The half-way revolution of the European Court of Human Rights, or the 'minimum' requirements of 'law'

Since 2015, the European Court of Human Rights has delivered three cases that revolve entirely around an assessment of 'the quality of law'. These cases are not brought by claimants that are able to demonstrate that they have been harmed individually and specifically by a violation of one of their human rights. Rather, the Court assesses in abstracto whether the legal regime abides by the principles of the rule of law and separation of power. Doing so, it has set out nine, what it calls, 'minimum requirements of law'. This is a revolution, because the ECtHR used to assess cases only when a claimant could prove to have been harmed substantially and individually by a concrete human rights violation, balancing the different rights at stake, in light of the circumstances of the case. Remarkably, however, the Court allows for a number of exceptions that make clear that these principles are neither exactly 'minimum' requirements, that must be respected always, nor principles that only the 'law' must adhere to, accepting that they find their meaning and significance in practice. Although the Court takes a seemingly revolutionary path, it is no Marat, but a Mirabeau at best.

0. Introduction

For a long time,[1] the requirement that an interference with a human right contained in the European Convention on Human Rights (ECHR) should have a legal basis was applied to the executive branch only and focussed on the question whether governmental agencies stayed within the limits set out by the law.[2] But around the 80ties of the previous century, a new doctrine started to emerge, namely that laws should be accessible and foreseeable.[3] By introducing these principles, the ECtHR shifts the attention from the question of whether the executive power has abided by the boundaries set out by the legislative power, to the question of whether the legislator has made laws that are sufficiently clear to citizens. Although the European Court of Human Rights was initially hesitant to apply the principles of accessibility and foreseeability to matters concerning the right to privacy, it was with cases on Article 8 ECHR that this doctrine gained significance, precisely because these principles are difficult to uphold in cases revolving around secret surveillance and special police investigations (secrecy and unforeseeability being essential to effective secret surveillance measures).

Because the guarantees of accessibility and foreseeability are applied flexibly in those types of cases, the Court has stressed that the law must provide for other guarantees to avoid abuse of power. The Court has emphasized that when the legislative branch transfers powers to the executive branch, especially in contexts where individuals are left in the dark when the executive has used its discretion, there is an extra onus on the legislator to set tight conditions and restrictions on the use of power: 'the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference.'[4]

[1] This contribution is partly based on: B. van der Sloot, 'The Quality of Law: how the European Court of Human Rights gradually became a European Constitutional Court for privacy cases', JIPITEC, 2020-3.
[2] See e.g.: ECtHR, Lewak v. Poland, application no. 21890/03, 06 September 2007.
[3] ECtHR, Sunday Times v. the United Kingdom, application no. 6538/74, 26 April 1979, § 49.
[4] ECtHR, Malone v. the United Kingdom, application no. 8691/79, 02 august 1984, § 68.

Although the Court still points to the importance of legal certainty for citizens, over time, its main concern has become not so much the abuse of power by the executive branch (using powers beyond the boundaries set by the legislator) but the arbitrary use of power (where the executive stays within those boundaries, but the problem is that the boundaries are very broad or non-existent). In addition, an important alteration is that the principle of foreseeability is interpreted not so much as requiring that citizens should be able to know which actions are or are not prohibited (as secret surveillance by police units or intelligence agencies are generally introduced to uncover terrorist cells, organised crimes, etc., with respect to which there is generally no discussion that they are prohibited) but with the foreseeability of how the executive branch would use its powers, when and as regards whom.

Consequently, while the original formulation of the notions of accessibility and foreseeability concerned the relationship between the legislative branch and citizens, this interpretation of the principles focusses primarily on the relationship between the legislative branch and the executive branch, as the legislative power must set clear boundaries for the use of power the executive must respect.[5] In an increasing number of cases, the Court focussed almost entirely on the existence of adequate safeguards against the abuse of power.[6] For example, in a case on wire-tapping, it stressed a number of legal requirements, such as, but not limited to:

- Clarity with respect to the categories of people liable to have their telephones tapped;
- Clarity with respect to the nature of the offences which may give rise to such an order;
- Existence of a limit on the duration of telephone tapping;
- Having in place a procedure for drawing up the summary reports containing intercepted conversations;
- Clarity on the point of the precautions to be taken in order to communicate the recordings for possible inspection by the judge and the defence; and
- Clarity about the circumstances in which recordings may or must be erased.[7]

More and more, the Court emphasised requirements such as oversight by an independent judge and whether the law indicates with sufficient clarity the scope and conditions of exercise of the authorities' discretionary power,[8] emphasising that it must 'be satisfied that there exist adequate and effective safeguards against abuse, since 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. In order for systems of secret surveillance to be compatible with Article 8 of the Convention, they must contain safeguards established by law which apply to the supervision of the relevant services' activities. Supervision procedures must follow the values of a democratic society as faithfully as possible, in particular the rule of law, which is expressly referred to in the Preamble to the Convention. The rule of law implies, *inter alia*, that interference by the executive authorities with an individual's rights should be subject to effective supervision, which should normally be carried out by the judiciary, at least in the last

[5] ECmHR, Mersch and others v. Luxemburg, application nos. 0439/83, 10440/83, 10441/83, 10452/83, 10512/83 and 10513/83, 10 May 1985.
[6] Ibi ECtHR, Olsson v. Sweden, application no. 10465/83, 24 March 1988, § 62.
[7] ECtHR, Kruslin v. France, application no. 11801/85, 24 April 1990. ECtHR, Huvig v. France, application no. 11105/84, 24 April 1990.
[8] ECtHR, Kopp v. Switzerland, application no. 23224/94, 25 March 1998. ECtHR, Amann v. Switzerland, application no. 27798/95, 16 February 2000. See also: ECtHR, Valenzuela Contreras v. Spain, application no. 27671/95, 30 July 1998.

resort, since judicial control affords the best guarantees of independence, impartiality and a proper procedure.'[9] Step by step, the notion of 'quality of law' became a full-fledged doctrine.[10]

An important next step was taken by the European Court of Human Rights in December 2015, in Zakharov v. Russia.[11] That case was revolutionary for two reasons. First, after more than 60 years of rejecting *in abstracto* claims, in which the applicant complains about the law or policy of a Member State as such, without claiming to be harmed herself, the Court made explicit that in cases revolving around secret surveillance, where people generally do not know whether they have been the target of data gathering activities, this principle could no longer be upheld.[12] Second, because the Court cannot evaluate whether there was an interference of the right to privacy of the claimant, whether that interference was prescribed by law, whether that interference was in the public interests and whether a fair balance was struck between the competing interests at stake, the Court's only task is to assess whether the law of the Member State abides by the minimum requirments of law.

