BRUSSELS PRIVACY HUB
WORKING PAPER
VOL. 3 • N° 9 • MARCH 2017

BRUSSELS PRIVACY HUB
Vrije Universiteit Brussel

EUROPEAN HUMAN RIGHTS, CRIMINAL SURVEILLANCE, AND INTELLIGENCE SURVEILLANCE: TOWARDS "GOOD ENOUGH" OVERSIGHT, PREFERABLY BUT NOT NECESSARILY BY JUDGES

by Gianclaudio Malgieri[1] & Paul De Hert[2]

Abstract

The two European Courts (the European Court of Human Rights, ECtHR and, to a lesser degree, the European Union Court of Justice, EUCJ) have contributed greatly to the development of a legal framework for surveillance by either law enforcement agencies in the criminal law area or by secret services. Both courts put great emphasis on a system of control ex ante and post hoc by independent supervisory authorities. A complex and controversial issue remains whether the human rights to privacy, respect of communications, and to an effective remedy (enshrined in Article 8 and 13 of European Convention on Human Rights (ECHR)), requires judicial review as a necessary safeguard for secret surveillance or alternatively, at which conditions, parallel systems of non-judicial review can be accepted as adequate safeguards against illegitimate interference in citizens' private life.

The European Courts have not yet established a clear doctrine in determining suitable thresholds and parameters. In particular, the ECtHR has a flexible approach in interpreting article 8 and 13 ECHR, depending on several factors ("vital" interests at stake, political considerations, etc.). In general terms, the Court has shown a preference towards judiciary oversight, but in the European legal order there are 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 judgements of the ECtHR and the EUCJ we see an increasing emphasis on declaring the necessity of a "good enough" judicial (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.

Keywords: Privacy, Surveillance, judicial review, European Court of Human Rights, European Convention on Human Rights

This contribution is a Chapter in David C. Gray & Stephen Henderson (eds.), *The Cambridge Handbook on Surveillance*, New York: Cambridge University Press, 2017

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
This version is for academic use only.

This contribution is based on 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 Available at SSRN: https://ssrn.com/abstract=2948270

Disclaimer

Article 8 , European Convention of Human Rights - **Right to respect for private and family life**

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

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

Article 13, European Convention of Human Rights - **Right to an effective remedy**

1. Everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity.

I. Introduction: Does Surveillance Require a Judge?

Surveillance raises many questions about human rights acceptability. Be it public or private, what it needs is a framework—organisational, legal, and technological—that allows the protection of the society and maintains a framework of freedoms in place[3].

European human rights case law on surveillance is considerable, and this chapter will review the leading opinions from the European Court of Human Rights (hereafter ECtHR or Strasbourg Court), and, to a lesser degree, from the European Union Court of Justice (hereafter EUCJ or Luxembourg Court)—most notably **Schrems v. Data Protection Commissioner** (2015).[4]

An indispensable element in every surveillance framework, at least for surveillance done by public actors, is a system of control **ex ante** and **post hoc** by an independent supervisory authority, which might be a judge or another national authority. A central question in European human rights law on surveillance is whether Article 8 of the European Convention on Human Rights (ECHR)[5]—containing the right to privacy and secrecy of communications and the inviolability of the house—requires judicial review as a necessary safeguard for secret surveillance or, alternatively, what conditions and systems of non-judicial review can be accepted as adequate safeguards against illegitimate interference in citizens' private lives.

So far, the question has not been resolved in a decisive way. In general terms, we can affirm that in the field of surveillance, where "abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, **it is in principle desirable to entrust supervisory con-**

1 PhD Researcher in Law at Vrije Universiteit Brussel, Brussels.
2 Full Professor of Law at Vrije Universiteit Brussel, Brussels.
3 David Lyon, Surveillance Studies: An Overview (Polity Press, 2007).
4 Under the term "European human rights" law we mean both the "Convention for the Protection of Human Rights and Fundamental Freedoms," better known as the **European Convention on Human Rights,** ECHR (which was opened for signature in Rome on 4 November 1950 and came into force in 1953 and whose application scope includes the 47 member States of the Council) and the EU Charter of Fundamental Rights (proclaimed in Nice in 2000) applicable to the 28 Member States of the European Union. Our text will focus on the ECHR.
5 Article 8 ECHR, Right to respect for private and family life: "1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

trol to a judge,"[6] but this is not a hard rule. In fact, the European Court of Human Rights has adopted a flexible approach. We will highlight when and under which conditions the ECtHR has accepted systems of non-judicial control over surveillance.

In recent judgments of both the ECtHR and the EUCJ we see an increasing emphasis on declaring the necessity of a **good enough** (**ex ante** or **ex post**) control over surveillance: not necessarily 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.

Part II of this chapter will clarify the general content of Article 8 ECHR and the terminology used in the field of surveillance oversight, considering different national criminal procedure legal systems. Part III will address specifically the application of Article 8 ECHR in criminal law surveillance, as crystallised in **Huvig v. France** (1990), one of the first cases of "strict scrutiny" by the Court. Next, Part IV will analyse the different measures of scrutiny in the Court's surveillance case law.

Considering that surveillance can be conducted by different actors for different purposes, a specific focus should be dedicated to secret service surveillance. Part V will analyse how the Court has assessed the necessity of an individual's effective remedy against secret service surveillance, according to Article 13 ECHR combined with Article 8 ECHR.

Typically, member states have provided "non-judiciary" oversight of secret service surveillance. Therefore, Parts VI and VII will highlight how the Court has assessed these "non-judiciary" methods of surveillance

6 Klass & Others v. Germany, No. 5029/71, Eur. Ct. H.R. 1, 21 (1978).

control. Particular attention will be dedicated to "quasi-judiciary" systems, as in the case of Data Protection Authorities (Part VIII).

Lastly, Part IX will analyse how the Court is assessing these oversight systems by using empirical means to assess the effectiveness of each system.

II. Some Preliminary Clarifications - Oversight and Remedy: Who and When

Before discussing European case law on surveillance, some clarifications are necessary, especially regarding the system of judicial control warranted by European human rights law.

Article 8 ECHR is divided into two paragraphs. In the first paragraph four rights are enumerated: the right to respect for an individual's private life, family life, home, and correspondence. A second paragraph contains three requirements for acceptable privacy limitations: these must have a legal basis (the '"in accordance with the law" requirement), must seek legitimate purposes (the legitimacy requirement), and must be proportional (the "necessary in a democratic society" requirement).

Second, we need to clarify some terms used in this chapter. **Oversight** means supervision, management, or control, while **review** means to view again, survey again, or take a retrospective view of events and activities that have already occurred.[7] Oversight can be **ex ante** and/or **ex post**. **Ex ante** oversight consists of an authorization to surveillance measures given by a supervisory authority, normally a judge. **Ex post** oversight consists of review over surveillance measures already started. This review may be triggered either by individuals who suspect they are under surveillance, or it could be automatic (e.g., a random control by judges or other supervisory authority), also within a criminal trial (i.e., during a judicial proceeding after investigation by surveillance).[8]

It is necessary to remind the non-European reader that in some European states investigatory powers within criminal law investigations are exercised by a **prosecutor**, and a **control judge** must authorize specific surveillance measures. This is the typical **adversarial** system.[9] In other countries, investigative powers are exercised by **investigative judges**, and no other judges control investigation until the trial. This is typical of **inquisitorial** systems.[10]

Unlike the US Constitution (Fourth Amendment), there is no provision in European human rights law stating that in some cases a warrant (by a judge) is needed. Neither the 'who' or the 'when' of oversight is made concrete. To understand the European approach (or lack of it), one must look at the conjunction between Article 8 ECHR (right to privacy) and Article 13 ECHR (right to an effective remedy): when the right to private life is violated, an "effective remedy by a national authority" is necessary. The Strasbourg Court considers judges an "effective remedy provided by national authorities," but it has never stated that Article 13 ECHR can be satisfied solely by judicial oversight (see more detail below in Part IV).

7 Marina Caparini, Controlling & Overseeing Intelligence Services in Democratic States 8 (Hans Born & Marina Caparini eds., Democratic Control of Intelligence Services, Hampshire 2007).

8 **See** Eur. Commission For Democracy Through Law (Venice Commission), Report On The Democratic Oversight Of The Security Services § 195 (2007).

9 **See id**. at § 197.

10 **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 welzijnswerk, 2003, VOL. 34/2, 155–98.

Articles 8 and 13 ECHR both fail to clarify the relation or choice between **ex ante** or **ex post** oversight, but in principle at least a **post hoc** control should be guaranteed. We will address this particular topic during our case law overview.

