Surveillance, Privacy and Security

Citizens' Perspectives

Edited by Michael Friedewald, J. Peter Burgess, Johann Čas, Rocco Bellanova and Walter Peissl

Routledge
Taylor & Francis Group
LONDON AND NEW YORK

First published 2017
by Routledge
2 Park Square, Milton Park, Abingdon, Oxon OX14 4RN

and by Routledge
711 Third Avenue, New York, NY 10017

Routledge is an imprint of the Taylor & Francis Group, an informa business

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library

Library of Congress Cataloging-in-Publication Data
Names: Friedewald, Michael, 1965– editor.
Title: Surveillance, privacy and security : citizens' perspectives / edited by Michael Friedewald, J. Peter Burgess, Johann Cas, Rocco Bellanova and Walter Peissl.
Description: Abingdon, Oxon ; New York, NY : Routlede, 2017. |
Series: PRIO new security studies | Includes bibliographical references and index.
Identifiers: LCCN 2016043185| ISBN 978-1-138-64924-8 (hardback) | ISBN 978-1-315-61930-9 (ebook)
Subjects: LCSH: Electronic surveillance—Social aspects. | Electronic surveillance—Government policy. | Privacy, Right of—Social aspects. | National security—Social aspects.
Classification: LCC HM846 .S884 2017 | DDC 323.44/82—dc23
LC record available at https://lccn.loc.gov/2016043185

ISBN: 978-1-138-64924-8 (hbk)
ISBN: 978-1-315-61930-9 (ebk)

Typeset in Bembo
by FiSH Books Ltd, Enfield

9 Moving away from the security–privacy trade-off

The use of the test of proportionality in decision support

Bernadette Somody, Máté Dániel Szabó, and Iván Székely

The trade-off model and its critiques

Contrasting security to privacy is one of the well-known manifestation areas of the popular approach according to which competing values and demands in a democratic society, as well as the fundamental rights reflecting them, can only be realized at the expense of each other, by creating a balanced result in a virtual zero-sum game. In other words, realizing such a demand or right prevents people from realizing a competing demand or right, or more precisely, they need to waive the same amount of their demands or rights as much as they expect them to increase on the other side. In a narrower sense this trade-off approach can also be applied in situations where the mere preserving of the existing level of realizability of a certain demand or right – or at least the mitigation of its erosion – presupposes the waiving of a competing right or demand.

Naturally, the legitimization of this trade-off approach always necessitates the defining of an antipole, a competing demand or right. Privacy is one of the most frequently referred such antagonists of security.[1] This approach, however, inherently disregards the complexity of demands, values and legal rules in society together with their interdependencies, and reduces the problem to a single conflict, real or imaginary. Although this intention for simplifying the problems and making them easily comprehensible and acceptable for the public is understandable from the policy-makers' point of view, the temptation for abusing this oversimplified approach can lead to propagating a false image in society according to which in a democratic society every demand or right – in general, the realizing of public goods[2] – has a 'price' in the domain of public goods, which has to be paid by waiving certain demands or rights. This image may suggest a 'reasonable trade-off' between the competing demands or rights but at the same time masks the longer-term consequences, namely that not only the complementing demand or right will be eroding but also a host of associated rights, freedoms and values that the trade-off is designed to protect, including democracy itself.[3]

Loader and Walker (2007) argue that the concept of 'public good' can usefully be applied to the study of security, and can be expanded beyond its narrow

economistic usage in which it refers to non-excludable and non-rivalrous goods from which everyone benefits, such as fresh air or national defence. The concept of public good can also include shared societal goods such as liberty or freedom of expression, but additionally, it is argued, can be expanded further still to capture its broader role as a 'constitutive public good'; that is, a societal good understood as an integral and essential element of society itself.

In the present historical period when the importance of security in general is becoming more and more emphasized in politics, mass communication and public discourse alike, and when rapid technological developments and the associated business interests stimulate the introducing of new technologically mediated security measures, in particular surveillance measures, this trade-off approach can easily serve as an ideology for legitimizing unreasonable restrictions of fundamental rights, including privacy.

Although not contesting the existence and necessity of such trade-off situations, several theoreticians have criticized the exclusivity of this approach in the area of fundamental rights and, consequently, its exclusive application at various levels of decision-making. Charles Raab in his chapter 'From balancing to steering: new directions for data protection' (Raab, 1999) critically analysed the 'balancing paradigm' in privacy-related control mechanisms and observed that 'balancing often constitutes steering towards a preferred privacy outcome' and that '"balancing"' as such is an inadequate normative conception'. He also noted that in practice '"striking a balance" or "getting the balance right" remains a *mantra* rather than a practical philosophy for decision-making in difficult circumstances where fundamental issues are at stake' (p. 69). Others (Wright and De Hert, 2012; Wright and Raab, 2012) developed impact assessment methodologies to be used in situations when decisions have to be made over the introduction of privacy-intrusive and security-enhancing measures, such as increased surveillance. These methodologies aim to clarify the longer-term impacts, the identity of the affected parties, and the social and economic costs of the decision to be made, thus forcing the decision-maker to legitimize the envisioned 'balance' between security and privacy. In Chapter 3 of this volume Vermeersch and De Pauw (2016), from the aspect of public acceptance of new security oriented technologies, experimented with replacing the trade-off approach with 'framing' technologies.

From another angle, everyday practice and common sense may also contest the absolute primacy of the trade-off between privacy and security over other approaches. For example, if the question is whether enhancing the security and safety of homes should be achieved by installing more CCTV cameras in the house or by installing stronger locks on the doors, many would opt for the latter, since this solution increases *both* security and privacy of the people concerned, and there is no need for a trade-off between the two demands. Also instructive is the recent history of body scanners installed at US airports, introduced as a result of a typical trade-off between the enhanced security of travelling and the privacy of individual travellers. Investigations initiated by advocacy groups[4] revealed that the early X-ray devices were ineffective but seriously infringed travellers' dignity and privacy, and caused medical harms, so the trade-off was hardly legitimate. After a series of

lawsuits the scanners have been removed and replaced by less intrusive devices that do not record and transfer naked images of air travellers, still fulfilling their function of detecting weapons and explosives.

In the field of empirical sociology, researchers of the EU-supported international research project PRISMS[5] recently conducted a large scale empirical survey, the first of its kind to sample public opinion in all Member States to determine whether people evaluate the introduction of security technologies in terms of a trade-off. Although it is not the task of the present study to interpret the findings of this survey, the preliminary results already show that the importance of the two values, privacy and security, do not depend on each other at all in people's mind.[6]

Privacy vs. security is not the only field of application of the trade-off model. Since the fundamental values of society are reflected in the legal systems, it was a historical necessity during the course of developing democratic rule-of-law systems to work out methodologies by the use of which it became possible to manage such conflicts within the legal domain, in particular to judge the lawfulness of measures restricting fundamental rights. The present study is using one of the two historically developed such methodologies as the basis of further research.

