The Rights of Notification after Surveillance is over: Ready for Recognition?

Paul DE HERT[a,1] and Franziska BOEHM[b,2]
[a] *Vrije Universiteit Brussel/Tilburg University*
[b] *Centre for Security Reliability and Trust, University of Luxembourg*

Abstract. The notification of individuals of surveillance measures is a crucial issue currently discussed in several EU Member States as well as at EU level. Provisions so far enacted in this area reflect a certain ambiguity in the regulation of this matter. The right to be informed of the fact that online malware installation have been set up on the computer, that the telephone has been tapped or that a person has been subject to secret visual and/or video surveillance measures are not harmonised in the EU. The article refers to the ongoing discussions and analyses in particular the jurisprudence of the European Court of Human Rights in this area. Questions such as the acceptance of a right of notification after surveillance is terminated and the possible recognition of this right are being tackled.

Keywords. surveillance society, notification of surveillance measures, control of police and secret service, information rights, Article 8 European Convention on Human Rights

Introduction

Since 9/11 the surveillance of citizens has increased in several ways: large crime fighting databases have been established and interlinked, travel behaviours are scanned and telecommunication and internet data have to be retained in order to be used in possible investigations[3]. The rights of individuals affected by such measures do not

[1] Professor Paul DE HERT holds a chair at the Vrije Universiteit Brussel as well as at the Tilburg University; E-mail: paul.de.hert@vub.ac.be.
[2] Dr. Franziska BOEHM is a post-doctoral researcher at the Interdisciplinary Centre for Security, Reliability and Trust (SnT) at the University of Luxembourg; E-mail: franziska.boehm@uni.lu.
[3] Several databases for police and immigration control purposes at EU level have been developed in recent years, compare the Schengen Information System (SIS), the Customs Information System (CIS), the Europol Information System (EIS), the Visa Information System (VIS), Eurodac; data of flight passenger are

always keep up with this fast developing field of different surveillance techniques. One crucial question currently discussed at EU as well as national level is therefore whether the individuals should be informed after they have been subjected to such measures. Provisions so far enacted in this area reflect a certain ambiguity in the regulation of this issue. While some Member States follow a quite transparent approach, others are more reluctant. The developments in the Member States, however, show a general tendency towards the establishment of a right to be informed. In Germany, for instance, public authorities are required to notify subjects in most of the cases after the termination of surveillance activities. The Belgian Constitutional Court has recently declared that the Belgian Secret Service Act violated the constitution because it did not provide for an active notification duty after the end of surveillance measures[4]. The discussions in the Member States are reflected at European level as well. Already in 1987, the Council of Europe issued Recommendation R (87) 15 requiring the notification of individuals after they had been subject of surveillance measures. More recent case-law of the European Court of Human Rights (ECtHR) in respect to the purpose and necessity of secret surveillance measures, links the right of notification to the existence of effective safeguards against the abuse of monitoring powers and consequently to the effectiveness of remedies before the courts[5]. Nonetheless, the Court's position in recent years was not perfectly clear. Although it seemed to be in favour of a notification duty, it hesitated to establish a general obligation. New developments seem to indicate that the ECtHR is becoming more favourable regarding the establishment of such a requirement. The paper aims at discussing the question of the right of notification after surveillance by reference to the case-law of the ECtHR and the EU instruments currently in force. First, it briefly examines the notification right enshrined in the EU Data Protection Directive 95/46 and second, it shows the development of this right at international level in the framework of the ECtHR, including a brief analysis of the national legal orders of Germany and Belgium. In the end, it ventures to suggest that a general notification duty in surveillance cases should be established.

1. The notification as an essential requirement in the EU Data Protection Directive

In EU law, the notification of individuals about the processing of their personal data is one crucial aspect of the Data Protection Directive 95/46[6]. In ordinary data protection law, the information provided to the data subject constitutes an important

transmitted to the US for analyses, compare: agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Unites States Department of Homeland Security (DHS), [2007] OJ L 204/18; similar plans to establish a comparable system allowing for the analyses of European flight passengers exist also at EU level: Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, COM(2011) 32 final Brussels, 2.2.2011 and the data retention directive 2006/24, [2006] OJ L 105/54.

[4] Belgium Constitutional Court, case No. 145/2011, 22 September 2011 at paras B.82-B.92.