III. Article 8 ECHR and the Huvig Requirements for Criminal Surveillance

The canonical judgments on surveillance mostly relate to interception of telecommunications, in particular telephone lines. Judgments like **Klass v. Germany** (1978) and **Malone v. UK** (1984), respectively on surveillance of telecommunications by German secret services and by UK police, are classics in this respect. Both center around Article 8 ECHR and contain clarifications of notions such as 'privacy' and the requirements of legality and proportionality. These judgments contain first guidelines on surveillance in Europe that further crystallized in **Huvig v. France** (1990).[11]

In **Huvig**, rendered at a time when most European states had recognized powers to intercept telecommunication, the ECtHR clarified in detail which safeguards are required with regard to telephone surveillance according to Article 8 ECHR. In particular, the Court gave a broad characterization of the requirement that privacy-limiting powers need a legal basis. The Court stated that the expression "in accordance with the law," within the meaning of Article 8(2) ECHR, requires that 1) the impugned measure should have **some basis in domestic law**, where "law" is understood in its substantive sense including both enactments of lower rank than statutes and unwritten law;[12] 2) that "law" also refers to the quality of the law in question, requiring that it should be **accessible** to the person concerned,[13] who must moreover be able to **foresee** its consequences for him; and 3) the measure must be **compatible with the rule of law**.[14]

In substance, what the law should indicate with reasonable clarity is **the scope and manner** of exercise of the relevant discretion conferred on the public authorities.[15] In particular, the Court insisted on six mandatory clarifications: the categories of people liable to be monitored; the nature of the offenses subject to surveillance; limits on the duration of such monitoring; the procedure to be followed for storing the data; the precautions to be taken when communicating the data; and the circumstances in which data is erased or destroyed.[16]

11 No. 11105/84 Eur. Ct. H.R. (1990).
12 **Id.** at § 28.
13 **Id**. at § 29.
14 **Id**. at § 26.
15 **Id**. at § 35. Note that these principles on surveillance partly come back in **Rotaru v. Romania**, No. 28341/95, Eur. Ct. H.R. (2000), where the Court looks at the law on processing data from surveillance for national security purposes.
16 **Huvig**, No. 11105/84, Eur. Ct. H.R. at § 34; **see**, in this regards, 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 welzijnswerk, 2003, VOL. 34/2, 155–98.

Table 1. Minimum safeguards that law should provide in order to avoid abuse of state powers **(Huvig)**.

Elements that surveillance law must provide, according to **Huvig**:
a) **categories** of people liable to be monitored
b) the **nature of the offenses** subject to surveillance
c) limits on the **duration** of such monitoring
d) **procedure** to be followed for processing the data
e) **precautions** to be taken when **communicating** the data
f) circumstances in which data is **erased** or destroyed
g) **Judicial control** [Eventual requirement]

An optional, seventh requirement concerned the need for a judge authorizing or reviewing surveillance measures: "the Court does not in any way minimise 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**."[17] This quote shows that the Strasbourg Court—though approving the French system of judicial control over 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 minimise the value of several of the safeguards**" is ambiguous, and the judgment therefore does not answer the question whether **a priori** judicial control is a necessary safeguard for surveillance in European human rights law. The reluctance of the Court can be explained by considering the different structure of criminal procedure in Europe.[18] If we wanted to consider **Huvig** as a model for **adversarial** systems, would it be sufficient that prosecutors authorize interceptions or, instead, would it be preferable that ordinary judges (acting as "control judges") authorize it?[19]

Another open question relates to the scope of **Huvig**: are the six or seven surveillance requirements generally applicable or only needed for individual surveillance measures in the context of criminal law? What about less intrusive measures or more intrusive measures (like mass surveillance)? What about surveillance led by secret services?

For our purposes here, the intrusiveness of telephone interceptions at issue in **Huvig** may well justify the high degree of detail in safeguards the Court required for surveillance laws.[20]

17 **Huvig**, No. 11105/84, Eur. Ct. H.R. at § 33.

18 French criminal procedure is based on the 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 prosecutors and not by investigative judges (thus, for example, there have not ben any "investigative judges" in the United Kingdom since the 1970s).

19 The following cases offer interesting stimuli to answer many of the above-mentioned questions. In particular, while in the next case (Uzun v. Germany, No 35623/05, Eur. Ct. H.R. (2010)) the safeguards required are consistently less strict than in **Huvig**, because of less intrusive measures of surveillance at issue (GPS tracking); the ECJ cases analysed infra (**Digital Rights Irelands** and **Schrems**) unexpectedly use the **Huvig** safeguards paradigm for mass surveillance, which is generally less intrusive and less delicate than individual surveillance.
The reason for this apparent contradiction is the increasing development of technologies which is blurring the difference between more intrusive and less intrusive surveillance measures, on the one hand; and a stricter scrutiny of the European Courts on surveillance after Snowden's revelations (**See** 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**, 10 UTRECHT L. REV. 1, 55, 61 (2014); **see also** Nora Loidleain, **Surveillance of communication data and Article 8 of the European Convention on Human Rights, in** Reloading Data Protection: Multidisciplinary Insights & Contemporary Challenges, 197 (S. Gutwirth et al. eds., 2014). However, these topics will be more profusely addressed in the next paragraphs.

20 **Huvig**, No. 11105/84, Eur. Ct. H.R. at § 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.**").

IV. The Inconsistent ECtHR Scrutiny of Article 8(2) ECHR: Strict v. Weak Scrutiny

The seven **Huvig** requirements with regard to the legality requirement in Article 8 ECHR place the bar very high and guarantee strict scrutiny. These requirements have been reiterated in many other cases like **Rotaru v. Romania** (2000),[21] **Kennedy v. United Kingdom** (2010),[22] **Gillian & Quinton v. United Kingdom** (2000),[23] **Zakharov v. Russia** (2015),[24] **Dragojević v. Croatia** (2015),[25] **Szabò and Vissy v. Hungary** (2016).[26]

However, no "robust" scrutiny or strict checking on surveillance safeguards took place in other surveillance cases such as **Uzun v. Germany** (2010)[27] and **Colon v. Netherland** (2012)[28] or in cases concerning workplace surveillance such as **Barbulescu v. Romania** (2016).[29]

Scholars have wondered why the Court sometimes adopts robust scrutiny and in other cases it does not. As for surveillance in the workplace (e.g., employers reading employees' emails and messages or installing CCTV cameras), the reason for less strict scrutiny could relate to the fact that there is a conflict between two "individuals' rights" (privacy of employees versus economic rights of employers), and no public interests are at issue.[30] As regards **Uzun v. Germany**, for example, scholars have suggested that the scrutiny of the Court was fainter because of the less intrusive means of interception at issue (geo-position-system instead of the telephone interceptions at issue in **Huvig**).[31]

The choice between strict and weak scrutiny is sometimes overtly political. Both **Gillian** and **Colon** concern not covert surveillance but patent physical surveillance: police "stop and search."[32] Though they are imilar cases—we see strict scrutiny in **Gilian** and weak scrutiny in **Colon**—revealing a tendency for increasingly "less robust scrutiny over policing powers" and a "greater reluctance of the Court to exert oversight in relation to counter-terrorist powers of general application than those of individual application."[33]

Most of the foregoing is guesswork, since the Court seldom theorizes its approach. Only sometimes does the ECtHR explicitly adopt strict scrutiny, either declaring it will interpret narrowly Article 8(2) ECHR or affirming a principle of "strict necessity." Such is the case in **Rotaru**[34] and **Kennedy**.[35] In **Szabò and**

21 No. 28341/95, Eur. Ct. H.R. (2000).
22 No. 26839/05, Eur. Ct. H.R. (2010).
23 No. 4158/05, Eur. Ct. H.R. (2000).
24 No. 47143/06, Eur. Ct. H.R. (2015).
25 No. 68955/11, Eur. Ct. H.R. (2015); **see** G. Gonzalez Fuster, **What Prior Judicial Scrutiny of Secret Surveillance Stands For**, 1–6 Eur. Data Protection L. Rev. 3 (2016).
26 No. 37138/14, Eur. Ct. H.R. (2016).
27 No. 35623/05, Eur. Ct. H.R. (2010).
28 No. 49458/06, Eur. Ct. H.R. (2012).
29 No. 61496/08, Eur. Ct. H.R. (2016)..
30 **See** Tor-Inge Harbo, **The Function of the Proportionality Principle in EU Law**, 16:2 EUR. L. J. 160 (2010) ("The court took a less coherent approach when applying the suitability and necessity test, applying a **strict test in cases where it believed that the individual interests should prevail and a less strict approach when it believed that public interest should prevail.**").
31 **See** Galetta & De Hert, **supra** note 17, at 55–75 (2014); **see also** Loideain, **supra** note 17, at 197.
32 **See** G. LENNON, (2016) Stop and search powers in UK terrorism investigations: a limited judicial oversight?, The International Journal of Human Rights, 20:5, 634-648,, at 634.. This needs to be the first full cite, but was not included. Ask author
33 **Id.** at 639.
34 **Rotaru**, No. 28341/95, Eur. Ct. H.R. at 15–16 ("That paragraph [Art. 8(2) ECHR], since it provides for an exception to a right guaranteed by the Convention, **is to be interpreted narrowly**. 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.").
35 **See Kennedy**, No. 26839/05, Eur. Ct. H.R. at 46 ("The Court recalls that powers to instruct secret surveillance of citizens are only tolerated under Article 8 to the extent that they are **strictly necessary** for safeguarding democratic institutions.").