The trade-off approach has infiltrated the policy level, too, sometimes simply serving the purpose of legitimizing those measures which restrict fundamental rights. Similarly, business entities, which have vested interests in introducing such measures, for example deploying and operating surveillance systems, and in convincing decision-makers to support the use of such systems, often use this argumentation for legitimizing their activities. In a broader sense it is the interest of the whole security industry (with a less polite term, risk industry) to use this argumentation for justifying the harmful side-effects of its activities on privacy, dignity, or equality, when fulfilling real demands for enhancing security. Those analyses, which evaluate the social advantages and harms of such measures, for example Norris (2012), Germain, Dumoulin and Douillet (2013) or Čas *et al.* (2014) often find these measures unreasonable, not only in terms of social costs but also in terms of economic costs (Groombridge, 2008).

The legal approach – the anatomy of the test

In the following we briefly present how democratic legal systems handle conflicting fundamental rights and legitimate interests, and show how the judicial practice seemingly corroborates the illusion of inevitableness of the trade-off. From among the two main methodologies developed in democratic rule-of-law traditions we analyse the European one, the test of proportionality in detail, and show how methodological rigour in using the test can help superseding the trade-off model within the legal domain.[7]

The concept of proportionality was originally developed by the German Federal Constitutional Court, but expanded far beyond Germany, and one can say that it became the post-war paradigm of human rights protection. The doctrine was also adopted by the European Court of Human Rights (ECtHR), since the interpretation of the limitation clauses of Articles 8-11 of the European

Convention of Human Rights (ECHR) were grounded on proportionality. The 'Strasbourg method' includes the identification of the legitimate aim of restrictions, and, under the 'necessary in a democratic society' clause, the examination of the necessity and proportionality of limitations.

Deciding about the lawfulness of the limitation of a fundamental right is also a methodological challenge. Should it be a constitutional or a conventional right, the responsible court – a constitutional court or the ECtHR – can make its decision verifiable, increase its persuasiveness and secure its authority if it strictly follows the steps of the limitation test where only the last step constitutes the actual balancing between the conflicting rights and interests, which involves, by its nature, moral arguments. Prior to that, the human rights courts, thus the ECtHR, too, have to decide, first, whether a fundamental right, protected by the given constitution or the Convention, is concerned in the case, and second, whether the quality of the law restricting the right meets the requirements.

The test of proportionality is not a single test: it consists of four sub-tests, namely the legitimate aim test, the suitability test, the necessity test and, finally, the proportionality test in the narrow sense (Figure 9.1).

During the first sub-test, a purpose can justify the limitation of a fundamental right if it is considered legitimate in society, if it is expresses a value on which the society is founded. In a constitutional democracy, generally speaking, safeguarding

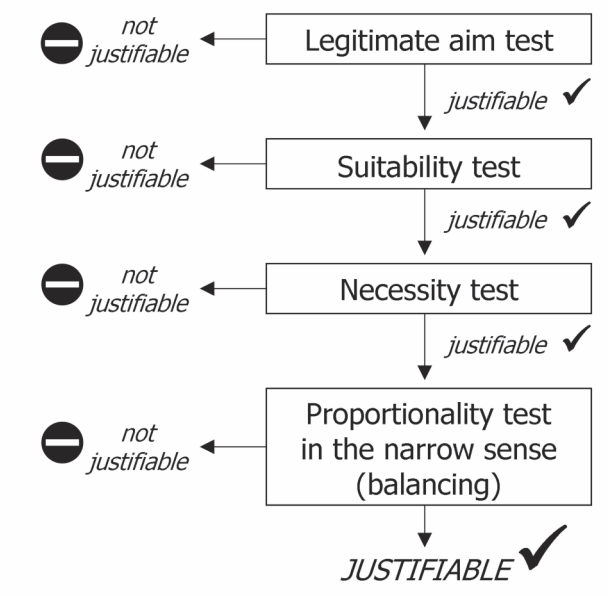

Figure 9.1 The structure of the test of proportionality

human rights and, to a certain extent, satisfying public interests can be taken into account as legitimate purposes. The ECHR contains special limitation clauses listing such legitimate purposes. It should be noted that from the viewpoint of a legal examination, the public interest of security as one of the legitimate aims does not need further justification when it or certain aspects thereof are explicitly named in the relevant limitation clause.

The function of the second sub-test is to determine whether the limitation of the fundamental right concerned – in case if it was found to have a legitimate aim – is suitable for realizing the aim. When deciding about the rational connection between the purpose of the limitation and the limiting measure, research results of other disciplines shall also be relied on. Sociology, criminology, and other disciplines offer scholarly achievements that make the decision on the suitability of the intrusive measure a question of fact. More CCTV cameras, for example – according to the results of criminological research – do not necessary lead to a higher level of security.[8]

In the third sub-test, after having established the legitimacy of the aim and the suitability of the limitation to achieve the given aim, the necessity of the limitation is examined, in other words, whether the limitation applies the *less restrictive means* in order to advance the legitimate aim. For example, justifying the necessity of a measure limiting privacy, non-legal measures also have to be taken into account: such measures, which are less intrusive or do not limit rights at all. Experience shows that there exist privacy-friendly, even non-surveilling, technologies for realizing the same security purposes.

The last sub-test, the proportionality test in the narrow sense, is the real field of (judicial) discretion which requires balancing between two values: on the one hand, the aim of the limitation and, on the other hand, the limited fundamental right. The limitation of a fundamental right is justified if there is a proper relation between the benefit gained by the realization of the aim and the harm caused to the fundamental right.

As we have seen, a series of methodological steps on the basis of these sub-tests should be taken in order to decide whether a limitation imposed on a fundamental right is justified. Even if these structural elements of the test of proportionality are not clearly identifiable in each judicial decision, the strict application of the methodology requires that the conducting of the next sub-test can only be permitted if the case concerned has successfully passed the preceding sub-test.[9]

The privacy/security conflict in the practice of the ECtHR

The test of proportionality is not explicitly recognized by the text of the European Convention on Human Rights. Nevertheless, the European Court of Human Rights interprets the limitation clauses attached to Articles 8-11 of the ECHR in accordance with the concept of proportionality and applies the methodological steps of the test.

The ECtHR – also known as the Strasbourg Court – can reasonably be considered to be the most significant *human rights* forum in Europe since it sets the

minimal standard of the protection of fundamental rights for European states and its case law is decisive also for the European Union and the European Court of Justice interpreting the EU Charter of Fundamental Rights.[10] A number of legal theorists and authors have analysed the ECtHR's case law in general and the application of the proportionality test in particular, presenting the steps of the test in great detail and quoting the most well-known cases extensively. The value added by the present study to this corpus of legal texts is the methodological rigour with which we followed and analysed the steps of the test of proportionality, the great number of cases analysed from this aspect, and the suggestions made in order to find legal solutions to supersede the predominant concept of 'balancing'.

In the following we focus on the Strasbourg Court's case law about privacy, especially the information aspect thereof which provides protection for human personality in connection with the processing of data relating to the person. This protection is guaranteed primarily by Article 8 of the ECHR on the right to respect for private and family life. The essence of the proportionality test here is that the limitation on privacy in the interest of security can be justified if the two values stand in balance. This method of legal interpretation seems to be favourable for the trade-off model according to which the debate between privacy and security is a zero-sum game and people are forced to choose between the two.[11] According to the test of proportionality, courts have to choose between conflicting rights and interests and set up a balance between privacy and security since, as the test of proportionality suggests, the conflict flows from the very fact that both of them cannot be secured at the same time. However, as we noted above, both practical experience and empirical surveys show that there exist means and methods the application of which can strengthen security and privacy at the same time; in addition, people regard security and privacy as separate values, thus they want both. Therefore, after analysing the application of the proportionality test in the practice of the ECtHR, we attempt to answer the question whether the trade-off between privacy and security can be superseded within the framework of the proportionality test.