[5] *Weber and Saravia v Germany* Application No 54934/00, Admissibility, 29 June 2006 at para 135; *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria* Application No 62540/00, Merits, 28 June 2007 at para 90.

[6] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, [1995] OJ L 281/31.

element of a fair processing of personal data. Knowing that one's personal data are processed guarantees transparency and enables the person concerned to assess its own position and to adapt its behaviour to a given situation[7]. Foreseeability and the control of the use of personal information play an essential role in this context. Although, due to the former pillar structure, Directive 95/46 does not apply to security related data processing and therefore not to surveillance measures, it illustrates the general data protection standard applicable to ordinary data processing activities[8].

Directive 95/46 distinguishes two situations with regard to information rights: first, data which have been obtained from the data subject and second, data which have been obtained by other means[9] In both cases, information has to be provided irrespective of whether the individual applies for access to the data[10] The information includes (a) the identity of the controller and of his representative, (b) the purposes of the processing for which the data are intended and (c) any further information, including information on the right to access and to rectify[11], in so far as such further information is necessary having regard to the specific circumstances in which the data are collected and to guarantee fair processing in respect of the data subject[12]. As the individual concerned has not itself taken part in the process of data collection[13], information on the categories of data must be additionally provided in the case that the information is not obtained from the data subject[14].

Regulation 45/2001, which regulates the processing of personal data by the EU institutions and bodies, additionally adds information on the legal basis of the processing operation for which the data are intended, the time-limits for storing the data and the right to have recourse at any time to the European Data Protection Supervisor and the origin of the data, except where the controller cannot disclose this information for reasons of professional secrecy[15] in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected and to guarantee fair processing in respect of the data subject[16].

---

[7] Dammann and Simitis (eds), *EG-Datenschutzrichtline*, Commentary to Directive 95/46, Baden-Baden: Nomos Verlag, 1997, Article 10 at para 1; Ehmann and Helfrich (eds), *EG Datenschutzrichtlinie – Kurzkommentar*, Köln: Verlag Dr. Otto Schmidt, 1999, Article 10 at paras 25-28.

[8] Article 3 of Directive 95/46, [1995] OJ L 281/31.

[9] Articles 10 and 11 of Directive 95/46, [1995] OJ L 281/31.

[10] Articles 10 and 11 of Directive 95/46, [1995] OJ L 281/31.

[11] Such as the recipients or categories of recipients of the data, the existence of the right of access to and the right to rectify the data concerning the individual concerned.

[12] Articles 10 (1) and 11 (1) of Directive 95/46, [1995] OJ L 281/31.

[13] Dammann and Simitis (eds), *EG-Datenschutzrichtline*, Commentary to Directive 95/46, Baden-Baden: Nomos Verlag, 1997, Article 11 at para 4.

[14] Article 11 (1) Directive 95/46, [1995] OJ L 281/31.

[15] Information on the origin of the data is only provided if the information is not obtained from the data subject.

[16] Article 12 (1) (f) Regulation 45/2001 of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, [2001] OJ L 8/1; compare also Court of First Instance: T-259/03 (judgment of 12 September 2007) Nikolaou v. Commission; In this case, Mrs. Nikolaou intended an action for damages, pursuant to the second paragraph of Article 288 EC, for her loss suffered following publication of information concerning an inquiry carried out concerning her by the European Anti-Fraud Office (OLAF) and OLAF's refusal to grant her access to the inquiry file and to supply her with a copy of its final report. In this case, the General Court stated that the rule of law requires that a person concerned shall be informed as soon as possible of the existence of an investigation as long as the information does not prejudice the ongoing investigation (for more information, see Boehm, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice*, Springer 2012, p. 231.

Derogations exist in the event of processing for statistical purposes, historical or scientific research[17]. When the information is not obtained from the data subject, the information must not to be given, if the 'provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law'[18]. Although the provision on the disproportionate effort allows for a certain discretion, Member States must nonetheless provide appropriate safeguards in these cases. Another important exception exists with regard to the freedom of expression. Article 9 of the Directive 95/46 allows to provide for exceptions and derogations for the processing of personal data for journalistic purposes or the purposes of artistic or literary expression, but, 'only if they are necessary to reconcile the right to privacy with the rules governing the freedom of expression'[19].

