when the authorities are likely to conduct monitoring so that she can adapt her conduct accordingly.[126] However, the Court also notes that especially where executive power is exercised in secret, the risks of arbitrariness are evident.[127] As a safeguard against arbitrariness, the Court refers to the

[123] *Roman Zakharov v. Russia* paragraphs 228, 236; *Szabó and Vissy v. Hungary* at 59.
[124] *Szabó and Vissy v. Hungary* paragraph 59, See cited: several other cases establishing the rule.
[125] *Szabó and Vissy v. Hungary* paragraph 62; *Roman Zakharov v. Russia* paragraph 229, See cited: several other cases applying the same clarification.
[126] *Szabó and Vissy v. Hungary* paragraph 62.
[127] Ibid.

importance of having "clear and detailed rules" governing the use of the different surveillance techniques and technologies, particularly in light of the fact that the technology available for use is constantly becoming more sophisticated.[128] Thus, "the domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures".[129]

Several important points may be derived from the aforementioned description. To begin with, one may observe that the foreseeability requirement addresses the exercise of power by the national authorities. It is evident that the secrecy of government surveillance is not easily compatible with the requirement of foreseeability. Therefore, as the Court attempts to establish a delicate balance between the legitimate use of power by national authorities for the purpose of national security, and the risk of abuse of power, it requires not "full foreseeability" but "clear and detailed rules". Already from the outset the paradox inherent in this aim is clear: one can only wonder how is it possible to maintain both a high level of secrecy and a high level of transparency, referred to with the "clear and detailed" rules, without compromising one or the other. Since the clarity of rules is one of the key procedural safeguards that determine the legitimacy of a measure imposed by the state authorities, the level of precision required by the ECtHR must be carefully scrutinised.

In this respect, the Court indicates that the law must be "sufficiently clear" to give an "adequate indication" as to the (a) circumstances in which and (b) conditions on which the authorities may conduct secret surveillance. This is the basic premise on which the ECtHR scrutiny of the domestic surveillance laws is founded on. The qualifiers "sufficiently" and "adequate" illustrate the extremely difficult task of striking a balance between secrecy and foreseeability, as well as of the uneasy role of the Court in dealing with matters of exercise of sovereign power.

Thus, the ECtHR may be seen to resort to the margin of appreciation. It leaves room for interpretation in the notions of "sufficient" and "adequate", while at the same time it states that in the implementation of measures of secret surveillance "it would be contrary to the rule of law for the discretion granted to the executive or to a judge to be expressed in terms of an unfettered power".[130] In other words, the Court recognises the discretionary power of the national authorities to deal with matters of secret surveillance as part of a national security strategy, although that discretion is not unlimited. Strangely, the Court considers that an indication in the underlying law of the "scope of any such discretion conferred on the competent authorities and the manner of its exercise with 'sufficient clarity' to give the individual 'adequate protection' against arbitrary interference" [emphasis added by the author] limits the discretionary powers

[128] Ibid.
[129] Ibid.
[130] *Roman Zakharov v. Russia* paragraph 230.

of the authorities.[131] In this respect it is difficult to comprehend how the mere indication in law of the scope of discretion limits that discretion, let alone when such an indication may be left vague.

In any case, these observations reflect the difficult context in which the Court attempts to strike a balance between competing interests, the right privacy and the right to security, where the latter falls firmly in the sensitive area of state sovereignty. In essence, the Court attempts to uphold the discretionary power of the states to deal with matters of national security, while at the same time it cannot permit unlimited discretion, if it is to uphold the right to privacy. Thus, with respect to the requirement of foreseeability, the Court attempts to uphold the state interest in secrecy and vagueness, when it comes to surveillance for the purpose of national security, while at the same time it cannot permit unlimited secrecy and vagueness, if it is to ensure the legitimacy of the state practice by objectively verified standards and safeguard against abuse of power.

Therefore, in the following analysis, it is important to look at both the extent of discretion left with the national authorities and the rigidness of the foreseeability rules, which usually go hand in hand. In other words, it will be important to pay attention to how clear and precise does the ECtHR require the laws authorising surveillance to be. The more there is discretion, secrecy and vagueness, the more likely it is that the scope of surveillance, the true scale and purpose of it, will be extended. Thus, to examine whether the scale tips on one way or the other, siding more strongly on the side of secrecy and unclarity, or that of transparency and foreseeability, it is necessary to look closer at the circumstances in which and the conditions on which national authorities may legitimately conduct surveillance.

On a preliminary note, while turning to the specific requirements that address the scope of surveillance, one may note that the Strasbourg Court has in its jurisprudence on surveillance established a list of minimum safeguards that should be set out in law. The law must lay down (a) the nature of offences which may give rise to an order to conduct surveillance; (b) a definition of the categories of people liable to be targeted by surveillance; (c) a limit on the duration of surveillance; (d) the procedure to be followed for examining, using and storing the data obtained; (e) the precautions to be taken when communicating the data to other parties; and (f) the circumstances in which recordings may or must be erased or destroyed.[132]

For the coming analysis the two first safeguards are the most important. The Court has required that the national laws define the scope of secret surveillance "by clearly setting out the nature

[131] Ibid.
[132] *Roman Zakharov v. Russia* paragraph 231; *Szabó and Vissy v. Hungary* paragraph 56, See cited: several other cases establishing the rule.

of the offences which may give rise to an interception order and a definition of the categories of people liable to have their telephones tapped".[133] As explained earlier, one may note that the activities or offences giving rise to surveillance indicate the purposes for which surveillance maybe used. In turn, the persons monitored reveal the scale of surveillance. Thus, these two aspects will form the structure of the following assessment.

4.2 Purposes of surveillance

4.2.1 The nature of offences or activities giving rise to surveillance

As a starting point, although the nature of the offences giving rise to interception is to be established in "sufficient detail", the states do not have to set out exhaustively by name the specific offences.[134] This goes again to the context of secret surveillance, in which "national security" constitutes one of the legitimate aims referred to in Article 8 (2). The Court has emphasised that the requirement of "foreseeability" of the law does not compel states to enact legal provisions listing in detail all conduct that may prompt a decision to subject an individual to secret surveillance on "national security" grounds.[135] One reason stated for this is the nature of threats to national security, which may vary in character and may be unanticipated or difficult to define in advance.[136] Another reason why laws may contain vague expressions is that there is a need to avoid excessive rigidity and keep pace with changing circumstances.[137] The flexibility here is an indication of the margin of appreciation given to the national authorities. Clearly, the authorities enjoy a certain discretion in defining the offences giving rise to surveillance, but this discretionary power is not unlimited: the scope of it must be indicated in law.[138]

For an assessment of the limits of the scope of surveillance, it is essential to examine the extent of the discretion granted for the authorities in this respect. This determines which activities will eventually be subjected to surveillance. The less in detail the underlying activities or offences need to be defined, the higher is the likelihood that a wide range of activities will fall within the scope of surveillance.