Information privacy, data protection and the ECtHR's jurisdiction

The right to privacy is one of the human rights of primary importance which protects various aspects of human personality. Decisional privacy guarantees freedom to make decisions about one's body and family. Its continental counterpart, the right to self-determination, covers matters such as termination of pregnancy, sterilization, refusing life-sustaining treatments, consumption of drugs and sexual decision-making. However, several traditional privacy issues do not raise the question of balancing with security interests at all. Surveillance for security purposes concerns expressly the right to *information privacy,* a special segment of privacy securing protection against collection, use and disclosure of a citizen's personal information.[12] Surveillance aimed at enhancing security affects citizens by the fact that these tools and methods involves collection, storage, use and disclosure of their personal information, the exclusion of the access to personal data related to them

or the restriction of the control over their personal information. In order to analyse the 'privacy vs. security' conflict in the framework of the present project, we will focus on cases where the intrusion into citizens' private life is the result of *processing information* relating to them.

We argue that in the ECtHR's practice the protection of information privacy is based on Article 8 of the Convention, which guarantees everyone's rights to respect for their private and family life, their home and their correspondence – despite the fact that this Article does not use the category of personal information or personal data. The ECtHR does not clarify the theoretical relation of the right to privacy and to data protection. This is still an open question, as it can be described with more than one logical relation within the European legal systems, including the jurisprudence of the ECtHR.[13] Since there are existing judgments that interconnect these rights, it is plausible to argue that these rights have an overlapping common segment, however, privacy protection can aim at a different kind of protection than data protection does, and the scope of data protection covers personal information in a distant or indirect relation with the private sphere.

Nevertheless, throughout its jurisprudence, the ECtHR has examined many situations in which the issue of data protection arose, and all these cases were adjudged on the basis of Article 8 of the ECHR. Interferences with the right to personal data protection, including cases concerning protection against the interception of communications,[14] various forms of surveillance[15] and storage of personal data by public authorities[16] may be brought before the Strasbourg Court through the allegation of breach of the rights covered by Article 8. Surveillance and record-keeping of personal data are in close connection with the protection of private life. In some cases, where the Court had to decide whether there was an interference with the applicants' privacy rights – thus, when it examined the applicability of Article 8 – it consequently used the notion of *private life* as a broad term that is not susceptible to exhaustive definition,[17] but it undisputedly covers data protection issues. The Court holds that elements such as gender identification, name and sexual orientation and sexual life are important elements of the personal sphere protected by Article 8.[18] Article 8 also protects the right to identity and personal development, and the right to establish and develop relationships with other human beings and the outside world.[19] It may include activities of a professional or business nature.[20]

According to the Court, there is a zone of interaction of a person with others, even in a public context, which may fall within the scope of 'private life'.[21] According to the Court, private-life considerations may arise when any systematic or permanent record comes into existence of such material from the public domain. It is for this reason that files gathered by security services on a particular individual fall within the scope of Article 8, even where the information has not been gathered by any intrusive or covert method.[22] The Court's case law has, on numerous occasions, found that the covert tapping of telephone conversations falls within the scope of Article 8 in both aspects of the right guaranteed, namely, respect for private life and correspondence. While it is generally the case that the recordings were made for the purpose of using the content of the conversations in

some way, the Court also stated that recordings taken for use as voice samples cannot be regarded as falling outside the scope of the protection afforded by Article 8. A permanent record has nonetheless been made of the person's voice and it is subject to a process of analysis directly relevant to identifying that person in the context of other personal data. In a case where the applicant being charged by the police had to answer formal questions in a place where police officers were listening to them, the recording and analysis of their voices on this occasion must still be regarded as concerning the processing of personal data about the applicants.[23]

The broad field of case law interpreting security as the purpose of limitation of privacy covers various situations (for example where, because of detention, refusal of a residence permit or expulsion from a country to another, the applicants were incapacitated to communicate with close relatives, etc.). However, regarding the importance of security-purpose surveillance in limiting the right to privacy, we further narrowed down the scope of the analysis to those cases in which surveillance measures are in interference with information privacy. These cases concern typical conflicts between security and information privacy/data protection, such as interception of private communication, secret surveillance of individuals, registration of citizens in various databases for lustration purposes, or investigation of crimes.

Security as a legitimate aim

One can observe that the possible legitimate aims are exhaustively enumerated in the limitation clause attached to the declaration on the right to respect for private life. According to the second paragraph of Article 8, the interference must pursue national security, public safety or the economic wellbeing of the country, the prevention of disorder or crime, the protection of health or morals, or the protection of the rights and freedoms of others.

On the one hand, we can state that security as the purpose of a limitation can be considered a justified aim. On the other hand, however, only those aspects of security are acceptable *which are explicitly listed* in the cited paragraph. On the basis of the text of Article 8, the ECtHR is entitled to take security into account as national security, public safety or the prevention of disorder or crime. From a descriptive viewpoint it can be stated that security is present in the Strasbourg Court's practice as any of the mentioned categories.

Identifying the legitimate aim and deciding whether or not the limitation imposed on the right to privacy serves this aim are matter of facts and rational argumentation. At least in theoretical terms, these steps of the limitation test do not leave room for the discretion which manifests in the last phase of the test, namely in proportionality *stricto sensu*. It could be a yes or no question of whether or not security (or more precisely, enumerated aspects thereof) stand in conflict with the right to privacy in the given situation.

Being a question of facts and having an *expressis verbis* basis in the text of the Convention, the realization of the public interest of security could be considered as a strict requirement of the proportionality test applied in 'privacy vs. security'

conflicts. In fact, however, the examination of the legitimate aim proves that *this is the weakest component of this methodology.*

When analysing the ECtHR's case law on privacy and security one can identify several components of the right to privacy on the basis of which the scope of this fundamental right can be determined rather precisely. However, we cannot reach a similar result regarding the security-related purposes of limitation. The content of the relevant legitimate aims (national security, etc.) expressly listed in Article 8 is not expounded in the Court's practice. We cannot find abstract definitions or explanations in the decisions from which the notion of different aspects of security, or security in general, can be built up. The lack of defined contours of these categories is also proved by the fact that, in general, the Court does not refer to a single purpose of the limitation which can assumedly be selected as the relevant aspect of security in the case. The ECtHR often lists two or three security-related categories from Article 8(2), without defining the specific relevance of the different purposes.

