BRUSSELS PRIVACY HUB
WORKING PAPER
VOL. 6 • N° 21 • APRIL 2020

BRUSSELS PRIVACY HUB
Vrije Universiteit Brussel

ARTICLE 8 ECHR COMPLIANT AND FORESEEABLE SURVEILLANCE: THE ECTHR'S EXPANDED LEGALITY REQUIREMENT COPIED BY THE CJEU. A DISCUSSION OF EUROPEAN SURVEILLANCE CASE LAW

Paul De Hert & Gianclaudio Malgieri

The Strasbourg based European Court of Human Rights has a long record of cases dealing with surveillance, starting with Klass v. Germany (1978). In Klass the Court explicitly accepted the necessity for secret surveillance performed by public authorities in European post-World War II democracies, provided respect of certain victim and legality requirements deduced from Article 8 and 13 of the 1950 European Convention on Human Rights (ECHR). After the introduction of this premise, the Court proposes several important guidelines for lawful and human rights compatible surveillance that taken together built up to a comprehensive framework answering equally to questions about power divisions and checks on potential power abuse. Today there is a vast body of case law developed by the ECtHR and the European Union Court of Justice (hereafter: CJEU) that confirms and adapts these guidelines, often in view of addressing recent technology (e.g. GPS surveillance) or institutional developments (e.g. overlap between police and secrete services). In this article we will focus on developments with regard to the legality principle in the context of surveillance in the realm of criminal law and intelligence work by secret services. A more rigorous interpretation of legality principle in post Klass surveillance case law certainly qualifies as one of the most remarkable developments in the European Courts case law on surveillance. In particular, we will show that the strict approach towards the legality requirement enshrined in Article 8 ECHR adopted by the ECtHR in Huvig (1990) in the context of telephone surveillance will be then re-applied in all the following judgments of the Strasbourg Court and even adopted by the CJEU (from Digital Rights Ireland on) in the context of other surveillance practices.

Contents

The Brussels Privacy Hub Working Papers are intended to circulate research in progress for comment and discussion. Available at www.brusselsprivacyhub.org/publications.html
ISSN N° 2565-9979. This version is for academic use only.
A final version of this working paper is published as Paul De Hert & Gianclaudio Malgieri, 'Article 8 ECHR compliant and foreseeable surveillance: the ECtHR's expanded legality requirement copied by the CJEU. A discussion of surveillance case law' [2020] in Mistilegas, V. & Vavoula, N. (eds.), ECLAN Volume, Hart (forthcoming 2020). Please refer to this final text.

Disclaimer

"In its case-law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power: the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed (see, inter alia, ***Huvig***, § 34; ***Amann***, § 76; ***Valenzuela Contreras***, § 46; and ***Prado Bugallo v. Spain***, § 30)" (***Weber and Saravia***, §95).[1]

"Although the applicant acknowledged that ***Valenzuela Contreras*** was an "interception case", he argued that the principles derived from the Court's "interception" case-law could be "read across" to the present case because, first, the Court had not drawn a distinction between the principles which applied in interception cases and covert-surveillance cases; secondly, it was the nature and degree of intrusion in certain types of covert surveillance cases which allowed the Court to "read across" from the principles set out in interception cases; thirdly, any distinction was therefore not appropriate when dealing with covert surveillance of the kind in issue in the present case; and finally, given that both types of case involved the handling of material obtained as a result of listening to and recording private conversations, it was difficult to see what valid distinction could be made between an interception operation and a covert-surveillance operation of the kind at issue in the present case" (***R.E. v. United Kingdom***, §104).[2]

Introduction. From interception to bulk surveillance: reading across and amending the principles

The Strasbourg based European Court of Human Rights (hereafter: ECtHR), has a long record of cases dealing with surveillance, starting with ***Klass v. Germany*** (1978). In ***Klass*** the Court explicitly accepted the necessity for secret surveillance performed by public authorities in European post-World War II democracies, provided respect of certain victim and legality requirements deduced from Article 8 and 13 of the 1950 European Convention on Human Rights (ECHR). After the introduction of this premise, the Court proposes several important guidelines for lawful and human rights compatible surveillance that taken together built up to a comprehensive framework answering equally to questions about power divisions and checks on potential power abuse. Amongst the milestones are guidelines and clarifications with regard to 1) the broadening of the victim status with regard to surveillance ('who can go to Strasbourg?'), 2) the need for individual notification as a right of every citizen to learn about surveillance measures concerning him or her, 3) the emphasis on the necessity principle ('surveillance is only justified when it is really needed'), 4) the need of an internal oversight on surveillance, 5) the importance of the legality principle, in particular when dealing with intrusive means of surveillance (e.g. telephone interception).[3]

Today there is a vast body of case law developed by the ECtHR ***and*** the European Union Court of Justice (hereafter: CJEU) that confirms and adapts these guidelines, often in view of addressing recent technology (e.g. GPS surveillance) or institutional developments (e.g. overlap between police and secrete services). In this article we will focus on developments with regard to the ***legality*** principle in the context of surveillance in the realm of criminal law and intelligence work by secret services. A more rigorous interpretation

1 ECtHR, ***Weber and Saravia v. Germany***, 29 June 2006 no. 54934/00, ***ECHR*** 2006XI
2 ECtHR, ***R.E. v. the United Kingdom***, 27 October 2015, application no. 62498/11
3 In particular, as regards the notification, the Court argues that individuals should be informed at least when and if notification can be made without jeopardizing the purpose of the restriction. As for the oversight, the Court accepted a form of non-judicial but parliamentary review on surveillance.

of legality principle in post ***Klass*** surveillance case law certainly qualifies as one of the most remarkable developments in the European Courts case law on surveillance. In particular, we will show that the strict approach towards the legality requirement enshrined in Article 8 ECHR adopted by the ECtHR in ***Huvig*** (1990) in the context of telephone surveillance will be then re-applied in all the following judgments of the Strasbourg Court and even adopted by the CJEU (from ***Digital Rights Ireland*** on) in the context of other surveillance practices.

In ***Huvig*** and ***Weber and Saravia*** (2006) the ECtHR identified six minimum requirements with regard to the foreseeability of surveillance laws. This case-law requires a description of the nature of the crimes for which telecommunications data may be intercepted (1), a definition of the category of persons whose communication may be surveilled or processed (2), limitations in time for the periods for the surveillance measure (3), a procedure for the use and storage or retention of the data (use of summary reports) (4), precautions when the data is communicated to others (5) and the circumstances when the data must be deleted or destroyed (6). We will discuss these ***Huvig*** criteria in the context of traditional and less traditional surveillance methods.

One author coins the term 'Weber minimum criteria', [4] a label that also makes sense since these six criteria were picked up and given more definitive formulation in ***Weber and Saravia*** (2006), one of the iconic surveillance judgements of Strasbourg. The predicate 'minimum' also makes sense. It is used by the ECtHR, without too much clarification. In a 2018 judgement the Court states that 'the Court has identified six minimum safeguards that both bulk interception and other interception regimes must incorporate in order to be sufficiently foreseeable to minimise the risk of abuses of power' (***Centrum För Rättvisa***, § 113).[5] The quote also hints at the purpose of the minimum requirements: they essentially amount to preventing arbitrary interception and use as this undermines the functioning of the rule of law. In view of the margin of discretion states have to deploy surveillance, testing these requirements is a minimum for the Court 'to be satisfied with'.[6]

In the next sections we will analyze how the European Courts have developed the requirements of legality and notification in the case law, starting from ***Klass*** (1978) until the most recent judgments of the two courts (the ECtHR cases ***Ben Faiza, Centrum för Rättvisa*** and ***Big Brother Watch*** the CJEU cases Tele2 and ***Ministerio Fiscal***). After a brief overview we discuss the historical importance of ***Klass*** (section 1) and ***Malone*** (section 2). In subsequent sections we introduce the ***Huvig*** foreseeability requirements (section 3), their role-out via 'creative reading' to all intrusive surveillance practices (section 5) and the possibility foreseen in ***Uzun*** to go ***below*** these standards in the case of less intrusive surveillance (section 4 and 6). Then we turn to the ***Segerstedt-Wiberg*** refinements of the margin that states have to regulate surveillance (section 7). The last judgement also introduced the need for strict testing of surveillance laws, especially for the more intrusive surveillance measures, obliging the Court to go further than abstract testing of the

4 C. Van de Heyning , 'Het bewaren en gebruik van telecommunicatie gegevens in het strafrechtelijk onderzoek: de hoogste hoven in dialoog', *Tijdschrift voor Strafrecht*, 2019, Issue 1, (p.38-47), p. 41

5 ECtHR, ***Centrum För Rättvisa v. Sweden,*** 19 June 2018, application no. 35252/08. See Plixavra Vogiatzoglou, 'Centrum för Rättvisa v Sweden: Bulk Interception of Communications by Intelligence Services in Sweden Does Not Violate the Right to Privacy', ***European Data Protection Law Review***, 2018, vol. 4/4, 563-567

6 ***Centrum För Rättvisa v. Sweden***, §104. "As to the question whether an interference has been "necessary in a democratic society" in pursuit of a legitimate aim, the Court has acknowledged that, when balancing the interest of the respondent State in protecting its national security through secret surveillance measures against the seriousness of the interference with an applicant's rights under Article 8, the national authorities enjoy a certain margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security. However, this margin is subject to European supervision embracing both legislation and decisions applying it. In view of the risk that a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it, ***the Court must be satisfied*** that there are adequate and effective guarantees against abuse" (italics added)

Article 8§2-requirements (section 8). Two sections are needed to explain why notification (the right to learn about surveillance once it is over) is not part of the ***Huvig/Weber*** foreseeability package, although its importance is more and more affirmed (section 9 and 10). A next section highlights the success of the foreseeability approach by analyzing case law from the CJEU where similar criteria are applied to test the compatibility of surveillance with the EU Charter on Fundamental Rights (section 11). Perhaps the CJEU has been too good a student, since the ECtHR has found it necessary in two 2018 judgments to open the door for ECHR compatible bulk data surveillance (***Big Brother Watch*** and ***Centrum för Rättvisa***) (section 12). This last section only points at certain limitations of the current legality test: all surveillance, including mass surveillance that targets all citizens without discrimination, can pass the legality test. In a final section we wrap up with a summary of the main findings (section 13).

1. First formulation of the European human right framework for surveillance (Klass)

In *Klass v. Germany* (1978) Strasbourg addresses secret surveillance by criminal law authorities and by secret services and identifies for the first time a range of limits and safeguards that national laws must provide in order to respect article 8 ECHR when controlling mail, post and telecommunications of citizens.[7] The judgement is a classic, pioneering in many regards: for the first time the ECtHR declares that telephone conversations, though not expressly mentioned in Article 8, §1, "are covered by the notions of 'private life' and 'correspondence'" (*Klass,* §41). Other milestones were highlighted in our introduction, where we emphasized the surveillance friendly premise set out by the Court: the risks of secret surveillance in terms of human rights are acknowledged,[8] but "*under exceptional conditions*" accepted as "necessary in a democratic society in the interests of national security and/or for the prevention of disorder or crime", considering that "democratic societies nowadays find themselves threatened by highly sophisticated forms of espionage and by terrorism, with the result 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" (*Klass*, §48).[9]

After this ***prise de position***, a favorable judgement followed: the German law was found to be ECHR-compatible since the three general requirements laid down in Article 8, §2 ECHR, - legality, legitimate purpose

7 ECtHR, *Klass and Others v. Germany*, 6 September 1978, application no. 5029/71. All cases are available via https://www.echr.coe.int/

The case deals with legislation passed in Germany in 1968 ("G10" Act) which authorized in certain circumstances surveillance without the need to notify the person concerned and excluded legal remedy before the Courts. The applicants claimed that the legislation was contrary to Articles 6(1) (fair trial right), 8 and 13 of the European Convention on Human Rights. The case mainly focuses on the proposed surveillance powers of secret services, since the claimants concentrated their arguments on the provisions in the G10 Act making possible surveillance measures ordered by the head (or his substitute) of one of the three German intelligence agencies. See *Klass*, §18: "an application for surveillance measures may be made only by the head, or his substitute, of one of the following services: the Agencies for the Protection of the Constitution of the Federation and the Länder (Bundersamt für Verfassungsschutz; Verfassungsschutzbehörden der Länder), the Army Security Office (Amt für Sicherheit der Bundeswher) and the Federal Intelligence Service (Bundesnachrichtendienst). Interesting for our purposes is that the same Act also addresses criminal law surveillance, but for the Court these provisions are not explicitly "in issue in the present case". See *Klass*, §§25 and 40. In the judgment these provisions are discussed where the Court compares non-judicial control over secret service surveillance with judicial control over police investigation.

8 "since the individual will necessarily be prevented from seeking an effective remedy of his 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 the individual's rights" (*Klass*, §55).

9 The conclusion of the Court is that "some compromise between the requirements for defending democratic society and individual rights is inherent in the system of the Convention" and so "a balance must be sought" between privacy and communication-based rights and the necessity to impose secret surveillance for the protection of the democratic society as a whole (*Klass*, §59).

and necessity- were met. The judgement is based on rich and careful reasoning and contains several important guidelines for lawful and human rights compatible surveillance (see our introduction ***above***). The onus is on the necessity test (in particular, on the political supervision of surveillance done by secret services). and less on the legality test, which does not surprise in the light of the German tradition to produce very detailed laws.

Klass has given the European fundamental rights constitution for surveillance its first formulation. The German ingredients in its entirety survived the scrutiny by the Court, with the acceptance of a complex double track arrangement of scrutiny (a judicial control system for criminal law surveillance, and a non-judicial control for secret service surveillance) as the most remarkable feature. The Court, although considering judicial review highly preferable in all cases, nevertheless accepted this German two track system. From the judgment also follows that these judicial and political controls can be alternatively organized ex ante or ex post.

2. Deepening first understandings in the context of criminal law and police needs for metadata (Malone)

Malone (1984), the second judgment of the Court concerning secret surveillance, came six years after ***Klass*** and deals (solely) with surveillance by police in criminal investigations.[10] The case concerned police interceptions of telecommunications on the authority of a warrant signed by the Secretary of State, without a legal basis and system to supervise such warrants [11]

Malone is a first (early) case of meta-data surveillance and one finds in it a progressive understanding of the subtleties of surveillance by the European judges.[12] It contains an emblematic discussion with the UK

10 ECtHR, *Malone v. the United Kingdom*, 2 August 1984, application no. 8691/79.

11 Its focus is on criminal law surveillance only and it is therefore historically the first surveillance case which "is directly concerned only with the question of interceptions effected by or on behalf of ***the police*** - and not other government services such as (…) the Security Service - within the general context of a ***criminal investigation***, together with the legal and administrative framework relevant to such interceptions" (***Malone***, §63). Malone, the complainant, asserted that his telephone conversation was tapped, and his post was opened by the police on the authority of a warrant signed by the Secretary of State, but that there was no legal basis and system to supervise such warrants. Therefore, the complainant claimed that such treatment was not in 'accordance with law' in the sense of the second paragraph of Article 8 ECHR that requires an adequate legal basis in domestic law to ground legitimate interferences with privacy-rights. The United Kingdom government maintained that there was a legal basis, partly laid down in the ***Post Office Act 1969*** and further developed in practice. The Court however followed the analysis of an English judge in an earlier phase of the case who had compared the English 'law' with the German law discussed in ***Klass*** and found the legal situation in the United Kingdom failing in the light of European Court's insistence in ***Klass*** on clearly spelled-out checks and balances to make effective control possible whenever the executive authorities interfere with an individual's rights. The precise wording of British law was considered so vague that it could also "authorize the laying of a requirement on the Post Office for whatever purposes and in whatever manner"

12 Malone did not only complain about opening postal letters and intercepting telephones by the police (on the authority of a warrant signed by the Secretary of State), but also about the telephone companies sharing their telecommunication data with the police. Today we would take about sharing *meta data,* but back then, the term used was "data obtained through *metering*". For the Court "the process known as 'metering' involves the use of a device (a meter check printer) which registers the numbers dialed on a particular telephone and the time and duration of each call. In making such records, the Post Office - now British Telecommunications - makes use only of signals sent to itself as the provider of the telephone service and does not monitor or intercept telephone conversations at all" (*Malone*, §56).

Government denying any Article 8, §1 ECHR- ('protectable') status for meta-data: the judges, although accepting that this data is less intrusive than intercepted (content) data, recognized the Article 8, §1-status.[13] Then the Court turned to the Article 8, §2- requirement of legality and found hardly any legal basis for the police to obtain the metering data. The Court declared that the "law of England and Wales does not indicate with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities. To that extent, the minimum degree of legal protection to which citizens are entitled under the rule of law in a democratic society is lacking" (***Malone***, §79). Indeed, "apart from the simple absence of prohibition, there would appear to be no legal rules concerning the scope and manner of exercise of the discretion enjoyed by the public authorities. Consequently, although lawful in terms of domestic law, the interference resulting from the existence of the practice in question by the English police was not "in accordance with the law", within the meaning of para. 2 of Art. 8 ECHR (***Malone***, §84).

This part of ***Malone*** has been at the basis of a powerful principle behind our European surveillance framework: even when there is consensus about a practice of surveillance being less intrusive than another (e.g. tapping), the basic Article 8 requirements of legality, legitimacy and proportionality remain applicable and are tested in Court: there always needs to be an adequate (from a Strasbourg perspective) legal basis in domestic law that clarifies the legitimate purposes of the surveillance and rests on a necessity assessment.

All surveillance is tested against this framework. However, that does not mean that the framework is applied in an identical way. The common feeling in the 1980s was that the more intrusive surveillance, the stricter should be the safeguards for individuals' privacy. ***Malone*** does not say so explicitly, but it could be deduced from it (and was actually done so in most legal systems).[14] Also, we do not always get full testing of all three Article 8 ECHR-requirements and of other ECHR-rights. ***Malone*** in this regard, contains fine examples of the ECtHR practice ***not*** to take a look at possible violations of Article 13 ECHR (effective remedy) once it has found a violation of Article 8 ECHR,[15] and ***not*** to look at the legitimacy or necessity requirements of Article 8, §2 ECHR once it has found a violation of the (first) requirement of legality. So, contrary to ***Klass***, ***Malone*** -that only deals with criminal law surveillance-, contains no analysis of the necessity and of the legitimacy of surveillance in this context.[16]

13 The UK Government indeed argued that the sharing of data *about* phone calls was not protected by Article 8 ECHR. There is no content monitoring and the metering is done legitimately by suppliers of telephone services notably in order to ensure that the subscriber is correctly charged or to investigate complaints or possible abuses of the service (*Malone*, §83-84). The Court went along with the reasoning that by 'its very nature, metering is (…) to be distinguished from interception of communications' because it is contrary to interception that is 'undesirable and illegitimate in a democratic society unless justified', but disagreed with the human rights analysis: "the Court does not accept, however, that the use of data obtained from metering, whatever the circumstances and purposes, cannot give rise to an issue under Art. 8. The records of metering contain information, in particular the numbers dialed, which is an integral element in the communications made by telephone. Consequently, release of that information to the police without the consent of the subscriber also amounts, in the opinion of the Court, to an interference with a right guaranteed by Art. 8" (*Malone*, §84).