The Court has held that where the national law merely lists the circumstances such as "national security", "public order", "protection of health", "protection of morals", "protection of the

[133] *Roman Zakharov v. Russia* paragraph 243.
[134] *Kennedy v. the United Kingdom* paragraph 159.
[135] *Roman Zakharov v. Russia* paragraph 247.
[136] *Kennedy v. the United Kingdom* paragraph 159.
[137] *Szabó and Vissy v. Hungary* paragraph 64.
[138] *Roman Zakharov v. Russia* paragraph 247; *Szabó and Vissy v. Hungary* paragraph 65.

rights and interests of others", "interests of ... the economic situation of the country", "maintenance of legal order",[139] as well as "receipt of information about events or activities endangering […] national, military, economic or ecological security",[140] giving rise to interception, the nature of the offences is not sufficiently clear.[141]

On the other hand, in *Weber and Saravia v. Germany*, the German legislation was considered by the Court to clearly and precisely define the offences potentially giving rise to secret surveillance, as it listed the following six dangers: an armed attack on Germany; the commission of international terrorist attacks in Germany; international arms trafficking and prohibited external trade in goods, data-processing programmes and technologies in cases of considerable importance; the illegal importation of drugs in substantial quantities into the territory of Germany; the counterfeiting of money committed abroad, and the laundering of money in the context of certain acts.[142] Surveillance measures could also be used against "serious crime", which was qualified in *R.E. v. the United Kingdom* as an offence to which the expected sentence is three years of imprisonment, or conduct, which involves the use of violence, results in substantial financial gain, or is conduct by a large number of persons in pursuit of a common purpose.[143] These cases illustrate how the Court requires some level of precision from the governments in defining the purposes for which surveillance measures may be used. This is an important limitation for the scope, since it restricts the discretion of the government authorities in determining which activities to target. However, one could wonder whether any qualification will be accepted without scrutiny of its content, since for example in the case of *R.E.* the mere conduct by a large number of persons in pursuit of a common purpose was accepted as one of the definitions of "serious crime", potentially leading to surveillance of any group action. This observation points towards the importance of assessing the legitimacy of a measure from a wider perspective, not only focusing on the procedural safeguards, but the overall acceptability of the power granted to the authorities. This will be turned to later in the research.[144]

The waters get muddier in the most recent *Szabó and Vissy* case. The ECtHR stated that the notions of "danger of terrorist acts" and the "needs of rescue operations" were sufficiently clear, and a "reference to terrorist threats or rescue operations" would give the citizens an adequate indication as to the circumstances in which public authorities could resort to surveillance.[145] The term "terrorist acts" was not defined in the Hungarian law authorising surveillance and

[139] *Iordachi and Others v. Moldova* paragraph 46.
[140] *Roman Zakharov v. Russia* paragraph 248.
[141] *Iordachi and Others v. Moldova* paragraph 46; *Roman Zakharov v. Russia* paragraph 203.
[142] *Weber and Saravia v. Germany* paragraphs 27, 96.
[143] *R.E. v. the United Kingdom* paragraph 133.
[144] See section 5.
[145] *Szabó and Vissy v. Hungary* paragraph 64.

could thus lead to a very wide range of activities being subjected to advanced surveillance technologies. For example, one may consider the difference between the *Weber and Saravia* case, where surveillance could be authorised only on the basis of international terrorist attacks in Germany, and that in *Szabó and Vissy*, where the danger of terrorism in general could warrant such surveillance. The former points to more concrete events and is limited to those within a given country, whereas the latter enables to gather information about nearly anything that relates to the phenomena in general. This is particularly worrying since there is no universally accepted definition of terrorism. Although, it is possible the Court has considered the definition of terrorism found in Hungarian Criminal Code applicable in the situation, as the Court refers to it in the judgment.[146] However, this definition is not explicitly discussed and therefore the content of the term "terrorist acts" remains unclear.

Also, some inconsistencies exist with respect to the notion of "national security". The Court first condemned the lack of definition in *Iordachi and others*.[147] Later in *Kennedy*, a very low degree of clarification, not found in the authorising law but in a Report of the Interception of Communications Commissioner dated 15 years prior to the law itself, was considered sufficient.[148] Finally, in *R.E.*, there was no requirement of any specification of the term visible in the decision, as the Court contended to merely note how the notion of "national security" is frequently employed in national and international legislation and constitutes one of the legitimate aims in article 8.[149] Less than two months later, the Grand Chamber in *Roman Zakharov* ruled that the absence of any indication in Russian law of the circumstances under which an individual's communications could be monitored, on account of events or activities endangering Russia's national security, meant there was no sufficient clarity of the circumstances required for the foreseeability of the law.[150] Although this was not the sole reason the interference with the right to privacy was found unjustified, it was mentioned as part of the main reasons for it.

In light of the foregoing, one may conclude that the exact extent to which the ECtHR requires the underlying activities to be specified in the laws authorising government surveillance remains unclear. The more in detail the activities triggering surveillance are defined, the less discretion the national authorities have in interpreting the law, and consequently, the more restrictive is the impact on the scope of surveillance in general. As stated by the Court in the case of *Roman Zakharov*, where the law did not specify the circumstances under which an individual's

[146] Ibid.
[147] *Iordachi and Others v. Moldova* paragraph 46.
[148] *Kennedy v. the United Kingdom* paragraphs 159, 33, The Commissioner had adopted the following definition for the term 'national security': "[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."
[149] *R.E. v. the United Kingdom* paragraph 133.
[150] *Roman Zakharov v. Russia* paragraphs 248, 302.

communications could be intercepted based on events or activities endangering national, military, economic or ecological security, the authorities would be left with "an almost unlimited degree of discretion in determining which events or acts constitute such a threat and whether that threat is serious enough to justify secret surveillance, thereby creating possibilities for abuse".[151] Although this decision is a clear indication that the ECtHR will require some level of specificity in defining the nature of the offences triggering surveillance, it remains unclear what is the exact level of precision and content the Court will accept from those definitions. Therefore, the situation cannot be considered as strictly limited, but there still seems to be plenty of room for interpretation left in the hands of the national authorities.

In the following section the paper turns to scrutinise the purposes for which the various surveillance methods may be employed, the activities or offences listed in the underlying law, from a wider perspective. To identify the exact limits of the scope of surveillance established by the ECtHR, one must look beyond the mere definition of the underlying acts or offences. Particularly, it is of utmost importance to consider the spectrum at which events unfold and identify how far from concrete situations an activity may still be considered to fall within the scope of the definition and thus become subjected to government surveillance.

4.2.2 The connection between the conduct monitored and the activities or offences giving rise to surveillance

To examine the real scale and purpose of surveillance more closely, one must look at the strength of a causal link required, for an activity to be considered as part of the sphere of influence of the underlying offence authorising surveillance in the first place. For example, in *Weber and Saravia* the ECtHR accepted the collection of information for the purposes of the "timely identification and avoidance" of the six "dangers" listed in the law authorising surveillance.[152] In *Kennedy* and *R.E.* intrusive surveillance could take place for the aim of "preventing or detecting" serious crime.[153] The concept of "detecting crime" was specified to include the "(a) establishing by whom, for what purpose, by what means and generally in what circumstances any crime was committed; and (b) the apprehension of the person by whom any crime was committed".[154] In *Szabo and Vissy* the Court raised no issues with the aim of the Hungarian domestic law, which authorised "the prevention, tracking and repelling" of terrorist acts.[155]

[151] Ibid., paragraph 248.
[152] *Weber and Saravia v. Germany* paragraphs 27, 96.
[153] *Kennedy v. the United Kingdom* paragraph 159; *R.E. v. the United Kingdom* paragraph 133.
[154] *Kennedy v. the United Kingdom* paragraph 35; *R.E. v. the United Kingdom* paragraph 58.
[155] *Szabó and Vissy v. Hungary* paragraph 63.