In contrast to Directive 95/46 and Regulation 45/2001, a clear obligation to provide the data subject with information on the processing in the framework of police and judicial cooperation does not exist in the Framework Decision (FDPJ) regulating data processing in this specific area[20]. The wording of the provision on the information of the data subject appears to be more a possibility rather than an obligation[21]. None of the FDPJ provisions stipulates a clear obligation to inform the person concerned about the processing. Recital (26) FDPJ mentions that '…' it may be necessary to inform data subjects regarding the processing of their data '…'. Article 16 FDPJ further details that 'Member States shall ensure that the data subject is informed regarding the collection or processing of personal data by their competent authorities, in accordance with national law'[22] Member States may additionally ask another Member State not to inform the data subject about data transferred from this first Member State to the other[23].

Thus, whereas the notification of individuals in the EU is left to the Member States in police and judicial related activities, it is established in ordinary EU data protection law since 1995 and constitutes an important element of Directive 95/46. Transparency is regarded as 'a fundamental condition for enabling individuals to exercise control over their own data and to ensure effective protection of personal data'[24]. With regard to future developments in this field, it is interesting to note that within the upcoming revision process of Directive 95/46, it is planned to increase the transparency for individuals by establishing a general transparency principle which goes beyond the current, above mentioned, information duties of Directive 95/46.

In addition, the scope of the new Directive should include the protection of personal data 'in the context of all EU-policies, including law enforcement and crime

[17] Articles 10 (2) and 11 (2) Directive 95/46, OJ L 281/31*;* Articles 11 (2) and 12 (2) Regulation 45/2001, [2001] OJ L 8/1.

[18] Article 11 (2) Directive 95/46, OJ L 281/31*;* Articles 12 (2) Regulation 45/2001, [2001] OJ L 8/1.

[19] Article 9 Directive 95/46, OJ L 281/31.

[20] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (FDPJ), [2008] OJ L 350/60.

[21] Opinion of the European Data Protection Supervisor on the Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, [2007] OJ C 139/1 at para 37.

[22] Article 16 (1) FDPJ, [2008] OJ L 350/60.

[23] Article 16 (2) FDPJ, [2008] OJ L 350/60.

[24] Communication from the Commission to the European Parliament, the Council, the Social Committee and the Committee of the Regions on 'A comprehensive strategy on data protection in the European Union', COM(2010) 609 final of 4 November 2010, at para 2.1.1, p. 6.

prevention'[25]. In a communication to the European Parliament and the Council of November 2010, the Commission concludes that the current information to be given to the individuals is 'not sufficient' and that it is therefore 'essential that individuals are well and clearly informed, in a transparent way, by data controllers about how and by whom their data are collected and processed, for what reasons, for how long and what their rights are if they want to access, rectify or delete their data'[26]. Taking the existing provisions as well as the plans to amend Directive 95/46 into account, it seems that the importance of the notification of individuals in EU data protection law, including in security related matters, will increase in the future.

2. The right of notification in view of the Council of Europe

Besides the notification duty enshrined in Directive 95/46, the Council of Europe has a long established tradition in the protection of individual rights against surveillance measures ordered by states. Already in 1978, in the case *Klass v. Germany* the ECtHR laid down essential criteria limiting the power of the states to enact surveillance measures by referring to the protection offered by the right to the protection of private life stipulated in Article 8 European Convention on Human Rights (ECHR). Since then, the ECtHR issued a number of judgements specifying the principles to be respected by states when they plan to implement security and surveillance legislation. The law permitting the surveillance measures must be sufficiently clear in its terms to give citizens an adequate indication of the conditions and circumstances in which authorities are empowered to resort to any measures of secret surveillance and collection of data[27]. Moreover, 'because of the lack of public scrutiny and the risk of abuse intrinsic to any system of secret surveillance, the following minimum safeguards should be set out in statute law to avoid abuses: 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, and the kind of remedy provided by the national law'[28]. In this context, the ECtHR increasingly often discusses the question of whether a right to be informed of surveillance measures must exist to guarantee an effective remedy after the termination of the surveillance measure. While transparency and the control of the use of personal information play an essential role in data protection law in non-police related activities since the beginning of data protection legislation[29], the information of individuals after surveillance has ended is a more recent development in the jurisdiction of the ECtHR. The EU instruments in this field, such as the above mentioned FDPJ, do not include a notification duty. The ECtHR however seems to have developed a more comprehensive protection in recent years

[25] Communication from the Commission to the European Parliament, the Council, the Social Committee and the Committee of the Regions on 'A comprehensive strategy on data protection in the European Union', COM(2010) 609 final of 4 November 2010, at para 2.3, p. 13.