14 We will see *infra* how this interpretation is accepted by the Court in later judgments (see, e.g. *Huvig* and *Uzun*), but is partly tempered in later judgments (see infra, e.g. ECJ *Digital Ireland Rights*), probably because the differences between hard and soft, more or less intrusive do not always convince.

15 Comp. *Malone,* 90-91: "The applicant submitted that no effective domestic remedy existed for the breaches of Art. 8 of which he complained and that, consequently, there had also been a violation of Art. 13 (…) Having regard to its decision on Art. 8 (see para. 89 above), the Court does not consider it necessary to rule on this issue. (…)"

16 Although there is a taken for granted feel in the judgment that governments in criminal law *can* go secret: "Undoubtedly, the existence of some law granting powers of interception of communications to aid the police in their function of investigating and detecting crime may be "necessary in a democratic society ... for the prevention of disorder or crime", within the meaning of paragraph 2 of Article 8 (art. 8-2)". Indeed, "the Court accepts, (…) that in Great Britain "the increase of crime, and particularly the growth of organised crime, the increasing sophistication of criminals and the ease and speed with which they can move about have made telephone interception an indispensable tool in the investigation and prevention of serious crime" (*Malone*, §81).

These methodological particularities of Strasbourg explain the focus of ***Malone*** on the legality principle.[17] The ECtHR requires that police investigation powers be clearly determined by primary law as for their manners and as for their purposes. Vague provisions are unacceptable if they allow surveillance for whatever purpose and in whatever manner and practices of surveillance collaborations (in this case between the police and the telecommunication operators), outside any legal framework, are contrary to the logic of the legality requirement since there is no way for the concerned citizen to understand these practices through the law. Surveillance requires laws - the Courts is saying - that need a considerable amount of detail: i.e. "how is the surveillance organized?", "for what purposes can the surveillance be done?" ***and*** "what methods are used?" (see ***Malone***, §75).

3. Perfectionating Malone's legality framework for telephone surveillance (Huvig)

Huvig v. France (1990) also deals with criminal law powers and their legal basis.[18] Like ***Malone*** the Court found a violation of the legality requirement, this time in French law where the powers of investigating judges to intercept telecommunications were poorly addressed.[19] If there is a common approach in Europe toward telephone interceptions and surveillance in the area of criminal law, it is due to ***Huvig*** (or the quasi identical ***Kruslin*** judgement the same day).[20] Famous is the observation of the Court that "it is essential to have clear, detailed rules on the subject***, especially as the technology available for use is continually becoming more sophisticated***" (***Huvig***, §32).

Sophisticated technologies require sophisticated laws and the full attention of the ECtHR in ***Huvig*** is therefore on the legality principle. In the view of the Court, "in accordance with the law" within the meaning of Article 8§2 ECHR, requires a material requirement of legality; an accessibility requirement of legality; a foreseeability requirement of legality ***and*** a rule of law requirement of legality. [21]

Table 1. Four basic legality requirements identified in **Huvig**

1. Material requirement of legality: the impugned measure should have some basis in domestic law, meaning that law is understood in its substantive sense including not only written formal laws but also lower rank enactments and unwritten law
2. accessibility requirement of legality: law also refers to the quality of the law in question, requiring that it should be accessible to the person concerned
3. foreseeability requirement of legality: law also must allow the person concerned to be able to foresee its consequences for him,
4. rule of law requirement of legality: the whole domestic arrangement should be compatible with the rule of law.

17 "On the evidence before the Court, it cannot be said with any reasonable certainty what elements of the powers to intercept are incorporated in legal rules and what elements remain within the discretion of the executive". Therefore, "the minimum degree of legal protection to which citizens are entitled under the rule of law in a democratic society is lacking". *Malone*, §79.

18 ECtHR, *Huvig v. France,* 24 April 1990, application no. 11105/84.

19 The case concerns a French judge who allowed for the tapping for 28 hours of the applicants' telephone. Charges were brought against the applicants, who were convicted on nearly all of them. The applicants claimed that the tapping violated Art. 8 ECHR, amongst others because of the lack of a clear and detailed legal basis in domestic law.

20 Kruslin v. France, 24 April 1990, application no. 11801/85,

21 *Huvig*, §26: "The expression "in accordance with the law", within the meaning of Article 8 §2,requires firstly that the impugned measure should have some basis in domestic law; it also refers to the quality of the law in question, requiring that it should be accessible to the person concerned, who must moreover be able to foresee its consequences for him, and compatible with the rule of law".

We do not want to pay too much attention to this presentation of the legality principle,[22] although its historical relevance is beyond doubt. The two first (material and accessibility) requirements, for instance, are of a nature to end all domestic arrangements with regard to criminal law and surveillance based on incomplete or secret laws.

More important here, however, is that the analysis by the Court of the legality requirement, led the Court to the further articulation of ***foreseeability***-criteria that will come back in many future cases. The contested French measures were based on very vague and general provisions like Article 81 of the French 1958 Code of Criminal Procedure ('***the investigative judge could do all necessary to investigate crimes***'). This and other similar provisions were seen as the basis for his power to command telephone interceptions by the French government. The ECtHR found, however, a problem with the third and fourth legality requirement (foreseeability linked to the idea of the rule of law). It found that domestic French law did not indicate with reasonable clarity ***the scope and manner*** of exercise of the relevant discretion conferred on the public authorities.[23] The ECtHR then identified six elements that surveillance laws on telephone tapping must provide to qualify as foreseeable in the context of human rights: 1) clarification of categories of people liable to be monitored; 2) clarification of the nature of the offenses liable of surveillance; 3) clarification of the limits on the duration of such monitoring; 4) clarification of the procedure to be followed for collecting the intercepted data in summary reports; 5) clarification of the precautions to be taken in order to communicate the recordings intact and in their entirety for possible inspection by the judge and by the defence; 6) clarification of the circumstances in which data needs to be erased or destroyed.

Table 2. Six criteria to test the foreseeability of domestic surveillance laws in **Huvig**

Six criteria to test the foreseeability of domestic surveillance laws in *Huvig* [24]
1) ***categories*** of people liable to be monitored
2) the ***nature of the offenses*** which may give rise to surveillance measures
3) limits on the ***duration*** of such monitoring
4) ***procedure*** to be followed for storing the data
5) ***precautions*** to be taken when ***communicating*** the data to the judges and defence
6) circumstances in which data is ***erased*** or destroyed
7) [Eventual element] ***Judicial control***
8) [Eventual element] ***Notification of the surveilled citizen***

The first six requirements will from here on be part of the 'minimum' foreseeability package that is checked by the ECtHR over and over in surveillance case law. The seventh and eight elements are labeled 'eventual' or 'optional', because of the difficulty experienced by the Court to embrace them, hesitating to make them mandatory requirements and hesitating to include them in the minimum foreseeability package. We will come to the issue of notification ***below*** (section 9). About the need to have a judge to authorize or review surveillance measures, the ECtHR observed the following: "the Court does not in any way minimize

22 The Court is not always as systematic in presenting it in this way. In particular the rule of law requirement seems to be volatile and is sometimes not mentioned or dealt with in other parts of judgments, for instance under the necessity test or other sections.

23 *Huvig*, §35. Note that these principles on surveillance partly come back in *Rotaru v Romania* (2000) where the court looks at the law on processing data from surveillance for national security purposes.

24 *Huvig*, §34. See, P. De Hert, 'Het recht op een onderzoeksrechter in Belgisch en Europees perspectief. Grondrechtelijke armoede met een inquisitoriale achtergrond' [The investigating judge in Belgian and European Law], *Panopticon. Tijdschrift voor strafrecht, criminologie en forensisch welzijns*werk, 2003, vol. 24/2, 155-198.

the value of several of the safeguards, ***in particular the need for a decision by an investigating judge***, who is an independent judicial authority, the latter's supervision of senior police officers and the possible supervision of the judge himself by the Indictment Division (***chambre d'accusation***) of the Court of Appeal, by trial courts and courts of appeal and, if need be, by the Court of Cassation" ***(Huvig***, §33). In fact, Strasbourg Court – though approving this aspect of the French surveillance - is unclear about the importance and the general necessity of this safeguard for any surveillance system. Indeed, its statement "***the Court does not in any way minimize the value of several of the safeguards***" appears ambiguous and unhelpful to solve a central problem: is the judicial control a necessary safeguard for ***all*** telephone surveillance (including those by secret services) and ***all*** methods of surveillance, also those that are (presumed) less intrusive? The insistence of the ECtHR on the seriousness of tapping telephones seems to suggest that a watered down version of all 7 elements, including the one on judicial authorization, is possible when considering less intrusive surveillance measures.[25] In our previous works we defined this issue as a "golden question" in our previous work.[26] Another factor that plays ***against*** a mandatory requirement for judicial involvement in criminal related surveillance in ordering or supervising the surveillance has to do with the differences between legal systems in Europe regarding the structure of their criminal procedures.[27] A related problem is that of the involvement of the judiciary in the work of secret services, which is rarely the case. The trend today imposed by Strasbourg, however, seems to go towards more involvement of magistrates or non-political but independent oversight.[28]

Huvig has in a powerful way enhanced our understanding of what domestic law needs to offer in the case of privacy and other intrusions. The four dimensions of legality (material, accessible, foreseeable, rule of law), combined with the extensive testing of foreseeability, are a powerful bulwark towards all arguments ***against*** complete and detailed written laws about investigative and surveillance powers in Western

25 *Huvig*, §32: "Tapping and other forms of interception of telephone conversations represent a serious interference with private life and correspondence and must accordingly be based on a "law" that is particularly precise. It is essential to have clear, detailed rules on the subject*, especially as the technology available for use is continually becoming more sophisticated*".

26 A. Galetta & P. De Hert, 'Complementing the Surveillance Law Principles of the ECtHR with its Environmental Law Principles: An Integrated Technology Approach to a Human Rights Framework for Surveillance', *Utrecht Law Review*, 2014, vol. 10, no. 1, (55-75), 60. Most of the elements identified in *Huvig* can be transposed in adversarial systems, but some bending needs to be done regarding the requirement of having a judge authorizing and reviewing the surveillance. In particular, we may wonder whether it would be sufficient that prosecutors authorize interceptions or, instead, it would be preferable that ordinary judges (acting as "control judges") authorize it. Judgements like *Dumitru Popescu v. Romania* (2007), *Iordachi and Others v. Moldavo* (2009) and *Uzun (below*) will teach us that only 'serious' interferences with the right to privacy and to secrecy of telecommunications, -such as telephone tapping-, are subjected to authorization that needs to be 'independent'.

27 We recall that French criminal procedure is based on inquisitorial system, where *investigative judges* lead investigations and authorize interceptions and *control judges* supervise investigation measures and review surveillance *post hoc.* Instead, in adversarial systems, investigations are led by police or by prosecutors and not by (investigative) judges. See, e.g., that in UK since 1970s there is no "investigative judge" any longer.

28 G. Malgieri & P. De Hert, 'European Human Rights, Criminal Surveillance, and Intelligence Surveillance: Towards "Good Enough" Oversight, Preferably but not Necessarily by Judges' in David C. Gray & Stephen Henderson (eds), *The Cambridge Handbook on* Surveillance, New York: Cambridge University Press, 2017, 509-532. The two courts (the ECtHR and, to a lesser degree, the CJEU) put great emphasis on a system of control ex ante and post hoc by independent supervisory authorities. A complex and controversial issue was whether the human rights to privacy (enshrined in Article 8 and 13 ECHR), requires judicial review as a necessary safeguard for secret surveillance or alternatively, at which conditions, systems of non-judicial review can be accepted as adequate safeguards against illegitimate interference in citizens' private life. In particular, the ECtHR, since *Klass*, accepted also non-judicial oversight and developed a flexible interpretation of article 8 and 13 ECHR, making the choice between judicial oversight or other oversight depending on several factors ("vital" interests at stake, political considerations, etc.). Although the Court always has shown a preference towards judiciary oversight, its case law contributed to a European legal order with several examples of alternative oversight systems assessed positively by the Court, such as the quasi-judiciary systems (where the independency of the supervisory body, its wide jurisdiction, its power to data access and its power to effective reactions are proved) or the system of oversight set by Data Protection Authorities in the EU member states. However, in recent ECtHR and CJEU judgments we see an increasing emphasis on real functioning of the oversight mechanism, even when it is predominantly judicial. Even in the preferred option of a system of judicial oversight, with is needed is "good enough" (ex-ante or post hoc) control over surveillance, meaning not simply a judicial control, but a system of oversight (judicial, quasi-judicial, hybrid) which can provide an effective control over surveillance, supported by empirical checks in the national legal system at issue.

democracies. The homework to the French legislator given in 1990 was considerable. The French government saw it coming and provided itself a long list of 'common' police powers that lacked a written basis in their continental and 'written' law system.[29]

4. Creating a complementary framework with fainter legality limits for fainter surveillance (Uzun)

In 2010 the ECtHR decided ***Uzun v. Germany***,[30] a case on criminal law surveillance and dealing with modern and non-conventional surveillance technologies.[31] The applicant, suspected of terrorist activities, was put under surveillance. The German "Federal Office for Criminal Investigation" secretly installed a Global Positioning System (GPS) receiver in his car, allowing it to determine the location and the speed of the car once per minute (***Uzun***, §12). The Court accepted that the systematic collection and storing of data by police on particular individuals, constituted an interference with the applicant's private life (***Uzun***, §46). However, the interference was considered of a lower intensity compared to, for instance, telephone tapping.[32] This last assessment bears consequences for the number of safeguards needed. ***Uzun***, compared to ***Huvig***, is remarkably less detailed about foreseeability:[33] there is silence about some requirements (procedures and precautions for treating, communicating and destroying data) and, -when requirements are mentioned-, there is predominant use of general terms[34] (see table 2). This situation points at a double standard of protection:[35] the threshold to be met in ***Uzun*** to comply with the lawfulness principle is lower than in ***Huvig***.

Table 3. Comparing the **light Uzun-testing**

Comparing the light *Uzun*-testing	
Huvig	Uzun
1) ***categories of people*** liable to be monitored;	"***grounds*** required for ordering them"
2) the ***nature of the offenses*** liable of surveillance;	
3) ***limits*** on the ***duration*** of such monitoring;	"(nature, scope and) ***duration*** of the possible measures"
4) the procedure to be followed for ***treating the data***;	N/A
5) ***precautions*** to be taken when ***communicating*** the data	N/A

29 *Huvig*, §27: "In the Government's submission, (…) the Code of Criminal Procedure (…) did not give an exhaustive list of the investigative means available to the investigating judge - measures as common as the taking of photographs or fingerprints, shadowing, surveillance, requisitions, confrontations between witnesses, and reconstructions of crimes, for example, were not mentioned in it either. The provisions added to Article 81 by Articles 151 and 152 were supplemented in national case-law".

30 *Uzun v. Germany*, 2 September 2010, application n. 35623/05.

31 In our previous work we have already highlighted the importance of *Uzun*. See A. Galetta & P. De Hert, 60-61. See also Murphy, Maria Helen, 'Investigative Use of GPS Tracking Devices and the European Court of Human Rights', *Irish Criminal Law Journal,* 2012). 22(1). Available at SSRN: https://ssrn.com/abstract=2385555

32 In the Court's view, "GPS surveillance is by its very nature to be distinguished from other methods of visual or acoustical surveillance which are, as a rule, more susceptible of interfering with a person's right to respect for private life, because they disclose more information on a person's conduct, opinions or feelings" (*Uzun*, §52).

33 The Court (only) clarifies that elements that law must provide are "all the circumstances of the case, such as the *nature, scope and duration* of the possible measures; the *grounds* required for ordering them; the *authorities* competent to permit, carry out and supervise them; the kind of *remedy* provided by the national law" (*Uzun*, §63. Italics added).

34 Judicial overview vs. overview by *"authorities"*, *"remedies"*; limits on the durations vs. 'duration'; offences, categories of people vs. 'grounds for surveillance'

35 See A. Galleta & P. De Hert, 60.

6) ***circumstances*** in which ***data*** is erased or ***destroyed***	N/A
7) judicial overview	an ***ex post*** safeguard
8) notification	an ***ex post*** safeguard

Uzun apparently teaches us three things about the legality requirement.

Firstly, the strictness and detailedness of legality requirements depends on the level of intrusiveness of the surveillance method in question.[36]

Secondly, the complete set of ***Huvig*** requirements only apply to more intrusive surveillance means.[37] Requirement 4, 5 and 6 are not checked in ***Uzun***.

Thirdly, requirements 7 and 8 are dealt with in ***Uzun***, but do not belong to the core requirements of foreseeability/legality. Why is this? German law does not require any judicial authorization before GPS surveillance that is controlled by the prosecutor and executed by the police. Given the hypothetical possibility of control ***post hoc***,[38] the only missing safeguard in the present case would be ***ex ante*** independent control of the GPS surveillance. However, the Court does not consider this requirement essential. In indirect language it seems to suggest that in view of several factors judicial or independent ***ex ante*** authorization could be replaced by other kinds of authorizations (e.g. by a prosecutor) and ***ex post*** safeguards, such as judicial review, the possibility to exclude evidence obtained from an illegal GPS surveillance and a provision ensuring the respect of the proportionality principle.[39]

Notification is also identified as a factor making up for the absence of ex ante judicial authorization. In ***Uzun,*** it is tested not as part of the legality check but as an ***ex post*** safeguard under the necessity test.[40]

36 This will be confirmed in *Segerstedt-Wiberg* (2006): "the Court considers 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 and combating terrorism must be balanced against *the seriousness of the interference with the respective applicants' right to respect for private life*" (*Segersted-Wiberg*, §88, emphasis added).

37 This second message should be received with prudence. More recent judgements (e.g. *Digital Rights Ireland)* teach us that the *Huvig* requirements do come back with most other surveillance methods, also when one could argue that they show a lower intrusiveness (*below*).

38 The Court affirms that this provision does not violate Article 8 ECHR, in particular because "in *subsequent criminal proceedings against the person concerned*, the criminal courts could review the legality of such a measure of surveillance and, in the event that the measure was found to be unlawful, had discretion to exclude the evidence obtained thereby from use at the trial" (*Uzun*, §71). One can criticize the value of this argument because it does not cover situations where police investigations do not lead to court cases or are not aimed to detect crimes, but for example to operate for the purpose of national security or public safety (and so overlapping secret services traditional task). In such cases, which are an emerging reality nowadays, the control *post hoc* during subsequent criminal trials is not feasible in fact. Comp. G. Lennon, 'Stop and search powers in UK terrorism investigations: a limited judicial oversight?', *The International Journal of Human Rights*, 2016, vol. 20/5, 634-648.

39 *Uzun,* §73: "The Court finally does not overlook that under the Code of Criminal Procedure, it was not necessary for a court to authorise and supervise surveillance via GPS which was carried out in addition to other means of surveillance and thus all surveillance measures in their entirety. It takes the view that sufficient safeguards against abuse require, in particular, that uncoordinated investigation measures taken by different authorities must be prevented and that, therefore, the prosecution, prior to ordering a suspect's surveillance via GPS, had to make sure that it was aware of further surveillance measures already in place. However, having also regard to the findings of the Federal Constitutional Court on this issue, it finds that at the relevant time the safeguards in place to prevent a person's total surveillance, including the principle of proportionality, were sufficient to prevent abuse".