Two important observations can be made. First, the fact that the ECtHR has accepted the use of the various surveillance measures for the purposes of "avoidance", "preventing" and "repelling" of the acts enumerated in law has significant implications. For the overall scope of surveillance, it makes a great difference whether surveillance may be authorised only on the basis of evidence of a concrete offence or act, which falls within the clear and specified definition for that offence or act set out in law, or whether the various surveillance methods may be employed in order to prevent an offence or act, which may or may not materialise in the future. If monitoring is permitted for the purpose of preventing a potential threat or danger, there is a real risk the entire requirement established by the Court, that the nature of the offences giving rise to interception must be defined in "sufficient detail", loses its meaning. The range of activities that may consequently be monitored expands considerably. For example, the purpose of preventing a potential terrorist act could be interpreted as permitting a surveillance of any activities regarded by the authorities as connected to terrorism.

Second, the terms "identification", "detecting" and "tracking", combined with the preventative logic explained above, illustrate the interest of the governments to use surveillance for the purposes of identifying events that may develop into acts that threaten/endanger the interests of a state, as well as for discovering the people that are behind the activities monitored. This was expressly mentioned in a case decided by the Investigatory Powers Tribunal ("the IPT") dealing with the lawfulness of the acquisition and use of bulk communications data by the United Kingdom ("the UK").[156] It was found that the "use of bulk communications data is of critical value to the intelligence agencies, and is of particular value in identifying potential threats by persons who are not the target of any investigation", as argued by the UK government.[157] Also, the government position advocating for "the need for the haystack in order to find the needle" was considered persuasive by the Tribunal.[158] A similar interest is expressed in a Report by the Ministry of Interior of Finland concerning a proposal for a new law authorising civil intelligence.[159] It is stated that the proposed surveillance measures ought be available for the purpose of "detecting/identifying threats and the actors behind them".[160] A "threat", according to the Report, "does not mean situations that immediately threaten national security".[161] Surveillance could thus include the monitoring of activities that may develop to endanger national security in the future.[162] Equally well, they may not develop in that direction at all.

[156] *Privacy International v. SSFCA and Others*.
[157] Ibid., paragraph 14.
[158] Ibid., paragraph 14.
[159] 'Siviilitiedustelulainsäädäntö'.
[160] Ibid., 186.
[161] Ibid., 185.
[162] Ibid.

A few conclusions may be drawn from the abovementioned observations. First of all, the acceptance of the ECtHR of the use of surveillance measures for prevention of threats is worrying. There is no clarification as to how imminent, concrete or potential the threat needs to be to warrant surveillance. The discussion about the implications of this for the scope of surveillance is entirely lacking in the case law. Moreover, there is a considerable amount of literature concerning the shift in national security strategies and criminal law to prevention in general, which discuss the several risks involved in this development, particularly for the rule of law, and ultimately, for the ideal of justice. Unfortunately, it is beyond the scope of this research to discuss these implications further. Second, the interest of the states in having "the haystack to find the needle" raises serious concerns. If surveillance is permitted for the purpose of identifying or detecting potential threats and the people behind them, this would necessitate the collection and processing of vast amounts of data, which are not known to have any connection to the objective sought. Therefore, it would be of utmost importance that a real connection of the events monitored to the activities giving rise to surveillance is required.

In the next section, the other key determinant for the scope of surveillance will be assessed, namely, the range of persons that may be subjected to monitoring.

4.3 Scale of surveillance

4.3.1 The person or categories of persons as the targets of surveillance

To begin with, it must be borne in mind that the ECtHR has repeatedly upheld that the requirement of "foreseeability" does not compel the states to list in detail all situations giving rise to secret surveillance. The states are thus left with some margin of appreciation to determine when to subject activities or persons to monitoring. However, as it was explained earlier, the discretionary power left in the hands of the national authorities is not unfettered. This context is to be kept in mind in the analysis of the level of precision required in defining the categories of persons that may be subjected to monitoring. The more there is room for interpretation, the higher the risk that a broad category of persons will fall within the scope of surveillance.

What seems clear is that some definition of the categories of people liable to become targets of surveillance must exist as part of the minimum safeguards provided in the law.[163] In *Amann*, the law authorised the surveillance of persons suspected or accused of a crime or major offence, or third parties presumed to be receiving information from or sending it to such persons.[164]

[163] *Roman Zakharov v. Russia* paragraph 231; *Szabó and Vissy v. Hungary* paragraph 56, See cited: several other cases establishing the rule.
[164] *Amann v. Switzerland* paragraph 61.

However, the applicant had been monitored "fortuitously" as a "necessary participant" in a telephone conversation recorded by the authorities pursuant to the earlier mentioned provisions.[165] Since such a circumstance was not regulated in detail in the law, which also did not specify any precautions to be taken with regard to those persons, there was no sufficient clarity as to the scope and conditions of the authorities' discretionary power in the area.[166] This decision highlights how not any person may be targeted by surveillance measures. In *Iordachi*, the ECtHR adopted a degree vaguer approach. The law authorised interception of "a suspect, defendant or other person involved in a criminal offence", as well as where circumstances such as "national security", "public order", "protection of health", "protection of morals", "protection of the rights and interests of others", "interests of ... the economic situation of the country" or "maintenance of legal order" were at stake.[167] The law gave no explanation as to who would fall within the category of "other person involved in a criminal offence", nor did it specify the grounds giving rise to surveillance.[168] Interestingly, the Court was merely "concerned by the fact that the impugned legislation does not appear to define sufficiently clearly the categories of persons liable to have their telephones tapped", and noted it was unclear who would be at risk of having his telephone communications intercepted.[169] However, it did not declare the law was insufficiently clear in this respect.

The situation in *Roman Zakharov* was quite similar to the two abovementioned cases. The contested legislation authorised interception of a suspect, an accused, "a person who may have information about an offence", "a person who may have other information relevant to the criminal case", as well as on the basis of "events or activities endangering Russia's national, military, economic or ecological security".[170] The Court noted there was no clarification as to how the terms "a person who may have information about a criminal offence" and "a person who may have information relevant to the criminal case" were to be applied in practice, nor were the grounds giving rise to surveillance defined.[171] Thus, the authorities were left with a wide margin of discretion in interpreting the broad terms, thereby creating possibilities for abuse.[172] Notably, again, the ECtHR did not declare the law as insufficiently clear, but turned to examine the effectiveness of a prior judicial authorisation for interceptions, which could serve to limit the law-enforcement authorities' discretion and thus constitute "an important safeguard against abuse".[173]

[165] Ibid.
[166] Ibid.
[167] *Iordachi and Others v. Moldova* paragraphs 44, 46.
[168] Ibid.
[169] Ibid.
[170] *Roman Zakharov v. Russia* paragraphs 245–246.
[171] Ibid.
[172] Ibid., paragraphs 248–249.
[173] Ibid., paragraph 249.