[26] Communication from the Commission to the European Parliament, the Council, the Social Committee and the Committee of the Regions on 'A comprehensive strategy on data protection in the European Union', COM(2010) 609 final of 4 November 2010, at para 2.1.1, p. 6.

[27] *Shimovolos v Russia* Application No 30194/09, Merits, 21 June 2011 at para 68.

[28] Ibid.

[29] At EU level, Articles 10 and 11 of Directive 95/46, OJ L 281/31 *and* Articles 11 and 12 of Regulation 45/2001, [2001] OJ L 8/1 ensure the information of the individual in activities not related to police work, compare above.

2.1. First steps in 1978: notification in the case Klass v. Germany

An early example of the protection offered by Article 8 ECHR against surveillance measures is the judgment in the case *Klass v. Germany* in 1978[30]. In this case, the Court established key criteria which are still applicable in similar cases.

In *Klass v. Germany* the German government referred to the protection of national security and the prevention of crime to justify security legislation (G-10 Act) implementing secret mail, post and telephone surveillance in the aftermath of the terrorist threats of the 1970s. The applicants, lawyers, public prosecutors and judges, claimed among others that the G-10 Act empowers the authorities to monitor their correspondence and telephone communication without requiring the authorities to subsequently inform the persons concerned of the measures taken against them.

Prior to discussing the details of the law at stake, the Court had to clarify an important admissibility criterion concerning the applicants' victim status in surveillance cases. As neither of the applicants had already been the subject of concrete surveillance measures (at least not knowingly) and Article 34 ECHR does not permit individuals to complain against a law in abstracto, it was questionable whether the applicants could invoke the protection of Article 8 ECHR[31]. The Court accepted that, due to the secrecy of the measures in question, and the establishment of a system of surveillance under which all German citizens could potentially have their mail, post and telecommunications unknowingly monitored, it was intolerable that the guarantees of Article 8 ECHR could be circumvented by the simple fact that the person concerned was kept uninformed of its violation [32]. Therefore, the applicants could claim to be victim of a violation of Article 8 ECHR without proving that they had been the concrete target of secret surveillance measures[33]. This argument plays an essential role, even today. It is not only important in surveillance cases, but also in the context of collective data processing measures where it seems to be impossible for an individual to demonstrate that precisely his/her personal data had been collected or processed. The Court clarified that the 'mere existence of the legislation' (G-10 Act) itself creates the threat of surveillance and that this danger necessarily attacks the 'freedom of communication between users of the postal and telecommunication services, and thereby constitutes an interference by a public authority with the exercise of the applicants' right' according to Article 8 ECHR[34], irrespective of any measures in fact taken against them[35].

In determining whether the interference through the establishment of surveillance legislation is justified, the ECtHR bases itself on two facts: Firstly, it recognises the technological progress made in espionage and surveillance techniques[36]. Secondly, it refers to the development of terrorism in Europe in the years before 1978. The ECtHR held 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

[30] *Klass v Germany*, A 28 (1978), 2 EHRR 214.
[31] Ibid. at paras 33 and 37.
[32] Ibid. at paras 36 and 37.
[33] Ibid. at para 38.
[34] Ibid. at para 41.
[35] Compare also *Liberty and others v the United Kingdom* Application No 58234/00, Merits, 1 July 2008 at para 56.
[36] *Klass v Germany*, A 28 (1978), 2 EHRR 214 at para 48.

> to counter such threats, to undertake the secret surveillance of subversive elements operating within its jurisdiction. Therefore, the Court has to accept that the existence of some legislation granting powers of secret surveillance over the mail and telecommunications is, under exceptional conditions, necessary in a democratic society in the interests of national security and/or for the prevention of disorder or crime[37].

Even though this statement was made in 1978, it exemplarily illustrates the Court's understanding with regard to secret surveillance measures and legislation enacted against terrorism. Member States enjoy a wide margin of appreciation relating to the implementation of counter terrorism measures. The Court, however, restricts its approach to the effect that it is nevertheless aware 'of the danger such a law poses of undermining or even destroying democracy on the ground of defending it'[38]. It affirms that the member states may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they consider appropriate[39] It demands adequate and effective guarantees against abuse[40].