Vissy,[36] the Court clearly affirms that "**given the particular character of the interference in question and the potential of cutting-edge surveillance technologies to invade citizens' privacy**, the requirement 'necessary in a democratic society' must be interpreted in this context as requiring '**strict necessity**.'"[37]

The EUCJ has also adopted, in its recent judgments, a strict necessity principle. In particular, in **Digital Rights Ireland Ltd**.[38] and then in **Schrems v. Data Protection Commissioner**,[39] the Court applieda "strict necessity" principle. Again, however, we find very little justification in terms of doctrine—little explanation of what does this principle mean?. Most likely, these statements influenced the ECtHR in judgments after **Digital Ireland** and **Schrems** (e.g., **Szabò and Vissy**).[40]

We should clarify that "strict necessity" refers to the three requirements of Article 8 ECHR, while the general discussion that we have conducted so far refers to the legality requirements of the surveillance framework. If all the above mentioned six (or seven) requirements from **Huvig** are applied by the Court, for us that is a case of "strict scrutiny." In general, the Court has never really set a clear doctrine about the strictness of its assessment: there are merely some sporadic suggestions and a multiform (or even ambiguous) use of the term "strict." In order to organise the case law of the ECtHR and to understand better when this Court adopts strict or weak scrutiny, we have identified in Table 2 the degree of scrutiny combined with other variables (means of interception, surveillance body, and the nature of the investigation).

Table 2. ECtHR scrutiny when applying Article 8(2) ECHR

ECtHR Surveillance Cases	Degree of scrutiny	How we can infer that the scrutiny is strict	Means of interception	Surveillance Body	What triggered surveillance	Conviction
Klass v. Germany	low		Telephone	Secret service	Non declared	No
Malone v. United Kingdom	**strict**	**Strict requirements**[41]	Telephone and metering	police	**Property crimes**	Yes
Huvig v. France	**strict**	**Strict requirements**[42]	Telephone tapping	police	**Tax crimes**	Yes
Rotaru v. Romania	**strict**	**The Court declares it**[43]	Public articles	Secret services	**Protesters against the government**	Yes

36 **Szabò**, No. 37138/14, Eur. Ct. H.R. at 33 (Article 8(2) "is to be narrowly interpreted."); **see also id**. at 38–39.
37 **Id**. at 38–39.
38 Case C-293/12, 2014 Eur. Ct. Just. §§ 52, 56, 62.
39 Case C-362/14, 2015 Eur. Ct. Just. § 92.
40 **See** Mark D. Cole & Annelies Vandendriessche, **From Digital Rights Ireland and Schrems in Luxembourg to Zakharov and Szabó/Vissy in Strasbourg: What the ECtHR Made of the Deep Pass by the CJEU in the Recent Cases on Mass Surveillance,** 2 EUR. DATA PROTECTION L. REV. 128 (2016).
41 Malone v. United Kingdom, No. 8691/79, Eur. Ct. H.R. §§ 67–68, 70.
42 Huvig, No. 11105/84, Eur. Ct. H.R. at § 34.
43 Rotaru, No. 28341/95, Eur. Ct. H.R. at 15–16
44 Kennedy, No. 26839/05, Eur. Ct. H.R. at 46.
45 As for the assessment of the Court in terrorism affairs, see Lennon, supra note 30, at 644.
46 Gillian, No. 4158/05, Eur. Ct. H.R. 34–35.
47 Zakharov, No. 47143/06, Eur. Ct. H.R. 57–58.
48 Dragojević, No. 68955/11, Eur. Ct. H.R. at 23–24.
49 Szabò, No. 37138/14, Eur. Ct. H.R. at 33, 37–38.

Kennedy v. United Kingdom	**strict**	**The Court declares it. Strict requirements.**[44]	Telephone tapping	Police & secret services	**Protester against the government**	No
Uzun v. Germany	low		Gps	Police	Terrorism[45]	No
Barbulescu v. Romania	low		e-mails	Employer	Work	No
Gillian v. United Kingdom	**strict**	**Strict requirements.**[46]	Stop and search	Police	**Protesters against the government**	Yes
Colon v. Netherlands	low		Stop and search	Police	Prevention of life crimes	No
Zakharov v. Russia	**strict**	**Strict parameters used (the same as Huvig).**[47]	Telephone tapping	Secret service	**Protesters against the government**	Yes
Dragojević v. Croatia	**strict**	**Strict parameters (the same as Huvig).** [48]	Telephone tapping	Police	**Drug crimes**	Yes
Szabò v. Hungary	**strict**	**The Court declares it.**[49]	Telephone tapping	Police	**Protesters against the government**	Yes

The Table allows us to see that the Court adopted robust scrutiny in cases in which a) the claimant was a protester against the government (**Rotaru, Gillian, Zakharov, Szabò**) or b) when an "economic crime" was at issue (tax evasion, forgery, drug dealers) (**Malone, Huvig, Dragojevi**). On the other hand, the scrutiny was weak when terrorism (**Uzun**), safety (prevention of murder, **Colon**) or workplace surveillance (**Barbulescu**) were at issue. From these findings, we can infer that the ECtHR does a strict balancing when there is no "vital" security interest at issue (economic crimes, anti-government protesters) or in general when public interests at issue are more political (anti-government) or economic (tax, forgery, drugs trade). The court is less strict when public interests at issue concern the protection of the life of an individual (terrorism, murder).

When surveillance is directed to protect (including indirectly) the safety of individuals, the ECtHR seems to accept a non-strict balancing approach, because life should typically prevail over privacy.[50] Whereas where other issues are at stake—economic crimes, anti-government protesters—privacy as a human right of individuals should typically prevail and so the scrutiny is stricter. Additionally, in cases of anti-government protesters, the risks of limiting democracy are high (see below on the empirical check of the rule of law effectiveness).

Again, all this is educated guesswork. What is sure is that the Court uses the flexibility afforded by the

50 **See, e.g.**, **General Data Protection Regulation** (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), recitals n. 46, 73, 112, where it appears clearly that any restriction to privacy and data protection is tolerated if it is due to the protection of "vital interests, including physical integrity" or to the "the protection of human life especially in response to natural or manmade disasters, the prevention, investigation and prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security."

wording of Articles 8 and 13 ECHR and so it adopts sometimes a weak scrutiny approach, and sometimes a robust scrutiny approach. The Court never explicitly explains its reasons for the different measures of scrutiny, but the logic inferred here—if confirmed in the future by other studies—could be a useful tool to foresee the degree of scrutiny the Court will apply under Article 8(2) ECHR in different circumstances.

V. Article 13 ECHR and an Effective Remedy for Secret Service Surveillance

Surveillance is not always conducted by private actors (like employers) or by law enforcement authorities (like the police); it is often conducted by secret services, or what in America would be referred to as "national security" services. The supervision of secret service surveillance is a delicate issue, which was first discussed in **Klass** (1978) and later on in judgments such as **Rotaru** (2000) and **Szabò & Vissy** (2016)**.**

For the sake of clarity, we distinguish between "criminal law surveillance or criminal surveillance" and "intelligence surveillance or secret services surveillance." The first is generally led by police for the purpose of crime detection; the latter by secret service agencies for the purpose of national security, public safety, and general national strategic interests.[51] In practice, we see that a system of **judicial overview**, generally based on judicial review, is always used for criminal law surveillance, whereas intelligence surveillance is sometimes (in some countries) controlled via **judicial overview** but more often via alternative systems of safeguards—**non judicial overview**.

This difference in regulation is due to the different purposes for which the surveillance is conducted: while for criminal law investigations ordinary judges are the most appropriate supervisory authority; intelligence affairs involve a more political evaluation, which is often better assessed by non-judiciary authorities (ministers, national agencies, parliamentary committees, etc.). Also, criminal law surveillance usually leads to prosecution and is therefore usually assessed by judges during ordinary trials, whereas secret service surveillance usually remains secret even after it is finished.