To sum up, it is so far clear that a law authorising the monitoring of persons suspected, accused or involved as third parties in the activity or offence giving rise to surveillance is considered by the ECtHR to fulfil the foreseeability requirement. However, the monitoring of persons "fortuitously", without giving any indication of such a basis in law, is not accepted. In turn, the laws, which authorised monitoring of vaguely defined categories of persons, such as "other persons", considered as "involved" in the underlying activity or potentially having knowledge about/relevant to it, or, which authorised monitoring of persons on the basis of vague grounds such as "national security", were not declared by the Court as insufficiently clear. The Court did express its concerns that such terms did not appear to define the categories of people with sufficient clarity, and would instead leave the national authorities with too much discretion. Nevertheless, it did not clearly state that such a situation would be unacceptable. With a view to the limits for the scope of surveillance, the silence of the Court may indicate that the national authorities are, despite the concerns, left with a wide margin of appreciation to define the broad categories, potentially leading to a wide range of persons becoming subjected to surveillance. This seems to be particularly so if a prior judicial authorisation mechanism is found effective.[174] Which is interesting, since the prior authorisation, even if effective, cannot be seen to considerably limit the scope when such broad terms are accepted in law as the basis for monitoring.

When turning to the cases in which the Court has accepted the definition of the categories of persons targeted by surveillance as sufficiently clear, the situation gets even more concerning. In *Kennedy*, the Court rules that the warrant authorising surveillance "must clearly specify, either by name or by description, one person as the interception subject or a single set of premises as the premises in respect of which the warrant is ordered".[175] Such specification could be made by "names, addresses, telephone numbers and other relevant information".[176] The same rule has been included in other cases, most recently in the case of *Roman Zakharov*.[177] The implications thereof are unclear. First, it is surprising the decisions seems to provide for a choice to target surveillance either to a person or a single set of premises. If there is no requirement to specify the persons who may expect to become subjected to monitoring, the foreseeability safeguard is considerably weakened as a much wider group of persons, potentially unrelated to the underlying activity or offence, may fall within the scope. This is especially so, since the ECtHR has nowhere defined the notion "a single set of premises". For example, if applied to the surveillance measure of tapping fibre-optic cables, it is possible a cable or a part of that cable, in which information about the activity or offence giving rise to monitoring is expected to flow, could qualify as a premise. Keeping in mind the massive amount of communication that flows through those cables, one may easily conclude what a loophole in the law could mean for the scope of

[174] See citation no. 173.
[175] *Kennedy v. the United Kingdom* paragraph 160.
[176] Ibid.
[177] *Roman Zakharov v. Russia* paragraph 264.

surveillance. In this regard, it is also to be noted that the Court accepts "other relevant information" as a way to specify the person or the premise monitored, and not only an address or a name. What is exactly meant with "other relevant information" is not clarified by the ECtHR, consequently paving way to creative interpretations by national authorities.

In *Weber*, the ECtHR found that the categories of persons liable to be subjected to strategic monitoring were sufficiently indicated in the law.[178] The persons concerned had to have taken part in an international telephone conversation via satellite connections or radio relay links, or via fixed telephone lines in the case of averting an armed attack on Germany.[179] Additionally, the persons concerned either had to have used catchwords capable of triggering an investigation into the dangers listed in the law, or to be foreign nationals or companies whose telephone connections could be monitored deliberately in order to avoid such dangers.[180] Clearly, these are examples of the "other relevant information", which are accepted by the Court to specify the targets of surveillance. And as we can see, the parameters are wide. For example, if again examined in light of the tapping of fibre-optic cables, which contain a huge amount of private communications, the filtering of such cables by the use of catchwords necessarily results in immense amounts of private communications being caught by the system, which have no links to the activity or offence warranting surveillance in the first place. Thus, for the scope of surveillance, the impact is worrying. The Court itself pointed out the central concern in *Roman Zakharov* by stating that "interception authorisations which do not mention a specific person or telephone number to be tapped, but authorise interception of all telephone communications in the area where a criminal offence has been committed […] grant a very wide discretion to the law-enforcement authorities as to which communications to intercept".[181]

Lastly, in the most recent case, the *Szabó and Vissy*, the ECtHR seemed to take a clearer stance on the matter. It found the Hungarian law authorising the surveillance of "persons concerned identified ... as a range of persons", giving no clarification as to how the notion ought to be applied in practice, would potentially include any person and could be interpreted as "paving the way for the unlimited surveillance of a large number of citizens".[182] In the present case, the Court finally declared the category as "overly broad".[183] Perhaps even more importantly, it stated as the primary reason for the finding to be the lack of requirement for the national authorities "to demonstrate the actual or presumed relation between the persons or range of persons 'concerned' and the prevention of any terrorist threat – let alone in a manner enabling an

[178] *Weber and Saravia v. Germany* paragraph 97.
[179] Ibid.
[180] Ibid.
[181] *Roman Zakharov v. Russia* paragraph 265.
[182] *Szabó and Vissy v. Hungary* paragraph 67.
[183] Ibid.

analysis by the authoriser which would go to the question of strict necessity with regard to the aims pursued and the means employed".[184]

To conclude, it is so far only clear that the ECtHR will not accept the monitoring of "any person", but otherwise seems to leave the potential scope of surveillance wide open. However, the reference of the Court to the importance of establishing a connection between the target persons and the activity or offence authorising the surveillance, may be decisive for the future scope of surveillance. It is this link the paper turns to examine more in detail.

4.3.2 The connection between the persons monitored and the activities or offences giving rise to surveillance

For a closer scrutiny of the limits of the scope of surveillance, one must again look at the strength of a causal link required and examine the required level of suspicion of involvement in the offences or activities giving rise to surveillance. This will determine the scope of persons that may legitimately be monitored. The weaker the required level of suspicion of involvement in the underlying activity or offence, the wider the potential scope of persons surveyed.

First, one may note how the ECtHR observed in *Kennedy*, and later repeated in other related cases, that "there is an overlap between the condition that the categories of persons be set out and the condition that the nature of the offences be clearly defined. The relevant circumstances which can give rise to interception, […] give guidance as to the categories of persons who are likely, in practice, to have their communications intercepted".[185] This rule raises the question whether it could be regarded sufficient for a state to merely define the activities or offences giving rise to surveillance, so that any person, even where inadvertently caught in the process of monitoring, would be a legitimate target? In other words, the question is, whether it is permissible for example to grant a warrant for the filtering of fibre-optic cables, solely for the purpose of identifying the threat of terrorism, without the limitation that the surveillance is only targeted to those people reasonably suspected of planning, preparing, financing, committing or having committed a terrorist act.

The Court found in 2002 in *Greuter* that the surveillance of a person who was not suspected of any offence but could possess information about such an offence might be justified under article 8 of the ECHR.[186] In the cases of *Kennedy* and *R.E.*, the law did not define the persons who could be subjected to intrusive surveillance, but it did set out the relevant circumstances giving

[184] Ibid.
[185] *Kennedy v. the United Kingdom* paragraph 160.
[186] *Greuter v. the Netherlands*.

rise to intrusive surveillance, which in turn was considered by the Court to provide sufficient guidance as to the categories of person likely in practice to be subject to such surveillance.[187]

Again, only two months after the Fourth Section Court decision in *R.E.*, the Grand Chamber took a considerably different stance in the matter. It made an important ruling in the case of *Roman Zakharov* by declaring it had to be able 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".[188] The same rule was previously mentioned in the *Iordachi and Others*, in which only "very serious reasons based on a reasonable suspicion that the person is involved in serious criminal activity should be taken as a basis for authorising [an interception]".[189] The importance of this threshold of involvement for the scope of surveillance is essential. The national authorities would be required to give "factual indications", in other words, to prove by factual evidence, that a person or a category of persons is suspected of planning, committing or having committed an act warranting surveillance. Consequently, the people not connected to the activity with this threshold could not be monitored. Clearly, such a limitation could be the key method by which to limit the large-scale, untargeted and indiscriminate "bulk surveillance" of any person.