One of the safeguards against abuse is constituted by the possibility to obtain a remedy in cases of misuse. In the view of the ECtHR, the notification guarantees the possibility to have recourse to the courts to be able to challenge the legality of the surveillance measures retrospectively and to ensure against abuses[41]. To be able to claim a possible violation of the rights, an individual must be aware of the fact that he was the subject of surveillance measures. The Court puts much emphasis on this possibility and therefore links the question of notification to the possibility of independent control (at least a posteriori) and effective remedies before courts:

> As regards review a posteriori, it is necessary to determine whether judicial control, in particular with the individual's participation, should continue to be excluded even after surveillance has ceased. Inextricably linked to this issue is the question of subsequent notification, since there is in principle little scope for recourse to the courts by the individual concerned unless he is advised of the measures taken without his knowledge and thus able retrospectively to challenge their legality[42].

In the *Klass* case, the Strasbourg Court was satisfied with the solution found by the German Constitutional Court in the contested judgement. The German Court came to the conclusion that the 'person concerned must be informed after the termination of the surveillance measures as soon as notification can be made without jeopardising the purpose of the restriction'[43]. This requirement, however, does not hinder long-term surveillance measures since, as long as the notification might jeopardise the purpose that provoked the surveillance, the notification must not be carried out. In addition, even if surveillance has stopped, the state is not necessarily obliged to immediately inform the person concerned. The Strasbourg Court recognises the argument of the German Constitutional Court that 'the fact of not informing the individual once surveillance has ceased cannot itself be incompatible with this provision since it is this

---

[37] Ibid.
[38] Ibid. at para 49.
[39] Ibid.
[40] They depend '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 respective national law', *Klass v Germany*, A 28 (1978), 2 EHRR 214 at para 50.
[41] *Klass v Germany*, A 28 (1978), 2 EHRR 214 at paras 56-57.
[42] Ibid. at para 57.
[43] Ibid. at para 58.

very fact which ensures the efficacy of the interference' [44]. Only after the risk of thwarting the investigation (even retrospectively) has been completely ruled out, the notification could be carried out. Summarising, the notification is in fact seen as a tool to guarantee effective remedies and independent control.

The Court concludes that the G-10 Act in principle complies with Article 8 ECHR as it lays down strict conditions regarding the implementation of surveillance measures and the processing of the information thereby obtained[45]. From a present day perspective, the ECtHR used the *Klass* case as a first opportunity to stipulate basic principles balancing the state's secret surveillance powers against the rights of targeted individuals, in particular the right to be informed of the surveillance measures and the possibility of having recourse to the courts after termination of such measures[46]. While, however, the notification was not seen as an indispensable criterion to comply with Article 8 ECHR, the Court put emphasis on the fact that the notification of the surveillance measure, taken without the knowledge of the person concerned, may represent one (of possibly other) tools to guarantee an effective remedy.

2.2. The notification duty of Recommendation R (87) 15 – the forgotten right in national and European legal frameworks?

In addition to the case-law of the ECtHR in relation to the protection of individuals in police related activities, the Council of Europe was also the first European organisation issuing a recommendation attempting to regulate the use of personal data in the police sector in 1987[47]. Principle 2.2. of Recommendation R (87) 15 is strongly reminiscent of the principles stipulated in the *Klass* case. It requires the notification of the individual concerned when data about him have been collected and stored without his knowledge, as soon as the object of the police activities is no longer likely to be jeopardised [48]. Although all EU Member States are also members of the Council of Europe, this important principle was however not introduced in most of them. The German provision, subject to the *Klass* case, remains until today the most far reaching notification duty introduced in Europe. Article 101 (4) of the German Criminal Code does not only stipulate a duty to notify the targeted person, but also other persons who might have also been concerned by the surveillance measures. The notification duty includes traditional forms of surveillance (e.g. telephone tapping, acoustical observation of private premises, or surveillance through undercover agents) as well as newer surveillance techniques such as the use of IMSI-catcher[49] or the use of profiling methods (Raster- und Schleppnetzfahndung). The duty to notify in German law is therefore part of the classical criminal procedure and an indispensable legal

[44] Ibid.

[45] Ibid. at para 52: 'The measures in question remain in force for a maximum of three months and may be renewed only on fresh application; the measures must immediately be discontinued once the required conditions have ceased to exist or the measures themselves are no longer necessary; knowledge and documents thereby obtained may not be used for other ends, and documents must be destroyed as soon as they are no longer needed to achieve the required purpose.'