It took a similar approach in two more cases since: Centrum För Rättvisa v. Sweden (2018)[13] and Big Brother Watch and others v. the United Kingdom (2019).[14] While Zakharov revolved around secret surveillance of selected persons or groups, the two others revolved around bulk interception regimes. While the claimant in Zakharov was a natural person, the Swedish case was brought by a legal person and the applicants in the Big Brother Watch case were both legal and natural persons. In the cases of Zakharov, Centrum för Rättvisa and Big Brother Watch, the Court distinguishes between various minimum requirements of law, which Member States' law must abide by. This article will discuss per section how the Court has interpreted these minimum requirements of laws and show that it will allow for exceptions to these principles in two types of cases. First, where a Member State performs poorly on one minimum requirement,

[9] ECtHR, Rotaru v. Romania, application no. 28341/95, 04 May 2000.

[10] See inter alia: ECtHR, Hasan and Chaush v. Bulgaria, application no. 30985/96, 26 October 2000. ECtHR, Gorzelik and others v. Poland, application no. 44158/98, 17 February 2004. ECtHR, Bordovskiy v. Russia, application no. 49491/99, 08 February 2005. ECtHR, Weber and Saravia v. Germany, application no. 54934/00, 29 June 2006, §94-95. See also: ECtHR, Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, application no. 62540/00, 28 June 2007. ECtHR, Liberty and others v. the United Kingdom, application no. 58243/00, 01 July 2008. ECtHR, Iordachi and others v. Moldova, application no. 25198/02, 10 February 2009. In 2010, the Court even applied the doctrine of quality of law to professional assistance with home births. ECtHR, Ternovsky v. Hungary, application no. 67545/09, 14 December 2010. But the Court also found limitations. For example, in the case of Uzun from 2010, the Court stressed that minimum requirements of law were developed by the Court in the context of applications concerning the interception of telecommunications. 'While the Court is not barred from gaining inspiration from these principles, it finds that these rather strict standards, set up and applied in the specific context of surveillance of telecommunications, are not applicable as such to cases such as the present one, concerning surveillance via GPS of movements in public places and thus a measure which must be considered to interfere less with the private life of the person concerned than the interception of his or her telephone conversations. It will therefore apply the more general principles on adequate protection against arbitrary interference with Article 8 [].' ECtHR, Uzun v. Germany, application no. 35623/05, 02 September 2010. See also: ECtHR, Del Rio Prada v. Spain, application no. 42750/09, 21 October 2013. ECtHR, Perincek v. Switzerland, application no. 27510/08, 17 December 2013. ECtHR, Szabó and Vissy v. Hungary, application no. 37138/14, 12 January 2016. ECtHR, Valenzuela Contreras v. Spain, application no. 7671/95, 30 July 1998. ECtHR, Craxi v. Italy, application no. 25337/94, 17 July 2003. ECtHR, Shimovolos v. Russia, application no. 30194/09, 21 June 2011. ECtHR, Sefilyan v. Armenia, application no. 22491/08, 02 October 2012. ECtHR, R.E. v. the United Kingdom, application no. 62498/11, 27 October 2015.

[11] ECtHR, Roman Zakharov v. Russia, application no. 47143/06, 04 December 2015.

[12] Zakharov, § 171.

[13] ECtHR, Centrum för Rättvisa v. Sweden, application no. 35252/08, 19 June 2018.

[14] ECtHR, Big Brother Watch and others v. the United Kingdom, application nos. 58170/13, 62322/14 and 24960/15, 13 September 2018.

but remedies that by performing exceptionally strong on another point. Second, when it is clear that in practice, power is not used arbitrarily, while the legal regime leaves room for doing so.

1. Accessibility of the domestic law

Although the Court makes explicit reference to the established notions of accessibility and foreseeability when discussing the minimum requirements of law, both principles are marginalised when the Court scrutinises data collection regimes by intelligence agencies. Although accessibility is still one of the minimum requirements of law, the principle of foreseeability is not. The first minimum requirement the Court sets out is the accessibility requirement. In its earlier jurisprudence, the ECtHR had already made clear that the requirement of accessibility, like that of foreseeability, has a different role and meaning in relation to surveillance activities by secret services and intelligence agencies.

Indeed, from the three cases it becomes clear that the ECtHR allows for quite a number of exceptions on this point. For example, in Zakharov, several rules and regulations were not made public by the government, but published in a journal that was accessible only to people with a subscription. However, because a private website had picked the rules up and made them freely available to the public, the Court did 'not find it necessary to pursue further the issue of the accessibility of the domestic law. It will concentrate instead on the requirements of "foreseeability" and "necessity".'[15] To give another example, in Big Brother Watch, the discussion concerned the access to so called 'below the waterline arrangements', which were not made public in any way. Instead of condemning such practice, the Court argued that in 'the context of secret surveillance, it is inevitable that "below the waterline" arrangements will exist, and the real question for the Court is whether it can be satisfied, based on the "above the waterline" material, that the law is sufficiently foreseeable to minimise the risk of abuses of power. This is a question that goes to the foreseeability and necessity of the relevant law, rather than its accessibility.'[16] Consequently, although accessibility is the first minimum requirement of law, it appears as though the Court prefers to lay emphasis on the other minimum requirements of law that derive from the principles of necessity and foreseeability.

2. Scope of application of secret surveillance measures

The second minimum requirement is that national law must define the scope of application of secret surveillance measures by giving citizens an adequate indication as to the circumstances in which public authorities are empowered to resort to such measures, in particular by clearly setting out (1) the nature of the offences which may give rise to an interception order and (2) a definition of the categories of people liable to be subject to surveillance measures. Although these are robust and clear principles, again, the Court seems willing to allow for a number of exceptions.

For example, in Zakharov, the Court noted with concern that Russian law allowed secret interception of communications in respect of a very wide range of criminal offences, including pickpocketing, and that interceptions could be ordered not only in respect of a suspect or an accused, but also in respect of a person who may have information about an offence or may have other information relevant to the criminal case. Furthermore, telephone or other communications could be intercepted following the receipt of information about events or activities endangering Russia's national, military, economic or ecological security,

[15] Zakharov, § 242.
[16] Big Brother Watch, § 326.

without any further detail being provided about which activities might fall under these categories. Although the ECtHR accepted that the Russian law 'leaves the authorities 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',[17] it did not find a violation on this point. Instead, it referred to the fact that 'prior judicial authorisation for interceptions is required in Russia. Such judicial authorisation may serve to limit the law-enforcement authorities' discretion [].'[18] This line of argumentation is remarkable, because the Court seems to treat the minimum requirements of law not so much as independent principles, each of which must be satisfied, but rather as communicating vessels. If one minimum requirement has been violated, such a flaw might be remedied by another minimum requirement, in particular by laying down adequate mechanisms of oversight.