40 The following paragraph is crucial in the argument: "The Court considers that such judicial review and the possibility to exclude evidence obtained from an illegal GPS surveillance constituted an important safeguard, as it discouraged the investigating authorities from collecting evidence by unlawful means. In view of the fact that GPS surveillance must be considered to interfere less with a person's private life than, for instance, telephone tapping (an order for which has to be made by an independent body both under domestic law (see Article 100b §1 of the Code of Criminal Procedure) and under Article 8 of the Convention (see, in particular, *Dumitru Popescu v. Romania (no. 2)*, and *Iordachi and Others*), the Court finds subsequent judicial review of a person's surveillance by GPS to offer sufficient protection against arbitrariness. Moreover, Article 101 §1 of the (German) Code of Criminal Procedure contained a further safeguard against abuse in that it ordered that the person concerned be informed of the surveillance measure he or she had been subjected to under certain circumstances" (*Uzun*, §72).

Like judicial review, it can help limiting abuse with secret surveillance practices in general. Also, in the context of criminal law investigations and surveillance, it can help to realize the rule of law idea in the (growing number of) cases where there is no independent control ***post hoc*** (during subsequent criminal trials). Through notification the surveilled person is enabled to go to the court and have the independent scrutiny that should be standard in a democracy (see section 9, ***below***).

5. Creating one coherent framework for surveillance not present in Klass (Weber and Saravia/Big Brother Watch)

Few years before ***Uzun*** the Court addressed mass surveillance led by secret services in ***Weber and Saravia v. Germany*** (2006) and, two years later, in ***Liberty and others v. the United Kingdom*** (2008).
Weber and Saravia is about new secret service powers to apply ***strategic monitoring*** based on ***catchwords*** added in 1994 to the German surveillance laws discussed in ***Klass***.[41] Strategic monitoring is the first legal recognition of what will be then called "mass surveillance" in more recent jurisprudence and legal literature, as we will show below.[42] Fundamental for us is the use of the (first) six ***Huvig*** legality requirements in this 2006 judgement on mass surveillance:

In its case-law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power: the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed (see, inter alia, ***Huvig***, § 34; ***Amann***, § 76; ***Valenzuela Contreras***, § 46; and ***Prado Bugallo v. Spain***, § 30)" (***Weber and Saravia***, §95).

Interception foreseeability is rolled out as surveillance foreseeability.[43] ***Weber and Saravia*** does not

41 ECtHR, ***Weber and Saravia v. Germany***, 29 June 2006 no. 54934/00, ***ECHR*** 2006XI. ***Weber and Saravia*** deals with certain provisions in the 1994 ***Fight against Crime Act*** amending the 1968 G10 Act (the law on intelligence surveillance in Germany, previously addressed when discussing ***Klass***) according to which the German Federal Intelligence Service (***Bundesnachrichtendienst***) can record telecommunications in the course of strategic monitoring, use the collected data and when necessary transmit it to other authorities. The new act allows both ***individual and strategic monitoring:*** the former is defined as the interception of telecommunications of specific persons, that serves to avert or investigate certain grave offences which the persons monitored are suspected of planning or having committed, whereas the latter aims at collecting information by intercepting telecommunications in order to identify and avert serious dangers, such as an armed attack on its territory or the commission of international terrorist attacks and certain other serious offences (***Weber and Saravia***, §4). The main novelty of ***strategic monitoring*** is the use of ***catchwords***. According to the new G10 Act such catchwords cannot contain distinguishing features (***Identifizierungsmerkmale)*** allowing the interception of specific telecommunications and had to be listed in the monitoring order ((***Weber and Saravia***, §40). In practice, at least according to the applicants, this kind of surveillance allows to monitor numerous telecommunications in the absence of any concrete suspicions, whereby the catchwords were kept secret (***Weber and Saravia***, §9).

42 The German government justified the use of this new form of surveillance (strategic monitoring with catchwords) with the need to deal with bigger threats to public security in the 21st century (e.g. international terrorism - in particular after 11 September 2001 - and international arms trafficking) (***Weber and Saravia v. Germany***, §110). We note that the term 'catchwords' looks like the best translation of "Suchebegriffe" which can be found in the first sentence of section 3(2) of the Amended G10 Act (see ***Weber and Saravia***, §32).

43 The only significant change regards the *Huvig* requirement that 'precautions are be taken in order to communicate the recordings intact and in their entirety for possible inspection by the judge (who can hardly verify the number and length of the original tapes on the spot) and by the defence' (*Huvig*, § 34) that now seems to subsumed under 'the procedure to be followed for examining, using and storing the data obtained' and partly under the new requirement of 'precautions to be taken when communicating the data to other parties'.

explain or justify this use of interception criteria to test surveillance practices other than telephone interception and does not engage in a deep analysis of different surveillance methods but presents the outcome as a general result of the 'surveillance' case-law of the Court (see §95 quoted ***above***). In the light of ***Uzun*** one would have expected more justification for applying telephone tapping criteria to other surveillance methods, but this is it. The rest of the judgement is less important, since the Court found all six ***Huvig***-requirements respected.[44] Other safeguards, such as notification and judicial review, are not addressed or not addressed under the legality check but touched upon elsewhere in the judgement.[45]

Weber and Saravia's importance for the history of the legal reception of surveillance in Europe, -applying the ***Huvig*** foreseeability criteria to other surveillance practices then telephone tapping-, is testified by the outcome of UK mass surveillance cases that will follow. In ***Liberty***, decided two years after ***Weber***,[46] the ECtHR refers explicitly to ***Weber*** and reaffirms that mass surveillance, although different from individual surveillance, can be addressed with the same system of safeguards used for individual surveillance, in

44 In the view of the Court all ***Huvig***-legality requirements were respected, a fact that helped reaching the general finding of compatibility of the German act with the legality requirement contained in Article 8, §2 ECHR (***Weber and Saravia***, §95). We can infer from the judgement that, according to the ECtHR, mass surveillance can be legitimate only if the keywords used are declared from the outset and so explicitly mentioned when requesting authorization for surveillance. As for legality requirement of foreseeability of categories of people liable to be monitored, the Court acknowledges that the legal provisions regulating mass surveillance in the case at issue were adequate since they required "an indication of which categories of persons were liable to have their telephone tapped" (***Weber and Saravia v. Germany***, §97). In addition, the Court argues that the use of "catchwords" (declared from the outset e.g. to the supervisory authority) in mass surveillance increases foreseeability of categories of people liable to be monitored (***Weber and Saravia v. Germany***, §97). The Court assesses positively that "the authorities storing the data had to verify every six months whether those data were still necessary to achieve the purposes for which they had been obtained by or transmitted to them". This issue will acquire greater importance several years later, in particular in the CJEU case law dealing with mass data retention (see ***Digital Rights Ireland*** and ***Tele2 Sverige***).

45 The seventh ***Huvig***-requirement (review by a magistrate) is not addressed in this part of the Article 8 ECHR- analysis but dealt with under the ***necessity***-assessment of the contested G10-provisions, and, like in ***Klass***, found to be non-applicable. In the ***Klass***-tradition, this part of the Article 8-analysis opens with a strong ***prise de position*** about the need for mass surveillance to combat serious crime and for giving member states some discretion in this regard. This surveillance-friendly starting point, is then followed by a detailed analysis of the guarantees build in the German law, with the final conclusion that the German system of mass surveillance is compatible with the requirement of 'necessary in a democracy' because of the rigid procedures to order it and because of the effective supervision by two 'independent' (though not judicial) bodies: the G10 Commission and a Parliamentary Board. The Court noted that the procedures for authorising surveillance and for reviewing it ensured that measures were not ordered haphazardly, irregularly or without due and proper consideration. For conducting mass surveillance, it was required to have "a reasoned application by the President of the Federal Intelligence Service and only if the establishment of the facts by another method had no prospect of success or was considerably more difficult". The decision to monitor had to be taken by a Federal Minister, who had to obtain prior authorisation from the G10 Commission (established by the G10 Act) and had to report at least every six months to a Parliamentary Supervisory Board, which consisted of nine members of parliament, including members of the opposition (***Weber and Saravia***, §115 & 117). As regards supervision and review of monitoring measures, the Court notes that the G10 Act provided for independent supervision by these two bodies (G10 Commission and Parliamentary Board) that both have a comparatively significant role to play. Interestingly, the Court recalls that "in ***Klass*** it found this system of supervision, which remained essentially the same under the amended G 10 Act at issue here adequate under article 8 ECHR (***Weber and Saravia***, §117). Both bodies figured already in the original G10 Act discussed in ***Klass*** but are slightly enhanced in the amended Act in order to supervise mass surveillance orders. Two other contested aspects of the amended Act, -powers to process data collected through mass surveillance and powers to transfer this to other authorities-, were also found compatible with the necessity requirement, in particular because the German Constitutional Court has topped off previously some sharp edges. The last issue, in particular, the question whether data could be transferred to criminal authorities to instigate criminal procedures, is of a certain interest in the context of this contribution. The Court agreed with the applicants that transmission of personal data obtained by general surveillance measures without any specific prior suspicion in order to allow the institution of criminal proceedings against those being monitored constitutes a fairly serious interference (***Weber and Saravia***, §125), but the possibility to transfer was limited to prevent or prosecute only certain serious criminal offences listed in the amended G10 Act (***Weber and Saravia***, §126) and could only be done if specific facts – as opposed to mere factual indications – aroused the suspicion that someone had committed one of the listed offences (***Weber and Saravia***, §127)

46 ECtHR, ***Liberty and Others v. the United Kingdom***, 1 July 2008, application no. 58243/00. ***Liberty*** deals with a system operated by the United Kingdom ***Ministry of Defence***, which monitored, between 1990 and 1997, up to 10,000 simultaneous telephone channels coming from Dublin to London and on to the continent. During this time the ***Ministry of Defence*** intercepted all public telecommunications, including telephone, facsimile and e-mail communications, carried on microwave radio between two of British Telecom's radio stations. Those telephone calls, faxes and emails were then stored and filtered using search engines and keyword lists before being passed to intelligence analysts.

particular regarding the legality principle.[47] In ***Kennedy*** (2010)[48] the ECtHR looks again at RIPA, but this time at the provisions on criminal law surveillance of communications.[49] The judgment reads as a copy of ***Liberty***, with its testing of ***Huvig/Weber***-foreseeability criteria.[50] A last part of RIPA, -on direct, covert and intrusive surveillance-, is looked at in ***R.E*** (2015). Again, the ***Huvig/Weber*** criteria were recognized as ***the*** benchmark for Article 8 compliance.[51]

More RIPA testing is presented in ***Big Brother Watch*** (2018), the famous post-Snowden case with the Court assessing no less than three controversial surveillance practices: international data sharing practices of the UK secret services, collection of data amongst service providers ***and*** bulk data surveillance. Very detailed ***Huvig/Weber*** criteria-testing was done with regard to the British bulk data surveillance regime (see Table 3). Because of the indiscriminate nature of bulk-surveillance the ECtHR simply merges the first two criteria[52] under one heading ***scope of application of secret surveillance measures***.

47 This position was partly based on a smart analogy with former cases concerning strategic screening of mail of prisoners. Indeed, the Court admits that "it is true that the surveillance requirements" developed in previous case law "were first developed by the Court in connection with measures of surveillance targeted at specific individuals or addresses". *Weber* and *Saravia* was also concerned with generalised "strategic monitoring", rather than individual monitoring, but "the Court does not consider that there is any ground to apply different principles concerning the accessibility and clarity of the rules governing the interception of individual communications, on the one hand, and more general programmes of surveillance, on the other" (*Liberty*, §63). It does not entail that, according to the Court, mass surveillance and individual surveillance pose the same problems, as we will show below. Consequently, the ECtHR applies the six *Huvig*-criteria (*Liberty*, §62) and finds them not all fully respected. *Liberty v. UK*, §68- 69. *Liberty* refers thoroughly to *Weber and Saravia*, making a comparison between the German system of surveillance (G10 Law) and the United Kingdom system (RIPA Act 2000). The Court finds that the RIPA Act does not adequately mention the procedures to be followed for selecting for examination, sharing, storing and destroying intercepted material (see point d of the *Huvig* test ("procedures to be followed for selecting for examination, sharing, storing and destroying intercepted material")

48 ECtHR, *Kennedy v. United Kingdom*, 18 May 2010, application n. 26839/05.

49 More in particular, the two chapters of Part I of the Act (art. 1-26) on the interception of communications (chapter 1) and on collection and disclosure of communications data (chapter 2). The applicant, believing to be the object of intensive police surveillance, argued that the RIPA changes were inadequate to address the flaws found in in *Liberty.* The claimant was a campaigner against police abuse. Suspecting that his business mail, telephone and email communications were being intercepted because of his high-profile case and his subsequent involvement in campaigning against miscarriages of justice, the applicant complained to the Investigatory Powers Tribunal, the oversight body installed by RIPA, but then turned dissatisfied to Strasbourg. In particular, he alleged that section 8(1) RIPA, which stipulated the basic contents of an interception warrant, did not indicate with sufficient clarity how decisions as to which individuals were to be put under surveillance were made; that RIPA did not define the categories of persons who could have their telephones tapped; and that it did not clarify the procedures in place to regulate the interception and processing of intercept material. He contended that the safeguards referred to in section 15 RIPA were inadequate as they were subject to unknown "arrangements" considered necessary by the Secretary of State. The other procedural safeguards in place including the possibility of launching proceedings before the IPT, were, in the applicant's view, also inadequate to protect against abuse. He complained that after alleging unlawful interception of his communications, the hearing and procedures before the *Investigatory Powers Tribunal* ('IPT') as laid down in the RIPA Act did not offer appropriate safeguards. His requests under the Data Protection Act 1998 to discover whether information about him was being processed had been refused on the grounds of national security. Complaints about such refusals to the *Investigatory Powers Tribunal* were examined in private. After deliberation this tribunal simply notified Kennedy that no determination had been made in his favour in respect of his complaints. This "meant either that there had been no interception or that any interception which took place was lawful" (*Kennedy*, §20).

50 This time, no violation was found.

51 ECtHR, *R.E. v. the United Kingdom*, 27 October 2015, application no. 62498/11 he applicant submitted that the combined effect of Part II of RIPA, the Revised Code and the PSNI Service Procedure did not provide, in relation to covert surveillance of lawyer/client consultations, the "adequate and effective guarantees against abuse" required by Article 8 of the Convention, especially when compared with the clear and precise statutory guidelines outlined in Part I of RIPA in respect of the interception of communications. The applicant, who was subjected to surveillance in a police station when meeting his lawyer, explicitly (and successfully) asked the ECtHR to apply the Huvig-criteria to these methods. The UK government, realizing that RIPA was less strict on surveillance methods other than interception, objected and called such a high level for testing for surveillance not related to intercepting telecommunications 'inappropriate'.

52 'Nature of the offences which might give rise to a surveillance order' – 'definition of the categories of people liable to be surveilled'.

Table 4. Questions to test the scope of application (foreseeability) -criterion (Big Brother Watch, §328 & 330)

a) legal clarity of the grounds upon which a warrant can be issued;
b) legal clarity to give citizens adequate indications of the circumstances in which their communications might be intercepted;
c) legal clarity to give citizens adequate indications of the circumstances in which their communications might be selected for examination

One would however be misguided by taking these questions too strict because that is not what the Court does. Making use of some statements in ***Liberty*** and by pushing the boundaries of accepted foreseeability with regard to surveillance further (compared to ***Liberty***), the Court accepts that that selectors and search criteria for analyzing bulk collected data need ***neither*** to be made public; ***nor*** to be listed in the warrant ordering interception, but is satisfied when these selectors and search criteria are subject to independent oversight (***Big Brother Watch***, §330). How oversight trumps foreseeability.

We started our contribution to this book with a quote from the 2015 judgment ***R.E.*** on direct surveillance in police stations. The applicant (R.E.) asked the Court ***that the principles derived from the Court's "interception" case-law could be "read across" to the present case*** (***R.E.*, §104**) and that is precisely what the Court does by applying ***Huvig*** to all intrusive surveillance practices.

In a 2018 judgement this creative reading process is taken to new levels. The ECtHR first recalls its case-law on secret measures of surveillance in criminal investigations and the six minimum safeguards (***Centrum För Rättvisa***, §103). It then underlines why ***all*** surveillance should be subjected to this test.[53] Third, and relevant here, it reads across even further applying the principles taken from case-law on secret measures of surveillance in criminal investigations to cases on dealing exclusively with national security, 'adapting these minimum safeguards where necessary' to reflect the specificity of this context (***Centrum För Rättvisa***, §114).

6. A difficulty with the framework remains: when applying Huvig-light for less intrusive surveillance?

The ***Huvig/Weber*** foreseeable surveillance-doctrine by now has taken solid shape and both applicant and governments have understood it: regardless of the surveillance practice (mass, individual or other) and of context (criminal law or not) the battle is on the applicability of all six requirements or not. That means that the battle is on understanding ***Uzun***, since lower intrusive technologies allow to drop some of

53 "all interception regimes (both bulk and targeted) have the potential to be abused, especially where the true breadth of the authorities' discretion to intercept cannot be discerned from the relevant legislation" and in this regard "the Court has identified six minimum safeguards that both bulk interception and other interception regimes must incorporate in order to be sufficiently foreseeable to minimise the risk of abuses of power (*Centrum För Rättvisa*, §113)

the requirements or 'only' use them as sources of inspiration.[54] In ***R.E.***, five years after ***Uzun***, the ECtHR was asked to speak out more systematically on surveillance and to clarify its leniency with regard to less intrusive surveillance practices. It does so, in our view, in a satisfactory way.

What counts, the Court clarifies, is not the technology or investigative power used, but the impact on privacy: deep impact practices need to be treated alike; lower impact practices can be treated differently.[55] The Court develops this impact-related rule of thumb based on a comparison between ***Valenzuela-Contreras*** (a telephone interception case),[56] ***Bykov*** (recording of a private conversation by way of a radio transmitting device)[57] and ***Uzun*** (GPS-surveillance of movements in public places). With regard to the last lower-impact case, the Court states that the ***Huvig***-principles merely serve as in inspiration without being 'directly applicable' (***R.E.***, §129). ***Bykov***, however, is about more intrusive practices 'virtually identical to telephone tapping' and therefore the relevant legislation should be assessed the relevant legislation using the ***Huvig***-principles' (***R.E.***, §128).