Unfortunately, the most recent decision, the *Szabó and Vissy*, departs from the said standard. Most of the observations here are based on the criticism raised by Judge Albuquerque in its concurring opinion of the judgement.[190] The Fourth Section Court ignored the paragraphs 260, 262, 263 of the *Roman Zakharov* judgment, which deal with the requirement of a "reasonable suspicion", and established a lower standard of an "individual suspicion" regarding the target person.[191] As the Judge Albuquerque points out, there was no any obstacle for the Court to apply the precise, demanding and qualified "reasonable suspicion" standard.[192] Most likely the real reason why the Court opted for the much lower standard, the "individual suspicion", which may be regarded "even below the lowest degree of bona fide suspicion or "initial suspicion" […] relevant in criminal law", is found in paragraph 79 of the judgment.[193] The Court refers to the importance of judicial control mechanisms that work to reinforce citizen's trust in the functioning of the guarantees of rule of law in the field of security and surveillance, as well as provide

[187] *Kennedy v. the United Kingdom* paragraph 160; *R.E. v. the United Kingdom* paragraph 134.
[188] *Roman Zakharov v. Russia* paragraph 260.
[189] *Iordachi and Others v. Moldova* paragraph 51.
[190] *Szabó and Vissy v. Hungary*, See attached in pages 43-59 of the judgment.
[191] Ibid., paragraph 71.
[192] Ibid., at 51–52, Concurring opinion of Judge Pinto de Albuquerque.
[193] Ibid., at 52, Concurring opinion of Judge Pinto de Albuquerque.

redress for the abuses sustained.[194] It notes the significance of these control mechanisms, particularly in view of the "magnitude of pool of information retrievable by the authorities applying highly efficient methods and processing masses of data, potentially about each person, should he be, one way or another, connected to suspected subjects or objects of planned terrorist attacks".[195] This shows how the Court believes in the "need for the haystack" in fighting terrorism,[196] and assumes that judicial control mechanisms will be enough to fix the consequent major legitimacy issues such as citizen's trust and abuse of power.

However, no control mechanism will remove the fact that unless a factually supported and suspicion based connection is required between the activities or offences giving rise to surveillance and the persons monitored, the national authorities are left with an unlimited discretion to monitor any person that may potentially link to the underlying activity or offence. The states have a growing interest for this kind of surveillance, as illustrated in the several recent legislative projects, and exemplified by the very clear statements of the UK and Finnish authorities. It is the employment of the surveillance capacities for "identifying potential threats by persons who are not the target of any investigation",[197] or for "detecting/identifying threats and the actors behind them",[198] which necessarily means there can be no, or at best very low, connection requirement.

Finally, as a brief conclusion of this section, one may note the importance of clearly and precisely defining both the activities or offences giving rise to surveillance as well as the categories of persons monitored in law. The vaguer the definitions, the more the national authorities have discretion in deciding whom and for what purpose to monitor. Moreover, it is important to require a clear link between the activities or offences and persons actually surveyed to the underlying activity or offence giving rise to surveillance. Again, the weaker the connection required, the wider the resulting scope of surveillance.

5 Necessary in a democratic society

The necessity test can be understood as the overarching test for an assessment of whether a restriction of a right is reasonably justified in a democratic society. It permits to go deeper into the substance of the restriction to evaluate the manner in which the authorities exercise public power and whether it can be considered fair. Thus, it corresponds to the broader understanding of the test of legitimacy used here. It is the test, which has the capacity to bring attention to, and

[194] Ibid., paragraph 79.
[195] Ibid.
[196] Ibid., at 52, Argued similarly in the Concurring opinion of Judge Pinto de Albuquerque.
[197] *Privacy International v. SSFCA and Others* paragraph 14.
[198] 'Siviilitiedustelulainsäädäntö', 186.

balance, both the values protected and jeopardised by the measure in question. Therefore, for the legitimate scope of surveillance, the test of necessity may well be the decisive element in determining on what scale and for what purpose can surveillance be justified in a democratic society. In the coming section, a brief overview of the strength and value of the "necessary in a democratic society" test in this respect is given.

5.1 The necessity test

The Court has noted that the notion of "necessary" is not equal to the expression "indispensable", nor does it have the flexibility of "admissible", "ordinary", "useful", "reasonable" or "desirable".[199] The term implies that the restriction of a right needs to be justified by a "pressing social need".[200] In its assessment, the Court will ascertain whether the respondent state has acted "reasonably, carefully and in good faith" and it will "look at the interference complained of in the light of the case as a whole and determine whether it was 'proportionate to the legitimate aim pursued' and whether the reasons adduced by the national authorities to justify it are 'relevant and sufficient'".[201]

For the purposes of this research, particular focus is given to the proportionality aspect of the test. The ECtHR has established in its case law, that a test of proportionality demands a balance to be struck between the restriction of a right and the legitimate aim pursued, taking into consideration the importance of the right limited in a specific instance.[202] In the context of surveillance this means striking a balance between the state obligation to respect the right to privacy, and the simultaneous obligation of the state to ensure the right to security through surveillance measures,[203] as discussed more extensively in the beginning of the this research. The task was aptly described in the case of *Klass and Others v. Germany*, where the Court agreed that "some compromise between the requirements for defending democratic society and individual rights is inherent in the system of the Convention […]. As the Preamble to the Convention states, 'Fundamental Freedoms ... are best maintained on the one hand by an effective political democracy and on the other by a common understanding and observance of the Human Rights upon which (the Contracting States) depend. In the context of Article 8, this means that a balance must be sought between the exercise by the individual of the right guaranteed to him under paragraph 1 and the necessity under paragraph 2 to impose secret surveillance for the protection of the democratic society as a whole".[204]

[199] *Handyside v. the United Kingdom* paragraph 48.
[200] *Observer and Guardian v. the United Kingdom* paragraph 59.
[201] Ibid. paragraph 59.
[202] *Ezelin v. France* paragraph 51.
[203] *Roman Zakharov v. Russia* paragraph 232.
[204] *Klass and others v. Germany* paragraph 59.