To provide another example, in Big Brother Watch, the applicants were mindful that the second sub-criterion (definition of the categories of people liable to be subject to surveillance measures) was null and void in bulk interception regimes, because of the indiscriminate nature of such programmes. Consequently, they suggested that this flaw should be remedied by including in the list of minimum requirements of law a requirement on objective evidence of reasonable suspicion in relation to the persons for whom data is being sought, prior independent judicial authorisation of interception warrants, and the subsequent notification of the surveillance subject. They argued that due to recent technological developments the interception of communications now has greater potential than ever before to paint an intimate and detailed portrait of a person's private life. ECtHR, however, felt it would be wrong automatically to assume that bulk interception constitutes a greater intrusion into the private life of an individual than targeted interception, which by its very nature is more likely to result in the acquisition and examination of a large volume of her communications. Although the Court agreed that the additional requirements proposed by the applicants might constitute important safeguards in some cases, it did not consider it appropriate to add them to the list of minimum requirements in the case at hand. 'Bulk interception is by definition untargeted, and to require "reasonable suspicion" would render the operation of such a scheme impossible. Similarly, the requirement of "subsequent notification" assumes the existence of clearly defined surveillance targets, which is simply not the case in a bulk interception regime. Judicial authorisation, by contrast, is not inherently incompatible with the effective functioning of bulk interception. While the Court has recognised that judicial authorisation is an "important safeguard against arbitrariness", to date it has not considered it to be a "necessary requirement" or the exclusion of judicial control to be outside "the limits of what may be deemed necessary in a democratic society".'[19]

Instead, the Court distinguished between four phases of bulk interception regimes: (1) the interception of bulk data, (2) initial filtering and selection of the relevant data, (3) more in depth filtering of relevant data and (4) the examination of the data finally deemed relevant. With respect to the first two stages, ECtHR discussed, among others, whether domestic law gives citizens an adequate indication of the circumstances in which their communications might be intercepted. Although this was certainly not the case with the bulk interception regime in place in Britain, the Court did not find a violation on this point: 'while anyone could potentially have their communications intercepted under the section 8(4) regime, it is clear that the intelligence

[17] Zakharov, § 248.
[18] Zakharov, § 249.
[19] Big Brother Watch, § 318. See the critical opinion of Judge Koskelo, joined by judge Turkovic on this point, Partly Concurring, Partly Dissenting Opinion, points 23-27.

services are neither intercepting everyone's communications, nor exercising an unfettered discretion to intercept whatever communications they wish.'[20] What makes this logic remarkable is that the question whether this minimum requirement of law has been met is answered by referring to practice, not law. Although the authorities could abuse their powers, they do not do so, the Court seems to hold; this line of argumentation seems to defeat the very idea behind the minimum requirements of law, which should limit the possibility of abuse of power, not by asking governmental authorities to act prudently, but by embedding strong limitations in the legal regime itself. In addition, what is important is that yet again, this flaw can be remedied by another minimum requirement of law, namely having adequate mechanisms of oversight.[21]

3. The duration of secret surveillance measures

A third minimum requirement of law regards a limitation on the duration of the secret surveillance measures. In its standard jurisprudence, the Court had already stressed that in general, it is not unreasonable to leave the overall duration of interception to the discretion of the relevant domestic authorities which have competence to issue and renew interception warrants, provided that adequate safeguards exist, such as a clear indication in the domestic law of (1) the period after which an interception warrant will expire, (2) the conditions under which a warrant can be renewed and (3) the circumstances in which it must be cancelled. With respect to this minimum requirement, the ECtHR seems to take a strict approach, though again, it allows for a substantial margin of discretion.

In Zakharov, the Court seemed to take a strict approach when it found that the first two points had been met, but that with respect to the third point, the requirement to discontinue interception when no longer necessary was mentioned in the in one of the two legal regimes under scrutiny only, which resulted in a violation of the minimum requirements of law.[22] But in Centrum för Rättvisa, where the same problem emerged, the Court seemed to take another approach. While finding clear legal standards on the first to points, in 'respect of the third safeguard, the circumstances in which interception must be discontinued, the legislation is not equally clear. [] Nevertheless, notwithstanding that the relevant legislation is less clear with regard to the third safeguard, it must be borne in mind that any permit is valid for a maximum of six months and that a renewal requires a review as to whether the conditions are still met.'[23] The Court emphasized the existence of other forms of control and oversight in place, such as the Foreign Intelligence Inspectorate having the power to decide that an intelligence interception should cease.[24] Again, the Court finds that a flaw with respect to the minimum requirements can be repaired by having in place adequate mechanisms of oversight.

In Big Brother Watch, discussion also concerned the third sub-requirement, as the national law only specified that the Secretary of State was under an obligation to cancel the orders when they were no longer necessary. Because the Secretary of State is part of the executive branch, it seems questionable whether this provision provides an adequate safeguard against potential abuse of power. The European Court of Human Rights, however, no violation of this

[20] Big Brother Watch, § 337.
[21] The Court did find a violation of the British regime because part of the collection of metadata/communication data was left unregulated, which is a violation not of the minimum requirements of law, but of the 'in accordance with the law' requirement.
[22] Zakharov, § 251-252.
[23] Centrum för Rättvisa, § 129-130.
[24] Centrum för Rättvisa, § 130.

minimum requirement, as 'the duty on the Secretary of State to cancel warrants which were no longer necessary meant, in practice, that the intelligence services had to keep their warrants under continuous review.'[25] Again, the Court refers to the self-restraint required in practice form intelligence services to ok the legal regime of the Member State.

4. Procedures for processing the data

A fourth minimum requirement is that the law or relevant regulation must lay down procedures for storing, accessing, examining, using, and destroying the gathered data. Although in essence, this requires of Member States to law down an data protection framework for intelligence agencies, the Court has been willing to condone rather broad and vague data protection regimes.

Again, in Zakharov, the Court seemed to take a strict approach when it found that although the Russian law had established an adequate framework on almost all accounts, it did not do so with respect to the deletion of data. Although the six-month storage time-limit set out in Russian law was in itself reasonable, the Court underlined the lack of a requirement to destroy immediately any data that are not relevant to the purpose for which they have been obtained. 'The automatic storage for six months of clearly irrelevant data cannot be considered justified under Article 8. Furthermore, as regards the cases where the person has been charged with a criminal offence, the Court notes with concern that Russian law allows unlimited discretion to the trial judge to store or to destroy the data used in evidence after the end of the trial. Russian law does not give citizens any indication as to the circumstances in which the intercept material may be stored after the end of the trial. The Court therefore considers that the domestic law is not sufficiently clear on this point.'[26]

Yet in Centrum för Rättvisa, the ECtHR found that under the prevailing law, intelligence had to be destroyed immediately when it appeared that they were deemed unimportant, their interception was unlawful or the data were shared in the context of professional secrecy; this regime, however, did not concern 'raw data', that is, data that have been collected, but have not yet been assessed on their potential value or relevance. 'Although the FRA may maintain databases for raw material containing personal data up to one year, it has to be kept in mind that raw material is unprocessed information. That is, it has yet to be subjected to manual treatment. The Court accepts that it is necessary for the FRA to store raw material before it can be manually processed.'[27] Consequently, it did not find a violation on this point, even though the raw data, of which in bulk interception regimes usually by far most are irrelevant for the purpose for which they have been collected, could be stored for up to a year.

In Big Brother Watch, the law required that every copy of intercepted material or data (together with any extracts and summaries) had to be destroyed as soon as retention was no longer necessary for the purposes. Again, the ECtHR seemed more lenient where it regarded the storage of raw data, storage of which, under the prevailing regime, would 'normally be no longer than two years'. The Court condoned this legal regime, referring both to practice and to the extensive of adequate mechanisms for oversight: 'while the specific retention periods are not in the public domain, it is clear that they cannot exceed two years and, in practice, they do not exceed one year (with much content and related communications data being retained for significantly shorter periods). Furthermore, where an application is lodged with the IPT

[25] Big Brother Watch, § 360.
[26] Zakharov, § 255-256.
[27] Centrum för Rättvisa, § 146.