Hence, the principles developed in the context of interception cases can be read out to other forms of surveillance (such as covert-surveillance) depending on the form of surveillance in question: the decisive factor is the impact or level of interference with an individual's privacy and not the technical definition of that interference.[58]

- In ***Big Brother Watch*** (2018), the ECtHR accepts as a starting point to use the ***Huvig/Weber***-criteria to check on UK data sharing practices with foreign intelligence agencies, but closer reading of the judgment reveals that this particular surveillance practice is only very loosely tested: The Court runs through the three general Article 8,§2-requirements legality, legitimacy and necessity without properly

54 In *Malone* the Court found that the use of geolocation data *could* give rise to an issue under Article 8 ECHR, but "by its nature" had to be distinguished from the interception of communications, which was undesirable and illegitimate in a democratic society unless justified (*Malone*, §84). A similar conclusion was reached in *Uzun,* where the Court found that the interception of communications represented a greater intrusion into an individual's private life than the tracking of his vehicle via GPS (*Uzun,* §52). Comp. *Big Brother Watch,* § 402: The UK government, as a first line of defence, objected against applying the *Huvig/Weber* criteria to the practices with regard to data sharing with foreign secret services : "They did not accept that the six criteria set down in Weber and Saravia (see paragraph 307 above) applied to an intelligence sharing regime in the same did not necessarily apply in other surveillance cases (for example, Uzun, cited above). While some of the material obtained from foreign governments might be the product of intercept, that would not necessarily be the case and the intelligence services might not even know whether communications provided to them by a foreign Government were the product of intercept". As a second line of defence they argued that 'even if the six minimum requirements did apply, (…) they were satisfied' (*Big Brother Watch,* §403).

55 Comp. ***R.E.***, §130. "The Court has not, therefore, excluded the application of the principles developed in the context of interception cases in covert- surveillance cases; rather, it has suggested that the decisive factor will be the level of interference with an individual's right to respect for his or her private life and not the technical definition of that interference". In a next section on ***Segerstedt-Wiberg***, we will see that ***impact*** criterion will not only determine the foreseeability test, but also the more general Article 8-margin given to member states.

56 ECtHR, ***Valenzuela Contreras v. Spain***, 30 July 1998, application no. 58/1997/842/1048

57 ECtHR, *Bykov v. Russia* [GC], 10 March 2009, application no. 4378/02

58 How does this apply to the surveillance methods discussed in *R.E.* (surveillance of legal consultations taking place in a police station)? For the Court, these practices are analogous to interceptions of telephone calls between a lawyer and client and to be considered as an extreme intrusion. Hence, extension of the *Huvig*-scope and application of the six principles '*insofar as those principles can be applied to the form of surveillance in question*'. "The Court has recognised that, while Article 8 protects the confidentiality of all correspondence between individuals, it will afford "strengthened protection" to exchanges between lawyers and their clients, as lawyers would be unable to defend their clients if they were unable to guarantee that their exchanges would remain confidential (*Michaud v. France*, no. 12323/11, § 118). The Court therefore considers that the surveillance of a legal consultation constitutes an extremely high degree of intrusion into a person's right to respect for his or her private life and correspondence; higher than the degree of intrusion in *Uzun* and even in *Bykov.* Consequently, in such cases it will expect the same safeguards to be in place to protect individuals from arbitrary interference with their Article 8 rights as it has required in cases concerning the interception of communications, at least *insofar as those principles can be applied to the form of surveillance in question*" (*R.E.*, §128, italics added).

checking the ***Huvig*** criteria (!), and gives green light based on the existence of a legal framework 'providing considerable safeguards against abuse' and a general willingness to accept sharing in the fight against global terrorism.[59] No Article 8-testing ***at all*** was needed for other shared data that could not be traced back to interception practices![60]

- In ***Ben Faiza v. France*** (2018)[61] the Court apparently contradicts itself, since it applies the full ***Huvig***-package to geolocation surveillance, where both ***Malone*** and ***Huvig*** pointed to a lighter treatment of this surveillance method.[62] The judgment therefore also seems apparently in contradiction with ***Uzun***,[63] but adds a relevant variable to the appraisal of existing surveillance methods: the timing of GPS Surveillance. Real-time GPS surveillance, in particular considering the huge development of technologies in the last years, is much more intrusive than ex post-GPS surveillance.
- ***Ministerio Fiscal*** (2018), a Luxembourg Court (CJEU)'s preliminary ruling, adds another relevant variable to the appraisal of existing surveillance methods.[64] The CJEU clarified that in view of the broad

59 ECtHR, ***Big Brother Watch and others v. the United Kingdom***, 13 September 2018 applications nos. 58170/13, 62322/14 and 24960/15, §§445-446. In this judgement data sharing of the United Kingdom intelligence services with US based services was accepted in principle and found to respect the Convention after superficial testing of the Article 8§2 requirements, on the basis of a broad statement about global terrorism: "Faced with such a threat, the Court has considered it legitimate for Contracting States to take a firm stand against those who contribute to terrorist acts (...). Due to the nature of global terrorism, and in particular the complexity of global terror networks, the Court accepts that taking such a stand – and thus preventing the perpetration of violent acts endangering the lives of innocent people – requires a flow of information between the security services of many countries in all parts of the world. As, in the present case, this "information flow" was embedded into a legislative context providing considerable safeguards against abuse, the Court would accept that the resulting interference was kept to that which was "necessary in a democratic society" (§446)

60 ECtHR, *Big Brother Watch and others v. the United Kingdom*, §449: "The third category of material identified at paragraph 417 above is material obtained by foreign intelligence agencies other than by the interception of communications. However, as the applicants have not specified the kind of material foreign intelligence agencies might obtain by methods other than interception they have not demonstrated that its acquisition would interfere with their Article 8 rights. As such, the Court considers that there is no basis upon which it could find a violation of Article 8 of the Convention".

61 ECtHR, *Ben Faiza v. France*, 28 February 2018, application no. 31446/1. See Katrien Keyaerts, 'Ben Faiza v France: Use of Cell Site Location Information by Police Is Acceptable Interference with Right to Privacy', *European Data Protection Law Review*, 2019, vol. 5/1, 120-126

62 The Court was asked to look at an order issued to a mobile telephone operator to provide lists of incoming and outgoing calls on four mobile telephones, together with the list of cell towers "pinged" by those telephones. Pursuant to domestic French law, prosecutors or investigators could, on the authorization of the former, require from establishments, organisations, persons, institutions and administrations to provide them with documents in their possession, which were required for the purposes of the investigation. According to the ECtHR, France violated Article 8 ECHR by following the suspects via 'real time' GPS tracking of a car, as this infringement of the suspects' privacy rights did not rest on a specific and foreseeable enough legal basis to pass the legality test of Article 8 §2 ECHR, and lacked sufficient guarantees against abuse. In the judgement, the Court distinguishes between the tracking of a vehicle that allows to geolocate a person in real time, and the lower level of intrusion occasioned by the transmission to a judicial authority of existing data held by a public or private body (*Ben Faiza*, §74). Real-time tracking is much more privacy intrusive than an ex-post control of the suspect's location (*Ben Faiza*, §76). Accordingly, real-time surveillance requires stricter safeguards than a posteriori or ex post surveillance.

63 In *Uzun* the ECtHR expressly affirmed that GPS surveillance is "by its very nature to be distinguished from other methods of visual or acoustical surveillance wish are, as a rule, more susceptible of interfering with a person's right to respect for private life" (*Uzun*, §52).

64 CJEU, (Grand Chamber) (request for a preliminary ruling from the Audiencia Provincial de Tarragona — Spain) — Proceedings brought by Ministerio Fiscal, 2 October 2018, Case C-207/16 (hereafter: *Ministerio Fiscal*). This case on access to retained data for the purpose of identifying the owners of SIM cards activated with a stolen mobile telephone, was not explicitly on the question of applying or not the *Huvig*-package, but about the related question whether ordinary crimes (as opposed to serious crime) could justify such a measure. The CJEU used the ruling to clarify its case law on bulk and mass surveillance such as *Digital Rights Irelands* and *Tele2/Watson* where it had insisted on the seriousnes of the crimes as a requirement for justifying these measures.

terms used in the relevant European law (the ePrivacy Directive),[65] and in view if the 'modest' purpose for accessing the retained data (solely to obtain the subscriber identity), there was no fundamental rights problem with the domestic laws that made this practice possible for fighting ***all*** crimes, including minor crimes.[66] The seriousness of a crime is a variable that should be combined with the seriousness of the privacy interference: a serious interference to privacy (combination of several meta-data and personal data, revealing e.g. the date, time, duration and recipients of the communications, or the locations) is justified only by serious crimes detection. On the other hand, non-serious crimes investigations can only justify non-serious privacy interferences (e.g. a mere identification of the SIM user).[67]

7. Segerstedt-Wiberg (2006) narrowing the margin of discretion for introducing surveillance?

In the following case-law, the Court addressed more deeply mass and bulk surveillance practices, including the practice of data retention (massive storing of all kinds of data without an immediate link with crime or public threats). ***Segerstedt-Wiberg*** (2006), released in parallel with ***Weber and Saravia***, does not address data retention as such, but deals with the related problem of long time storing of (traditional) police data.[68] Other famous cases with regard to this issue of long time storage are of course of ***Rotaru*** (2000)

65 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). ELI: http://data.europa.eu/eli/dir/2002/58/2009-12-19 . Article 15(1) of the ePrivacy Directive allows restrictions of the rights provided for by the Directive for the prevention, investigation, detection, and prosecution of *criminal offences – not just serious criminal offences.* Article 15(1): "Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union".

66 Interestingly, in the aforementioned *Tele2* case, the CJEU had ruled that access to the retained data is limited to cases involving *serious* crime. To reconcile the two rulings, the Court argues that this is because the objective pursued by the access must be "proportionate to the seriousness of the interference with the fundamental rights that the access entails" (CJEU, *Ministerio Fiscal* (2018), §55). The Tele2 case is concerned with access to retained data which, taken as a whole, allows precise conclusions to be drawn regarding the private lives of the persons concerned. Such access constitutes a serious interference with fundamental rights and can be justified only by the objective of fighting serious crime. If, however, the access to retained data is a non-serious interference (e.g. it just involves access to the subscriber's identity, as in *Ministerio Fiscal* case), *access can be justified by the objective of fighting criminal offences generally.* Disappointingly, the CJEU does not define what can constitute a "serious crime". Similarly, the *Ministerio Fiscal* ruling does not clearly refer to why the data was retained in the first place or whether that should affect the conditions for access to the retained data. Because there is no apparent connection to why the data is retained, the CJEU now seems to say in paragraphs 54-61 of the *Ministerio Fiscal* ruling that if access is only sought to minor parts of the retained data, for example only for the purpose of obtaining the subscriber identity, accessing that data does not constitute a *serious* interference, even if the data is only available in the first place because of a (targeted) data retention order that can only be justified by the objective of fighting serious crime.

67 Disappointingly, the CJEU does not define what can constitute a "serious crime". Similarly, the ***Ministerio Fiscal*** ruling does not clearly refer to why the data was retained in the first place or whether that should affect the conditions for access to the retained data. Because there is no apparent connection to why the data is retained, the CJEU now seems to say in paragraphs 54-61 of the ***Ministerio Fiscal*** ruling that if access is only sought to minor parts of the retained data, for example only for the purpose of obtaining the subscriber identity, accessing that data does not constitute a ***serious*** interference, even if the data is only available in the first place because of a (targeted) data retention order that can only be justified by the objective of fighting serious crime.

68 ECtHR, *Segerstedt-Wiberg and others v. Sweden,* 6 June 2006, application no. 62332/00. The judgement deals with the police long-term storage of personal data (both private and publicly available data) concerning five appellants in Sweden: two anti-Nazi activists, two members of the KPML Party (Marxist-Leninist revolutionaries Party) and a former member of the GUE/NGL Party at the European Parliament. The monitoring at issue does not involve mass surveillance, but only individual surveillance. In addition, the storage of these data, though led by police, was not carried out within criminal procedure surveillance, but for strategic surveillance for the prevention of public security threats. The five applicants had asked to access to the whole amount of data concerning them, but only a part of that data was disclosed to them. Accordingly, they appealed the ECtHR for an infringement of their rights under Article 8 ECHR. On the privacy of public available data, see, Lilian Edwards & Lachlan Urquhart, 'Privacy in public spaces: what expectations of privacy do we have in social media intelligence?', *International Journal of Law and Information Technology*, 2016, vol. 24, 279–310

on holding and use of data regarding the applicant by the Romanian intelligence service,[69] and ***Marper*** (2008) on long term DNA storage.[70] It is however ***Segerstedt-Wiberg*** that deserves to be highlighted here. The judgement lays some of the groundwork for further judgements data retention, but more importantly, corrects the idea of a wide margin for Member States regarding surveillance and puts to the foreground the idea of strict necessity testing of mass surveillance:[71]

"While the Court recognises that intelligence services may legitimately exist in a democratic society, it reiterates that powers of secret surveillance of citizens are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions (see ***Klass***, §42 and ***Rotaru***, §47). Such interference must be supported by relevant and sufficient reasons and must be proportionate to the legitimate aim or aims pursued. In this connection the Court considers 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 and combating terrorism must be balanced against the seriousness of the interference with the respective applicants' right to respect for private life" (***Segerstedt-Wiberg***, §88).

Important in the fine tuning of the margin of discretion left to Member States. The Court moves beyond its general and state-friendly reflections about the necessity of surveillance in democracies in ***Klass***[72] echoed some decades later in ***Weber and Saravia***[73] (*'**member states can fight with all available means including surveillance dangers such as terrorism and other evils**'*). ***Segerstedt-Wiberg*** tempers this margin: *'**states have a margin, but the scope will depend on two factors: the precise aim pursued (factor 1) and the level of intrusion proposed (factor2)**'*.[74] This sector factor is new,[75] and introduces contextuality: the intrusiveness can impact on the margin given to member states to introduce surveillance.[76]

69 ECtHR, *Rotaru v. Romania*, 4 May 2000, application no. 28341/95.

70 ECtHR, *S. and Marper v. the United Kingdom*, 4 December 2008, applications no. 30562/04 and 30566/04.

71 *Rotaru* already contained the last item (insisting on strict necessity) but does not dwell on the margin. Note that the principle of strict necessity will be eagerly adopted by the CJEU in its *Digital Rights Ireland* data retention judgement

72 In *Klass* -and this contrary to *Weber and Saravia*-, one finds human rights reflections and important paragraphs clarifying that a margin left to the states do not 'unlimited discretion to subject persons within their jurisdiction to secret surveillance' (*Klass*, §49), but these parts of the judgement are snowed under other paragraphs on the benefits of surveillance and the threats of espionage and terrorism making surveillance necessary (*Klass*, §48)

73 In the ***Klass***-tradition, the discussion of the necessity requirement in this judgement opens with a strong ***prise de position*** about the need for mass surveillance to combat serious crime and for giving member states some discretion in this regard. The Court affirmed that "when balancing the interest of the respondent State in protecting its national security through secret surveillance measures against the seriousness of the interference with an applicant's right to respect for his or her private life, it has consistently recognised that the national authorities enjoy a fairly wide margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security" (***Weber and Saravia v. Germany***, §106). In the case at issue, the Court observes that "it was merely in respect of certain serious criminal acts – which reflect threats with which society is confronted nowadays and which were listed in detail in the impugned section 3(1) – that permission for strategic monitoring could be sought" (***Weber and Saravia***, §115).

74 See *Segersted-Wiberg*, §88: "will depend not only on the nature of the legitimate aim pursued but also on the particular nature of the interference involved".

75 We find an explicit affirmation of the importance of considering the impact or the level of intrusiveness of surveillance measures, in order to find a balance with other protected interests. We recall that in *R.E.* impact was used to determine whether *Huvig*-foreseeability principles needed to apply or only serve as an inspiration. Here, impact is used as a factor to determine the margin left to member states.

76 *Segerstedt-Wiberg* imposes a narrow margin for storing data and a broader margin for access-refusals. Towards the end of the judgement a lower scrutiny-level is advanced with regard to the right of the police to give or refuse access to the applicants to their data held by the police. Here member states have a wider margin (*Segersted-Wiberg*, §104). Not giving citizen access to their stored data can be necessary for law enforcement authorities 'where the State may legitimately fear that the provision of such information may jeopardise the efficacy of a secret surveillance system designed to protect national security and to combat terrorism' (*Segersted-Wiberg*, §102). This approach does not equal *not* testing the requirements of Article 8§2, but the proposed testing of access refusals is rather loose, and no violation was found. Since the possibility to refuse access was foreseen in Swedish law, that was moreover constructed with various guarantees, and since there was no evidence that contradict the views of the national administrative and judicial authorities involved that all held that full access would jeopardise the purpose of the system, the Court found no violation of the requirements of legality, legitimate purpose and necessity (*Segersted-Wiberg*, §§99-104).

Usually broader margins go hand in hand with more loose testing of the three Article 8§2-requirements.[77] A more recent approach of the Court seems to be to theorize less on the margin by just accepting that in the name of terrorism (factor 1) just about everything in surveillance matters is allowed, -including bulk surveillance[78] and data sharing with the US-, but that there is almost no margin left to states in operating the surveillance practice, which in practice means that there be will be a sometimes meticulous sometimes more superficial testing of the 6 ***Huvig/Weber*** requirements.

The foregoing shows that there is no mathematical certainty about the consequences of a certain margin left (or not) to Member States. However, statements about the margin usually produce certain specific results in terms of reasoning of the Court. The margin is not a neutral rhetorical device, but bears consequences.[79] It is therefore possible to identify some effects of the doctrine ***when*** it is applied by the Court in explicit terms with regard to surveillance (Table 4).

77 See the foregoing footnote.

78 ECtHR, ***Centrum För Rättvisa v. Sweden,*** 19 June 2018, application no. 35252/08. See Plixavra Vogiatzoglou, 'Centrum för Rättvisa v Sweden: Bulk Interception of Communications by Intelligence Services in Sweden Does Not Violate the Right to Privacy', ***European Data Protection Law Review***, 2018, vol. 4/4, 563-567. ***Centrum För Rättvisa v. Sweden*** (2018) on bulk data collection recognizes a broad margin. National authorities, in view of the Court, enjoy a wide margin of appreciation in choosing how best to achieve the legitimate aim of protecting national security (***Centrum För Rättvisa***, §112), in particular "in view of the current threats facing many Contracting States (including the scourge of global terrorism and other serious crime), advancements in technology which have made it easier for terrorists and criminals to evade detection on the internet, and the unpredictability of the routes via which electronic communications are transmitted" (***Centrum För Rättvisa***, §113). Accordingly, the Court considers that the decision to operate a bulk interception regime in order to identify hitherto unknown threats to national security falls within States' margin of appreciation (***Centrum För Rättvisa***, §112). However, while States enjoy a wide margin of appreciation in deciding ***what type*** of interception regime is necessary to protect national security, ***the discretion afforded to them in operating an interception regime must necessarily be narrower***. In this regard, the Court applies the six-requirements test developed in ***Huvig*** to the ***in abstracto*** examination of bulk data collection regulation in Sweden (***Centrum För Rättvisa***, §113).

79 *Below*, when discussing notification, we will see that a broad margin given by the ECtHR to states with regard to a practice such as bulk data, forces the ECtHR in a defensive position when it comes to testing the six *Huvig/Weber* requirements or adopting additional safeguards not included in this minimum package such as requiring objective evidence of reasonable suspicion in relation to the persons for whom data is being sought and the subsequent notification of the surveillance subject (*Big Brother Watch*, §317)".