The most frequently used formula by the Court simply enumerates *in one sentence a set of legitimate aims* that may be taken into account, for example *'the interests of national security or the economic well-being of the country or, just as equally, for the prevention of disorder or crime'*.[24] In other cases, the legitimate aims are *not even specified* in the judgment, the Court only declares that the '*restrictions pursued* one or more *of the legitimate aims enumerated in Article 8 § 2*.'[25] The eventuality of the referred legitimate aims is best proven when *the wording of the judgment indicates exemplification*, for example when the Court states that '*In the Court's view, it is not open to doubt that the monitoring of the applicant's correspondence pursued the legitimate aims of,* inter alia*, protecting 'national security' and/or preventing 'disorder or crime' referred to in Article 8 § 2*'.[26]

Analysing the cases where security-related purposes justified the limitation, one can find only a few sentences about the relevant legitimate aim where the ECtHR is satisfied with the mere indication of the purpose. In general, the Court does not make an attempt to define the conception of the referred legitimate aims and avoids any kind of reasoning on how and why the intervention by the state is serving the referred legitimate aim.

The lack of argumentation is represented by the wording used by the Court in paragraphs of judgments assessing the existence of one or more relevant legitimate aims of the intervention, such as '*the Court finds it established*'[27] or '*[t]he Court is prepared to accept*'[28] what the Government refers to, or when, according to the Court, the purpose pursued '*is not open to doubt*'.[29] The same occurs when '*the Court accepts the assertion by the Government*'.[30] The lack of a reverse statement of the applicant may be enough for the establishment of the legitimate aim: '*the applicant did not appear to deny that the impugned restrictions were imposed in pursuit of legitimate aims*'.[31] Furthermore, when none of the parties refers to or denies the establishment of a legitimate aim, the Court itself may assist them to do so:'*While the applicant contested the existence of a legitimate aim, the Government did not expressly refer to any legitimate aim pursued in this case. The Court, for its part, is ready to accept that the impugned measure pursued the legitimate aims of safeguarding national security and preventing disorder*'.[32]

The probability or possibility of the establishment of a legitimate aim may be enough to satisfy the Court: for instance, the intervention '*could have been in the interests*' of the relevant purposes, or '*the Court therefore concludes that the interference pursued a legitimate aim…*'.[33]

This leads us to the conclusion that, according to the Court's view, the reference to the security-related legitimate purpose of the restriction on privacy basically falls within the competence of the Government, which competence is untouched by the ECHR and is not subject to reconsideration by the ECtHR, resulting in that Strasbourg organs have very rarely found a violation of Convention rights by reference to the legitimate aim standard.[34,35]

Necessity and proportionality of the limitation of privacy

As we argued above, the ECtHR is rather reluctant to revise the governments' references to the different interests of security. Consequently the emphasis gets to the latter components of the test of proportionality. However, in these phases of the test the general tendency of the Court's argumentation is similar: it focuses the scrutiny on the 'necessary in a democratic society' standard.[36] This also means that the justification of a limitation on privacy is mostly a matter of balancing. The protection of privacy against the states' interests depends on the Court's discretion, which is manifested in comparing the weight of the interest of security with privacy.

We have to add here to the methodology of the test of proportionality that the ECtHR has developed, among others, the notion of the 'margin of appreciation'. This doctrine provides some sort of latitude to the national governments in certain cases, namely in lack of a European agreement, which is taken into consideration by the Strasbourg Court when it decides on the justification of a limitation and the proportionate balance. In respect of the limitation on privacy in the interest of security, this concept is of high importance, in these cases the ECtHR acknowledges the Member States' wide margin of appreciation.

In one of the most referred judgments about the justification of surveillance for security purposes, the Court summarized the relevant methodological steps of the legal evaluation, namely the assessment of necessity, proportionality and the consideration of the margin of appreciation, as follows: 'The notion of necessity implies that the interference corresponds to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued […]. However, the Court recognises that the national authorities enjoy a margin of appreciation, the scope of which will depend not only on the nature of the legitimate aim pursued but also on the particular nature of the interference involved. In the instant case, the interest of the respondent State in protecting its national security must be balanced against the seriousness of the interference with the applicant's right to respect for his private life'.[37]

Superseding the trade-off model within the test

Although the steps and the structure of the test of proportionality are well-known in legal literature and judicial practice alike, few have studied the possibility of

categorizing the phases of the test from another aspect, namely, whether the respective sub-test is based primarily on factual or moral considerations. If we compare the structural composition of the test with the cases analysed above and the ECtHR's practice in general, we will find that the first three sub-tests are based on factual elements, and only the last sub-test involves moral considerations, that is, the actual balancing that may be based on a trade-off approach (Figure 9.2).

Judicial practice in which the sub-tests are merged or not sufficiently separated, and in which the first three sub-tests are concluded in a nonspecific manner, may result in making the whole procedure subject to moral balancing, and this is a methodological reason for the seeming inevitableness of the trade-off. The first thesis of the present study is therefore that the better separation of the factual and moral phases in the test of proportionality and a shift in the weight of factual and moral elements of the test to the advantage of the factual ones, coupled with an enhanced methodological rigour, can lead to more substantiated judicial decisions in the security vs. privacy conflicts and reduce the application area of the trade-off model.

In the Strasbourg case law several other principles and factors can be identified which are to be taken into consideration when evaluating the 'privacy vs. security' conflict within the framework of the proportionality test. Therefore, we can formulate some auxiliary theses that may further specify and facilitate the application of the proportionality test to the specific conflict between surveillance and information privacy by national courts or other responsible authorities. One such auxiliary thesis is that Article 8(2) is to be interpreted narrowly. Being exceptions

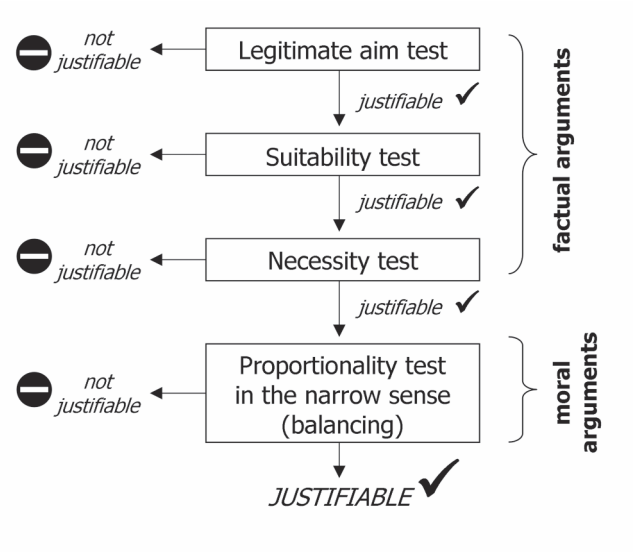

Figure 9.2 Factual and moral arguments in the test of proportionality

to the right to respect for private life, permissible limitations, such as the possibility of surveillance, have to be subject to a rigorous scrutiny. This general principle is acknowledged by the ECtHR: '[p]owers of secret surveillance of citizens, characterising as they do the police state, are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions'.[38]

Today, surveillance is realized mainly through various surveillance technologies,[39] consequently – as a second auxiliary thesis – it needs to be emphasized that the peculiarities of the surveillance technology used in the case under judgment are to be investigated. This may seem as a trivial requirement; however, the structured analysis of the peculiarities of technologies is relevant equally when the necessity and when the proportionality of the interference is adjudged. The use of an intrusive surveillance technology is considered to be necessary only if less intrusive methods of surveillance were considered ineffective. As for the proportionality in the narrow sense, the balance between the interest of security and the right to privacy can also be influenced by the characteristics of the technological means or the use thereof. Several questions can be raised, such as whether the technology used is interconnected with other technologies, who has access to the collected data, or when and for how long the surveillance technology have been operating.[40]