[Investigatory Powers Tribunal], it can examine whether the time-limits for retention have been complied with and, if they have not, it may find that there has been a breach of Article 8 of the Convention and order the destruction of the relevant material.'[28] In addition, when the Court scrutinized the State's receipt of material intercepted by the U.S. National Security Agency, it acknowledged that while the compliance of the British intelligence agencies with the data protection principles was subject to exemption by ministerial certificate, they could not be exempted from the obligation to comply with two data protection principles, namely the storage limitation principle and the obligation to take adequate technical and organizational security measures, which is why it deemed that sufficient data protection standards were in place on this point.[29]

5. Authorisation procedures

As a fifth minimum requirement of law, the Court has made clear that there must be an adequate authorisation procedure in place. In general, it will take into account a number of factors in assessing whether the authorisation procedures are capable of ensuring that secret surveillance is not ordered haphazardly, irregularly or without due and proper consideration. These factors include, in particular, (1) the authority competent to authorise the surveillance, (2) its scope of review and (3) the content of the interception authorisation. Although the authority competent to authorise the surveillance may be a non-judicial authority provided, it should be sufficiently independent from the executive. Again, although these are robust and concrete criteria, in the three cases the Court has applied those, it allows for broad exceptions.

In Zakharov, the Court did not find a violation with respect to the first point, because the law-enforcement agency seeking authorisation for interception had to submit a reasoned request to that effect to a judge and because that judge had to give reasons for the decision to authorise interceptions. On the second point, however, the Court found a violation, reiterating that 'it must be capable of verifying 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.'[30] The Court found the Russian legal system did not meet the minimum requirements of law, both because judicial scrutiny did not extent to materials about undercover agents or police informers or about the organisation and tactics of operational-search measures, disabling the court to assess whether there was 'a sufficient factual basis to suspect the person in respect of whom operational-search measures are requested of a criminal offence or of activities endangering national, military, economic or ecological security',[31] and because the courts were not required to execute a necessity or proportionality check. Here, it referred to the fact that in practice, courts never requested the interception agency to submit additional materials and 'that a mere reference to the existence of information about a criminal offence or activities endangering national, military, economic or ecological security is considered to be sufficient for the authorisation to be granted.'[32] With respect to the content of the interception authorisation, the Court underlined that 'it must clearly identify a specific person to be placed under surveillance or a single set of premises as the premises in respect of which the

[28] Big Brother Watch, § 372-374.
[29] Big Brother Watch, § 43.
[30] Zakharov, § 260.
[31] Zakharov, § 261.
[32] Zakharov, § 263.

authorisation is ordered',[33] which the ECtHR found one relevant regulatory regime did, while the other one did not because it did 'not contain any requirements either with regard to the content of the request for interception or to the content of the interception authorisation. As a result, courts sometimes grant 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. Some authorisations do not mention the duration for which interception is authorised.'[34]

The Court found a violation of the minimum requirements of law on this point, also because an urgency procedure allowed authorities to side pass ordinary limitations to the use of powers. In addition, the Court stressed that 'the requirement to show an interception authorisation to the communications service provider before obtaining access to a person's communications is one of the important safeguards against abuse by the law-enforcement authorities',[35] and found that in certain circumstances, communications service providers had to install equipment giving the law-enforcement authorities direct access to all mobile-telephone communications of all users and that they were under an obligation to create databases storing information about all subscribers, and the services provided to them, for three years; the secret services had direct remote access to those databases. This system, the Court found, was particularly prone to abuse, which is why it stressed that the need for safeguards against arbitrariness and abuse was particularly great. But the Court did not find a violation of the minimum requirements of law, instead suggesting that it would 'examine with particular attention whether the supervision arrangements provided by Russian law are capable of ensuring that all interceptions are performed lawfully on the basis of proper judicial authorisation.'[36] This shifts the attention from ex ante to ex post oversight.

In Centrum för Rättvisa, the ECtHR underlined that although 'a requirement of prior judicial authorisation constitutes an important safeguard against arbitrariness. Nevertheless, prior authorisation of such measures is not an absolute requirement *per se*, because where there is extensive subsequent judicial oversight, this may counterbalance the shortcomings of the authorisation.'[37] In addition, the Court stressed that although in Zakharov it had underlined the importance of public scrutiny, in the case of prior authorisations, complete secrecy is allowed, when adequate safeguards are put in place, which the ECtHR felt there were: 'while the privacy protection representative cannot appeal against a decision by the Foreign Intelligence Court or report any perceived irregularities to the supervisory bodies, the presence of the representative at the court's examinations compensates, to a limited degree, for the lack of transparency concerning the court's proceedings and decisions. [] As an additional safeguard against abuse and arbitrariness, the task of examining whether the mission is compatible with applicable legislation and whether the intelligence collection is proportional to the resultant interference with personal integrity has been entrusted to a body whose presiding members are or have been judges. Furthermore, the supervision of the Foreign Intelligence Court is extensive as the FRA, in its applications, must specify not only the mission request in question and the need for the intelligence sought but also the signal carriers to which access is needed and the search terms – or at least the categories of search terms – that will be used.'[38] In addition, it condoned the urgency procedure in place

[33] Zakharov, § 264.
[34] Zakharov, § 265.
[35] Zakharov, § 269.
[36] Zakharov, § 271.
[37] Centrum för Rättvisa, § 133.
[38] Big Brother Watch, § 138-139.

wherewith the executive power could itself decide to grant a permit, as the 'legislation states that such a decision must be followed by an immediate notification to and a subsequent rapid review by the Foreign Intelligence Court where the permit may be changed or revoked'.[39]

In Big Brother Watch, quite remarkably, the Court went even further. While the Court considered judicial authorisation to be an important safeguard, and perhaps even "best practice", it stressed that by itself it can neither be necessary nor sufficient to ensure compliance with Article 8 of the Convention. Even the requirement such a non-judicial body should be independent was put up for discussion by the Court, when it assessed the fact that under the prevailing legal regime, the executive branch assessed and authorised the warrants and it concluded: 'It is true that the Court has generally required a non-judicial authority to be sufficiently independent of the executive. However, it must principally have regard to the actual operation of a system of interception as a whole, including the checks and balances on the exercise of power, and the existence (or absence) of any evidence of actual abuse, such as the authorising of secret surveillance measures haphazardly, irregularly or without due and proper consideration. In the present case there is no evidence to suggest that the Secretary of State was authorising warrants without due and proper consideration.'[40] Yet again, the Court refers to the fact that in practice, the authorities did not abuse their powers to confirm a legal regime which in itself did not abide by the minimum principles of law.