This separation of tasks and oversight mechanisms between police and secret services is typical of the German legal system, but is echoed in several other systems. It is based on the so-called "**Trennungsgebot**,"[52] a German constitutional principle according to which the differences between police and secret service activities in terms of **purposes** (national security vs. crime detection) and **means** (police investigations are usually led by investigative judges or prosecutors within criminal procedure law) impose strictly separate regulations of the national bodies in order to preserve the rule of law.

In other countries, like the United Kingdom or Russia, this separation is not considered a constitutional safeguard. An example is the UK Regulation of Investigatory Power Act (RIPA) of 2000 (assessed in **Kennedy v. UK** discussed below), which regulates both police and secret service surveillance in the same manner. Another example is the Russian Operational-Search Activities Act (OSAA) of 12 August 1995 (assessed in **Zakharov v. Russia**, discussed below), which is "applicable to the interception of communications both in the framework of criminal proceedings and outside such framework" and does not make a distinction according to the purposes of thesurveillance.[53]

51 **See** Hans Born & Marina Caparini, Democratic Control of Intelligence Services, 5–6 (Routledge 2007) (regarding the specific purposes of secret services: counterintelligence and security intelligence).

52 **See, e.g**., A. Dorn, Das Trennungsgebot in verfassungshistorischer Perspektive: zur Aufnahme inlandsnachrichtendienstlicher Bundeskompetenzen in das Grundgesetz vom 23. Mai 1949, (Verlag Duncker & Humblot, 2004); **see also** J. Singer, Das Trennungsgebot – Teil 1: Politisches Schlagwort oder verfassungsrechtliche Vorgabe?, (Die Kriminalpolizei, 2006).

53 According to OSAA, "the aims of operational-search activities are: (1) the detection, prevention, suppression and investigation of criminal offences and the identification of persons conspiring to commit, committing, or having committed a criminal

This non-separation between police and secret services has been increasing lately. For example, a recent Hungarian law regulates both police and secret services surveillance without a strict separation: the police can act both for the purpose of crime detection and for the purpose of national security, which brings them into the territory traditionally occupied by secret services.[54] This example illustrates a trend in many states to provide police forces with broader and broader powers, especially in areas once reserved to secret services, such as terrorism investigation or national security.[55] Another trend, relevant here, is the increasing reduction of judicial procedural guarantees towards police and prosecutors' activity.[56]

With regard to judicial oversight in secret service surveillance, the ECHR provides in Article 13 that "everyone whose rights and freedoms as set forth in this Convention are violated shall have an **effective remedy** before a national authority," but it does not require judicial redress as the only effective remedy, as already discussed. For the ECtHR, judges are an "effective remedy provided by national authorities," but it has never stated that Article 13 strictly requires judicial review. On the contrary, the Court has often accepted alternative remedies, including for secret services surveillance. In the Court's view, "the authority referred to in Article 13 … may not necessarily in all instances be a judicial authority in the strict sense. Nevertheless, the powers and procedural guarantees an authority possesses are relevant in determining whether the remedy before it is effective."[57]

In the following sections, we will describe how the Court has differently interpreted the flexible wording of Articles 8 and 13 ECHR,[58] especially in the field of secret service surveillance.

offence; (2) the tracing of fugitives from justice and missing persons; (3) obtaining information about events or activities endangering the national, military, economic or ecological security of the Russian Federation." **Zakharov**, No. 47143/06, Eur. Ct. H.R. 6–7.

54 On the 1st of January 2011, a specific Anti-Terrorism Task Force was established within the Hungarian **police** force under the control of the Police Act, amended by a reform in 2011 which gave the task force prerogatives **in the field of secret intelligence gathering**, including surveillance with recording and secret house search.

55 Lennon, **supra** note 30, at 634–48.

56 J. Vervaele, **Surveillance and Criminal Investigation: Blurring of Thresholds and Boundaries in the Criminal Justice System?**, 115 **in Reloading Data Protection: Multidisciplinary Insight and contemporary challenge,** Dodrecht (S. Gurtwirh, R. Leenes, & P. De Hert eds., 2014).

57 **See Klass**, No. 5029/71, Eur. Ct. H.R. at 25;.**see also** the Golder judgment of 21 February 1975, Series A no. 18, p. 16, para. 33.

58 **See, e.g.**, Fuster, **supra** note 23, 4.

VI. The "Non-Judicial Oversight" from Klass to Szabò

Klass (1978) is the first case in which ECtHR accepted non-judicial oversight as adequate in the light of Articles 8 and 13 ECHR.[59] The Court had to assess a new German law organising the supervision of surveillance methods (like interception of telephone conversations and postal letters) via two different, alternative methods: judicial control over criminal law investigations[60] and non-judicial control over secret service surveillance.[61] The starting point in the Court's reasoning is its understanding that the "rule of law implies that an interference by the executive authorities with an individual's rights should be subject to an effective control which should normally be assured by the **judiciary**, at least in the last resort, **judicial control** offering the **best guarantees** of independence, impartiality and a proper procedure."[62] A fortiori, in a field where "abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, **it is in principle desirable to entrust supervisory control to a judge**."[63]

Nevertheless, "having regard to the nature of the supervisory and other safeguards provided for" by the law,[64] the Court "conclude[d] that the exclusion of judicial control does not exceed the limits of what may be deemed necessary in a democratic society."[65] Therefore, the ECtHR accepts, under certain conditions, a system of non-judicial review over secret surveillance,[66] though it considers judicial review highly preferable.

We saw earlier that control of surveillance, whether judicial or otherwise, can operate either **ex ante** or **ex post**. **Klass** teaches that the number of options is considerable in the light of the acceptance of non-judicial oversight as an alternative or complement to traditional, judicial oversight.

In **Szabò and Vissy** (2016), the Court takes a much more critical view of non-judiciary oversight systems. Without abandoning **Klass** doctrine (accepting a "two tracks" system of supervision), the Court scrutinizes oversight systems—especially those of a more political nature—much more strictly, advancing the requirement that whatever system of oversight is used, it needs to make possible an 'assessment of strict necessity.'[67]

59 The case deals with legislation passed in Germany in 1968 ("G10" Law) amending Article 10.2 of the German Constitution which authorized in certain circumstances secret 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, 8 and 13 of the ECHR. 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 the exercise by the individual of the right guaranteed to him under paragraph 1 (art. 8-1) and the necessity under paragraph 2 (art. 8-2) to impose secret surveillance for the protection of the democratic society as a whole." **Klass**, No. 5029/71, Eur. Ct. H.R. at 23,.

60 Under Article 100 (b) of the Code of Criminal Procedure, surveillance measures "may be ordered only by a court and for a maximum of three months; they may be renewed. In urgent cases, the decision may be taken by the public prosecutor's department but to remain in effect it must be confirmed by a court within three days." **See Klass**, No. 5029/71, Eur. Ct. H.R. at 9.

61 In particular, the German review system over secret service surveillance was based on two Parliamentary committees: "a Board consisting of five Members of Parliament, appointed by the Bundestag in proportion to the parliamentary groupings, the opposition being represented on the Board" and a Commission (the "G 10 Commission") consisting of "three members, namely, a Chairman, who must be qualified to hold judicial office, and two assessors." Klass, § 21. The Commission members are appointed for the current term of the Bundestag by the above-mentioned Board after consultation with the Government; "they are completely independent in the exercise of their functions and cannot be subject to instructions." **Klass**, No. 5029/71, Eur. Ct. H.R. at 8. The competent Minister must, at least once every six months, report to the Board on the application of the G 10. In addition, "the Minister is bound every month to provide the G 10 Commission with an account of the measures he has ordered (Article 1, § 9). In practice, and except in urgent cases, the Minister seeks the prior consent of the Commission." **Id**. at 19.

62 **Id.** at 20.

63 **Id**.

64 **Id**. ("The Parliamentary Board and the G 10 Commission are independent of the authorities carrying out the surveillance, and are vested with sufficient powers and competence to exercise an effective and continuous control.").

65 **Id**.

66 **Id.** at 22—23.

67 See supra, Part IV. Note that the Court will also consider and accept hybrid systems of supervision mixing judicial and non-judicial elements, as is the case **Kennedy**, where a hybrid "quasi-judicial" control was tested.