Before analysing the proportionality test more in detail, one must note how the Court has dealt with the necessity test in its recent case law on surveillance. First of all, it is to be kept in mind that also with respect to the question whether an interference is "necessary in a democratic society" in pursuit of a legitimate aim, the national authorities enjoy a certain margin of appreciation in assessing the pressing social need, in choosing the means for achieving the legitimate aim sought and the necessity of the measure to that end.[205] However, as it was earlier explained, the margin is not unlimited. In both of the most recent cases on surveillance, the *Roman Zakharov* and the *Szabó and Vissy*, the Court has stated that in order to determine whether the interference is kept to what is necessary in a democratic society, it must be satisfied there are adequate and effective guarantees against abuse.[206] The assessment is to take into account "all the circumstances of the case", such as the nature, scope and duration of the measures, the grounds for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law.[207] Notably, this means that the "necessity" test is equated with the test of lawfulness, the requirement that a restriction of a right needs to be "in accordance with law". The ECtHR expressly states in both cases that it will examine the two tests "jointly".[208]

Moreover, since the 1978 *Klass and Others v. Germany* decision, the Court has applied a test of "strict necessity" to the powers of secret surveillance of citizens.[209] Recently, in the case of *Szabó and Vissy*, the Fourth Section Chamber created a new definition of the "strict necessity" test.[210] The test would apply to two purposes: "as a general consideration, to the safeguarding democratic institutions and […], as a particular consideration, for the obtaining of vital intelligence in an individual operation.[211] However, it remains unclear what the "strict necessity" test consists of in practice. The clarification of the Court merely refers to the purposes for which the surveillance technologies may be used, which does not help to understand the content of the "strict necessity test".[212]

Consequently, some observations can be made of the manner in which the ECtHR deals with the necessity test in the context of secret surveillance. First, the absence of any clear indication as to how the test of necessity is to be applied in practice strengthens the conclusion that the treating of the two tests jointly, the "in accordance with law" and the "necessary in a democratic

[205] *Handyside v. the United Kingdom* paragraph 49; *Leander v. Sweden* paragraph 59; *Roman Zakharov v. Russia* paragraph 232.
[206] *Roman Zakharov v. Russia* paragraph 232; *Szabó and Vissy v. Hungary* paragraph 59.
[207] *Roman Zakharov v. Russia* paragraph 232; *Szabó and Vissy v. Hungary* paragraph 59.
[208] *Roman Zakharov v. Russia* paragraph 236; *Szabó and Vissy v. Hungary* paragraph 58.
[209] *Klass and others v. Germany* paragraph 42.
[210] *Szabó and Vissy v. Hungary* paragraph 73.
[211] Ibid.
[212] Ibid., at 53, Concurring opinion of Judge Pinto de Albuquerque.

society", in reality removes the test of necessity from the picture. It is clear that the Court only focuses on the procedural safeguards provided in law. This, in turn, reflects the difficult position of the Court in addressing directly the exercise of power by national authorities, particularly in matters of national security. Since it is essentially the use of sovereign power generally in a given context, rather than the use of power in a particular situation, that the Court deals with in the cases concerning secret surveillance, judged *in abstracto*. As the Court pointed out in *Szabó*, the interference found under article 8 concerns the applicants' "general complaint" and not "any actual interception activity allegedly taking place".[213] Therefore, in its scrutiny of the justification for the interference, the Court chose to focus on the legislation in question and the safeguards built into the system allowing for secret surveillance, rather than the proportionality of any specific measures taken in respect of the applicants.[214]

It might be that in the *in abstracto* cases concerning secret surveillance, the ECtHR is wary to address the issue of abuse of power by national authorities directly, since it is a societal interest that relates to the sovereignty of a state. Thereby the question of legitimacy would not only concern a specific action in a particular situation, but the exercise of power in general in a broader context. It might thus be a strategic move permitting the Court to engage in a matter threatening the rights protected by the ECHR, without taking too strong of a stance in a sensitive field, which might be met with total disregard by the states.

Although understandable, the choice of the Court to only focus on an assessment of the adequacy of procedural safeguards provided in a law authorising surveillance without going deeper in to the necessity test, has several implications, particularly, with respect to the scope of surveillance. A closer look at the proportionality aspect of the test will reveal the most important consequences of the Court's decision regarding the legitimate scope of surveillance.

5.2 The proportionality test

The proportionality test is essentially a balancing act which allows to examine whether the measure challenged is justified.[215] In the context of electronic surveillance, the test addresses the question whether the interference with the right to privacy is justified.[216] Proportionality is a general principle of EU law, which consists of an assessment of three components. First, the test includes an evaluation of the suitability or appropriateness of a measure to achieve the aim pursued. Second, there is an assessment of whether the measure is necessary to fulfil the said objective or whether a less intrusive means could be used to attain the same result. Last, the test

[213] Ibid., paragraph 58.
[214] Ibid., paragraph 58.
[215] Craig, 'Proportionality, Rationality and Review', 268.
[216] Tranberg, 'Proportionality and Data Protection in the Case Law off the European Court of Justice', 239.

calls for an assessment of proportionality *stricto sensu*, which is to ensure that the disadvantages caused by the measure are not disproportionate to the objectives sought by it. It is particularly within this last step of the assessment, taken if the measure conforms with the two other requirements of suitability and necessity, that the weighing of the two competing interests takes place.[217]

The normative value of the proportionality assessment, as a component of the necessity test, is that of substance.[218] While the requirement for the restriction of a right to be "in accordance with law" concerns the safeguards of form and procedure, the proportionality test goes deeper into the substance of a case. It is the test that demands a public body, which exercises power to achieve certain ends, to give reasoned justifications for the choices it has made.[219] Thus, it addresses the wider understanding of legitimacy used in this research. The public body is "to demonstrate that its contested action was necessary and suitable to achieve the end in view and that it did not impose excessive burdens on the individual".[220] Therefore, the test is an important element of the justification of a measure, such as surveillance, imposed by the public authorities. It is a check on the exercise of power to ensure that the measure is undertaken genuinely in the interest of democracy and that it "is not merely political expediency in disguise".[221]

Notably, the ECtHR has not looked at the suitability of surveillance technologies or techniques to achieve the goal of safeguarding national security. Nor has it made any evaluation of the necessity of the increasingly intrusive systems of secret surveillance in the sense that it has not paid any attention to the question whether the aims pursued could be achieved by less intrusive means. Most importantly, the Court has not assessed the surveillance technologies from the perspective of proportionality *stricto sensu*, although this would be vital in drawing a balance between the two rights.

With respect to the legitimate scope of surveillance, it may first be noted that the absence of the proportionality test has a broadening effect on the margin of appreciation exercised by the states in the field. The margin of appreciation leaves the national authorities with discretion to define the circumstances in which and the conditions on which surveillance may be conducted. The broader the discretion, the wider the scale and the range of purposes triggering surveillance, and consequently the interference with the right to privacy. The principle of proportionality in turn, would serve to limit the power of the national authorities and guard against excessive

[217] Andenas and Zleptnig, 'Proportionality: WTO Law: In Comparative Perspective', 389.
[218] Craig, 271.
[219] Ibid.
[220] Ibid., 272. See also: citations in footnote 26.
[221] Greer, 'The Exceptions to Articles 8 to 11 of the European Convention on Human Rights', 14.

interferences with human rights.[222] Where a strict proportionality test is applied by the ECtHR, the margin of appreciation is narrowed, and vice versa.[223]

Generally, for a comprehensive assessment of the legitimacy of an interference with the right to privacy, such as by the various surveillance technologies and techniques, the "in accordance with law" test alone is not sufficient.[224] The broader issues addressed by the proportionality test ought to be genuinely included in the review.[225] Blurring the functions of the two separate questions, the legality and necessity, poses a real risk that the protection of the right to privacy will be reduced.[226] The rapid development towards ever more intrusive surveillance technologies emphasises the importance to assess whether the means are suited to achieve the ends sought or whether less intrusive means could be used, and also whether the potential costs incurred are proportionate to the expected benefits. If the ECtHR took the requirements of the proportionality test under serious scrutiny in its judgments on government surveillance, it "could enable greater consideration of the context and scope of surveillance legislation and foster more effective protection of private life at the domestic level".[227]

6 Conclusion

This research was written in the wake of several legislative projects in Europe authorising the use of increasingly intrusive methods of surveillance. These systems interfere with the right to privacy, the deterioration of which may generate considerable negative consequences, culminating in the potential destruction of democracy. The paper was built on the premise that it is the scope of surveillance that differentiates democratic states from authoritarian police states. The term "scope" was understood in this context to comprise of the scale, in terms of the categories of persons monitored, and the purpose, the activities or offences giving rise to surveillance of surveillance. If the state is permitted to monitor any person and for any purpose, the right to privacy loses its position in shielding against the "tyranny of subjective interests", indefinitely justified in the name of "national security".