Table 5. Possible effects of the margin-doctrine when testing surveillance

Step 1 (affirming the right and the narrow interpretation of limitations).	As a rule, ***all*** limitations of the Article 8§1-rights that are proposed under Article 8§2 should be seen as exceptions to rights and thus should remain the exception. This rule explains the narrow of strict interpretation of requirements of legality, of legitimate aim and of necessity.[80]
Step 2 (broadening the limitation due to aim pursued (factor 1) and applying loose or in abstracto testing)	Surveillance to combat terrorism and other threats to democracy is one of these aims allowing for a broader, be it not unlimited discretion (the first factor mentioned ***above***).[81] Looser testing of the three Article 8§2-requirements will follow. Laws on surveillance powers need to be accessible and foreseeable and be equipped with adequate and effective guarantees against abuse that are inspired by the ***Huvig***-criteria.[82] Aims and necessity of the envisaged surveillance practices can be demonstrated in general terms that are accepted unless there is evidence that contradict the views of national states and their national administrative and judicial authorities involved (***Segerstedt-Wiberg,*** §99-100 and 102)
Step 3 (narrowing the broadness due to intrusiveness (factor 2) and applying stricter testing)	When the Court announces that the level of intrusiveness or discretion (factor 2) is high or relevant, it will temper or balance its broad acceptance of surveillance (factor 1) (***Segerstedt-Wiberg,*** §88).[83] Concretely, the parties involved are then reminded about step 1 and narrow or strict testing of the three Article 8§2-requirements will follow (***Segerstedt-Wiberg,*** §88): -the legal basis needs to be detailed, meaning that accessible, foreseeable and complying 'with the strict conditions and procedures laid down in the legislation itself' (***Klass***, §43) -individual as opposed to general testing of the advanced legitimate aim to surveille a person (prevention of crime, interests of national security, …) (***Segerstedt-Wiberg,*** §§82 and 87). -strict testing of necessity: surveillance laws need to be strictly necessary for safeguarding democracies (***Klass***, §42).

80 ***Klass***, §42: "The cardinal issue arising under Article 8 (art. 8) in the present case is whether the interference so found is justified by the terms of paragraph 2 of the Article (art. 8-2). This paragraph, since it provides for an exception to a right guaranteed by the Convention, is to be narrowly interpreted. Powers 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". See also ***Rotaru***, §47

81 ***Klass***, §49: "Nevertheless, the Court stresses that this does not mean that the Contracting States enjoy an unlimited discretion to subject persons within their jurisdiction to secret surveillance. The Court, being aware of the danger such a law poses of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate".

82 Klass, §50: "The Court must be satisfied that, whatever system of surveillance is adopted, there exist adequate and effective guarantees against abuse. This assessment has only a relative character: it depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering such measures, the authorities competent to permit, carry out and supervise such measures, and the kind of remedy provided by the national law".

83 Tempering means, in the case of surveillance by public authorities, balancing the state interest in carrying out surveillance to protect its national security and combating terrorism against the seriousness of the interference with the respective applicants' Article 8§1-rights (*Segerstedt-Wiberg,* §88). See also *Mosley* on private surveillance of a public figure by the press (further discussed *below*). Note that in principle the Court recognizes that in such field, Member states have a margin of appreciation (*Mosley*, 108). Nevertheless, "in cases concerning Article 8, where a particularly important facet of an individual's existence or identity is at stake, the margin allowed to the State is correspondingly narrowed" (*Mosley*, §109). Obviously, freedom

8. Segerstedt-Wiberg (2006) adding strict scrutiny to Klass

There is another reason to re-read ***Segerstedt***'s paragraph 88 (quoted in the previous section). The paragraph clarifies not only the ECtHR's view on state margins while implementing surveillance, but also what is meant by ***strict testing*** of the necessity requirement of surveillances practices.[84] In the view of the Court, a justification for police data storage by a Member State can never be of a too general level. Paragraph 88 insists on very concrete balancing beyond the legality principle: the balancing needs to be done in the light of the seriousness for the privacy rights of the ***respective*** applicants.

This review of all individual complaints is precisely what follows in the judgement. There are four applicants in ***Segerstedt-Wiberg*** and the Court plunges in a detailed case by case analysis to test the necessity in every single case, continuously insisting on a very concrete perspective avoiding general statements,[85] and concluding that the storage was only acceptable in one out of the four cases (***Segersted-Wiberg***, §92). In the case of the three other applicants the Court saw problems with ***sufficiency*** (some relevance for data collection was not denied) and in one other case the Court found neither relevance nor sufficiency for data storage in the light of the protection of national security (***Segersted-Wiberg***, §§89-92). Lacking either sufficiency or relevance or both, in the view of the Court, amounts to a disproportionate interference with the Article 8§1-right. Hence, strict necessity testing is testing the presence of relevant and sufficient reasons in the light of the advanced aim. Disproportionality is concluded when the reasons are not both present and disproportionality equals failing the (strict) necessity test.

Strict necessity testing, in our understanding of the Strasbourg case law, is a subset of strict article 8 ECHR-testing or strict scrutiny. The rule of thumb is that more intrusive surveillance measures require stricter scrutiny, while less intrusive means require a milder scrutiny.[86] Strict testing implies individualized or ***in concreto*** testing of ***all*** Article 8§2-requirements: the legal basis needs to be complete and simple evidence that the basis does not offer protection against abuse is not enough; the aim and necessity need to be justified not only in a general way but also ***in concreto***, in cases advanced by the applicant. Evidence that a surveillance law in general respects or not the Article 8§2-requirements is always taken into account, even in cases of strict scrutiny, but in the latter case this evidence is of an additional nature,[87] complementing a series of test that are kept as concrete and individualized as possible.

---

of expression is a relevant counter-interest, but it "must not overstep the bounds set for, among other things, 'the protection of ... the rights of others', including the requirements of *acting in good faith* and on *an accurate factual basis* and of *providing "reliable and precise" information* in accordance with the ethics of journalism" (*Mosley*, §113).

84 *'Such interference must be supported by relevant and sufficient reasons and must be proportionate to the legitimate aim or aims pursued'* (*Segerstedt-Wiberg,* §88).

85 Comp. "the constitution and programme of a political party cannot be taken into account as the sole criterion for determining its objectives and intentions; the contents of the programme must be compared with the actions of the party's leaders and the positions they defend" (***Segersted-Wiberg***, §91) and "Continued storage must be "supported by reasons which are relevant and sufficient as regards the protection of national security", considering in particular "the nature and age of the information"(***Segersted-Wiberg,*** §90).

86 This principle could be already found in practice in *Malone* and *Huvig* and will be then reaffirmed in *Uzun* (2010) where the consequences are spelled out with regard to the legality requirements (see *above*).

87 Comp. ***Klass,*** §59: "The Court has examined above (at paragraphs 51 to 58) the contested legislation in the light, inter alia, of these considerations. The Court notes in particular that the G 10 contains various provisions designed to reduce the effect of surveillance measures to an unavoidable minimum and to ensure that the surveillance is carried out in strict accordance with the law. In the absence of any evidence or indication that the actual practice followed is otherwise, the Court must assume that in the democratic society of the Federal Republic of Germany, the relevant authorities are properly applying the legislation in issue".

The CJEU recently copied and developed the idea of strict scrutiny in ***Digital Rights Ireland*** (2014)[88] and gave it a final place the discussion of surveillance.[89] More applications followed in ***Schrems v. Data Protection Commissioner*** (2015), ***Tele2*** (2016) and the judgment on the EU-Canada PNR Agreement (2017).

In ***Schrems,***[90] ***strict necessity*** becomes a fundamental requirement for surveillance powers and laws even in the assessment of foreign legislations or international agreements. Addressing the validity of the Commission's Decision on the Safe Harbour Agreement for the international transfer of data from EU to US[91] and so the adequacy of the respect of personal data protection rights in the United States, the CJEU affirms that "above all, protection of the fundamental right to respect for private life at EU level requires derogations and limitations in relation to the protection of personal data to apply only in so far as is strictly necessary (judgment in ***Digital Rights Ireland and Others***, § 52 and the case-law cited)".[92]

The ECtHR took note of these CJEU developments and adapted its policy on strict scrutiny and strict necessity. In particular, ***Szabò and Vissy v. Hungary*** (2016)[93] contextualizes better the idea of strict scrutiny in the surveillance case law. The judgement is about surveillance carried out by police in Hungary for national security purposes. Surveillance is only compliant if it is strictly necessary in a double sense: 1. as a general consideration, ***for the safeguarding the democratic institutions***; 2. as a particular consideration, for ***the obtaining of vital intelligence in an individual operation***" (***Szabò and Vissy***, § 73).

9. Notification: from valuable to essential (part of the Huvig/Weber package?)

There is no reason not to include in surveillance laws a right of citizen to be notified of secret surveillance, once this is done (provided that notification would not hamper legitimate state interest). We see no other way of combining surveillance with rule of law-based democracy. Simple as it might look, Strasbourg (and most domestic systems) are not there yet.[94]

88 CJEU, Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications*, 8 April 2014.
89 We recall that CJEU, *Satamedia* (2008), CJEU, *Volker* (2010) and CJEU, *Ipi v. Englebert* (2013) are unrelated to surveillance issues.
90 CJEU, Case C-362/14, *Maximillian Schrems v. Data Protection Commissioner*, 6 October 2015.
91 Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441) (Text with EEA relevance.)
92 Interestingly, in paragraph 92 of Schrems the Court gives a negative definition of strict necessity: "Legislation is not limited to what is strictly necessary where it authorises, on a generalised basis, storage of all the personal data of all the persons whose data has been transferred from the European Union to the United States without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down by which to determine the limits of the access of the public authorities to the data, and of its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference which both access to that data and its use entail" (italics added).
93 ECtHR, *Szabò and Vissy v. Hungary,* 12 January 2016, application no. 37138/14
94 See P. De Hert & F. Boehm, 'The Rights of Notification after Surveillance is over: Ready for Recognition?', in J. Bus, M. Crompton, M. Hildebrandt, & G. Metakides (eds.), *Digital Enlightenment Yearbook 2012*, Amsterdam, IOS Press, 2012, (19-39) 26.

In *Malone* and *Huvig* notification was not addressed, although it was not absent in the latter.[95] In *Klass* it was addressed, but at the end not seen as an indispensable criterion to comply with Article 8 ECHR, but as only one of the tools to guarantee effective remedies and independent control.[96] *Segersted-Wiberg*'s message regarding the broader discretion for states to limit data protection rights (such as of access to data and regarding scrutiny of access refusals) help understand the Court's hesitating approach to notification. The general approach of the Courts is pragmatic and the testing of refusals to give access or to notify is not too strict. Access to data and notification are seen by the Court as logical extensions of the right to privacy and should be always made possible in the legal framework. However, for legitimate purposes and when necessary (but not when strictly necessary) exceptions can be built-in and can be invoked without being tested too strictly.[97]

The feeling is that for Strasbourg notification is still far from a game-breaker or a ***must have***, but its importance and place amongst the guarantees that states must foresee in surveillance laws is growing,[98] and that we are witnessing the emergence of a new recognized right for individuals to be informed about infringements of their private life in the context of surveillance measures by the state (as in other contexts

95 Both cases started and ended with a finding of a violation of the legality requirement. Like *Malone*, there is in *Huvig* no further analysis of the French surveillance system: since the legality requirement was found to be violated, there was no need, in the Court's view, to continue the analysis and to verify compatibility of French law with other requirements contained in Article 8 ECHR, such as necessity, or contained in other provisions of the same Convention ((*Huvig*, §36). Unfortunately, since French law equally did not foresee a system of notification *a posteriori* and since *Huvig* apparently made some remarks about this. Perhaps the Court did not follow this up and did not include notification in its list of legality surveillance requirements, because the French government suggested that notification 'in reality' was connected with the requirement of necessity!(*Huvig*, §30) In our view, this understanding by the French government, is questionable. Notification is intimately related with the third and fourth legality dimension of the legality requirement: foreseeability and the rule of law. It might not be necessary or feasible to notify every subject of surveillance afterwards for reasons such as the interest of the state, but as a rule domestic law should position notification as a legal starting point. In what other way could the idea of rule of law (questioning through law state actions; law as the ultimate arbiter of state actions) be realized?

96 *Klass* contains a misunderstood passage about the need to inform citizens after the surveillance about the fact of the surveillance (notification). The applicants presented notification as fundamental in order to have recourse to the courts to be able to challenge the legality of the surveillance measures retrospectively (*Klass*, §57). The contested German law foresaw such a notification but only conditional. The full attention of the Court is on the possible not to notify the individual in certain circumstances, but the main fact remains that the German provision that contained the notification duty was sees as a positive element. *Klass* does not impede long-term surveillance measures without transparency given that, as long as in those cases the notification might jeopardize the purpose that triggered the surveillance, the notification must not be carried out. Furthermore, even if surveillance has finished, public authorities are not forced to immediately inform the person concerned: the notification could be carried out only after the risk of jeopardizing the investigation (even retrospectively) has been completely excluded. The Court is aware that "subsequent notification to each individual affected by a suspended measure might well jeopardize the long-term purpose that originally prompted the surveillance" (*Klass*, §58). Therefore, in the Court's view, "*the fact of not informing the individual once surveillance has ceased cannot itself be incompatible*" with Article 8 para. 2 ECHR, "since it is this very fact which ensures the efficacy of the 'interference'" (*Klass*, §58). Nevertheless, the person concerned must be informed after the termination of the surveillance measures "as soon as notification can be made without jeopardizing the purpose of the restriction" (*Klass*, §58)

97 We observe in passing that legitimate purposes to refuse notification can be of a private nature: In *Mosley* (2011) and *Barbulescu* (2017), both dealing with private surveillance, absence of notification was contested before the Court, but twice the Court found no violation. See ECtHR, *Mosley v. the United Kingdom*, 10 May 2011, application n. 48009/08; ECtHR, *Bărbulescu v. Romania*, 5 September 2017, application no. 61496/08. See also P. De Hert & Fr. Boehm, 'The Rights of Notification after Surveillance is over Ready for Recognition?', 35. The ECtHR, -after balancing privacy with press freedom in *Mosley* and privacy with economic interests of employers in *Barbulescu*-, did not find a violation and rejected both claims in the light of press interests (*Mosley*) or employer interests (*Barbulescu*). See Paul De Hert & Franziska Boehm, 'The Rights of Notification after Surveillance is over Ready for Recognition?', 35.

98 Even *Mosley* and *Barbulescu* can be seen as illustrations of this greater emphasis on the notification of surveillance measures. In *Barbulescu* one finds a statement on the importance of notification principle. In particular, ECtHR affirmed that the member state failed at verifying whether the applicant "had been *notified* in advance of the possibility that the employer might introduce monitoring measures, and of the scope and nature of such measures" (*Barbulescu*, §133). The central message from *Mosley* is stronger: the answer to surveillance must be transparency, in particular implemented through notification, but exceptions are possible even with regard to private surveillance when these serve the 'public interest'. Comp. *Mosley*, §126: "it is generally accepted that any pre-notification obligation would require some form of "public interest" exception (…). Thus a newspaper could opt not to notify a subject if it believed that it could subsequently defend its decision on the basis of the public interest. The Court considers that in order to prevent a serious chilling effect on freedom of expression, a *reasonable belief* that there was a "public interest" at stake would have to be sufficient to justify non-notification, even if it were subsequently held that no such "public interest" arose". (italics added).

such as media communication[99]). The ECtHR - echoing notification and information requirements in European data protection law[100] - seems to proceed on the assumption that individuals should be in general informed about the information held on them, if not they are not able to exercise their rights laid down in the Convention. This information may nonetheless be subject to restrictions.

The right to notification seems in particular necessary in situations where the access to courts is not open to any person suspecting to be victim of surveillance (see, ***Kennedy v. UK, §167).***[101]

In the context of surveillance by public authorities one can point to *Roman Zakharov* (2015)[102], *Szabó and Vissy* (2016),[103] *Centrum För Rättvisa* (2018)[104], and *Big Brother Watch* (2018).[105] All illustrate this trend towards seeing notification as an essential (as opposed to valuable) component in the whole of guarantees that together must ensure that no abuse takes place.[106] *Roman Zakharov* is the most obvious point of reference emphasizing that without notification there cannot be an effective remedy for the citizen. Its discussion of the virtues of notifications is repeated in the other judgments mentioned (see for instance,

99 In *Mosley* the applicant disputed the lack of a legal requirement to pre-notify the subject of an article which discloses material related to his private life. The Court found no violation but conceded that the right to notification was an essential safeguard. Indeed, the Court clarifies that *ex ante* notification would be highly desirable for a full awareness of persons concerned, but what is sufficient is an ex post notification (i.e. as soon as it does not jeopardize the purpose of that data collection), so that it allows individuals to have judicial redress against illegitimate interferences to their privacy. In other terms, ex post notification is not seen any longer as an important though optional tool for the respect of human rights, but it is seen for the first time as an essential safeguard because it allows to have adequate redress against illegitimate surveillance.

100 See Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *OJ L* 119, 4.5.2016, p. 1-88; Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, *OJ L* 119, 4.5.2016, p. 89–131 and Council of Europe (1981) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg 28 Jan 1981, as modernized in the 128th session of the Committee of Ministers (Elsinore, Denmark, 17-18 May 2018. The Regulation or GDPR aims to harmonise data protection legislation across EU member states, enhancing individuals' rights. The texts consist of 99 provisions became direct applicable in EU Member States on 25 May 2018. The GDPR applies to organizations established in the EU as well as organizations operating outside the EU which offer goods or services to, or monitor the behaviour of, individuals in the EU. The provisions on transparency, access and notification, including the exceptions, are contained in Article 12 to 15. Similar provisions, this time explicitly focusing on law enforcement authorities, are contained in the Data Protection Law Enforcement Directive and the modernized 1981 Data Protection Convention of the Council of Europe

101 ECtHR, Kennedy v. UK, application no. ***26839/05,*** 18 August 2010.

102 ECtHR, *Zakharov v. Russia*, 4 December 2015, application no. 47143/06, §287. See P. De Hert & P.C. Bocos, *Case of Roman Zakharov v. Russia. The Strasbourg follow up to the Luxembourg Court's Schrems judgement,* in *Strasbourg Observers,* 23 December 2015, available at: https://strasbourgobservers.com/2015/12/23/case-of-roman-zakharov-v-russia-the-strasbourg-follow-up-to-the-luxembourg-courts-schrems-judgment/

103 ECtHR, *Szabò and Vissy v. Hungary,* 12 January 2016, application no. 37138/14, §86

104 ECtHR, *Centrum För Rättvisa v. Sweden,* 19 June 2018, application no. 35252/08. §105

105 ECtHR, *Big Brother Watch and others v. the United Kingdom*, 13 September 2018 applications nos. 58170/13, 62322/14 and 24960/15.