Szabò and Vissy deals with legal provisions creating new police powers concerning national security, of which some are typical of secret services.[68] The Court notes that the Hungarian law at issue in that case does not offer a proper framework of prior **judicial review** for police investigations acting for the purpose of national security. According to the Court, the supervision created by the Hungarian law, eminently political and carried out by the Minister of Justice who appears to be formally independent of both the police force and of the Minister of Home Affairs—"is inherently incapable of ensuring the **requisite assessment of strict necessity** with regard to the aims and the means at stake. In particular, although the security services are required, in their applications to the Minister for warrants, to outline the necessity as such of secret information gathering, this procedure does not guarantee that an assessment of **strict necessity** is carried out, notably in terms of the range of persons and the premises concerned."[69]

In particular, the Court restated that "it is desirable to entrust supervisory control to a judge,"[70] and, specifically in cases like **Szabò**, "the external, preferably judicial, **a posteriori** control of secret surveillance activities, both in individual cases and as general supervision, gains its true importance."[71]

The departure from **Klass** is evident: the Court explained that it "recalls that in **Klass and Others** a combination of oversight mechanisms, short of formal judicial control, was found acceptable," but that was in particular because of "an initial control effected by an official qualified for judicial office,"[72] which is not provided by the Hungarian scheme of authorization.[73]

In other words, it seems that, according to the ECtHR, the general system of non-judicial oversight is appropriate only if it is somehow related to a judicial office.

68 On the 1st January 2011, a specific Anti-Terrorism Task Force was established within the Hungarian **police** force under the control of the Police Act, amended by a reform in 2011 which gave the task force prerogatives **in the field of secret intelligence gathering**, including surveillance with recording and secret house search, checking and recording the contents of electronic or computerized communications and opening of letters and parcels, all this without the consent of the persons concerned. The 2011 reform of the Hungarian Police Act allows surveillance activities in two cases: on the one hand, in cases where secret surveillance is linked to the investigation of **certain specific crimes** enumerated in the law, the surveillance is subject to **judicial authorization** (Section 7/E (2) of the 2011 Hungarian Police Act). On the other hand, in cases where secret surveillance takes place **within the framework of intelligence gathering for national security**, the surveillance takes place within the framework of intelligence gathering for national security, the surveillance is authorized by the Minister in charge of justice, in order to prevent terrorist acts or in the interests of Hungary's national security, or in order to rescue Hungarian citizens from capture abroad in war zones, or in the context of terrorist acts (Section 7/E (3) of the 2011 Hungarian Police Act). In June 2012, the two applicants denounced that the prerogatives presented above under section 7/E (3) breached their right to privacy. They argued that the framework on secret surveillance linked to the investigation of particular crimes provided more safeguards for the protection of the right to privacy than the provision on secret surveillance measures for national security purposes.

69 **Szabò**, No. 37138/14, Eur. Ct. H.R. at 39. Regarding the procedures for redressing any grievances caused by secret surveillance measures, the Court noted that the executive did have to give account of surveillance operations to a parliamentary committee. However, it could not identify any provisions in Hungarian legislation permitting a remedy granted by this procedure to those who are subjected to secret surveillance but, by necessity, are not informed about it during their application. Nor did the twice-yearly general report on the functioning of the secret services presented to this parliamentary committee provide adequate safeguards, as it was apparently unavailable to the public. Moreover, the complaint procedure outlined in the National Security Act also seemed to be of little relevance, since citizens subjected to secret surveillance measures were not informed of the measures applied. Indeed, no notification of secret surveillance measures is foreseen in Hungarian law. The Court reiterated that as soon as notification could 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. **Id**. at 43.

70 **Id.** at 40–41.

71 **Id.** at 41.

72 **Klass**, No. 5029/71, Eur. Ct. H.R. at 21—22.

73 **Szabò**, No. 37138/14, Eur. Ct. H.R. at 43.

VII. Alternative Tracks: Quasi-Judiciary and Hybrid Systems

Before one concludes on the basis of **Szabò and Vissy** that all oversight needs to involve judges, it is worthwhile to go back to **Kennedy v. UK** (2010), where the Court assessed positively other forms of (non-judicial) surveillance oversight. The Court focused on the specific surveillance framework established by the UK **Regulation of Investigatory Power Act (RIPA)** of 2000 which utilizes two supervisory bodies: the Interception of Communications Commissioner and the Investigatory Powers Tribunal (IPT).[74]

The **Kennedy** Court notes that the Commissioner is independent of both the executive and the legislature, and is a person who holds or has held high judicial office. The obligation on intercepting agencies to keep records ensures that the Commissioner has effective access to details of surveillance activities undertaken. Therefore, "the Court considers that the Commissioner's role in ensuring that the provisions of RIPA and the Code are observed and applied correctly is of particular value."[75] As for the Investigatory Powers Tribunal, the Court—though recalling its previous indication that judicial supervisory control is in principle desirable in a field where abuse is potentially so easy in individual cases and having such harmful consequences—"highlights the extensive jurisdiction of the IPT to examine any complaint of unlawful interception and emphasises that "the IPT is an independent and impartial body, which has adopted its own rules of procedure."[76]

In conclusion, the combination of an **ex ante** authorization by an independent Commissioner (which holds judicial office) and a **post hoc** review by a special court (IPT) can well approach the requirement of judicial control.[77] In particular, the important characteristics that a quasi-judicial system of control should have are independence, wide jurisdiction (any person may apply to it), and effective powers to access data and documents and to react accordingly.[78]

A different form of quasi-judicial oversight (which has not been assessed by the ECtHR yet) is be the Belgian Commission on "exceptional methods of surveillance,"[79] an administrative commission comprised of three security-cleared magistrates (acting in a non-judicial capacity) appointed by the executive, which gives "binding advice" to the security services when they apply to use "exceptional measures" (including surveillance).[80]

Some might be tempted to label these two examples as 'judicial oversight.' For example, the Council of Europe Commissioner for Human Rights has defined the UK oversight system set by RIPA a "judiciary"

74 The first is tasked with overseeing the general functioning of the surveillance regime and the authorization of interception warrants in specific cases. The latter must examine any complaint of unlawful interception by any person who suspects that his communications have been or are being intercepted may apply to the IPT. The jurisdiction of the IPT does not, therefore, depend on notification to the interception subject that there has been an interception of his communications.

75 **Kennedy**, No. 26839/05, Eur. Ct. H.R. at 51.

76 Id. at 51–52. Note also that "members of the [IPT] tribunal must hold or have held high judicial office or be a qualified lawyer of at least ten years' standing." Id. at 19.

77 **See** P. De Hert & F. Boehm, **The Rights of Notification after Surveillance is over Ready for Recognition?,** Digital Enlightenment Yearbook 2012, 33.

78 **See** A. Deeks, **An International Legal Framework for Surveillance**, 55:2 VA. J. INT'L L.,391–68, 362 (2014); **see also** The Council of Europe Commissioner for Human Rights**, Democratic and effective oversight of national security services**, 13 (2015) ("on the effectiveness of oversight bodies").

79 Its full title is "La commission administrative chargée de la surveillance des méthodes spécifiques et exceptionnelles de recueil de données des services de renseignement et de sécurité."

80 Belgium 2010, Articles 18(2)(3)(9)(10),43(1); **see also** The Council of Europe Commissioner for the Human Rights, **supra** note 76, at 56.

oversight.[81] On the other hand, more political oversight, like the system set by G10 Law in Germany (and addressed in **Klass v. Germany**), is sometimes defined as a "quasi-judicial" supervisory system.[82] In our view, systems like the one in the United Kingdom and Belgium should be understood as "quasi-judicial." We prefer to reserve the term "judicial oversight" for control operated by ordinary courts, while by "quasi-judicial" we mean all special supervisory bodies that are independent and have effective powers of information and reaction (and eventually of auto-regulation).

VIII. Reinforced Quasi-Judicial Systems: The Case of Data Protection Authorities

Another well-known example of quasi-judicial oversight are the Data Protection Authorities established in most European states to monitor processing activities by governments, corporations, and private persons. Data Protection Authorities are specific, independent national bodies created by European data protection laws—such as EU Data Protection Directive (1995/46/EC)—in order to enforce personal data protection principles and rules and to provide individuals with a guarantee similar to an Ombudsman. Data Protection Authorities do not replace the role of the courts, because they are administrative bodies.[83] But are they an effective remedy when it comes to answering questions about surveillance raised by concerned citizens?