A similar finding was put forward by the Court when it regarded the fact that under the British regime, any breaches of safeguards should be notified to the Interception of Communications Commissioner, while the Commissioner observed that the process by which analysts selected material for examination, which did not require pre-authorisation by a more senior operational manager, relied mainly on the professional judgment of analysts, their training and subsequent management oversight. Although the Court agreed that it would be preferable for the selection of material by analysts to be subject at the very least to preauthorisation by a senior operational manager, given that analysts were carefully trained and vetted, records were kept and those records were subject to independent oversight and audit, 'the absence of pre-authorisation would not, in and of itself, amount to a failure to provide adequate safeguards against abuse.'[41]

6. Ex post supervision of the implementation of secret surveillance measures

As a sixth minimum requirement of law, the regulatory regime must put a robust and independent ex post oversight mechanism in place on the use of powers by the executive branch. As has become clear from the previous sub-sections, it is this minimum requirement that is arguably the most important one to the ECtHR, as it allows flaws with respect to the other minimum requirements to be repaired when there is a good mechanism for oversight in place. Again, like with ex ante oversight, the Court stresses that although it is in principle desirable to entrust supervisory control to a judge, supervision by a non-judicial body may be considered compatible with the Convention, provided that the supervisory body is independent of the authorities carrying out the surveillance, and is vested with sufficient powers and competence to exercise an effective and continuous control. In addition, the Court stresses, it is essential that such an oversight body has access to all relevant documents, including closed materials, and that all those involved in interception activities have a duty to disclose to it any material required. But yet again, the ECtHR allows for a number of exceptions to this rule.

[39] Big Brother Watch, § 140.
[40] Big Brother Watch, § 377-378.
[41] Big Brother Watch, § 344-345.

In Zakharov, for example, the Court found the safeguards and competences of the various authorities in with respect to oversight and control quite limited. Still, a legal framework exists was in place which, at least in theory, introduced some supervision by prosecutors, although their capacity to do so was limited and oversight on their activities is minimal. Yet again, the Court turns to the practical implementation and working of these safeguards, stressing that 'it is for the Government to illustrate the practical effectiveness of the supervision arrangements with appropriate examples.'[42] And because the Member State could not demonstrate that prosecutors' supervision of secret surveillance measures was effective in practice, because the prosecutor did not have access to all relevant documents, because it could not scrutinise all relevant interceptions and because its operations were not subject to public scrutiny, the Court considered that the prosecutors' supervision of interceptions as it was organised was not capable of providing adequate and effective guarantees against abuse. Interestingly, the Court did note that the public prosecutor could hardly be said to be an independent supervisory authority, but still it did find a violation on that specific point.[43]

In Big Brother Watch, the Court distinguished between the four phases of bulk interception regimes previously mentioned: (1) the interception of bulk data, (2) initial filtering and selection of the relevant data, (3) more in depth filtering of relevant data and (4) the examination of the data finally deemed relevant. Because of the meagre legal regime with respect to the first to stages, the Court required more rigorous safeguards to be in place with respect to the third and fourth stages. On this point, the Court stressed that it was not persuaded that the safeguards governing the selection of bearers for interception and the selection of intercepted material for examination were sufficiently robust to provide adequate guarantees against abuse. Of greatest concern, it continued, was the absence of robust independent oversight of the selectors and search criteria used to filter intercepted communications. 'In practice, therefore, the only independent oversight of the process of filtering and selecting intercept data for examination is the *post factum* audit by the Interception of Communications Commissioner and, should an application be made to it, the IPT. [] In a bulk interception regime, where the discretion to intercept is not significantly curtailed by the terms of the warrant, the safeguards applicable at the filtering and selecting for examination stage must necessarily be more robust.'[44] The fact that this is perhaps the most important minimum condition of law was emphasized by the fact that on this point, the Court did not allow the Member State to remedy this flaw by referring to practice; rather, the ECtHR reasoned the other way around when it stresses that 'while there is no evidence to suggest that the intelligence services are abusing their powers – on the contrary, the Interception of Communications Commissioner observed that the selection procedure was carefully and conscientiously undertaken by analysts –, the Court is not persuaded that the safeguards governing the selection of bearers for interception and the selection of intercepted material for examination are sufficiently robust to provide adequate guarantees against abuse.'[45]

7. Conditions for communicating data to and receiving data from other parties

A seventh minimum requirement of law concerns the sharing of intelligence data. The Court has held that when receiving data from foreign intelligence agencies, the minimum requirements of law should apply mutatis mutandis. Again, although it seems as though the Court is taking an exceptionally strict stance in this respect, in fact, it is quite willing to allow

[42] Zakharov, § 284.
[43] Zakharov, § 279.
[44] Big Brother Watch, § 346.
[45] Big Brother Watch, § 347.

for exceptions and adopts a flexible approach when assessing this minimum requirement of law.

For example, in Centrum för Rättvisa, the ECtHR stressed that the purpose of signals intelligence naturally demands that it may be reported to concerned national authorities, in particular the authority which ordered the mission. Under the Swedish legal regime, discretion was given to the government to communicate personal data to states or organisations when deemed in the Swedish interest. The Court did note that the Swedish law did not indicate that possible harm to the individuals concerned must also be considered and that there was no legal provision requiring the recipient to protect the data with the same or similar safeguards as those applicable under Swedish law, which meant that there were no legal limits imposed on the authority of the Swedish authorities when deciding on whether to share data with foreign counterparts. Still, although in 'the Court's view, the mentioned lack of specification in the provisions regulating the communication of personal data to other states and international organisations gives some cause for concern with respect to the possible abuse of the rights of individuals. On the whole, however, the Court considered that the supervisory elements described below sufficiently counterbalance these regulatory shortcomings.'[46] Yet again, a flaw can be repaired by the existence of a strong mechanism for oversight and supervision.

To provide another example, although in Big Brother Watch, the Court assessed whether obtaining intelligence from foreign counterparts abided by the minimum requirements of law, the Court did not assess the situations in which data were sent by foreign intelligence agencies to the British authorities on their own initiative, because the British government asserted that this rarely happens. 'As the Government, at the hearing, informed the Court that it was "implausible and rare" for intercept material to be obtained "unsolicited", the Court will restrict its examination to material falling into the second and third categories.'[47] Consequently, yet again, the Court refers to the fact that in practice, a certain power or discretion is seldom used in order to justify that it the law itself may not meet the minimum requirements of law. The Court did discuss instances in which the British authorities could request intelligence from their counterparts and acknowledged that under the regulatory regime, in exceptional circumstances, a request for communications could be made in the absence of a relevant interception warrant, albeit only if such did not amount to a deliberate circumvention of the legal requirements in place. In such a case the request had to be considered and decided on by the Secretary of State personally and be notified to the Interception of Communications Commissioner. Again, the Court found such a regime unproblematic because in practice, it was not used, stressing that 'no request for intercept material has ever been made in the absence of an existing RIPA warrant.'[48]

8. Notification of interception of communications

The eighth minimum requirement of law is that the people subject to secret surveillance should be notified thereof. The Court has been clear when it stressed that it may not be 'feasible in practice to require subsequent notification in all cases. The activity or danger against which a particular series of surveillance measures is directed may continue for years, even decades, after the suspension of those measures. Subsequent notification to each individual affected by a suspended measure might well jeopardise the long-term purpose that originally prompted the surveillance. Furthermore, such notification might serve to reveal the working methods and

[46] Centrum för Rättvisa, § 150.
[47] Big Brother Watch, § 417.
[48] Big Brother Watch, § 429-430.

fields of operation of the intelligence services and even possibly to identify their agents.'[49] Consequently, this requirement has played a minor role of significance only.