106 *Zakharov* underlines the essential nature of a posteriori notification to the citizen of interception measures due to its inextricably link to the rule of law idea of effective combating possible surveillance abuses. The development is not just about minimal transparency, but about an active duty of notify by the government: authorities must notify themselves persons affected by surveillance when this is possible. Organizing a passive system of transparency (not notifying unless the citizen actively demands it in a concrete case) will no longer do. In *Szabó and Vissy* the full focus is therefore on an active duty of notification by the government to its citizens (§ 86). Analysis of *Zakharov* and *Szabó and Vissy*, brought the Belgium constitutional court to a rejection of new provisions on a a passive system of notification proposed in 2017 as amendments to the Act of 30 November 1998 on the intelligence and secret services. In the view of the Belgian Court, only an active duty or notification for the respective authorities guarantees an effective system of protection of abuse. Not being notified means not being able to stand up before the courts and seeking remedy. Comp. Court constitutionelle de Belgique, 14 mars 2019, application no. 6758, via http://www.const-court.be/public/f/2019/2019-041f.pdf

Big Brother Watch, §309-310).[107] The CJEU will follow a year later in *Tele2 Sverige* (2016) and hold that with regard to bulk data retention competent national authorities must notify the persons affected by the data access, under the applicable national procedures, as soon as such notification no longer jeopardises the investigations. Such notice is necessary to enable these individuals to exercise their right to a legal remedy pursuant to the Directive and EU data protection law (*Tele2 Sverige*, §121). In *Canadian PNR* we observe a similar emphasis on notification.[108]

10. If notification is so valuable, why is it missing in many criminal and other law provisions?

Notification has many positive effects. As said by the CJEU in *Tele2* it enables individuals to exercise their right to a legal remedy pursuant to the Directive and EU data protection law. It is a significant procedural right is likely to play an important role in acting as a check on abusive access requests.[109] In the 2014 *Digital Rights Ireland* judgement, the CJEU found data retention 'a particularly serious interference' because it is 'wide-ranging' and is not accompanied with a notification duty to notify, which is 'likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance' (*Digital Rights Ireland*, §37). Notification to individuals is a valid option in delicate fields where political discretion is involved and so where judicial control *ex ante* or *ex post* is not incorporated but is replaced with ex ante quasi-judiciary overview (*Kennedy*) or ex post non-judiciary overview (*Segersted-Wiberg*). In this context it is helpful to go back to Article 101 §1 of the German Code of Criminal Procedure (cf. *Uzun* (*above*)) with its long list of notification duties in particular for surveillance measures contained in the Code that do not require judicial approval *ex ante* or *ex post*.[110] Apparently the ECtHR was charmed by it, since the provision contributed to the acceptance by the court of the German GPS-based police surveillance (only) controlled by the prosecutor *without* any magistrate intervening.

107 *Roman Zakharov v. Russia* deals with telephone interceptions led by secret service in Russia. A journalist (Roman Zakharov) claimed that the privacy of his communications had been violated and provided proof that mobile network operators and law-enforcement agencies were technically capable of intercepting all telephone communications without obtaining prior judicial authorization. His case was rejected at several instances of the judicial Russian system under the argument that his proofs didn't cover his particular case. In Strasbourg, the applicant claimed that the Russian mobile network operators had installed equipment, which permitted the *Federal Security Service* to intercept all telephone communications without prior judicial authorisation" (*Zakharov*, §10). The Court found that the authorisation procedures provided by the Russian law were not capable of ensuring that secret surveillance measures are ordered only when "necessary in a democratic society" and that "the effectiveness of the remedies is undermined by the absence of notification at any point of interceptions, or adequate access to documents relating to interceptions" (*Zakharov*, §285). It is therefore the opinion of the Court that citizens must enjoy a right to notification of surveillance measures in order to defend their rights: the issue of notification of interception of communications is considered "inextricably linked to the effectiveness of remedies before the courts" (*Zakharov*, §286). We find in the foregoing a definitive consolidation of the principle according to which "as soon as notification can be carried out without jeopardising the purpose of the restriction after the termination of the surveillance measure, information should, however, be provided to the persons concerned" (*Zakharov*, §287). The Court also takes note of the Recommendation of the Committee of Ministers regulating the use of personal data in the police sector, which provides that where data concerning an individual have been collected and stored without his or her knowledge, and unless the data are deleted, he or she should be informed, where practicable, that information is held about him or her as soon as the object of the police activities is no longer likely to be prejudiced.

108 CJEU (Grand Chamber), Opinion 1/15 of the Court on the envisaged agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data, 26 July 2017, EU:C:2017:592. See C. Kuner, 'International agreements, data protection, and EU fundamental rights on the international stage: Opinion 1/15, *EU-Canada PNR*', ***Coomon Market Law Review***, 2018, vol. 55/3, 857-882

109 Orla Lynskey, 'Tele2 Sverige Ab And Watson Et Al: Continuity and Radical Change', *European Law Blog*, 12 January 2017, via http://europeanlawblog.eu/2017/01/12/tele2-sverige-ab-and-watson-et-al-continuity-and-radical-change/

110 The notification is not only made possible on behalf of the suspected or accused person or other persons under surveillance, but also on behalf of sender and addressees of the postal items, participants in the telecommunication under surveillance; persons who owned or lived in the private premises under surveillance at the time the measure was effected; other persons significantly affected. No less than 12 surveillance measures are considered with every time detailed organization of the notification duty.

Notification in the context of criminal law investigations helps to realize the rule of law idea: through it the surveilled and other affected persons are enabled to go to the court and have the independent scrutiny that should be the standard in a democracy (see also Article 13 ECHR). Notification is not at the periphery of guarantees (as it is currently in many domestic systems) but should be a core element of all surveillance laws because of the right to an effective remedy. Proof for that is given by ***Uzun*** discussed in a previous section: although the Strasbourg Court deems the surveillance via GPS to be a rather small infringement of Article 8 ECHR, it does not abstain from requiring and positively assessing the general ***notification*** requirement laid down in the German Code of Criminal Procedure. The German approach therefore needs to be followed in all European criminal procedure codes: a legal framework on criminal law surveillance is incomplete without notification duties.[111]

But if notification is so important, why is it still at the periphery of guarantees in surveillance discussions? The recognition if still not complete. Many domestic surveillance laws, also of recent origin, do not foresee notification provisions along the lines of the German example. Notification, -and other data protection ideas for that manner-, does not seem to be a top of the list regulatory issue. We could refer to, for instance, Spanish developments,[112] but can also go back to the UK RIPA Act as discussed in ***Kennedy*** (***above***). Missing in the analysis of the Act by the ECtHR is notification. It is actually very difficult to find. Notification is just referred to as a "Rule" of the IP Tribunal (Rule 13, §87).[113] So obviously the British forgot, and the ECtHR did not really pay attention of value its quasi hidden presence. Part of that might have to do with hesitations by the Court about the place of notification as a sub-right guaranteed by Article 8 ECHR, by Article 13 ECHR, or both.[114] The hesitations might also relate to the value of notification ('is it a strong guarantee in practice or will it always be omitted by the responsible authorities that invoke exceptions?) to integrate notification amongst the ***must-haves***, in our case the ***Huvig***-criteria. In our view this would be the right approach and it would definitely render the Article 8§2-testing of the ECtHR more coherent.[115]

Only in ***Big Brother Watch*** (2018) we observe some more clarity about the ECtHR's view on the notification requirement. The judgement was mentioned in a previous section as an example of the success of the ***Huvig/Weber*** foreseeability criteria (in the context of bulk data surveillance). The six criteria were amended and bended to make this surveillance a legitimate option for states. Notification was not included in the

111 See the position of the Nineteenth International Congress of Penal Law, Rio de Janeiro, 31st august – 6th September 2014, *International Review of Penal Law*, vol. 86, 2014, p. 446, See section 3, §14: "persons whose right to privacy has been affected by investigative measures involving ICT should be informed of the measures as soon as this disclosure does not jeopardize the purpose of the measure and/or the results of the criminal investigation.

112 On the lack of attention to notification and data protection by the Spanish regulator updating the Spanish surveillance laws, see Juan José González López & Julio Pérez Gil, 'The New Technology-Related Investigation Measures in Spanish Criminal Proceedings: An Analysis in the Light of the Right to Data Protection', *European Data Protection Law Review*, 2016, vol. 2/2, 242-246

113 So, notification is not officially in the RIPA, but in the official guidelines of the RIPA Entity (The IPT). This is Rule 13: "(1) In addition to any statement under section 68(4) of the Act, the Tribunal shall provide information to the complainant in accordance with this rule.(2) Where they make a determination in favour of the complainant, the Tribunal shall provide him with a summary of that determination including any findings of fact....(4) The duty to provide information under this rule is in all cases subject to the general duty imposed on the Tribunal by rule 6(1).(5) No information may be provided under this rule whose disclosure would be restricted under rule 6(2) unless the person whose consent would be needed for disclosure under that rule has been given the opportunity to make representations to the Tribunal."

114 In *Mosley* the Court addresses article 13 only in conjunction with Article 8 and specifically focuses on the latter since the alleged "absence of an effective domestic remedy is seen as a reformulation of the applicant's complaint under Article 8 of the Convention that the respondent State did not ensure respect for the applicant's private life (*Mosley*, §66).

115 Amusing in ***Weber and Saravia*** is the part on notification. It is not integrated in the analysis of foreseeability or necessity but dealt with separately at the end of the Article 8-analysis as a left over. The Court assessed positively the duty of notification "as soon as informing the concerned persons does not jeopardize the purpose of surveillance" (***Weber and Saravia***, §136). The exceptions to the notification duty laid down in the amended Act are, the ECtHR held, respectful of the necessity requirement, in particular because of two important extra safeguards to prevent authorities to circumvent the notification duty. Thanks to an intervention of the German Constitutional Court, the G10 Commission had now the competence to order notification if needed and equally due to this German Court a smart provision was built in the new Act that created a presumption that in certain cases notification ***had to be done,*** unless: in cases in which data were destroyed within three months there was justification for never notifying the persons concerned only if the data had not been used before their destruction (***Weber and Saravia***, §136).

basic package and (mis)treated separately. The line of reasoning of the ECtHR is very subtle, moving back and forwards. It first quotes a 2015 Report on the ***Democratic Oversight of Signals Intelligence Agencies*** written by the ***Venice Commission*** expert group (European Commission for Democracy through Law) that observes that notification of the subject of surveillance is not an absolute requirement of Article 8 of the Convention and that a general complaints procedure to an independent oversight body could compensate for non-notification (***Big Brother Watch***, §213).The ECtHR then emphasizes that although notification is not part of the minimum package, it did test in ***Zakharov*** its presence in Russian surveillance laws.[116] The Court recalls the many positive features of notification (***Big Brother Watch***, §309-310 with ref. to ***Zakharov***), but then drops a bomb on the beloved requirement: one cannot accept bulk data surveillance ***and*** notification. The six ***Huvig*** requirements can in one form or another be applied to bulk data surveillance, but other possible sound safeguards like notification ***not***,[117] hence it cannot be part of the mandatory minimum package for Article 8 foreseeability compliance. Good to have but, depending on the surveillance, not always possible to have.

116 ***Big Brother Watch***, §307: "In ***Roman Zakharov*** the Court confirmed that the same six minimum requirements also applied in cases where the interception was for reasons of national security; however, in determining whether the impugned legislation was in breach of Article 8, it also had regard to the arrangements for supervising the implementation of secret surveillance measures, any notification mechanisms and the remedies provided for by national law (***Roman Zakharov***, § 238)".

117 "requiring objective evidence of reasonable suspicion in relation to the persons for whom data is being sought and the subsequent notification of the surveillance subject would be inconsistent with the Court's acknowledgment that the operation of a bulk interception regime in principle falls within a State's margin of appreciation. 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 (*Big Brother Watch*, §317)".

11. Influencing the surveillance testing by the CJEU (Digital Ireland, Tele2Sverige, Canadian PNR Agreement)

We discussed the maturing of Strasbourg's approach to surveillance based on reading across from principles formulated in interception cases. The attractiveness of this Strasbourg approach did not go unnoticed. In recent years the European Court of Justice of the EU (CJEU) has come to the forefront in surveillance discussions taking strong positions on the values of personal data protection and privacy.[118] Its decision in ***Digital Rights Ireland*** (2014) has had a wide impact on surveillance debates (and on ECtHR decisions that came after!).[119] The case deals with ***mass*** metadata surveillance by police within the context of criminal law.[120]

The approach in ***Digital Rights Ireland,*** -apart from some methodological differences-,[121] is in line with the Strasbourg jurisprudence. Firstly, there is a general statement, echoing ***Segerstedt-Wiberg***, that state

118 See M. Brkan, 'The Unstoppable Expansion of EU Fundamental Right to Data Protection. Little Shop of Horrors?', *Maastricht Journal of European and Comparative Law,* 2016, vol. 23(5), 812-841, in particular p.825 on *Digital Rights Ireland* as a judgement that 'demonstrates the importance that the CJEU accords to data protection'.

119 We recall that before the European Court of Justice, no "victim requirements" must be proved. Indeed, contrarily to Strasbourg Court, the admissibility of the cases in Luxembourg Court does not depend from an actual involvement of the applicant in the alleged violation. See Digital Rights Ireland, §33: "To establish the existence of an interference with the fundamental right to privacy, it does not matter whether the information on the private lives concerned is sensitive or whether the persons concerned have been inconvenienced in any way". CJEU, ***Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others***, 8 April 2014, C-293/12 (available via https://eur-lex.europa.eu/). See in general, T. Wisman, 'Privacy: Alive or Kicking', ***EDPL***, 2015/1, 80-84; Andrew J. Roberts, 'Privacy, Data Retention and Domination: Digital Rights Ireland Ltd v Minister for Communications (May 2015)', ***The Modern Law Review***, 2015, vol. 78/ 3, 535-548; O. Lynskey, 'The The Data Retention Directive is incompatible with the rights to privacy and data protection and is invalid in its entirety: Digital Rights Ireland', ***Common Market Law Review*** 2014, Issue. 6, 1789-1811; S. Peyrou, 'La Cour de justice, garante du droit 'constitutionnel' à la protection des données à caractère personnel', ***Rev.trim.dr.Eur***. 2015, Isue 1, 117-131. We recall that the ***Liberty*** case also addressed mass surveillance, but surveillance led by secret service (on behalf of the Ministry of Defence). ***Digital Rights Ireland*** deals with ***mass*** surveillance by police within the context of criminal law. More specifically the case addresses the legitimacy of the EU Data Retention Directive which provided that traffic and location data and subscriber data needed to be kept by the service providers on behalf of the law enforcement authorities. See Article 5 of Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, ***OJ***, L 105, 13 April 2006, 54–63. Article 1(1) states that data should be collected "in order to [make them] available ***for the purpose of investigation, detection, prosecution of crimes***", which are typical functions of criminal procedure law. The High Court of Ireland and the Austrian Constitutional Court asked about the validity of the Directive under the light of the European Charter of Fundamental Rights. They argued that by requiring data retention and by allowing the authorities to access the data, the Directive interfered with the rights to respect for private life and to the protection of personal data.

120 We are not confronted with mass surveillance based on a program classifying emails, faxes or telephone calls (as in *Liberty*), or with GPS surveillance (*Uzun*), but with a mass surveillance program that centers around collecting data that we can call metadata. More technically: *online identifiers*. To have a clear definition of this kind of data it would be useful to refer to the new General Data Protection Regulation (hereafter: GDPR). Indeed, recital 30 lists all possible "*online identifiers*": "Internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags". It also adds that since "natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols", this "may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them". In wider terms also article 4(1) of the GDPR defines an identifier "as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person". We recall that the ECtHR had already addressed a more primitive kind of metadata surveillance in *Malone,* where the Court had asserted for the first time that collecting metadata is an interference with the right guaranteed by Article 8 ECHR (*Malone*, §84). The analysis of the Court in that case was mainly based on the legality principle, i.e. secret investigation powers should be clearly determined by primary law as for their manners and as for their purposes. As already mentioned, the main lesson from *Malone* was that a practice of surveillance collaboration between the State (e.g. the police) and private telecommunication operators, *outside any legal framework*, is (even when not explicitly forbidden by domestic law) contrary to the logic of the legality requirement since there is no way for the concerned citizens to understand these practices through the law (*Malone*, §81). In *Digital Rights Ireland*, the public-private collaboration for the retention of metadata was not "*outside any legal framework*", but the relevant legal framework in question (the EU Data Retention Directive) raised fundamental rights questions because of the novelty of the method of data retention it introduced.

121 The differences between the two Courts are not fundamental. There is a slight differences in wording between Article 8,§2 ECHR and the corresponding paragraph in the EU Charter to be found under Article 52(1). A bit more fundamental is the CJEU's settled case-law that focusses on on a German law inspired proportionality test. This principle of proportionality requires EU surveillance laws to appropriate for attaining their objectives pursued by the legislation (appropriateness) not exceed the limits of what is necessary in order to achieve those objectives (necessity). See *Digital Rights Ireland*, §45-46.

discretion regarding surveillance might be under certain circumstances be limited (and, consequently, judicial scrutiny by the CJEU might be up-leveled) with a central position amongst those circumstances for 'the nature and seriousness of the interference'.[122] Secondly, there is an appraisal of the data retention surveillance set up by the EU Directive. Although the data retention method spelled out in the EU Directive does not negatively affects the essence of the fundamental right to personal data protection, to privacy and to communications, -'because the directive does not permit the acquisition of knowledge of the content of the electronic communications'), it constitutes a particularly serious interference with those rights (***Digital Rights Ireland***, §§37 & 39-40) because it is 'wide-ranging' and is not accompanied with a notification duty to notify.[123] Thirdly, and as a consequence of the foregoing,[124] there is the application of the full ***Huvig***-package,[125] a judgement that is not explicitly referred to.[126]

Based on these strict requirements, the CJEU found that the proposed data retention powers proposed by the EU Directive do not comply with the principle of proportionality. The interferences made possible by the Directive are not sufficiently circumscribed to ensure that they were actually limited to what was "strictly necessary" (***Digital Rights Ireland***, §69). All ***Huvig***-criteria proved problematic. One stands out more than the others, the first, on ***categories of people*** liable to be monitored: all persons using electronic communications services were targeted, even without the slightest link with crime and no exception was made to protect persons whose communications are subject to the obligation of professional secrecy (***Digital Rights Ireland***, §58).

Canadian PNR contains a heavy structure, but basically assessments of appropriateness (Part VIII C.2.b and c) and necessity (Part VIII.C.2.d), are complemented with assessments of individual rights (Part VIII C.3) and of oversight mechanisms (Part VIII C.4). Notification is checked under '*The individual rights of air passengers*' (Part VIII C.3 of the judgement). The *Huvig*-criteria are included under Part, VIII.C.2.d ('The necessty of the interferences entailed by the envisaged agreement'

122 *Digital Rights Ireland*, §47: "With regard to judicial review of compliance with those conditions, where interferences with fundamental rights are at issue, the extent of the EU legislature's discretion may prove to be limited, depending on a number of factors, including, in particular, the area concerned, the nature of the right at issue guaranteed by the Charter, the nature and seriousness of the interference and the object pursued by the interference (see, by analogy, as regards Article 8 of the ECHR, Eur. Court H.R., *S. and Marper v. the United Kingdom* [GC], nos. 30562/04 and 30566/04, § 102, ECHR 2008-V)".