Third, it also needs to be emphasized that the significance of security reasons may depend on the 'historical' context. The Court often states that nowadays democratic societies find themselves threatened by highly sophisticated forms of espionage and by terrorism, with the result recognized by the Court that the state must be able, in order effectively to counter such threats, to undertake the secret surveillance of subversive elements operating within its jurisdiction. The Court therefore accepts that some surveillance measures, under exceptional conditions, are necessary in a democratic society in the interests of national security and/or for the prevention of disorder or crime.[41] The intensity of the threat of terrorism changes over the years, and the Court is aware of that: it accepts the context of threat of terror because of actual terror events as a reason for the adoption of intrusive measures by the legislation, but it also warns that the maintaining or the reinforcement of such measures over the years may not be justified for longer periods of time.[42] Passage of time may also blur the significance of personal data collected and therefore weakens the connection between the storage of the personal data and its legitimate aim, security. Continued storage may not be supported by the original reasons that may become irrelevant and insufficient after a longer period of time.[43]

Finally, it should be noted that in order to establish the balance between security served by surveillance measures and information privacy, certain procedural guarantees also have to be taken into consideration. These safeguards include the effective domestic judicial proceedings; the Court examines whether the domestic proceedings were attended by sufficient procedural guarantees. The Court emphasizes that even where national security is at stake, the concepts of lawfulness and the rule of law in a democratic society require that measures affecting fundamental human rights must be subject to some form of adversarial proceedings before an independent body competent to review the reasons for the decision and rele-

vant evidence, if need be with appropriate procedural limitations on the use of classified information. The individual must be able to challenge the executive's assertion that national security is at stake. Failing such safeguards, the state authorities would be able to encroach arbitrarily on rights protected by the Convention.[44]

The application of the test in decision support

Security/privacy trade-off is an established approach in judicial practice, but it is also popular in decision-making situations where privacy-restricting measures are introduced in the interests of greater security. This approach is regarded as natural not only by those communicators and PR professionals whose task is to 'sell' and make socially acceptable the security measures originating from business, policy or other interests, but also by the decision-makers who can legitimate for themselves, too, the measures to be introduced.

The above analysis and the resulting theses have shown that by the use of the necessary methodological rigour it is possible to move away from the primacy of the trade-off model even within the legal domain. In the next phase of our study we examined whether the methodology of the test of proportionality can be exported to the field of decision support, more precisely, to decisional situations regarding the introducing of surveillance measures which may infringe people's privacy.

Naturally, there exist significant differences between the two application domains: the test had originally been developed for the vertical relationship between the state and the citizens, whereas in the decision-making environment the test will serve as a decision support tool for the decision-maker itself, or will be relating to the relationship between the decision-maker and the supervisory authorities, or will help defend the decision in a political or social debate. A further difference is that it is not the task of the courts to suggest solutions for improving the acceptability of a privacy-restricting surveillance measure, or to call the decision-maker's attention to possible win-win type solutions; however, the decision-maker should expressly be encouraged to apply such solutions.

These differences made it necessary to modify certain steps in the test, their order and weight and to increase their detailedness, while keeping the fundamental elements of the test and the separation of factual and moral arguments.

The list below contains the questions the decision-maker needs to answer before making its decision on the introducing (maintaining, or expanding) surveillance measures that may infringe people's privacy. It should be noted that there exist decision support tools in this area, developed in recent years, which offer question lists, thus inducing stakeholders to ask questions from themselves and from the decision-maker alike.[45] Such a tool can *support* the decision-making process, indeed, but leaves it to the discretion of the stakeholders concerned which questions they want to ask and what weight they give to the respective answers. In contrast, our suggested methodology obliges its users to follow the questions step by step, and to proceed to the next question only if the previous one has been answered successfully – according to the logic of the test of proportionality, otherwise the decision will not be legitimate.

The list of questions

The user has to read all of the questions below and answer them to the best of his knowledge. If the user does not have enough information for the proper answering of the question concerned, he has to acquire the missing information before answering the question and continuing the procedure. Depending on the content of the answer, the user may proceed to the next question, or has to modify the planned measure, or – if the modification is not feasible – should desist from the implementation of the planned surveillance measure. The entire procedure is summarized in Figure 9.3.

1.1 Does the planned application of surveillance have implications on people's privacy?
It must be presumed that any kind of the application of surveillance technologies has such implications, however, there may be exemptions. The question is whether the surveillance in question can be qualified as such an exemption.

1.2 If the surveillance does not have privacy implications at present, will it likely have such an implication in the future?
It is possible that a CCTV system monitoring traffic uses low resolution cameras at present that do not allow the identification of individuals, however, when new, high resolution cameras will be installed, pedestrians and car drivers will become directly identifiable.

2.1 Does the surveillance in question have a legal ground? Could you identify the relevant legal ground?
Usually laws do not provide an explicit entitlement or prohibition on establishing a surveillance system. Instead, the application of one of the general legal grounds (e.g. informed consent of the subjects affected) is required.

2.2 Could you interpret the legal ground in a strict way? Could the strict interpretation result that the identified legal ground does not serve as a suitable basis?
For example, informed consent cannot be considered as a valid legal ground if it is not freely given (e.g. an employee's consent to the installation of a CCTV system at his workplace). In case of an explicit entitlement its scope has to be considered and interpreted narrowly (e.g. the specific legal ground for the surveillance of employees is not applicable for that of students).

2.3 Does the surveillance in question break an explicit legal prohibition?
Explicit legal provisions may inhibit surveillance in situations where the subject may have a reasonable expectation of privacy (e.g. in changing-rooms).

3 Could you identify the purpose of surveillance in question as precisely as possible?
The mere fact that surveillance systems are widespread and seem to be

useful for various purposes is not satisfactory here. The purpose should be specific as much as possible (e.g. recording potential thefts and identifying the perpetrators).

4.1 Could you identify the security risks that the surveillance is supposed to react against?
Similarly to the question of the purpose of surveillance, the concrete security risk should be identified precisely (e.g. vandalism, robbery, employees' idleness).

4.2 Is the surveillance in question capable of decreasing these security risks?
The fact that the surveillance system is suitable for decreasing the risks specified in the previous point should be verified, which means that it should be proven by sociological, criminological, psychological etc. evidence.

5.1 Can the purpose served by surveillance (identified in Question 3) be achieved without surveillance?
The decision-maker has to consider various alternatives to surveillance. Alternatives not having privacy implications (e.g. physical protection of property) should be preferred.

5.2 If the purpose can be served without surveillance, would it involve further implications on rights or interests other than privacy?
When considering alternative measures, possible consequences on legitimate rights and interests should be taken into account (e.g. physical protection of property can cause damages to the objects of property). The interference with a legitimate right or interest also requires answering a list of questions similar to this algorithm.

5.3 Could you identify the characteristics of the surveillance technology planned to be applied?
For example, what kind of personal or sensitive data are collected? Who will access to the data collected? Where, when and for how long will the surveillance means be applied?