For example, in Zhakarov, although the Court formally underlined that notification should happen as soon as it is possible, although that might take years, in practice, persons were not notified at any point or under any circumstances. That meant that unless criminal proceedings had been opened against the interception subject and the intercepted data had been used as evidence, or unless there had been a leak, the person concerned would never find out that her communications had been intercepted. In addition, access to the information was conditional on the person's ability to prove that his communications were intercepted. Information was provided only in very limited circumstances, namely if the person's guilt has not been proved in accordance with the procedure prescribed by law, that is, she had not been charged or the charges had been dropped on the ground that the alleged offence was not committed or that one or more elements of a criminal offence were missing. Even then, only information that did not disclose State secrets would be provided, where information concerning the facilities used in operational-search activities, the methods employed, the officials involved and the data collected were considered a State secret. Although the Court was clearly unsympathetic to this approach, it did not find a violation on this point, stressing that it would bear the absence of notification and the lack of an effective possibility of requesting and obtaining information, when assessing the effectiveness of remedies available under Russian law.[50]

To provide another example, in Centrum för Rättvisa, there was a legal obligation to inform natural persons that were subject of surveillance activities, the latest one month after the signals intelligence mission was concluded, except where secrecy was required. Just as in Zakharov, in practice, a notification had never been made by the governmental authorities, citing reasons of secrecy. Remarkably, the Court did not find a violation on this point because the claimant in the Swedish case was a legal person. 'Taking into account that the requirement to notify the subject of secret surveillance measures is not applicable to the applicant and is, in any event, devoid of practical significance,'[51] like in Zakharov, the Court underlined that its findings on the point of the notification would be taken into account when evaluating the last minimum requirement of law: the available remedies.

9. Available remedies

The final minimum requirement of law is that the legal regime of the Member State must lay down robust and effective remedies, in particular for people having been subject to secret surveillance. In this respect, the Court has made clear that review and supervision of secret surveillance measures may come into play at three stages: when the surveillance is first ordered, while it is being carried out, and after it has been terminated. As regards the first two stages, the very nature and logic of secret surveillance dictate that not only the surveillance itself but also the accompanying review should be effected without the individual's knowledge. Consequently, since the individual will necessarily be prevented from seeking an effective remedy of her own accord or from taking a direct part in any review proceedings, it is essential that the procedures established should themselves provide adequate and equivalent guarantees safeguarding her rights.

[49] Zakharov, § 287; Centrum för Rättvisa, § 164.
[50] Zakharov, § 290-291.
[51] Centrum för Rättvisa, § 167.

In Zhakarov, where the remedies were available only to persons who were in possession of information about the interception of their communications, while the subjects of interception were not notified at any point and there was no possibility of requesting and obtaining information about interceptions from the authorities, the Court found that Russian law did not provide for effective remedies to a person who suspects that he has been subjected to secret surveillance.[52]

In Centrum för Rättvisa, the Foreign Intelligence Inspectorate, at the request of an individual, could investigate whether her communications had been intercepted through signals intelligence, and if so, could verify whether the interception and treatment of the information was in accordance with law. A request could be made by legal and natural persons regardless of nationality and residence, which is why the Court was satisfied that the remedies available were not dependent on prior notification, and were adequate. This is remarkable because, speaking of practical relevance, being able to submit a claim without having any indication that one's rights may be violation seems illusory; in addition, the Court acknowledged that the Inspectorate did not have the authority to order compensation to be paid, that the individual could not obtain information whether her communications had actually been intercepted, only if there had been any unlawfulness, that the decision of the Inspectorate was final, which meant that an individual who was not satisfied with the response from the Inspectorate could not seek review and that the procedure to correct, block or destroy personal data was dependent on the individual's knowledge that personal data had been registered and on the nature of that data.[53]

The reason for the Court's lenience was based on the fact that Swedish law provides for several remedies of a general nature, in particular the possibility of addressing individual complaints to the Parliamentary Ombudsmen and the Chancellor of Justice. The two institutions had the right of access to documents and other materials. While their decisions were not legally binding, their opinions command great respect in Sweden, according to the Court. They also had the power to initiate criminal or disciplinary proceedings against public officials for actions taken in the discharge of their duties. The Court deemed it of relevance that a practice has developed in the last several years according to which the Chancellor may receive and resolve individual compensation claims for alleged violations. The Court also noted that the Data Protection Authority could receive and examine individual complaints under the Personal Data Act. 'In the Court's view, the aggregate of remedies, although not providing a full and public response to the objections raised by a complainant, must be considered sufficient in the present context, which involves an abstract challenge to the signals intelligence regime itself and does not concern a complaint against a particular intelligence measure. In reaching this conclusion, the Court attaches importance to the earlier stages of supervision of the regime, including the detailed judicial examination by the Foreign Intelligence Court of the FRA's requests for permits to conduct signals intelligence and the extensive and partly public supervision by several bodies, in particular the Foreign Intelligence Inspectorate.'[54] Yet again, both practice and the fact that there is judicial oversight remedy a flaw as to this minimum requirement.

10. Conclusion

To understand the significance of the willingness of the European Court of Human Rights to scrutinise the legislative branch of the Member States of the Council of Europe, it is necessary to go back to the time that the European Convention on Human Rights was drafted. It was in

[52] Zakharov, § 300.
[53] Centrum för Rättvisa, § 173.
[54] Centrum för Rättvisa, § 178.

the wake of the Second World War, in which regimes that had trampled human rights on a large scale had just been defeated and in which both communist and fascist totalitarian regimes still existed. The rule of law virtually did not exist under those administrations; laws were applied retroactively and arbitrarily, while there was no real separation of power. Relying on the state of emergency, most regimes either passed aside the legislative power or turned it into a puppet of the executive branch. Laws and policies were designed not to serve the general interest but those of selected groups and constitutions were revised to legitimise these administrations rather than to provide legal certainty to minorities.