The role of these new authorities was scrutinized both by the ECtHR in **Segerstedt-Wiberg and others v. Sweden** (2003) and by the EUCJ, in the **Schrems** Case (2015).[84]

Segerstedt-Wiberg and others v. Sweden deals with Article 13 ECHR and the question of Data Protection Authoritie' roles, and it affirms that, in view of their competencies, Data Protection Authorities can be considered government authorities that offer an actual possibility of appeal, within the meaning of Article 13 ECHR if it has **effective powers** to stop data processing and to have data destroyed.[85]

The **Schrems Case** concerns the transfer of personal data from European Union countries to the United States, regulated by the European Commission Decision 2000/520/EC, which implemented Article 25 of the Data Protection Directive, 95/46/EC.[86] After Edward Snowden's revelations and the consequential scandal regarding the surveillance program PRISM of the US National Security Agency, the applicant considered that the law and practices of the United States offer no real protection against surveillance by the United States and in general offer much lower safeguards than required by the EU data protection paradigm. The EUCJ stated that the existence of a Commission decision declaring 'adequate' certain parts

81 The Council of Europe Commissioner for the Human Rights, **supra** note 76, at 56.
82 **Id.** at 57.
83 **See** Antonella Galetta & Paul De Hert, **The Proceduralisation of Data Protection Remedies under EU Data Protection Law: Towards a More Effective and Data Subject-Oriented Remedial System?** 8:1 REV. EUR. ADMIN. L. (REALaw) 125–51 (2015) (on the three-layer system of remedies built in to European data protection law). The right to remedy data protection breaches is laid down in Directive 95/46/EC (Art. 22), as well as in the Council of Europe Data Protection Convention no. 108 (Art. 8 (d)). As a result of an unlawful processing operation, this right is coupled with the right to obtain compensation for the damage suffered. These rights are implemented in Member States' law with some variations. The right to remedy data protection violations can be exercised in several ways under EU law. The remedial system in place relies on individual initiatives taken by citizens who need to exercise their data protection rights by contacting the data controller or processor first. Secondly, violations can be remedied by Data Protection Authorities (Data Protection Authorities), which assist individuals and enforce data protection law through the exercise of administrative power. Thirdly, all kinds of courts can remedy data protection violations (from civil and commercial courts to criminal courts). Fourthly, European courts can provide remedies for data protection violations.
84 Case C-362/14, Data Protection Commissioner v. Schrems, 2015.
85 De Hert, **supra** note 8, at 26.
86 According to that article, the Commission may find that a third country ensures an adequate level of protection and so it can adopt a decision to that effect. Consequently, the transfer of personal data to the third country concerned may take place.

of the American legal system in terms of data protection, cannot eliminate or even reduce the national supervisory authorities' (i.e., the Data Protection Authorities') powers,[87] especially since the contested decision of the Commission—Decision 2000/520[88]—does not contain any redress mechanism for European citizens and doesn't refer to the existence of effective legal protections against interference of that kind.[89]

In principle, one could consider European data protection law's insistence on a system of data protection authorities to be an alternative to judicial review. The system of requirements provided by data protection law is based on several strict safeguards—the "consent" rule, the principle of necessity, controller's duties, processor's duties, individual rights such as the right to data access, the right to object, the right to information, the right to rectification, etc.—that can be 'easily' checked by these authorities so long as they have sufficient effective powers, such that judicial control is not as necessary as in secret surveillance.[90]

In the **Schrems** Case, the Court[91] affirms that "the very existence of **effective judicial review** designed to ensure compliance with provisions of EU law **is inherent in the existence of the rule of law**."[92] Interestingly, the Court seems to compare "judicial review" to the function of Data Protection Authorities, implicitly comparing traditional judicial powers in reviewing surveillance activities (analysed above) and the typical functions of Data Protection Authorities, as provided by Article 28 of the Data Protection Directive.[93] In **Schrems,** the EUCJ does not consider judicial review as a necessary requirement, but it assesses Data Protection Authorities as effective remedies provided by national authorities.

We think it is indeed possible to understand a Data Protection Authority's tasks within the "quasi-judicial control" paradigm settled in **Kennedy v. UK** (see table 3). This authority can indeed act both as an **ex ante** authorization authority (like the UK Interception of Communications Commissioner) and as **post hoc** review authority (like the UK Investigatory Powers Tribunal).

Its functioning as an **ex ante** authorization authority is made possible by Article 18 of the Data Protection Directive: "member States shall provide that the controller or his representative, if any, **must notify the supervisory authority** referred to in Article 28 before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes." Consequently, Data Protection Authorities, "following receipt of a notification from the controller," shall carry out "**prior checks**" over "processing operations likely to present specific risks to the rights and freedoms of data subjects."[94]

A Data Protection Authority's role as a **post hoc** review authority is laid down in Article 28 of the Data

87 Indeed, the access enjoyed by the United States constituted an interference with the right to respect for private life and such interference is contrary to the principle of proportionality**. Schrems**, 2015 Eur. Ct. Just. §§ 66, 71–97.

88 "Commission Decision 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."

89 **Schrems**, 2015 Eur. Ct. Just. § 90. Moreover the Commission has found that the United States authorities were able to access the personal data transferred from the EU to the United States and process it in a way incompatible, with the purposes for which it was transferred. Therefore the Commission's decision allowing data transfers from the EU to the USA was declared invalid. **See** X. Tracol, **"Invalidator" strikes back: The harbour has never been safe**, 32 COMPUTER L. & SECURITY REV., 361 (2016).

90 **See** De Hert, **supra** note 26.

91 Following Article 47 of the EU Charter of Fundamental Rights, which echoes Article 13 of ECHR: "Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article. Everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law. Everyone shall have the possibility of being advised, defended and represented. Legal aid shall be made available to those who lack sufficient resources in so far as such aid is necessary to ensure effective access to justice."

92 **Schrems**, 2015 Eur. Ct. Just. § 95.

93 **See id.** in conjunction with §§ 99–103.

94 Article 20, DP directive.

Protection Directive, providing rules and powers of Data Protection Authorities, and there we can find interesting parallels to the UK Investigatory Power Tribunal. A Data Protection Authority is "an independent and impartial body,"[95] and a public "authority acting with complete independence."[96]

Moreover, as for the power of "effective access to details of surveillance activities"[97] and to all related "documents and information"[98] which is provided for UK IPT, Data Protection Authorities have "powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties."[99]

Furthermore, as for the scope of jurisdiction, **Kennedy** refers to the "extensive jurisdiction of the IPT (Investigatory Powers Tribunal) to examine **any complaint** of unlawful interception."[100] Similarly, Article 28(4) states that Data Protection Authorities "shall hear claims lodged by **any person**, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data".[101]

Finally, as for the power of intervention, the UK IPT can "**quash any interception order, require destruction of intercept material and order compensation to be paid**." Analogously, Data Protection Authorities have "effective **powers of intervention**, such as, for example, that of … **ordering** the **blocking, erasure or destruction of data**, of **imposing** a temporary or definitive **ban on processing**, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions."[102] Moreover, as for the power (of IPT) to "adopt its own rules of procedure," we must acknowledge that in several member States auto-regulation is also a reality for Data Protection Authorities.[103]

In sum, as the EUCJ noted, "national supervisory authorities must be able to examine, with complete independence, any claim concerning the protection of a person's rights and freedoms in regard to the processing of personal data relating to him,"[104] and this too is typical of Data Protection Authorities.[105] It therefore seems clear that Data Protection Authorities guarantee a level of safeguards that is perfectly comparable to the best-developed quasi-judiciary supervisory systems and it is not just a coincidence that Data Protection Authorities have been defined an "indispensable link in the modern constitutional state."[106]

95 **Kennedy**, No. 26839/05, Eur. Ct. H.R. at 51–52..
96 Article 28 (1), 95/46/EC; **see also** recital 62: "Whereas the establishment in Member States of supervisory authorities, exercising their functions with complete independence, is an essential component of the protection of individuals with regard to the processing of personal data." About the independence of the Data Protection Authorities, **see also** the EUCJ in Case C-518/07, Commission v. Germany (2010), Case C-614/10, Commission v. Austria (2012) and Case C-288/12, Commission v. Hungary (2014).
97 **Kennedy**, No. 26839/05, Eur. Ct. H.R. at 20; **see also** The Council of Europe Commissioner for Human Rights, **supra** note 76, at 13.
98 **Kennedy**, No. 26839/05, Eur. Ct. H.R. at 20.
99 Article 28(3)
100 "It has jurisdiction to investigate **any complaint** that a person's communications have been intercepted and, where interception has occurred, to examine the authority for such interception." **Kennedy**, No. 26839/05, Eur. Ct. H.R. at 20.
101 Article 28(4) (emphasis added).
102 Article 28(3).
103 **See, e.g.**, Ducth Data Protection Authorities, as analysed by De Hert**, supra** note 8, 30 ("A legal framework is needed that provides **discretionary powers that allow the Dutch Data Protection Authorities to decide the enforcement methods** (and also allows it to take no action if desired) and that provides for the organisation of a consultation procedure prior to the current imposition of sanctions. Call it negotiated enforcement or enforced negotiation.") (emphasis added).
104 **Schrems**, 2015 Eur. Ct. Just. § 99.
105 **See also** De Hert, **supra** note 8, 30.
106 **Id.**