5.4 Considering the characteristics identified in Question 5.3 one by one, can the purpose served by surveillance (identified in Question 3) be achieved by surveillance that intrude into privacy to a lesser extent?
For example, remote monitoring does not require a CCTV system storing the recordings.

6.1 Do the individuals affected by the surveillance in question have the possibility to exert control over their surveillance?
Individuals may have rights to influence the surveillance affecting them, i.e. to obtain information about and to challenge data relating to them. If individuals have some ability to have their data erased, rectified, completed or amended, it provides them with more practical protections.

6.2 Could you identify these possibilities of the individuals?
For example, are they informed proactively? Are they given further information about the details? Are they allowed to object to the surveillance in general or to certain parts of it, etc.

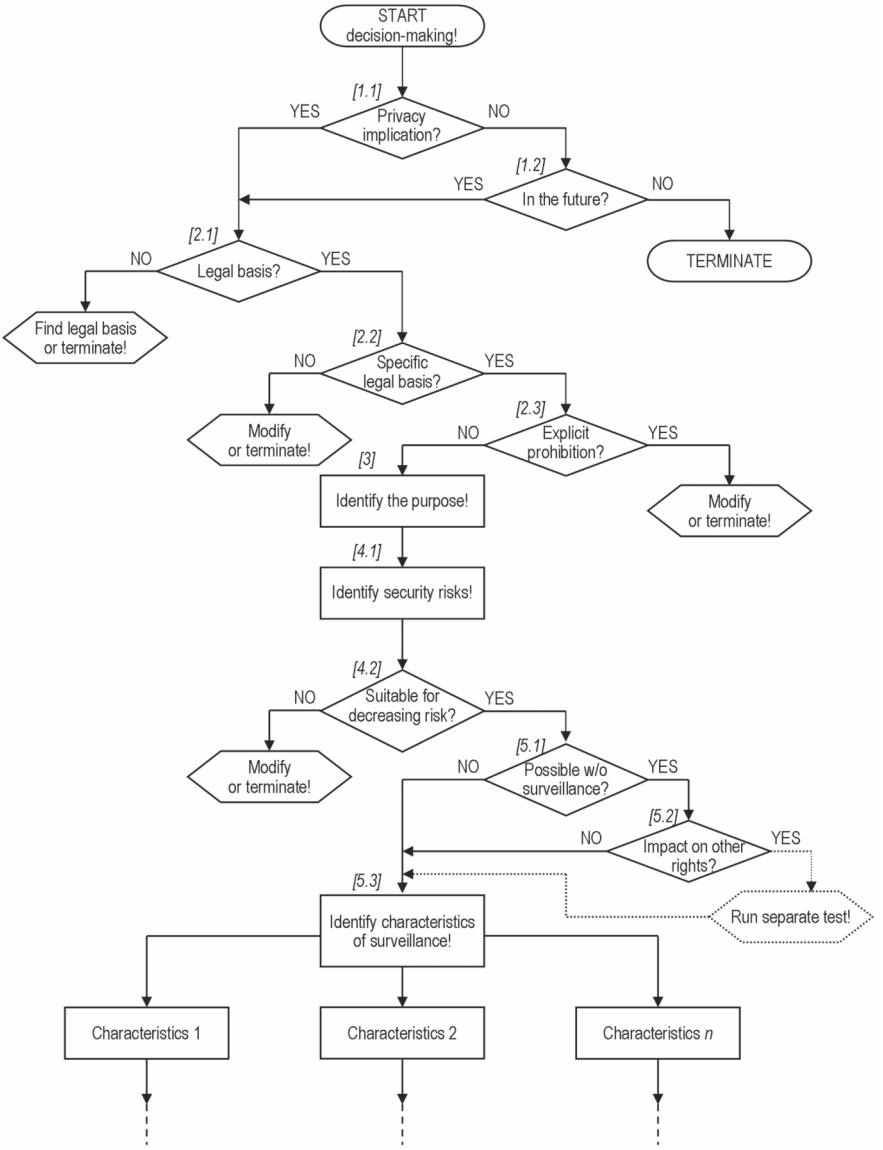

Figure 9.3a The steps of surveillance-related decision-making inspired by the test of proportionality (Part 1)

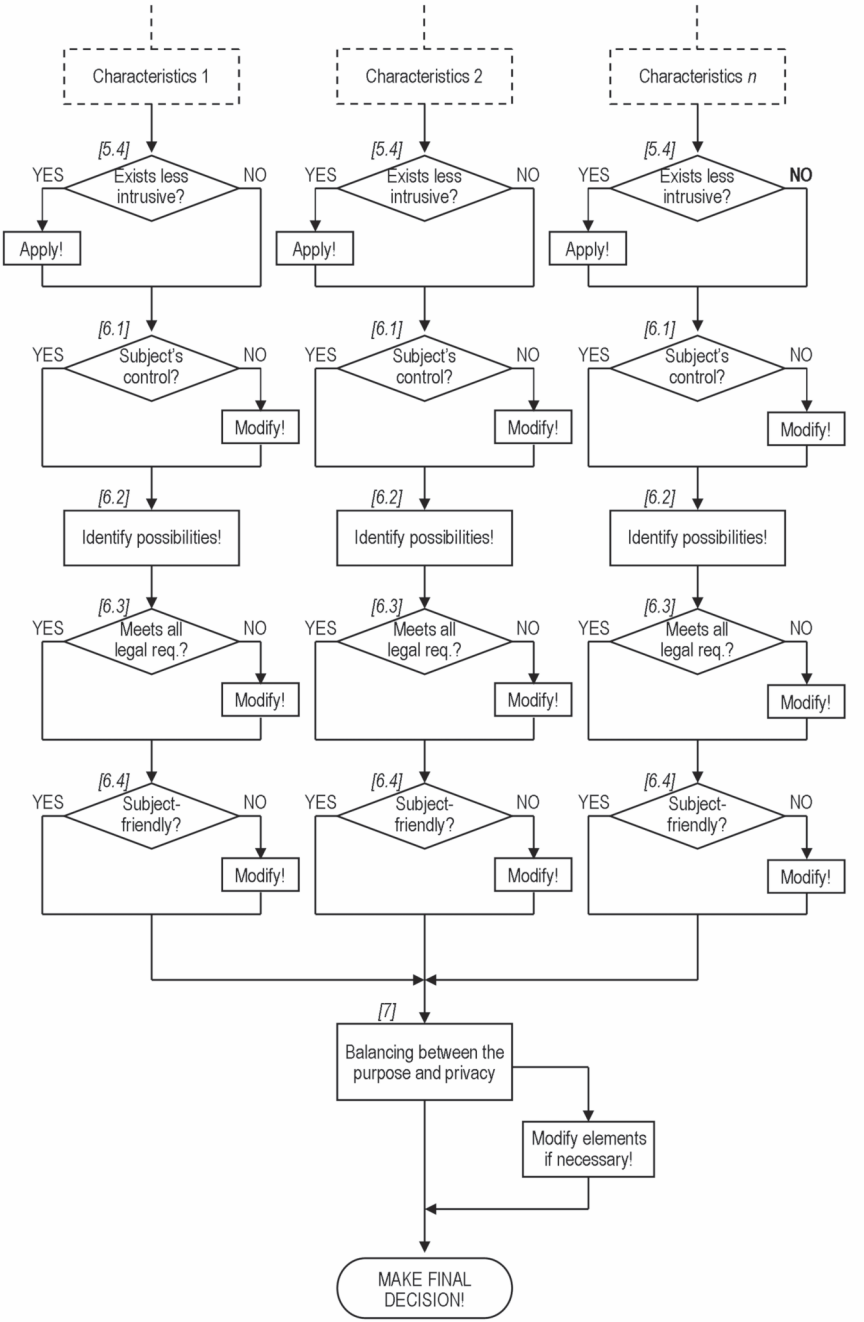

Figure 9.3b The steps of surveillance-related decision-making inspired by the test of proportionality (Part 2)

6.3 Do these possibilities meet all the requirements prescribed by law?
Certain rights of data subjects can be expressly regulated by legal provisions. For example, an opportunity shall be provided where the data subjects may personally view the recordings made and stored of their personal data, at the data controller's official premises, and make statement about the manner in which they wish to exercise their rights. The operator of a CCTV system has to obey this regulation.