A significant part of the representatives of the countries that would later join the Convention that were present at the discussions over the drafting of the European Convention on Human Rights consequently wanted the Court to focus especially on questions over whether laws and the legal regime as such were in conformity with the rule of law and whether they served the general interests. But both through changes made to the Convention and through its interpretation by the Court, the Convention-system moved more and more towards providing relief only to natural persons who have been harmed in their individual interests in specific cases. By far most cases under the Convention are brought by natural persons. Importantly, the Court has made clear that they can do so only when their claim concerns the protection of their own, private interests. So-called *in abstracto* claims, which revolve around the legitimacy of a law or policy as such, are as a rule inadmissible. 'Insofar as the applicant complains in general of the legislative situation, the Commission recalls that it must confine itself to an examination of the concrete case before it and may not review the aforesaid law *in abstracto*. The Commission therefore may only examine the applicant's complaints insofar as the system of which he complains has been applied against him.[55] *A priori* claims are rejected as well, because the Court will only receive complaints about injury which has already materialized. Consequently, claims about future damage will in principle not be considered.[56] To provide a final example, the ECtHR will not receive an *actio popularis*, a case brought by a claimant, not to protect its own interests, but that of others or of society as a whole.[57]

As an effect of this interpretation of the Convention, by far most cases before the Court concern the executive and the judicial branch of Member States and how they have acted in concrete cases. With the judiciary, the Court will assess whether the courts at the national level have struck a fair balance between the competing interests of both parties involved and with respect to the executive, it will do the same, in addition to assessing whether the executive abided by the conditions laid down in the national law.[58] The Court has also been willing to say that a state is under a positive obligation to provide protection to the human rights of a claimant, but even in these types of cases, it is important to note that the ECtHR will not say that the Member State should change it laws, but only that in the specific case of the applicant, the state should have done more to provide adequate protection to her human rights or should have made an exception to the prevailing laws and policies.[59] Even where, for example, a Member State's law or policy would grant the executive branch the power to violate human rights, for example allowing prison authorities to structurally monitor the correspondence of prisoners, the Court would not hold that the law or policy should be altered or revoked, but merely stress that in the

[55] ECtHR, Lawlor v. The United Kingdom, application no. 12763/87, 14 July 1988.
[56] ECmHR, Tauira and others v. France, application no. 28204/95, 04 December 1995.
[57] ECtHR, Asselbourg and 78 others and Greenpeace Association-Luxembourg v. Luxembourg, application no. 29121/95, 29 June 1999.
[58] The Court has almost never found a violation on the ground that the law or action by a Member State was not in one of the interests specified in the Convention.
[59] See e.g.: ECtHR, B. v. France, application no. 13343/87, 25 March 1992.

specific case of the applicant, her human rights were violated by the unlawful actions of the executive branch.[60]

That is why it is so significant that the Court is now willing to scrutinise Member States' laws at a very detailed level, evaluating whether a considerable number of minimum requirements and sub-requirements have been met. It is a revolution in the proper sense of the word. 'The word 'revolution' was originally an astronomical term which gained increasing importance in the natural sciences through Copernicus's *De revolutionibus orbium coelestium.* In this scientific usage it retained its precise Latin meaning, designating the regular, lawfully revolving motion of the starts, which, since it was known to be beyond the influence of man and hence irresistible, was certainly characterized neither by newness nor by violence. On the contrary, the word clearly indicates a recurring, cyclical movement'.[61] Consequently, a revolution meant the return to a prior stage, not entering uncharted territory. Similarly, the ECtHR now does what many authors of the Convention hoped it would do: not so much focus on whether a right of an individual person was violated in a specific case and provide for monetary relief where appropriate, but look at the underlying structural problem, no so much look at the how the executive branch uses its powers, but which types of powers are attributed to it by the legislative branch.

As the rapporteur stressed when drafting the Convention, focussing only on providing relief to individual claimants whose rights have been harmed 'seems to suggest that the European Court will be able to grant indemnities to victims, damages and interest, or reparation of this kind. It does not say that the European Court will be able to pronounce the nullity or invalidity of the rule, or the law, or the decree which constitutes a violation of the Convention. That, Ladies and Gentlemen, is something very grave. True, reparation in kind may be advisable where the victim is a specified individual. In case of an action ultra vires of this sort on the part of the local police, a mayor, a prefect, or even a minister, satisfaction may be given in the form of reparation in cash or the awarding of an indemnity. But can the graver form of violation which consists in removing a fundamental law guaranteeing a specific freedom for the whole nation, from the laws of a country in virtue of some law or decree, can such a violation be redressed by awarding a symbolic farthing darn- ages to the citizens of the country? If, tomorrow, France were to sink into a dictatorship, and if her dictator were to suppress the freedom of the Press, would the European Court award a franc damages to all Frenchmen so as to compensate for the injury which the suppression of this fundamental freedom had caused them? Such a proceeding would not make sense. If we really want an European Court to succeed in guaranteeing the rights which we have placed under its protection, we must grant jurisdiction to declare void, if need be, the laws and decrees which violate the Convention.'[62]

Now, the European Court seems willing to do exactly that. But the Court is a half-hearted revolutionary. First, when scrutinising laws, it often assesses how certain powers are used in practice. Although formally speaking, a governmental organisation may be vested with too broad powers, devoid of the necessary safeguards and conditionalities, the ECtHR may still deem the law convention-compliant when in practice, the organisation uses its powers discretely. Second, when the Court establishes what seems to be a flaw in the legal regime with respect to one of the minimum requirements of law, it often allows Member States to remedy

[60] See e.g.: ECtHR, Drozdowski v. Poland, application no. 20841/02, 06 December 2005.
[61] H. Arendt, 'On Revolution', Penguin Books, 1990, p. 42.
[62] Collected edition of the "Travaux préparatoires" of the European Convention on Human Rights / Council of Europe, 1975-1985, The Hague, Martinus Nijhoff, Vol V, p. 300-302.

that flaw by performing strongly on one of the other minimum requirements of law, in particular the existence of adequate judicial oversight. Consequently, it is questionable whether both the term 'minimum' and the term 'law' are entirely appropriate when the Court speaks of the 'minimum requirements of law'. The European Court of Human Rights is still to deliver its judgement on Big Brother Watch in Grand Chamber setting. Perhaps soon, the revolution will be over and there will be fixed standards to determine what is and what isn't a law proper.

Marat certainly had an idea: 'They accuse me of raising myself above the law because I don't obey their arbitrary and tyrannical orders. In order to demonstrate the absurdity of their accusation, it will suffice to show them what a law is. What is a law? It's an expression of the general will on an object of common interest. A law can thus never be anything but a deliberation taken with maturity for the common good after a tranquil, wise and in-depth discussion. When the people cannot make laws itself, it does it through representatives. I won't examine here whether in the current state of affairs, whether they who have concealed themselves behind imposter masks, who have played at patriotism and who have displayed love of liberty in order to better fool the people, capture their confidence and be named to the Convention and use its powers to satisfy their base passions — can be regarded as true national representatives. But I maintain that the henchmen of the ancien régime cannot be the deputies of the people under the new regime. Or rather I maintain that vile scoundrels, schemers and traitors to the fatherland who have shamelessly trafficked in the interests and rights of the people with the enemies of the republic cannot in any way be considered representatives of the nation. Such are the statesmen who voted the appeal to the people and the detention of Louis Capet in order to save the tyrant by lighting the torches of civil war; such are the statesmen who the traitor Dumouriez declared his accomplices by declaring that he was going to march on Paris to support them against the patriots of the Mountain. It is these men who rendered the decree against me. In not paying any heed to this decree I thus don't violate the law, since they are, de facto — since the declaration of the traitor Dumouoriez — deprived of any right to represent the people they betrayed. But even if they aren't avowed traitors their decrees would still have no force in law.'[63]