123 ***Digital Rights Ireland***, §37: "It must be stated that the interference (is) wide-ranging, and it must be considered to be particularly serious. Furthermore, (…) the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance".

124 Despite the breadth of "metadata" definitions and the potential scope of Data Retention Directive, one could argue that *Digital Rights Ireland* is not about very intrusive surveillance, such as telephone interceptions or email interceptions. In other words, considering the similarity between non-intrusive GPS monitoring of *Uzun* and "metadata" monitoring of the case at issue, the CJEU could have been expected to adopt the "mild assessment" of surveillance safeguards from *Uzun*, rather than falling back on the tougher set of requirements developed in *Huvig*. Rightly, however, we find in *Digital Rights* a strict application of legality requirements very similar to *Huvig.* Metadata can be highly intrusive to personal privacy - even more revealing in certain regards than data such as the contents of our communications. See Bryce Clayton Newell & Joseph T. Tennis, 'Me, My Metadata, and the NSA: Privacy and Government Metadata Surveillance Programs', in *Proceedings of iConference 2014*, 345-355. In particular, metadata surveillance can be considered particular intrusive because the initial purpose for which that data was collected was not surveillance, but private commercial purposes. See on this point J. Milaj, *Privacy, surveillance and the proportionality principle: The need for a method of assessing privacy implications of technologies used for surveillance,* 119. The differences in scrutiny between *Uzun* (with its milder requirements) and *Digital Rights Irelands* are warranted: whereas in the first case *location data* taken alone do not allow pervasive data mining operations; in the second case the broad definition of "metadata" and "online identifiers" allow any form of information discovery. In a more recent judgment (see Tele2 Sverige below) the CJEU has explicitly admitted that "even though that [intercepted] data does not include the content of a communication it could be highly intrusive into the privacy of users of communications services" (§55).

125 In Table 5, we summarize the wide similarity between legality requirements of *Huvig* and *Digital Rights Ireland.*

126 The CJEU does not refer to *Huvig*, but does refer to some other, less appropritate ECtHR judgements in §54: "the EU legislation in question must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards so that the persons whose data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data *(*see, by analogy, as regards Article 8 of the ECHR, Eur. Court H.R., *Liberty and Others v. the United Kingdom*, 1 July 2008, no. 58243/00, §62 and 63; *Rotaru v. Romania,* §57 to 59, and *S. and Marper v. the United Kingdom*, §99)".

Table 5. Digital Rights Ireland: revealing the Huvig-impact when assessing the legality principle.

The law should specify:	
ECtHR, *Huvig v. France*	*EUCJ Digital Rights Ireland*
1) ***categories of people*** liable to be monitored;	"The ***relationship between the data whose retention is provided for and a threat to public security*** and, in particular, (…) (i) to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of ***particular persons likely to be involved (…) in a serious crime***, or (ii) to ***persons who could***, for other reasons, ***contribute***, by the retention of their data, to the prevention, detection or prosecution of serious offences. (§§58 and 59)
2) the ***nature of the offenses*** liable of surveillance;	***"Any objective criterion by which to determine the limits of the access*** (…) to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions concerning ***offences that (…) may be considered to be sufficiently serious to justify such an interference".*** (§60).
3) ***limits*** on the ***duration*** of such monitoring;	[The directive] requires that those data be retained for a period of ***at least six months, without any distinction*** (§63). [And] it is not stated that the ***determination of the period*** of retention must be based on ***objective criteria*** in order to ensure that it is limited to what is strictly necessary (§64).
4) the procedure to be followed for ***treating the data***;	"The rules relating to the ***security and protection of data retained*** by providers of publicly available electronic communications services or of public communications networks (…) to ensure ***effective protection*** of the data retained against the risk of abuse and against any unlawful access and use of that data". (§66).
5) ***precautions*** to be taken when ***communicating*** the data	
6) ***circumstances*** in which ***data*** is erased or ***destroyed***	Directive 2006/24 does not ensure the ***irreversible destruction of the data*** at the end of the data retention period (§67).
7) judicial overview	***The access by the competent national authorities to the data retained is not made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued (§62).*** ***It cannot be held that the control, (…) by an independent authority of compliance with the requirements of protection and security***, (…) is fully ensured (§68).

In ***Schrems v. Data Protection Commissioner***[127] the CJEU implicitly adopted (again) the strict ***Huvig***-like criteria, echoing ***Digital Rights Ireland***.[128] The influence of ***Digital Rights*** can be also found in the use of the "strict necessity" principle.

Digital Rights Ireland critical testing of bulk data collection was repeated in ***Tele2 Sverige AB v. Post-och Telestyrelsen*** (2016).[129] The CJEU was asked by Swedish and British courts respectively to consider the scope and effect of its judgement: should ***Digital Rights Ireland*** be interpreted as meaning that the general and indiscriminate retention of data was to be condemned as a matter of principle?[130] Or could bulk data surveillance be deemed acceptable under certain circumstances?

The main effect of ***Tele2 Sverige*** has been the reaffirmation of ***Digital Rights Ireland***, in particular against the reluctance of Member States to implement that decision.[131] Again, the onus is on the ***Huvig*** criteria. In particular the CJEU assessed whether British and Swedish legal systems provided clearly: the categories of people liable to be monitored (***Tele2 Sverige***, §105), the nature of offences that could trigger surveillance (***Tele2 Sverige***, §§105 and 108), precautions to be taken for security of data collection (***Tele2 Sverige***, §122), circumstances for erasure and destruction (***Tele2 Sverige***, §122), duration period of data retention (***Tele2 Sverige***, §108), a system of independent oversight (***Tele2 Sverige***, §119).

Only through strict application of those criteria, -and this (only) for the preventive purpose of fighting serious crime-, bulk data retention can become lawful and acceptable. The proposed surveillance powers must be limited to what is strictly necessary in terms of these criteria (***Tele2 Sverige***, §108) and must be evidence-based: data retention should meet objective criteria that establish a connection between the data to be retained and the objective pursued (***Tele2 Sverige***, §110 & 111).

127 CJEU, *Schrems v. Data Protection Commissioner*, 6 October 2015, Case C-362/14. See in general M.D. Cole & A. Vandendriessche, 'From Digital Rights Ireland and Schrems in Luxembourg to Zakharov and Szabó/Vissy in Strasbourg: What the ECtHR Made of the Deep Pass by the CJEU in the Recent Cases on Mass Surveillance', *EDPL* 2016, vol. 1, 127-128.

128 *Schrems*, §§ 91 and 93: "Legislation is not limited to what is strictly necessary where it authorises, *on a generalised basis*, storage of all the personal data of *all the persons* whose data has been transferred from the European Union to the United States *without any differentiation*, *limitation* or *exception being made in the light of the objective pursued* and without *an objective criterion being laid down by which to determine the limits of the access of the public authorities to the data, and of its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference which both access to that data and its use entail*". See also § 95: "legislation not providing for any possibility for an individual to *pursue legal remedies* in order to have access to personal data relating to him, or to obtain the *rectification or erasure of such data*, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter". Italics added.

129 CJEU, *Joined Cases C-203/15 Tele2 Sverige AB v Post-och Telestyrelsen and C-698/15 Secretary of State for the Home Department v Tom Watson and Others*, 21 December 2016. (hereinafter: *Tele2 Sverige*)

130 Tele2 Sverige, a provider of electronic communications services established in Sweden, informed the Swedish Post and Telecom Authority that, following the Digital Rights Ireland judgment that had declared invalid the Directive 2006/24, it would cease to retain electronic communications data, covered by the Swedish Law on Electronic Communications (LEK), and that it would erase data retained prior to that date. The Post and Telecom Authority argued that the Digital Rights judgment could not be interpreted as meaning that the general and indiscriminate retention of data was to be condemned as a matter of principle, but that it was necessary to assess all the circumstances (access to data, duration, security means, etc.) and thus informed Tele2 Sverige that it was in breach of its obligations under the national legislation in failing to retain the data. Tele2 Sverige challenged that decision before the Swedish Court, which referred to the CJEU for a preliminary ruling on the compatibility of a general obligation to retain traffic data covering all persons with Article 15(1) of the e-privacy directive and with Articles 7 and 8 of the EU Charter of Fundamental Rights and article 8 ECHR. At the same time, two citizen (Brice and Lewis) lodged, before the High Court of Justice of England & Wales, applications for judicial review of the legality of Section 1 of the Data Retention and Investigatory Powers Act 2014 , claiming, inter alia, that that section was incompatible with Articles 7 and 8 of the Charter and Article 8 of the ECHR. The Court of Appeal decided to refer to the CJEU for a preliminary ruling asking whether the Digital Rights judgment lays down mandatory requirements to a Member State's domestic regime governing access to data retained in accordance with national legislation, in order to comply with Articles 7 and 8 of the EU Charter. In other terms, the CJEU is here asked to clarify the exact scope and impact of Digital Rights Ireland both on the EU law and – in particular – on the national legislations regulating data retention.

131 See Abu Bakar Munir, Siti Hajar Mohd Yasin, Siti Sarah Abu Bakar, 'Data Retention Rules: A Dead End?', *European Data Protection Law Review*, 2017, vol. 3/1, 71-83.

Interestingly, is the view of the Court that the interference should be considered "to be particularly serious".[132]

Interesting also, the Court states that in the few cases where lawful mass retention of data can be deemed acceptable, ***prior review by an independent authority*** is considered essential, while a mere ***post-hoc review*** it is not sufficient (***Tele2 Sverige***, §125).[133] Finally, CJEU remarked also here that the lack of any exception to monitor "persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy" is a further violation of EU law (***Tele2 Sverige***, §105).

12. A pragmatic ECtHR in Big Brother Watch and Centrum för Rättvisa. Rejecting the CJEU?

In the foregoing we mainly focused on targeted surveillance. However, the debate today is on bulk data surveillance, -untargeted and indiscriminate surveillance in which data storage and data access are often two separate moments-. Can bulk data surveillance can ever be acceptable for the ECtHR in the light of its ***Huvig/Weber***-criteria and in the light of the firm case law by the CJEU?

The answer seems to be no, for two reasons: 1) the use of a strict legality test and 2) the explicit protection of data of people whose communication are protected by professional secrecy.[134] But then, around 2018, we were still awaiting an answer from the ECtHR that, strictly speaking had never considered bulk data

132 The fact that the data is retained without the subscriber or registered user being informed is likely to cause the persons concerned to feel that their private lives are the subject of constant surveillance" (***Tele2 Sverige***, §100). The Court seemingly struggles with its ***Digital Ireland*** finding that the interference does not affect adversely the essence of the rights to privacy and data protection and by insisting on the particularly seriousness and the constant nature of the surveillance apparently tries to close the gap, adding the significant remark that the retention of data has 'an effect on the use of means of electronic communication and, consequently, on the exercise by the users thereof of their freedom of expression, guaranteed in Article 11 of the Charter' (***Tele2 Sverige***, §101).

133 This last statement seems a clear departure from the above-described case-law on judicial review: while in the previous jurisprudence of ECtHR the Court had not clarified whether post-hoc review over surveillance is sufficient or also prior review is necessary, here the CJEU affirms that – at least in the field of mass surveillance - prior authorization is essential in order to protect fundamental rights of concerned persons. Interestingly this position had already been held by distinguished scholars. See, inter alia J. Milaj, *Privacy, surveillance and the proportionality principle: The need for a method of assessing privacy implications of technologies used for surveillance,* supra, 119 who argues that ex post and ex ante are not equal, neither it's true that the "ex post oversight is sufficient": the ex ante is better (…) than that the ex post". The use of these high standards is a further confirmation of the non-admissibility of bulk dataset collection or other forms of indiscriminate mass surveillance in the EU. Indeed, this case is even more relevant than Digital Irelands for its implications on bulk data collection: the Court strongly remarks that *general and indiscriminate retention* of all traffic and location data can never be considered necessary (*Tele2 Sverige*, §103). In particular, the retention of data must "meet *objective criteria*, that establish a *connection* between the data to be retained and the objective pursued. In particular, such conditions must be shown to be such as actually to *circumscribe*, in practice, the extent of that measure and, thus, *the public affected*" (*Tele2 Sverige*, §110 italics added). *Discriminants*, *identifiers* and *keywords* might all be objective criteria circumscribing the public affected by mass surveillance. Accordingly, the absence of these discriminants in bulk collection cannot be considered proportionate and necessary.

134 ***Firstly***, we can infer that mass surveillance in the form of bulk dataset collection is not admissible because of the application of ***Huvig***-legality requirements to data retention, and so the use of a very strict legality standard for data retention. Indeed, the CJEU underlined that ***any*** retention of data should be restricted to specific categories of people (considering the nature of their offences (***Digital Rights Irelands***, §59)) with specific precautions, procedures and limitations (***Digital Rights Irelands***, §61) also regarding the duration of the data retention period (***Digital Rights Irelands***, §63). Following the strict scrutiny in ***Weber and Saravia*** and ***Liberty,*** bulk collection should be always limited. In particular, if bulk collection system cannot allow the identification of people liable to be monitored (e.g. on the basis of the seriousness of their crime), we should conclude that the bulk collection should not be compatible with the European Courts jurisprudence. A second element that may suggest us the non-admissibility of bulk datasets in the European framework is the explicit protection by the CJEU of data of people whose communication are protected by professional secrecy (***Digital Rights Irelands***, §58; ***Tele2 Sverige***, §105). Therefore, if States cannot collect such data they should either create a digital environment in which they exclude people with professional secrecy duties (e.g. doctors, lawyers, etc.) from mass surveillance or they should not practice mass surveillance at all. Considering the first option is presently not technically reasonable, we should conclude that a wide mass surveillance through bulk datasets appears unlawful under the European framework.

retention.[135] Only in 2018 the ECtHR was explicitly asked in two occasions to decide whether bulk data collection was admissible under Article 8 ECHR or not. The two judgements are ***Centrum För Rättvisa v. Sweden*** (2018) [136] and ***Big Brother Watch v. the United Kingdom*** (2018).[137] Both reach similar conclusions and state that bulk interception regimes do not violate themselves the Convention if they respect the ***Huvig***-criteria. The ECtHR tries to conceal the disruptiveness of these new judgements

We briefly discussed ***Centrum För Rättvisa*** in our section on the Strasbourg margin of discretion left to Member States (section 7). Setting a broad margin allowed the ECtHR to accept state use of bulk surveillance, granted that their laws pass the ***Huvig/Weber***-minimum requirements.[138] Swedish data retention law allowing the Swedish secret service (FRA) to monitor international communications, passes this test.[139] The ECHR, though identifying in Swedish law "some areas where there is scope for improvement – notably the regulation of the communication of personal data to other states and international organisations and the practice of not giving public reasons following a review of individual complaints –, concludes that "the system reveals no significant shortcomings in its structure and operation. It has developed in such a way that it minimises the risk of interference with privacy and compensates for the lack of openness" (***Centrum För Rättvisa***, §180).[140]

Centrum För Rättvisa's message is a gift to the law enforcement community (bulk data surveillance is possible under the ***Huvig***-test), but it does raise evident questions in the light of the CJEU's ***Digital Rights Ireland*** and ***Tele2*** judgements.[141]

135 In *Weber and Saravia* and *Liberty* the *Huvig* legality requirements were applied, but the object of the scrutiny was not an untargeted surveillance like bulk collection, but a targeted mass surveillance, based on "catchwords" (*Weber and Saravia*) or "keywords" (*Liberty*). Moreover, according to the ECtHR the use of keywords - though criticized by the applicants - is seen a positive element: an objective parameter that may better delimit the scope of surveillance thus increasing foreseeability of categories of people liable to be monitored. See *Weber and Saravia*, §97: "The Court further observes that the conditions for strategic monitoring, as laid down in section 3(1) and (2) of the amended G 10 Act, in particular, indicated which categories of persons were liable to have their telephone tapped: the persons concerned had to have taken part in an international telephone conversation via satellite connections or radio relay links (...). In addition, the persons concerned either had to have used catchwords capable of triggering an investigation into the dangers listed in section 3(1), points 1-6, or had be foreign nationals or companies whose telephone connections could be monitored deliberately in order to avoid such dangers (section 3(2))". Compare with *Centrum För Rättvisa*, §112 where the ECtHR seems to suggest that *Weber and Saravia* and *Liberty* are *also* about bulk data and seems to minimalize the differences.

136 ECtHR, ***Centrum För Rättvisa v. Sweden,*** 19 June 2018, application no. 35252/08. See Plixavra Vogiatzoglou, 'Centrum för Rättvisa v Sweden: Bulk Interception of Communications by Intelligence Services in Sweden Does Not Violate the Right to Privacy', ***European Data Protection Law Review***, 2018, vol. 4/4, 563-567

137 ECtHR, *Big Brother Watch and others v. the United Kingdom*, 13 September 2018 applications nos. 58170/13, 62322/14 and 24960/15.

138 We recall that the Strasbourg Court considers that the decision to operate a bulk interception regime in order to identify hitherto unknown threats to national security is one which continues *to fall within States' margin of appreciation* (*Centrum För Rättvisa*, §112). This margin with regard to the choice of *type* of interception regime, is however narrowed with regard to the operational aspects of the surveillance method: *the discretion afforded to states in operating an interception regime must necessarily be narrower* and subjected to the six-requirements *Huvig*-test (*Centrum För Rättvisa*, §113).

139 Crucial steps in the argumentation are to be found under the testing of the requirements on '*Procedures to be followed for storing, accessing, examining, using and destroying the intercepted data*' (*Centrum För Rättvisa*, §142-147) where the Court basically holds that bulk data collection is collection of raw data and this is, provided limitations on duration, less innocent that manual processing and analyzing of the data: "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. At the same time, the Court stresses the importance of deleting such data as soon as it is evident that it lacks pertinence for a signals intelligence mission" (*Centrum För Rättvisa*, §146).

140 The one weakness the ECHR identifies in Swedish surveillance law is about the international communication of personal data: Swedish law lacks detailed provisions regulating these kinds of transfers, so very little is known about what happens with Swedish data send abroad and about data send and shared by foreign players with Swedish secret services. This legal issue continues to dominate the surveillance discussions. It was already largely addressed by CJEU in *Digital Rights Ireland, Tele2 and Schrems*, and will also lead the ECHR to declare a violation of Article 8 ECHR in *Big Brother Watch*.

141 Of course, the ECtHR and CJEU judgements deal with different actors and context. The ECHR's *Centrum för Rättvisa* (and *Big Brother Watch*) deal with data retention by secret services with regard to international threats to national security, whereas the CJEU judgements deal with data retention in the context of criminal procedure. Nevertheless, the judgement conveys a deliberate attempt of the ECHR to temper the very principled stand on surveillance taken by the CJEU in *Tele2* judges 18 months earlier. Comp. C. Van de Heyning , 'Het bewaren en gebruik van telecommunicatie gegevens in het strafrechtelijk onderzoek: de hoogste hoven in dialoog', *Tijdschrift voor Strafrecht*, 2019, Issue 1, (p.38-47), p. 41

Big Brother Watch, rendered three months after ***Centrum för Rättvisa***,[142] confirms the broad margin of discretion of Member States to set up bulk data retention against terrorism and to engage in international intelligence data sharing and applies a ***Huvig***-light testing to this practice of international intelligence data sharing.[143] The judgment also assess the Article 8 ECHR compatibility of two other surveillance practices: the UK bulk interception regime on behalf of secret services and its regime for obtaining communications data from communications service providers based on the basis in the Regulation of Investigatory Powers Act 2000. The Court finds two violations but keeps the door open for the United Kingdom with the caveat that it intended to replace the RIPA Act by the 'significant better' Investigatory Powers Act 2016. Although some violations of Huvig-criteria were found, there is little in ***Big Brother Watch*** to suggest a no-go for states to organize bulk interception of communications and to obtain communications data from communications service providers.