Although the state obligation to ensure the right to security may be a legitimate reason to employ some legislation on surveillance, a proportionate balance between the two interests, privacy and security, must be sought. To this end, the paper analysed the jurisprudence of the

[222] Arai and Arai-Takahashi, *The Margin of Appreciation Doctrine and the Principle of Proportionality in the Jurisprudence of the ECHR*, 2.
[223] Ibid.
[224] Murphy, 90.
[225] Ibid., 86.
[226] Ibid., 86.
[227] Ibid., 89.

ECtHR. It examined the manner in which the Court has dealt with the scope of surveillance from the perspective of legitimacy, a judicial principle broadly understood to refer to the substantive question of whether a measure or restriction can be considered justified, or valid, in a democratic society, including a narrower test of procedural conformity of the systems of surveillance with law.

The review of the ECtHR case law on surveillance, focusing on the key principles governing the scope of surveillance, permits to identify a few points of concern. First, the manner in which the Court deals with the most important procedural limitations, which have the potential to limit the scope of surveillance as analysed under the "in accordance with law" test, demonstrates a considerable level of unclarity with respect to the limits of surveillance. The fact that the Court considers that the "requirement of "foreseeability" of the law does not go so far as to compel States to enact legal provisions listing in detail all situations that may prompt a decision to launch secret surveillance operations", illustrates how there is ample room for creative interpretation by national authorities.[228] It is not clear exactly which activities or offences may authorise surveillance, as they do not need to be precisely defined in law. Moreover, there is no clear limitation as to what is the acceptable sphere of influence, or the connection, required for an activity or an event to fall within the scope of the underlying activity or offence triggering surveillance in the first place. Consequently, there is currently a great risk that the intrusive systems of surveillance can be used for purposes unforeseeable and potentially unacceptable in a democratic society.

Second, it is not clear which persons may be legitimately subjected to monitoring. The ECtHR does not require a precise definition in law of the categories of persons monitored, nor is the question of the required level of involvement in the underlying activities or offences straightforward. The Grand Chamber of the Court in 2015 referred to a requirement of "reasonable suspicion", whereas the Section IV Chamber in 2016 used the standard of an "individual suspicion". Whether the ECtHR eventually settles with the former threshold, which is more precise, qualified and demanding, or the latter, which at worse permits the surveillance of any person with a "potential link" to the underlying activity, is likely to have a considerable impact on the legally permissible scale of surveillance.

Thirdly, a scrutiny of the choices made by the Court with respect to the test of "necessary in a democratic society", reveal a gaping hole in the protective system of the ECtHR. The equation of the said test with the procedural "in accordance with law" test, together with the total lack of clarification of the content of the "strict necessity test", shows how the Court does not engage with a more substantive analysis of whether the intrusive systems of surveillance are justified

[228] *Szabó and Vissy v. Hungary* paragraph 64, See: concurring opinion of Judge Pinto de Albuquerque, p. 51.

in a democratic society. Particularly, the proportionality test, which demands that a measure must be justified as both suitable and necessary to achieve the aim sought, and that it may not cause disproportionate disadvantages, could lead to an important discussion of the permissible scope of surveillance. To conclude, in light of these observations, it seems the security side of the scale is currently given considerable weight, as opposed to the side of privacy. Whether the balance is just, ought to be carefully and repeatedly evaluated.

Finally, a word must be said of the scope of this research. It is acknowledged that the focus of this research is broad, compared to the time and space available, which limits the depth of the analysis. Nevertheless, one of the motivations for this research is to provide for an introduction to the key make-or-break points with respect to the present and pressing concern, the potentially ever-widening scope of surveillance. This paper may thus contribute to the forming of the basis for a more focused discussion and research on the legitimate scope of surveillance.

7 Table of reference

Primary sources

Case law of the European Court of Human Rights

Amann v. Switzerland, App no. 27798/95 (16 February 2000).

Bucur et Toma c. Roumanie, Requête no 40238/02 (Avril 2013).

Copland v. the United Kingdom, App no. 62617/00 (3 April 2007).

Greuter v. the Netherlands, App no. 40045/98 (19 March 2002).

Halford v. the United Kingdom, App no. 20605/92 (25 June 1997).

Handyside v. the United Kingdom, App no. 5493/72 (7 December 1976).

Huvig v. France, App no. 11105/84 (24 April 1990).

Iordachi and Others v. Moldova, App no. 25198/02 (14 September 2009).

Ireland v. the United Kingdom, App no. 5310/71 (18 January 1978).

Janowiec and others v. Russia, Apps no. 55508/07 and 29520/09 (21 October 2013).

Kennedy v. the United Kingdom, App no. 26839/05 (18 August 2010).

Klass and others v. Germany, App no. 5029/71 (6 September 1978).

Leander v. Sweden, App no. 9248/81 (26 March 1987).

Liberty and Others v. the United Kingdom, App no. 58243/00 (1 October 2008).

Malone v. the United Kingdom, App no. 8691/79 (2 August 1984).

Marckx v. Belgium, App no. 6833/74 (13 June 1979).

Observer and Guardian v. the United Kingdom, App no. 13585/88 (26 November 1991).

Öneryildiz v. Turkey, App no. 48939/99 (30 November 2004).

Osman v. the United Kingdom, App no. 23452/94 (28 October 1998).

R.E. v. the United Kingdom, App no. 62498/11 (27 January 2016).

Roman Zakharov v. Russia, App no. 47143/06 (4 December 2015).

Rotaru v. Romania, App no. 28341/95 (4 May 2000).

Szabó and Vissy v. Hungary, App no. 37138/14 (12 January 2016).

Tyrer v. The United Kingdom, App no. 5856/72 (25 April 1978).

Weber and Saravia v. Germany, App no. 54934/00 (29 June 2006).

Case law of the Investigatory Powers Tribunal

Privacy International v. SSFCA and Others (8 September 2017).

Secondary sources

Andenas, Mads, and Stefan Zleptnig. 'Proportionality: WTO Law: In Comparative Perspective'. *Texas International Law Journal* 42, no. 3 (2007). http://www.tilj.org/content/journal/42/num3/Andenas-Zleptnig371.pdf.

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

Bennoune, Karima. 'Terror/Torture'. *Berkeley Journal of International Law* 26, no. 1 (2008). https://doi.org/https://doi.org/10.15779/Z385Q0Q.