[63] Translation taken from: https://www.marxists.org/history/france/revolution/marat/1793/law.htm Original at: https://gallica.bnf.fr/ark:/12148/bpt6k1049584g/f5.item

	References to how prudently (or not) powers are used in practice	References to another minimum requirement of law
1. Accessibility of the domestic law		the Court did 'not find it necessary to pursue further the issue of the accessibility of the domestic law. It will concentrate instead on the requirements of "foreseeability" and "necessity". Zakharov 'This is a question that goes to the foreseeability and necessity of the relevant law, rather than its accessibility.' Big Brother Watch
2. Scope of application of the secret surveillance measures		
2.1 The nature of the offences which may give rise to an interception order;		Although the Russian law 'leaves the authorities 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', the Court did not find a violation on this point. Instead, it referred to the fact that 'prior judicial authorisation for interceptions is required in Russia. Such judicial authorisation may serve to limit the law-enforcement authorities' discretion [].' Zakharov
2.2 A definition of the categories of people liable to be subject to surveillance measures.	'while anyone could potentially have their communications intercepted under the section 8(4) regime, it is clear that the intelligence services are neither intercepting everyone's communications, nor exercising an unfettered discretion to intercept whatever communications they wish.' Big Brother Watch	'Bulk interception is by definition untargeted, and to require "reasonable suspicion" would render the operation of such a scheme impossible. Similarly, the requirement of "subsequent notification" assumes the existence of clearly defined surveillance targets, which is simply not the case in a bulk interception regime. Judicial authorisation, by contrast, is not inherently incompatible with the effective functioning of bulk interception. While the Court has recognised that judicial authorisation is an "important safeguard against arbitrariness", to date it has not considered it to be a "necessary requirement" or the exclusion of judicial control to be outside "the limits of what may be deemed necessary in a democratic society".' (Big Brother Watch)
3. The duration of secret surveillance measures		
3.1 The period after which an interception warrant will expire;		
3.2 The conditions under which a warrant can be renewed;		
3.3 The circumstances in which it must be cancelled.	'the duty on the Secretary of State to cancel warrants which were no longer necessary meant, in practice, that the intelligence services had to keep their warrants under continuous review.' Big Brother Watch	'notwithstanding that the relevant legislation is less clear with regard to the third safeguard, it must be borne in mind that any permit is valid for a maximum of six months and that a renewal requires a review as to whether the conditions are still met.' Centrum för Rättvisa
4. The procedures for processing data		
4.1 Storing;	'Although the FRA may maintain databases for raw material containing personal data up to one year, it has to be kept in mind that raw material is unprocessed information. That is, it has yet to be subjected to manual treatment. The Court accepts that it is necessary for the FRA to store raw material before it can be manually processed.' Centrum för Rättvisa 'while the specific retention periods are not in the public domain, it is clear that they cannot exceed two years and, in practice, they do not exceed one year (with much content and related communications data being retained for significantly shorter periods).' Big Brother Watch	IPT 'can examine whether the time-limits for retention have been complied with and, if they have not, it may find that there has been a breach of Article 8 of the Convention and order the destruction of the relevant material.' Big Brother Watch
4.2 Accessing;		

4.3 Examining;		
4.4 Using;		
4.5 Destroying.		
5. Authorisation procedures		
5.1 The authority competent to authorise the surveillance;	'It is true that the Court has generally required a non-judicial authority to be sufficiently independent of the executive. However, it must principally have regard to the actual operation of a system of interception as a whole, including the checks and balances on the exercise of power, and the existence (or absence) of any evidence of actual abuse, such as the authorising of secret surveillance measures haphazardly, irregularly or without due and proper consideration. In the present case there is no evidence to suggest that the Secretary of State was authorising warrants without due and proper consideration.' Big Brother Watch	
5.2 Its scope of review;	In practice, courts never requested the interception agency to submit additional materials and 'that a mere reference to the existence of information about a criminal offence or activities endangering national, military, economic or ecological security is considered to be sufficient for the authorisation to be granted.' Zakharov	'while the privacy protection representative cannot appeal against a decision by the Foreign Intelligence Court or report any perceived irregularities to the supervisory bodies, the presence of the representative at the court's examinations compensates, to a limited degree, for the lack of transparency concerning the court's proceedings and decisions.' Centrum för Rättvisa
5.3 The content of the interception authorisation.		'examine with particular attention whether the supervision arrangements provided by Russian law are capable of ensuring that all interceptions are performed lawfully on the basis of proper judicial authorisation.' Zakharov
6. Ex post supervision of the implementation of secret surveillance measures		
6.1 Independence;	The ECtHR noted that the public prosecutor could hardly be said to be an independent supervisory authority, but still it did find a violation on that specific point. Zakharov	
6.2 Competence.	'it is for the Government to illustrate the practical effectiveness of the supervision arrangements with appropriate examples.' Zakharov 'while there is no evidence to suggest that the intelligence services are abusing their powers – on the contrary, the Interception of Communications Commissioner observed that the selection procedure was carefully and conscientiously undertaken by analysts –, the Court is not persuaded that the safeguards governing the selection of bearers for interception and the selection of intercepted material for examination are sufficiently robust to provide adequate guarantees against abuse.' Big Brother Watch	
7. Conditions for communicating data to and receiving data from other parties		
7.1 Communicating;		Although in 'the Court's view, the mentioned lack of specification in the provisions regulating the communication of personal data to other states and international organisations gives some cause for concern with respect to the possible abuse of the rights of individuals. On the whole, however, the Court considered that the supervisory elements described below sufficiently counterbalance these regulatory shortcomings.' Centrum för Rättvisa
7.2 Receiving.	'As the Government, at the hearing, informed the Court that it was "implausible and rare" for intercept material to be obtained "unsolicited", the Court will restrict its examination to material falling into the second and third categories.' Big Brother Watch	

	'no request for intercept material has ever been made in the absence of an existing RIPA warrant.' Big Brother Watch	
8. Notification of interception of communications		Court was clearly unsympathetic to this approach, it did not find a violation on this point, stressing that it would bear the absence of notification and the lack of an effective possibility of requesting and obtaining information, when assessing the effectiveness of remedies available under Russian law. Zakharov 'Taking into account that the requirement to notify the subject of secret surveillance measures is not applicable to the applicant and is, in any event, devoid of practical significance,' like in Zakharov, the Court underlined that its findings on the point of the notification would be taken into account when evaluating the last minimum requirement of law: the available remedies. Centrum för Rättvisa
9. Available remedies		'In the Court's view, the aggregate of remedies, although not providing a full and public response to the objections raised by a complainant, must be considered sufficient in the present context, which involves an abstract challenge to the signals intelligence regime itself and does not concern a complaint against a particular intelligence measure. In reaching this conclusion, the Court attaches importance to the earlier stages of supervision of the regime, including the detailed judicial examination by the Foreign Intelligence Court of the FRA's requests for permits to conduct signals intelligence and the extensive and partly public supervision by several bodies, in particular the Foreign Intelligence Inspectorate.' Centrum för Rättvisa