6.4 Besides fulfilling the legal requirements, are the above mentioned measures (Questions 6.1–6.2) carried out in a 'data subject friendly' way?
Legal provisions usually leave some latitude for the implementation, i.e. the concrete manner of the fulfilment of obligations.

7 This is the ultimate balancing between the purpose identified in Question 3 and the privacy rights.

Summary of the decision support procedure

The above detailed flowchart reflects the logic of the above list of questions, completed with branching points, tasks, loops and termination points (Figure 9.3).

Conclusion

We have seen that the use of the test of proportionality is not merely an issue of legal dogmatics but it is highly relevant in judicial practice. According to our first thesis, by laying more emphasis on the first three phases of the test, the factual subtests, and by applying the necessary methodological rigour, the scope of balancing can be significantly reduced, and the primacy of the trade-off approach superseded. These effects can be further improved by taking our auxiliary suggestions into consideration.

We have also shown that this methodology, which had originally been developed for the relationship between the state and the citizens, can successfully be transposed into a different environment, namely the decision support procedures relating to the implementation of surveillance measures, which potentially infringe people's privacy. This new environment made it necessary to modify the order and relative weight of the steps in the test and to include detailed questions relating to the characteristics of the planned surveillance measures and their potential privacy implications. Nevertheless, we preserved the fundamental elements of the test of proportionality and the separation of factual and moral arguments. We formulated these methodological steps in the form of questions to be asked by the decision-maker himself. The whole procedure has been illustrated by a detailed flowchart.

In conclusion, our suggestions, if implemented, make it possible to move away from the security–privacy trade-off both in judicial practice and decision-making environments.

Notes

1 'Balancing privacy and security' results in more than 24 million Google hits in general search, and about 10.000 hits for the exact string.
2 We understand the concept of 'public goods' beyond its narrow economistic usage and include shared societal goods which are essential elements of society itself, see Loader and Walker (2007) or Raab, Jones and Székely (2015).
3 Raab, Jones and Székely (2015) analysed in detail the double-facedness of surveillance in the context of resilience in society.
4 The campaign was led by the Electronic Privacy Information Center (EPIC) and supported by a host of other NGOs, including religious organizations, see http://epic.org/privacy/airtravel/backscatter/
5 Privacy and Security Mirrors, www.prismsproject.eu The project declared as one of its main research ambitions to critically analyse the traditional trade-off model between privacy and security and devise a more evidence-based perspective for reconciling privacy and security. The present study is the outcome of a spin-off research originally started in PRISMS.
6 See the study of van den Broek *et al.* (2016) in Chapter 1 of this volume.
7 In the US conflicting fundamental rights are typically handled with the methodology of balancing between the rights, while the European approach is the use of the test of proportionality. The two end in analytically similar results and perform similar functions, and, leastwise, the final subtest of proportionality, i.e. proportionality in the strict sense, is analogous to the American balancing. The principal difference between the two methodologies is that the European approach, before arriving to the step of the ultimate balancing, follows a more analytical structure. For more details see Cohen-Eliya and Porat (2010).
8 There are a number of studies that have found security purpose CCTV systems to be ineffective. For a collection of these studies see: www.no-cctv.org.uk/caseagainst/reports.asp.
9 From the most current jurisprudence see Barak (2012).
10 It has to be noted that in one of its recent judgments on a privacy vs. security issue the European Court of Justice applied the test of proportionality in a very detailed and dogmatically rigorous manner. See judgment in joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others of 8 April 2014, on the invalidity of the Data Retention Directive.
11 Robert Alexy illustrates the balancing between the two conflicting principles with an indifference curve as it is used in economics (Alexy, 2010, 102–105).
12 Several well-known definitions or typologies of privacy attempt to grasp the essence of privacy as information privacy: the right to control knowledge about oneself (Fried, 1968, p. 475), the claim of individuals to determine for themselves when, how and to what extent information about them is communicated to others (Westin, 1967, p. 7), or, from among the recent studies, the 'seven types of privacy' (Finn *et al.*, 2013) also include information-centric elements, such as privacy of communication and privacy of data and image. On the distinction among different aspects of privacy and defining information privacy, see Solove *et al.* (2006).
13 On the relationship between privacy and data protection in contemporary European law, see Kokott and Sobotta (2013), or González Fuster (2014). See also González Fuster's study in Chapter 10 of this volume.
14 For example *Malone v. the United Kingdom*, no. 8691/79, 2 August 1984, *Copland v. the United Kingdom*, no. 62617/00, 3 April 2007.
15 For example *Klass and Others v. Germany*, no. 5029/71, 6 September 1978, *Uzun v. Germany*, no. 35623/05, 2 September 2010.
16 For example *Leander v. Sweden* no. 9248/81, 26 March 1987, *S and Marper v. the United Kingdom*, no. 30562/04, 4 December 2008.