Table 3. Comparison between quasi-judicial system set by **Kennedy** and Data Protection Authorities assessed by **Schrems** and **Segerstedt-Wiberg**

	Quasi-judiciary (Kennedy)	Data Protection Authorities (**Schrems** and **Segerstedt-Wiberg**)
Establishment	Commissioner is "**independent of the executive and the legislature and is a person who holds or has held high judicial office**" (§ 167) **IPT is an independent and impartial body**, which has adopted its own rules of procedure. (§ 167)	National "authorities acting with **complete independence**". Article 28(1), 95/46/EC directive
Jurisdiction	**Extensive jurisdiction** of the IPT (Investigatory Powers Tribunal) to examine **any complaint of unlawful interception**. It has jurisdiction to investigate any complaint that a person's communications have been intercepted and, where interception has occurred, to examine the authority for such interception (§ 76).	Data Protection Authorities "shall hear claims lodged by **any person,** or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data". Article 28(4), 95/46/EC directive
Powers to access to information	Commissioner has **effective access to details** of surveillance activities undertaken. The IPT has the power to require a relevant Commissioner to provide it with all such assistance as it thinks fit. Section 68(6) and (7) requires those involved in the authorisation and execution of an interception warrant to disclose or provide to the IPT all documents and information it may require (§78).	Data Protection Authorities have "**powers of access to data** forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties". Article 28(3), 95/46/EC directive
Powers of intervention	**"In the event that the IPT finds in the applicant's favour, it can, inter alia, quash any interception order, require destruction of intercept material and order compensation to be paid (see paragraph 80 above)".** (§167)	Data Protection Authorities have "**effective** powers of intervention, such as, for example, that of (…) ordering the blocking, e**rasure or destruction of data**, of **imposing a temporary or definitive ban on processing,** of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions" Article 28(3), 95/46/EC directive

Interestingly, Data Protection Directive (95/46/EC) also creates an interesting link between Data Protection Authorities and the judicial system: according to Article 28(3), Data Protection Authorities have the "power to engage in legal proceedings where the national provisions adopted pursuant to this Directive have been violated or to bring these violations to the attention of the judicial authorities." This could be interpreted to reveal the non-autonomy of Data Protection Authorities from the judicial power. But it should be interpreted as an interesting safeguard for any non-judicial review system: upon certain conditions (e.g., serious violations of law), non-judicial authorities should engage ordinary judges in the decision because it will enhance the protection of individuals' rights.[107] Furthermore, considering that interceptions are a form of data processing, Data Protection Authorities could in principle be invested with the control of any form of surveillance.

In conclusion, **Segerstedt-Wiberg** and **Schrems** have emphasised the role of Data Protection Authorities as a safeguard comparable to the most developed "quasi-judicial control" systems. The only problem for Data Protection Authorities is that in national legal systems they are often excluded entirely from the domain of surveillance in order to avoid an overlap between Data Protection Authorities and other entities specifically committed to surveillance control (e.g., the G10 Commission in Germany).[108] However, there are several opportunities that should be explored in the near future: taking into account the new approval of the GDPR and the new proposal for a directive on the use of personal data for police purposes ("Police directive"),[109] EU Member States may choose to "use" the supervisory authorities of a Data Protection Authority for monitoring compliance with the Police Directive, or to set up "special" supervisory authorities for the purposes of the Police Directive.[110]

107 Compare this double oversight (independent authorities at the first step and judges at the second eventual step): it "could enable close, independent scrutiny providing a robust method of oversight." Lennon, **supra** note 30, at .643; **id**. ("The authorization of oversight powers could be subjected to **judicial confirmation**, whether as an alternative or **in addition to oversight by other bodies**. This could enable close, independent scrutiny providing a robust method of oversight.") (emphasis added).

108 **See** The Council of Europe Commissioner for Human Rights, **supra** note 76, at 52.

109 **Proposal for a Directive of The European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data**, EUR-LEX (2012), **available at** http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52012PC0010.

110 For example, Belgium already decided to set up a special police and criminal justice data protection authority (DPA).

IX. "Good Enough Judicial Oversight" and Empirical Checks

We can summarize the foregoing as follows: the ECtHR considers that "control by an independent body, normally a judge with special expertise, should be the rule and substitute solutions the exception, warranting close scrutiny,"[111] but neither judicial **ex ante** authorization nor judicial **post hoc** review are absolute requirements.[112]

Judicial oversight is generally considered the best safeguard for human rights[113] since judges are generally regarded as impartial, independent, and consequently unlikely to be swayed by political considerations surrounding secret service activity (which might for example influence a minister making authorisation decisions). Judges are also regarded as "being better suited to assessing legal criteria such as necessity and proportionality, which is clearly important when the measures sought may have significant human rights implications."[114]

But the foregoing should not be understood as an exclusive preference in law for judicial oversight. For example, the Geneva Academy of International Humanitarian Law and Human Rights has affirmed that an independent judiciary should scrutinize surveillance requests,[115] but it also argues that judicial oversight alone is not enough. Rather, all three branches of government should be engaged because many states have not established effective, independent oversight mechanisms to monitor surveillance practices.[116] Equally careful is the Council of Europe Commissioner for Human Rights and the Venice Commission. Both emphasize that judicial control is not a panacea that guarantees respect for human rights in the authorisation and use of intrusive measures by security services.[117]

Scholars have underlined several potential drawbacks to judicial authorisation or oversight. First, the lack of independence and impartiality in countries where judges are not fully independent, and second, that expertise is integral to the efficacy of judicial authorisation.[118] Judges with limited experience in security matters may be highly reluctant to second-guess the national security assessments of a security service official applying for a warrant.[119] Even for a specialised judge, the invocation of "national security" is very

111 **See Szabò**, No. 37138/14, Eur. Ct. H.R. at 40–41; **see also Klass**, No. 5029/71, Eur. Ct. H.R. at 42, 55.

112 **See, e.g.**, **Szabò**, No. 37138/14, Eur. Ct. H.R. at 40–41 ("The ex ante authorisation of such a measure is not an absolute requirement per se, because where there is extensive post factum judicial oversight, this may counterbalance the shortcomings of the authorisation."); **see also Kennedy**, No. 26839/05, Eur. Ct. H.R. at 51–52.

113 Council of Europe Parliamentary Assembly Recommendation 1402 (1999), **Control of internal security services in Council of Europe member States**, **available at** http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=16689&lang=en.

114 The Council of Europe Commissioner for Human Rights, **supra** note 76, at 55. It is interesting to notice that similar reflections can also be found in the late 18th century jurisprudence of English High Court: judicial control on surveillance is highly preferable to avoid arbitrary powers that can adversely affect rights of individuals. In the late 1700s a number of judgments strictly scrutinized such "general warrants" delivered by the Secretary of State arguing that only a judge can order search and seizure of letters, papers, etc. At the same time, the arbitrary powers of administrative officers (as the Secretary of State) for more "political" purposes of investigation (i.e. national interests) were looked askance. **See** Wilkes v. Wood, 98 Eng. Rep. 489, 489–99 C.P. 1763 in **The Founders' Constitution**, Volume 5, Amendment IV, Document 4, **available at** http://presspubs.uchicago.edu/founders/documents/amendIVs4.html; **Entick v. Carrington**, 95 Eng. Rep. 807 K.B. 1765, in **The Founders' Constitution**, Volume 5, Amendment IV, Document 6, **available at** http://presspubs.uchicago.edu/founders/documents/amendIVs6.html; **see also** B. WHITE, THE CANADIAN FREEHOLDER: IN THREE DIALOGUES BETWEEN AN ENGLISHMAN AND A FRENCHMAN, SETTLED IN CANADA (Vol. II, London 1779) **distributed by** Internet Archive of the Univ. of Cal..

115 Geneva Academy, **The Right to Privacy in the Digital Age: Meeting Report** 9, **available at** http://www.geneva-academy.ch/docs/ResearchActivities/Report_TheRightoPrivacy.pdf.

116 **Id.** at 5; **see also** Lennon, **supra** note 30, at 644.

117 The Council of Europe Commissioner for Human Rights, **supra** note 78, at 55; Venice Commission, Report on the democratic oversight of the security services, CDL-AD (2007)016, §§ 205–06 (2007).