Bigo, Didier, Sergio Carrera, Nicholas Hernanz, Julien Jeandesboz, Joanna Parkin, Francesco Ragazzi, and Amandine Scherrer. 'Mass Surveillance of Personal Data by EU Member States and Its Compatibility with EU Law'. *CEPS Paper in Liberty and Security in Europe*, no. 61 (2013). http://aei.pitt.edu/45597/1/No_61_Surveillance_of_Personal_Data_by_EU_MS.pdf.

Bygrave, Lee A. *Data Protection Law: Approaching Its Rationale, Logic and Limits*. Information Law Series 10. Dortrecht: Kluwer, 2002.

Council of Europe. 'Annual Report 2016 of the Euroepan Court of Human Rights', March 2017. http://www.echr.coe.int/Documents/Annual_report_2016_ENG.pdf.

———. European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14 (1950). http://www.echr.coe.int/Documents/Convention_ENG.pdf.

Craig, Paul. 'Proportionality, Rationality and Review'. *New Zealand Law Review*, Articles by Maurer Faculty, 2010, 265–301.

Duffy, Helen. *The 'War on Terror' and the Framework of International Law*. 2nd ed. Cambridge: Cambridge University Press, 2015.

European Court of Human Rights Press Unit. 'Fact Sheet - Mass Surveillance', July 2017. http://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf.

'European Court of Human Rights Web Page'. Accessed 13 November 2017. http://www.echr.coe.int/Pages/home.aspx?p=court/judges&c=#newComponentl1346152138668_pointer.

European Parliament. European Parliament resolution on US NSA surveillance programme, surveillance bodies in various Member States and impact on EU citizens' fundamental rights, 2013/2188(INI) § (2014). http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0230.

Forsvarsdepartementet. 'Utreder et digitalt grenseforsvar'. Pressemelding. Regjeringen.no, 20 February 2017. https://www.regjeringen.no/no/aktuelt/utreder-et-digitalt-grenseforsvar/id2539809/.

Greer, Steven. *The European Convention on Human Rights: Achievements, Problems and Prospects*. Cambridge University Press, 2006.

———. 'The Exceptions to Articles 8 to 11 of the European Convention on Human Rights'. Council of Europe Publishing, 1997. http://www.echr.coe.int/LibraryDocs/DG2/HRFILES/DG2-EN-HRFILES-15(1997).pdf.

Guest author. 'Austria Creates New Agency with Unprecedented Surveillance Powers'. *EDRi* (blog), 9 September 2015. https://edri.org/austria-creates-new-agency-with-unprecedented-surveillance-powers/.

———. 'Italy: Anti-Terrorism Decree to Strengthen Government Surveillance'. *EDRi* (blog), 22 April 2015. https://edri.org/italy-anti-terrorism-decree-strengthen-government-surveillance/.

Gulijk, Coen van, Bert-Jan Kooij, Michelle Cayford, Martin Scheinin, Juha Lavapuro, Tuomas Ojanen, Jonathan Andrew, et al. 'SURVEILLE Paper Assessing Surveillance in the Context of Preventing a Terrorist Act', 2014. https://surveille.eui.eu/wp-content/uploads/sites/19/2015/09/D2-8-SURVEILLE-Paper-on-a-Terrorism-Prevention-Scenario-rev.pdf.

Gulijk, Coen van, Hauke Vagts, Sebastian Höhn, and Olexander Yaroyvi. 'SURVEILLE Deliverable 2.1: Survey of Surveillance Technologies, Including Their Specific Identification for Further Work', 2012. https://surveille.eui.eu/wp-content/uploads/sites/19/2015/04/D2.1-Survey-of-surveillance-technologies.pdf.

Koops, Bert-Jaap, and Ronald Leenes. '"Code" and the Slow Erosion of Privacy'. *Michigan Telecommunications and Technology Law Review* 12, no. 1 (2005): 115–88.

Koskenniemi, Martti. 'What Is International Law For?' In *International Law*, edited by Malcolm Evans, 4th ed. Oxford: Oxford University Press.

Lubin, Asaf. 'A New Era of Mass Surveillance Is Emerging Across Europe'. *Just Security* (blog), 9 January 2017. https://www.justsecurity.org/36098/era-mass-surveillance-emerging-europe/.

MacAskill, Ewen, Julian Borger, Nick Hopkins, and James Ball. 'GCHQ Taps Fibre-Optic Cables for Secret Access to World's Communication'. *The Guardian*, 21 June 2013. https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

Maria 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’. *Irish Journal of Legal Studies* 3, no. 2 (2013). http://ijls.ie/wp-content/uploads/2013/07/IJLS_Vol_3_Issue_2_Article_8_4_Comparative_Murphy.pdf.

‘Oxford Dictionaries’. Oxford Dictionaries | English. Accessed 29 November 2017. https://en.oxforddictionaries.com/definition/legitimacy.

Research Division of the European Court of Human Rights. ‘Sécurité Nationale et Jurisprudence de La Cour Européenne Des Droits de l’homme’. Council of Europe, 2013. http://www.echr.coe.int/Documents/Research_report_national_security_FRA.pdf.

Rodley, Nigel. ‘International Human Rights Law’. In *International Law*, edited by Malcolm Evans, 4th ed. Oxford: Oxford University Press, 2014.

Simmons, Ann M. ‘Two Years of Terror: 278 People Have Died in Recent Terror Attacks in Europe’. *Los Angeles Times*, 15 July 2016. http://www.latimes.com/world/europe/la-fg-europe-terror-20160715-snap-htmlstory.html.

Sisäministeriö. ‘Tiedustelulainsäädäntö’. Sisäministeriö. Accessed 2 November 2017. http://intermin.fi/tiedustelu.

‘Siviilitiedustelulainsäädäntö’. Mietintö. Ministry of Interior of Finland, 2017. http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/79759/SM_08_2017_Siviilitiedostelulainsaadanto.pdf?sequence=1.

Sloot, Bart van der. ‘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 *Data Protection on the Move*, 411–36. Law, Governance and Technology Series. Springer, Dordrecht, 2016. https://doi.org/10.1007/978-94-017-7376-8_15.

‘The European Convention on Human Rights - Introduction’. Accessed 13 November 2017. http://echr-online.info/echr-introduction/.

‘The SURVEILLE Website’. SURVEILLE. Accessed 29 November 2017. https://surveille.eui.eu/research/publications/.

The Venice Commission. ‘The Venice Commission Opinion No. 839/ 2016 on the Act of 15 January 2016 Amending the Police Act and Certain Other Acts’. Council of Europe Publishing, 13 June 2016. http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2016)012-e.

Tranberg, Charlotte Bagger. ‘Proportionality and Data Protection in the Case Law off the European Court of Justice’. *International Data Privacy Law* 1, no. 4 (2011): 239–48.

Tyler, Tom R. ‘Procedural Justice, Legitimacy, and the Effective Rule of Law’. *Crime and Justice* 30 (1 January 2003): 283–357. https://doi.org/10.1086/652233.

UN Special Rapporteur. ‘Report of the Right to Privacy A/HRC/13/37’. United Nations General Assembly, 2009. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G09/178/04/PDF/G0917804.pdf?OpenElement.