17 See, for example, *Glor v. Switzerland*, no. 13444/04, § 52, ECHR 2009; *Tysi c v. Poland*, no. 5410/03, § 107, ECHR 2007-I; *Hadri-Vionnet v. Switzerland*, no. 55525/00, 14 February 2008, § 51; *Pretty v. the United Kingdom*, no. 2346/02, § 61, ECHR 2002-III; and *S. and Marper v. the United Kingdom*, nos. 30562/04 and 30566/04, § 66, ECHR 2008.
18 See, for example, *B. v. France*, 25 March 1992, Series A no. 232-C, § 63; *Burghartz v. Switzerland*, 22 February 1994, Series A no. 280-B, § 24; *Dudgeon v. the United Kingdom*, 22 October 1981, Series A no. 45, § 41; and *Laskey, Jaggard and Brown v. the United Kingdom*, 19 February 1997, *Reports* 1997-1, § 36.
19 See, for example Case of *Burgartz v. Switzerland,* no. 16213/90, opinion of the Commission, p. 37, § 47, and *Friedl v. Austria*, 31 January 1995, Series A no. 305-B, opinion of the Commission, § 45.
20 See *Niemietz v. Germany*, 16 December 1992, Series A no. 251-B, pp. 33–34, § 29, and *Halford v. the United Kingdom,* no. 20605/92, 25 June 1997, § 44.
21 See *von Hannover v. Germany (No. 2),* nos. 40660/08 and 60641/08, § 95.
22 See *Rotaru v. Romania*, no. 28341/95, §§ 43–44, ECHR 2000-V, *P.G. and J.H. v. the United Kingdom* no. 44787/98, 25 September 2001, § 59.
23 *P.G. and J.H. v. the United Kingdom*, § 59.
24 Example from case *Mubilanzila Mayeka and Kaniki Mitunga v. Belgium*, no. 13178/03, 12 October 2006, § 79.
25 See for example *Nada v. Switzerland*, no. 10593/08, 12 September 2012, § 174.
26 *Erdem v. Germany*, no. 38321/9, 5 July 2001, § 60.
27 *Nada v. Switzerland*, § 174.
28 *Liu v. Russia (No. 2),* no. 29157/09, 26 July 2011, § 80.
29 *Erdem v. Germany*, § 60.
30 *Drakšas v. Lithuania*, no. 36662/04, 31 July 2012, § 58.
31 *Nada v. Switzerland*, § 174.
32 Example from *Ciubotaru v. Moldova*, no. 27138/04, 27 April 2010, § 55.
33 Example from case *Mubilanzila Mayeka and Kaniki Mitunga v. Belgium*, § 79.
34 The same is true in general, regardless of the connection of purposes with security (van Dijk *et al.*, 2006, p. 340).
35 It deserves noting, however, that when dealing with privacy violations by the state through (mass) surveillance, the Court is willing to relax its focus on individual rights and interests. In some cases the Court is willing to accept claims based not on actual and concrete harm but on hypothetical harm or 'reasonable likelihood' (e.g. in *Malone v. the United Kingdom*). In other cases the Court recognizes the 'chilling effect' or the future harm as the basis for a claim (see for example *Marckx v. Belgium*). In certain cases the Court is even willing to accept *in abstracto* claims, despite the general inadmissibility of claims regarding the legality and legitimacy of laws and policies (see *Liberty and others v. the United Kingdom*). See van der Sloot (2016).
36 Van Dijk *et al.* (2006) p. 335.
37 *Leander v. Sweden*, no. 9248/81, 26 March 1987, §§ 58–59.
38 E.g. *Klass and Others v. Germany,* § 42.
39 In the field of security such technologies are called surveillance-oriented security technologies (SOST). Naturally, there exist a range of security technologies, which are not surveillance-oriented.
40 *Uzun v. Germany,* §§ 78–80.
41 *Klass and Others v. Germany*.
42 *Nada v. Switzerland*, § 186. The judgment refers to the years of the fear of terror after 9/11.
43 *Segerstedt-Wiberg and Others v. Sweden*, no. 62332/00, 6 June 2006, § 90.
44 *Liu v. Russia (No. 2)*. Procedural guarantees were the most significant element of the decision in cases *Klass and Others v. Germany* and *Leander v. Sweden*.
45 See for example the Handbook on Increasing Resilience in a Surveillance Society, developed by the IRISS consortium, available at http://irissproject.eu/?page_id=9

References

Alexy, R. (2010) *A Theory of Constitutional Rights.* Oxford: Oxford University Press.

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

Broek, T. van den, Ooms, M., Friedewald, M., van Lieshout, M. and Rung, S. (2016) 'Privacy and security – citizens' desires for an equal footing'. In: Friedewald, M., Burgess, J.P., Čas, J., Bellanova, R., and Peissl, W. eds. *Surveillance, Privacy and Security*. Abindgon; New York: Routledge, 15–35.

Čas, J., Strauß, S., Amicelle, A., Ball, K., Hallinan, D., Friedewald, M. and Székely, I. (2014) 'Social and economic costs of surveillance'. In: Wright, D. and Kreissl, R. eds. *Surveillance in Europe*. Abingdon; New York: Routledge, 211–258.

Cohen-Eliya, M. and Porat, I. (2010) 'American balancing and German proportionality: The historical origins', *International Journal of Constitutional Law,* 8(2): 263–286.

Dijk, P. van, van Hoof, F., van Rijn, A. and Zwaak, L. eds. (2006) *Theory and Practice of the European Convention on Human Rights*. Antwerp; Oxford: Intersentia.

Finn, R.L., Wright, D. and Friedewald, M. (2013) 'Seven types of privacy'. In Gutwirth, S., Leenes, R., de Hert, P. and Poullet, Y. eds. *European Data Protection: Coming of Age.* Dordrecht: Springer Science+Business Media B.V., 3–32.

Fried, C. (1968) 'Privacy', *Yale Law Journal*, 77: 475–493.

Germain, S., Dumoulin, L. and Douillet, A.-C. (2013) 'A prosperous "business": The success of CCTV through the eyes of international literature', *Surveillance and Society,* 11(1/2): 134–147.

González Fuster, G. (2014) *The Emergence of Personal Data Protection as a Fundamental Right of the EU.* New York; Dordrecht: Springer.

Groombridge, N. (2008) 'Stars of CCTV? How the Home Office wasted millions – a radical "Treasury/Audit Commission" view', *Surveillance and Society,* 5(1): 73–80.

IRISS Consortium (2014) 'Handbook on increasing resilience in a surveillance society: key considerations for policy-makers, regulators, consultancies, service providers, the media, civil society organisations and the public'. IRISS project, EC Grant Agreement No. 285593, available at http://irissproject.eu/?page_id=9 (accessed November 3, 2016).

Kokott, J. and Sobotta, C. (2013) 'The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR', *International Data Privacy Law,* 3(4): 222–228.

Loader, I. and Walker, N. (2007) *Civilizing Security.* Cambridge: Cambridge University Press.

Norris, C. (2012) 'The success of failure. Accounting for the global growth of CCTV'. In Ball, K., Haggerty. K.D. and Lyon, D. eds. *Routledge Handbook of Surveillance Studies.* London and New York: Routledge, 251–258.

Raab, C. (1999) 'From balancing to steering: new directions for data protection'. In Bennett, C.J. and Grant, R. eds. *Visions of Privacy: Policy Choices for the Digital Age*. Toronto: University of Toronto Press, 68–93.

Raab, C., Jones, R. and Székely, I. (2015) 'Surveillance and resilience in theory and practice', *Media and Communication,* 3(2): 21–41.

Sloot, B. van de (2016) '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 Gutwirth, S., Leenes, R. and De Hert, P. eds. *Data Protection on the Move.* Dordrecht: Springer, 411–436.

Solove, D.J., Rotenberg, M. and Schwartz, P.M. (2006) *Privacy, Information and Technology.* New York: Aspen Publishers.

Vermeersch, H. and De Pauw, E. (2016) 'The acceptance of new security oriented technologies, a "framing" experiment'. In: Friedewald, M., Burgess, J.P., Čas, J., Bellanova, R., and Peissl, W. eds. *Surveillance, Privacy and Security*. Abindgon; New York: Routledge, 52–70.

Westin, A. (1967) *Privacy and Freedom*. New York: Atheneum.

Wright, D. and De Hert, P. eds. (2012) *Privacy Impact Assessment*. Dordrecht: Springer.

Wright, D. and Raab, C. (2012) 'Constructing a surveillance impact assessment', *Computer Law & Security Review,* 28(6): 613–626.