118 Venice Commission, **supra** note 115, §§ 205–06.

119 I. Cameron, **National Security and the European Convention on Human Rights – Trends and Patterns,** Stockholm International Symposium on National Security & the Euroepan Convention on Human Rights, 4–5 (Dec. 2008,)..

potent, conveying as it does a need for urgent and decisive action.[120] This is sometimes amplified by the tendency of some judges to be strongly deferential to the government on matters of national security. Third, in many jurisdictions judicial authorisation amounts to "rubber-stamping" decisions taken by security services, with very few requests for warrants being turned down.[121] And fourth, judges cannot normally be held to account for the warrants they issue to security services. In order to preserve judicial independence and the separation of powers, warrant-issuing processes are not usually subject to **ex post** scrutiny by an oversight body.[122] By contrast, a minister or quasi-judicial authorising body are considered more easily controllable by parliament or by an independent oversight body for the decisions they make.[123]

Therefore scholars—in order to find a balance between advantages and drawbacks—are increasingly proposing not "judicial oversight" but a "**good enough judicial oversight**."[124] How should one understand this term? Judging by the case law of the ECtHR it definitely invites consideration of **realpolitik** or, in general, empirical evaluations.[125] Indeed, we believe the Strasbourg Court has never failed to do so. As early as **Klass**, it considered not only independence and effectiveness of surveillance control, but it also assessed the national legal framework in its totality and the effectiveness of the rule of law in this field, noting that "various provisions are designed to reduce the effect of surveillance measures to an unavoidable minimum" so that "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".[126]

And recently with **Colon** (2006), **Zakharov** (2015), and **Szabò and Vissy** (2016), this evidence-based approach rises more to the surface and becomes more understandable. Indeed, the Court in these most recent surveillance cases is considering more and more the effectiveness of the rule of law safeguards in the specific member state at stake.

For example, in **Colon**, the Court highlighted the fact that the Dutch government had provided two independent studies attesting to the effectiveness of powers and recommending their continued use.[127] Whereas in **Zakharov**, the Court noted that "the shortcomings in the **legal framework as identified above** appear to have an impact on the actual operation of the system of secret surveillance which exists in Russia. ECtHR is not convinced by the Government's assertion that all interceptions in Russia are performed lawfully on the basis of a proper judicial authorisation."[128] Therefore, "the Court finds that **Russian law does not meet the "quality of law" requirement** and is incapable of keeping the "interference" to what is "necessary in a democratic society"".[129] In addition, the **Zakharov** Court explicitly affirmed the **empirical** nature of its scrutiny; the secret nature of surveillance measures should not stand in the way of an effectiveness review—remedies must be **practical and effective**, rather than **theoretical and illusory**.[130]

120 Venice Commission, **supra** note 115, at 208.
121 UNHCR, The Right to privacy in the digital age, A/HRC/27/37, UN High Commissioner for Human Rights, (30 June 2014), **available at** http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx §38.
122 I. Cameron, **Parliamentary and specialised oversight of security and intelligence agencies in Sweden, in** Parliamentary oversight of security and Intelligence agencies in the European Union", European Parliament, (A. Willis & M. Vermeulen eds., Brussels, 2011).
123 J. Borger, **Minister should assess UK surveillance warrants, says Philip Hammond,** THE GUARDIAN, 23 October 2014.
124 **See** Lennon, **supra** note 30, at 644.
125 **Id.** at 642.
126 **Klass**, No. 5029/71, Eur. Ct. H.R. at 22—23.
127 **See** Lennon, **supra** note 30, at 640.
128 **Zakharov**, No. 47143/06, Eur. Ct. H.R. 79.
129 **Id.**
130 **Id.** at 74; **see also** Cole, **supra** note 38, 128.

Also, the Council of Europe Report on the democratic and effective oversight of national security services emphasises the importance of scrutinizing practical effectiveness of safeguards (rather than merely assessing national legal provisions).[131]

In other words, the Court is now more focussed on an **empirical check** or **reality check** on the compatibility of a Member State legal framework with Article 8 ECHR, rather than merely an abstract legal check.[132] This new tendency has led the court to apply stricter rules in the assessment of a specific legal system if the quality of rule of law and the application of democratic rules has proved inadequate with the European Charter of Human Rights.

In sum, the choice between judicial oversight and an alternative model retains relevance for the ECtHR, which still prefers the judicial system (as it made clear in **Szabò)**, but even such system needs to be assessed through the "test" of reality and so needs to prove its quality and effectiveness in the specific legal order at issue.

Conclusion

In this chapter we addressed how the European human rights framework deals with surveillance, and in particular surveillance oversight. We have not addressed other relevant issues of the European surveillance law, such as the interpretation of the legality principle or the victim's requirement. Our scope has instead been limited to an issue that deserves particular theoretical attention. The two European Courts (the ECtHR and the EUCJ) have not yet established a clear doctrine in determining suitable thresholds and parameters, but recent European jurisprudential trends show relevant developments. There are also interesting similarities with common law cases.[133]

After Part II's general clarification of the ECHR surveillance framework and the terminology used in the field of surveillance oversight (taking into account different national criminal procedure legal systems), in Part III we addressed the application of Article 8 ECHR in criminal law surveillance, as crystallised by the ECtHR in **Huvig v. France** (1990), which established six (or seven) requirements within the legality principle. Although **Huvig** is a fine example of strict scrutiny, one cannot claim that the Court has always used a strict approach when assessing surveillance law. Part IV analysed the Court's different standards of scrutiny in this field, acknowledging that the ECtHR has a flexible approach in interpreting Articles 8 and 13 ECHR,[134] which depends upon several factors: specific facts at issue, "vital" interests at stake, and political considerations.

One interesting variable is the public body conducting surveillance. In particular, secret service surveillance is problematic in terms of oversight. In Part V we analysed how the ECtHR has assessed the respect of individuals' right to a remedy against intelligence surveillance, according to Article 13 ECHR (combined with Article 8 ECHR). The ECtHR has shown a preference towards judiciary oversight, but in the European legal order there are several examples of non-judicial oversight systems. In Parts VI and VII we highlighted how the Court has accepted these alternative methods of surveillance control, where the **independence** of the oversight body, its **wide jurisdiction**, its **power to access data**, and its **power to effective reactions** are proved. An interesting example of such a recognized alternative is the oversight conducted by Data

131 The Council of Europe Commissioner for Human Rights, **supra** note 78, at 13–14.
132 **See also** Fuster, **supra** note 23, at 4–5.
133 **See Wilkes**, 98 Eng. Rep. at 489–99; **Entick**, 95 Eng. Rep.; **see also** White, **supra** note 112.
134 **See, e.g.**, Fuster **supra** note 23, at 4. The preference for flexibility in surveillance law is also highlighted by Deeks, **supra** note 76, at 366.

Protection Authorities in the EU member states because of the eventual involvement of ordinary judges as a second step of oversight according to Article 28(3) of Data Protection Directive (Section 8).[135]

After this overview, we acknowledge that although the ECtHR prefers judicial oversight, alternative methods of surveillance control could be considered suitable. However, this assessment is based not merely on the independence and powers of the non-judicial authorities deputed to review surveillance activities, but also on empirical tests proving the effectiveness of the rule of law in the field of secret surveillance in a specific Member State (Section 9).[136]

In conclusion, we noticed an increasing emphasis on requiring a **good enough** judicial (**ex ante** or **ex post**) control over surveillance, meaning not a mere judicial control, but a system of oversight (preferably judicial, but also "quasi-judicial" or "hybrid") which can provide an effective control over surveillance, supported by **empirical checks** in the national legal system at issue.

135 This eventual double (**non-judicial** and **judicial**) oversight has already been positively welcomed by scholars (**see, e.g.,** Fuster, **supra** note 76, at 4. The preference for flexibility in surveillance law is also highlighted by Deeks, **supra** note 76, at 366) also considering that Data Protection Authorities have constant relationships with national Parliaments; **see** Lennon, **supra** note 30, at 643 ("The authorization of oversight powers could be subjected to **judicial confirmation**, whether as an alternative or **in addition to oversight by other bodies**. This could enable close, independent scrutiny providing a robust method of oversight." (emphasis added)).

136 **See** P. DE HERT A HUMAN RIGHTS PERSPECTIVE ON PRIVACY AND DATA PROTECTION IMPACT ASSESSMENT, IN PRIVACY IMPACT ASSESSMENT, 47 (Springer Netherlands 2012) ("It is less painful to tell a Member Stat that it has violated the Convention because of a problem with its legal basis that to pass the message that an initiative favoured by Member States or accepted by a Member State is, in fact, not necessary in a democratic society.").

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.org

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 & Paul De Hert (25 pages)