In the background one senses the presence of the CJEU. The ECtHR is aware that its own jurisprudence on surveillance law is not totally overlapping with the CJEU-case law, e.g. in terms of proportionality, safeguards, etc: the Court does not want to go as far, but wants to avoid a brutal confrontation.[144]

13. Synthesis: overview of the evolutions from Klass in recent years

The incredible evolutions in surveillance technologies have strongly challenged the principle of legality in Article 8 ECHR. In particular, the shift from telephone interception to meta-data surveillance, from individual monitoring to mass monitoring, from human-led investigation to machine-led investigation, from traditional policing to predictive policing and bulk data surveillance have suggested to re-consider the traditional notion of 'foreseeability' (or detailedness) of law as an element of the legality principle. But the contrary has produced itself: the requirements regarding legality in the context of telephone tapping have more often than not been applied to surveillance practices, even to those that could be, by some, considered as less harmful to privacy and human rights. Since the distinction between hard and soft intrusions in the context of surveillance is often hideous, we cannot but agree with this development.

The story of the Strasbourg case law on interception of communication is well known. After a pioneering judgement in ***Klass*** (1978) it was made clear that communications are protected by Article 8 ECHR and that all limitations needed to pass a test of legality, legitimacy and necessity. ***Malone*** (1984) and ***Huvig*** (1990) added clarifications about possible limitations of communications in the sphere of criminal law,

142 We recall that the case deals with three joint cases triggered by disclosures by Edward Snowden as to the surveillance measures used by the UK and the US intelligence services, including the practices of intercepting electronic communications in bulk as well as the sharing of intercepted data between intelligence services. The claims asserted interferences with the applicants' rights under Articles 8, 10 and 14 ECHR, as well as a challenge under Article 6 ECHR to the compatibility of the procedure before the specialist domestic tribunal, the Investigatory Powers Tribunal (IPT), in which some of the Applicants had brought complaints.

143 See section 6 and 7, *above*

144 The ECTHR affirms that Article 8 ECHR requires that the surveillance measure should be "in accordance with the law" and the national law in a EU Member State is not only based on national legislations, but more importantly on the EU law. Therefore, if an investigation practices is based on national surveillance legislations which are in conflict with the EU law (and so which are in conflict also with the CJEU case law), such practice is not "in accordance with the law" and so it is also a violation of Article 8 ECHR. In particular, the ECtHR acknowledges that the CJEU in (*Digital Rights Irelands*, *Tele2* and *Ministerio Fiscal*) requires that any regime permitting the authorities to access data retained by Communication Service Providers should be limited to the purpose of combating "serious crime" and should be subject to *prior* review by an independent body. As the UK RIPA Chapter II regime permits access to retained data for the purpose of combating crime (rather than "serious crime") and it is not subject to prior review by a court or independent administrative body, it cannot be in accordance with the law within the meaning of Article 8 of the Convention.

with first guidance on meta-data surveillance and practices of data collection gathering amongst private providers (***Malone***) and more importantly detailed guidance on how foreseeability, as a core feature of the legality requirement, should be understood in the context of intrusive and less intrusive surveillance (***Malone*** and ***Huvig***).

In ***Weber and Saravia*** (2006) the Court confirms the ***Klass*** findings and the ***Huvig*** surveillance requirements and adapts them to the new challenges of mass surveillance. Milestones taken from ***Klass*** (notification duties, oversight procedures, the necessity principle) are combined with the ***Huvig*** legality requirements and with more detailed indications on ***keywords*** used for monitoring and storage of data. Accordingly, the ***Klass*** framework is not overcome, but only updated with stricter requirements, so that it can adequately face the emerging challenges of mass surveillance. The judgement also echoes the positive starting point of ***Klass*** regarding the need or necessity for democracies to fall back on surveillance methods. The message that Member States have some flexibility in setting up surveillance (some 'margin') will be partly corrected or rephrased in ***Segerstedt-Wiberg*** (2006) that proposed a strict necessity test to assess the compatibility of surveillance with the ECHR.

Weber and Saravia (2006), which has widely influenced ***Liberty*** (2008), does not entail that any form of mass surveillance is admissible under the ECHR, but only if strict safeguards are included in the legal system where mass surveillance is led. Mass surveillance can be admissible if the ***Huvig*** requirements are respected and in particular if:

- the keywords used for strategic monitoring are mentioned when requesting authorization for surveillance;
- surveillance is restricted to the prevention of serious criminal acts enlisted in the law;
- the data are stored for a specified period and the necessity of this storage is periodically checked;
- there is an authorization procedure that prevents haphazard, unnecessary or disproportionate surveillance;
- there is a periodical review by independent bodies vested with substantial powers;
- surveillance measures are notified to the concerned persons as soon as it does not jeopardize the purpose of surveillance.

Whether it is about laws creating powers for intercepting individual telephone calls in criminal law, or about laws setting up on behalf of secret services complex structures of mass recording of telephone, fax and e-mail communications selected and organized through key, the human rights-check on legality will follow the same approach.

In sum, ***Weber and Saravia*** (confirmed in ***Liberty***) have clarified that mass surveillance is not prohibited under the ECHR, but national laws regulating mass surveillance must respect the strict legality requirements set in ***Huvig***.

Weber and Saravia and ***Liberty*** were till 2018 the first ECtHR "mass surveillance" judgements, and, as developed in the foregoing, served as fundamental point of references for CJEU when addressing mass surveillance (e.g. in ***Digital Rights Ireland***, ***Schrems***, and in ***Tele2***, ***Weber***)[145].

More recent ECtHR-judgements such as ***Zakharov*** (2015) ***Szabò and Vissy*** (2016) received less attention in this contribution on the legality principle, but they can be considered as a "litmus paper" for changes

145 See, e.g., *Digital Rights Ireland*, §54. See also Schrems case, §91 referring back to that §54 of *Digital Rights Ireland*.

and developments of ECtHR case law about secret surveillance in general during these four decades. The main difference is the technological and socio-political background. Although ***Klass*** already voiced a concern about "technical advances made in the means of espionage and, correspondingly, of surveillance", but counterbalanced this concern by pointing at "the development of terrorism in Europe in recent years" and "sophisticated forms of [private] espionage" (***Klass***, §48), one senses more genuine concerns about the risks of state surveillance in ***Zakharov Szabò and Vissy***, both judged after Snowden Case and in a context of powerful technologies enabling intrusive and indiscriminate mass surveillance by the States.[146] Indeed, in ***Szabò*** the Court explicitly explains that "***given the technological advances since the Klass case, the potential interferences with email, mobile phone and Internet services as well as those of mass surveillance attract the Convention protection of private life even more acutely***"(***Szabò***, §53).

This is probably why the safeguards are scrutinized more strictly[147] so that the application of ECHR in the protection of privacy can have a broader impact. It partly explains in our view why the ***right to notification*** appears strengthened through the development of Strasbourg case law[148]. In ***Klass v. Germany*** the role and importance of notification is fainter and also the wording is less strict than in ***Mosley***, ***Zakharov*** and ***Szabò v. Hungary***, where the importance of surveillance notification is considered high[149]. The definitive principle is that ***as soon as notification can be carried out without jeopardising the purpose of the restriction after the termination of the surveillance measure, information should, however, be provided to the persons concerned.*** Also, the scrutiny of "necessity" principle has been much increased with surveillance case law. The Court created a new guarantee to deal with the extra power that the state obtained from the new technologies: the ***strict necessity*** requirement. Even though this principle had already been declared in ***Klass***[150], it will assume a real normative role only in ***Segerstadt-Wiberg*** and in the CJEU ***Digital Ireland*** case.[151] A similar statement comes from the International Congress of Penal Law, according to which ICT investigative measures shall only be allowed in the cases specified by law when the desired information cannot be gathered through less-intrusive means[152].

146 As regards the impact that NSA revelations and new technologies can have on Surveillance regulation see B. van der Sloot, 'Privacy in the Post-NSA Era: Time for a Fundamental Revision?', *Journal of intellectual property, information technology and electronic commerce law*, 2014, vol. 5/1.

147 See infra about the role of notification, the "strict necessity principle, and the applicants' victim status.

148 This has been also the position of the Nineteenth International Congress of Penal Law, Rio de Janeiro, 31st august – 6th September 2014, International Review of Penal Law, vol. 86, 2014, p. 446, See section 3, §14: "persons whose right to privacy has been affected by investigative measures involving ICT should be informed of the measures as soon as this disclosure does not jeopardize the purpose of the measure and/or the results of the criminal investigation.

149 Indeed, in ***Klass*** the Court argues that subsequent notification to each individual affected by a suspended measure "might well jeopardise the long-term purpose that originally prompted the surveillance. (…) Such notification might serve to reveal the working methods and fields of operation of the intelligence services and even possibly to identify their agents. (…) The fact of not informing the individual once surveillance has ceased cannot itself be incompatible with this provision since it is this very fact which ensures the ***efficacy*** of the 'interference'" ***Klass***, §58. (italics added). On the contrary, ***Szabò*** highlights how notification "is inextricably linked to the ***effectiveness*** of remedies and hence to the existence of ***effective*** safeguards against the abuse of monitoring powers, since there is in principle little scope for any recourse by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their justification retrospectively. As soon as notification can be carried out without jeopardising the purpose of the restriction after the termination of the surveillance measure, information should be provided to the persons concerned" (italics added), ***Szabò*** at §86. It is interesting to underline that the "efficacy/effectiveness" argument is used on the one hand in order to limit notification duty ("efficacy of surveillance") and on the other hand to strengthen notification duty ("effectiveness of safeguards").

150 See *Klass*, §42; *Segerstedt-Wiberg*, §88; *Rotaru*, §47; Digital Rights Ireland §52.

151 In one jugement the CJEU underlined, "when considering the necessity for such use in the main proceedings, it must be assessed in particular, (…), whether the use is proportionate to the aim pursued, examining whether all the necessary information could not have been obtained by means of investigation that interfere less with the right guaranteed by Article 7 of the Charter than interception of telecommunications and seizure of emails, such as a simple inspection at WML's premises and a request for information or for an administrative enquiry" (CJEU, WebMindLicenses Kft. V Nemzeti Adóés Vámhivatal Kiemelt Adó- **és** Vám Főigazgatóság, 17 December 2015, §8).

152 Nineteenth international congress of Penal Law, Rio de Janeiro, 31st august – 6th September 2014, *International Review of Penal Law*, 2014, vol. 86, 446, See section 3, §12.

A strong limitation to indiscriminate mass surveillance comes also from the CJEU cases ***Digital Rights Irelands*** and ***Tele2 Sverige*** because of the large application of ***Huvig*** strict requirements (with prior specification of categories of people liable to be monitored) and the explicit protection of people covered by professional secrecy (and so the impossibility of an indiscriminate surveillance to any people). [153]

All these developments (development and expansion of the foreseeability framework, strict testing, insistence on notification and on the need of a ***judicial review*** over surveillance) deserve a broader analysis than the one proposed in this contribution dedicated to the legality principle and its notions of quality and foreseeability. Actually, the "quality" of the rule of law is adversely affected by a recent trend in several national legal systems: "a regrettable overlap of roles and tasks and potentially a perilous blur"[154] between police and secret services in detecting the most serious crimes.

Scholars have remarked that "surveillance-led enforcing has become a dominant feature of criminal justice and security law" so that "the criminal justice system is risking perverting into a security system"[155]. Real risks of this development are that wide range of investigation technologies may be used in relation to different offences, at different phases of the procedure (prevention or investigation) and for different purposes (crime detection, national security) and it would lead to an unwelcome legal uncertainty and a disagreeable competition between the different actors involved[156].

This trend can be observed for example in ***Kennedy*** and ***Zakharov***, where domestic surveillance laws are brought before the ECtHR providing for a unique system of surveillance, a hybrid applicable both to police and to secret surveillance. These laws make no or little difference in procedures and guarantees according to purposes, tasks and phases. Another example is ***Szabò***, where - although separate procedures are provided - the same public authority (police) can act both for the detection of crimes and for the investigation in the field of strategic national security. Probably, it is not only a coincidence that in Member States where police are increasingly used for investigations related to national security and public safety, rather than only for criminal prosecution, the system of safeguards has been declared insufficient to prevent private life interferences that are not necessary in a democratic society (***Szabò v. Hungary***, §89).

In conclusion, we can assert that the ***legality*** test and related ideas such as notification safeguard against surveillance in Europe and evolve both as an answer to the technologies available for surveillance and as an answer to the recent blur of tasks and players in the surveillance field.

In particular the 6-steps legality test adopted firstly in ***Huvig*** has then been re-adopted in any following case. At the beginning, the test was applied less strictly in surveillance cases not based on telephone interception (see ***Uzun),*** but since the development of technologies has grown exponentially, the strictness of the ***Huvig*** test has then been accepted also in cases of meta-data surveillance or data retention in general. However, a certain contextuality remains. In ***Ben Faiza*** and ***Big Brother Watch*** the legality testing is based on different levels of strictness according to different levels of crime seriousness under investigation. Even bulk surveillance has been accepted, but only if the public authority can prove that even in that case the ***Huvig*** test on legality was respected.

153 *Digital Rights Irelands*, §58.
154 C. Cocq & F. Galli, 'The Catalysing Effect of Serious Crime on the Use of Surveillance Technologies for Prevention and Investigation Purposes', *New Journal of European Criminal Law*, 2013, vol. 4/ 3. 40.
155 J. Vervaele, 'Surveillance and Criminal Investigation: Blurring of Thresholds and Boundaries in the Criminal Justice System?', in S. Gurtwirh, R. Leenes, P. De Hert (eds.), *Reloading Data Protection: Multidisciplinary Insight and contemporary challenge,* Dodrecht: Springer, 2014, 115
156 C. Cocq & F. Galli, 6.

The effect of these last decisions does not appear to go against a state's ability to conduct surveillance, but rather defines the framework that must be in place to strike the right balance between a citizen's right to privacy and the unfettered discretion of the government to conduct surveillance in the name of 'national security'.

The Brussels Privacy Hub Working Papers series

N°1 "The data protection regime applying to the inter-agency cooperation and future architecture of the EU criminal justice and law enforcement area" (November 2014) by Paul De Hert and Vagelis Papakonstantinou (35 pages)

N°2 "The new cloud computing ISO/IEC 27018 standard through the lens of the EU legislation on data protection" (November 2014) by Paul de Hert, Vagelis Papakonstantinou, Irene Kamara (25 pages)

N°3 "Towards efficient cooperation between supervisory authorities in the area of data privacy law" (October 2015) by Dariusz Kloza, Antonella Galetta (24 pages)

N°4 "The data protection regime in China" (November 2015) by Paul De Hert and Vagelis Papakonstantinou (30 pages)

N°5 "The right to privacy and personal data protection in Brazil: time for internet privacy rights?" (February 2016) by Vinícius Borges Fortes (23 pages)

N°6 "Permissions and Prohibitions in Data Protection Jurisdiction" (May 2016) by Mistale Taylor (25 pages)

N°7 "Structure and Enforcement of Data Privacy Law in South Korea" (October 2016) by Haksoo Ko, John Leitner, Eunsoo Kim and Jong-Gu Jung (20 pages)

N°8 "The "Right to be Forgotten" and Search Engine Liability" (December 2016) by Hiroshi Miyashita (15 pages)

N°9 "European Human Rights, Criminal Surveillance, and Intelligence Surveillance: Towards "Good Enough" Oversight, Preferably but Not Necessarily by Judges" (March 2017) by Gianclaudio Malgieri and Paul De Hert (25 pages)

N°10 "Does Technology Drive Law? The Dilemma of Technological Exceptionalism in Cyberlaw" (July 2017) by Meg Leta Jones, JD, PhD (31 pages)

N°11 "The Microsoft Ireland case and the cyberspace sovereignty trilemma. Post-territorial technologies and companies question territorial state sovereignty and regulatory state monopolies" (July 2018) by Paul De Hert and Johannes Thumfart (27 pages)

N°12 "Understanding the balancing act behind the legitimate interest of the controller ground: a pragmatic approach" (August 2018) by Irene Kamara and Paul De Hert (35 pages)

N°13 "Big data analytics by telecommunications operators and the draft ePrivacy Regulation" (September 2018) by Vagelis Papakonstantinou and Paul de Hert (13 pages)

N°14 "Enforcement in Indonesia Data Privacy Laws: The 2018 Facebook-Cambridge Analytica scandal as a case study" (October 2018) by Anbar Jayadi (21 pages)

N°15 "Belgium, Courts, Privacy and Data Protection. An inventory of Belgian case law from the pre-GDPR regime (1995-2015)." (January 2019) by Paul De Hert (34 pages)

N°16 Big data analytics in electronic communications: A reality in need of granular regulation (even if this includes an *interim* period of no regulation at all) (June 2019) by Vagelis Papakonstantinou and Paul de Hert (25 pages)

N°17 Data Localisation: Deconstructing myths and suggesting a workable model for the future. The cases of China and the EU (September 2019) by Author: Yanqing Hong, Senior Fellow, Law and Development Institute, Peking University of China, Edited by Vagelis Papakonstantinou, Brussels Privacy Hub (31 pages)

N°18 Challenging algorithmic profiling: The limits of data protection and anti-discrimination in responding to emergent discrimination (January 2020) by Dr Monique Mann and Professor Tobias Matzner (18 pages)

N°19 Access to the Internet in the EU: a policy priority, a fundamental, a human right or a concern for eGovernment? (February 2020) by Lina Jasmontaite and Paul de Hert (23 pages)

N°20 The Proposed ePrivacy Regulation: The Commission's and the Parliament's Drafts at a Crossroads? (March 2020) by Elena Gil González, Paul De Hert & Vagelis Papakonstantinou (31 pages)

N°21 Article 8 ECHR compliant and foreseeable surveillance: the ECtHR's expanded legality requirement copied by the CJEU. A discussion of European surveillance case law (April 2020) by Paul De Hert & Gianclaudio Malgieri (42 pages)

The Brussels Privacy Hub Working Papers series

The Brussels Privacy Hub Working Papers are intended to circulate research in progress for comment and discussion. The Working Papers focus on all areas of data protection and privacy research and can contain empirical research on privacy issues and analytical work on privacy governance and regulation in the EU; global flows of data; reconciling law enforcement and privacy interests; privacy challenges posed by new technologies; comparative research on privacy in different regions; jurisprudential issues of privacy protection; and many others

Available at www.brusselsprivacyhub.org/publications.html

Contact: info@brusselsprivacyhub.eu

BRUSSELS PRIVACY HUB