[46] Ibid. at para 39.

[47] Recommendation R (87) 15 of the committee of ministers to member states regulating the use of personal data in the police sector, 17 September 1987.

[48] Principle 2.2. of Recommendation R (87) 15: 'Where data concerning an individual have been collected and stored without his knowledge, and unless the data are deleted, he should be informed, where practicable, that information is held about him as soon as the object of the police activities is no longer likely to be prejudiced.'

[49] IMSI means international mobile subscriber identity.

requirement to be respected in the aftermath of surveillance measures. This right assures transparency within the framework of secret surveillance measures and enables the persons concerned to verify the legality of the surveillance measure afterwards.

A development raising hopes that the notification duty will be implemented in other Member States as well is the recent decision of the Belgian Constitutional Court on the powers and duties of the Belgian intelligence services. The background of this case dates back to 1998 where a general framework governing the intelligence and security services in Belgium was established spelling out their tasks and responsibilities. There were hardly any coercive or secret powers in the law of 1998. The services were entitled to gather and analyse information and to follow people, but not to interfere. Recently, the Act of 4 February 2010 on special intelligence methods by the intelligence and security services was passed and came into force on 1 September 2010[50]. This Act changed a series of existing Acts and inserted provisions in the 1998 Act containing new far reaching powers for the secret services, so called special intelligence methods. These powers relate, among others, to: the possibility to put taps on phones, to enter homes of people suspected of being involved in terrorist activities without them knowing, or to detain and question people.

In September 2011, the Belgian Constitutional Court ruled for a partial annulment of the reform Act of February 2010. The demand to declare the Bill unconstitutional was lodged by the Flemish bar council and the francophone as well as germanophone bar councils. The case was joined with an action for the annulment of the Ligue des Droits de l'Homme. The Constitutional Court declared the Bill partly incompatible with the Constitution. In particular Article 2 § 3 of the 1998 Act, as rewritten by the 2010 reform, was declared unconstitutional. The provision which stated that a person, who has been subjected to a secret intelligence method like tapping or secret house searches, is only informed afterwards 'on request', was found contrary to the respect of human rights as enshrined in the Belgian Constitution and the ECHR. By reference to the case law of the ECtHR, in particular to the cases *Klass* and *Weber and Saravia v. Germany*, the Constitutional Court came to the conclusion that the relevant intelligence service itself must actively inform the person concerned as soon as it is possible without compromising the intelligence work[51]. The omission of an active notification duty was taken very seriously by the Court as it observed that the question of notice is inseparable from the actual control and safeguards against abuse [52]. By not notifying the citizens, every possibility to effective supervision and subsequent legality control would be excluded[53]. It is worth mentioning that the arguments used by the Belgian Constitutional Court to underline the necessity of an active notification duty exactly mirror the reasoning of the ECtHR applied in the *Klass* case.

While at national level, Member States seems to recognise the notification duty in their legal orders, the situation at EU level is different. When now, almost 25 years after its recognition by the Council of Europe, looking at the concrete application of principle 2.2 of Recommendation R (87) 15 within the Europe's legal framework, it seems that the EU has forgotten about this right over the years. None of the existing instruments in police and judicial cooperation matters entail a similar right. Although most of the instruments in this area, for instance the Europol Decision or the Schengen

[50] Loi du 4 février 2010 relative aux méthodes de recueil des données par les services de renseignement et de sécurité, Official Journal Belgium, 10 March 2010, No. 2010009144, p. 14916.
[51] Belgium Constitutional Court, case No. 145/2011, 22 September 2011 at paras 88 and 92.
[52] Ibid at para 86.
[53] Ibid at para 86.

Information System, refer in their legal bases to Recommendation R (87) 15[54], they do not establish a notification duty. This lack of information does not only concern the missing notification in cases of surveillance, but also as it regards the entry of personal data in EU databases, the transfer of such data to other databases or even to third states. Individuals are informed at no point. In this context it is worth considering that not only (potential) criminals are concerned, but also individuals who have their data entered due to their special relation to a crime (witnesses, victims, contacts etc.).

Diana Alonso Blas, the data protection officer at Eurojust, argues in this context that the notification of contact persons after surveillance measures have ended 'could have [a] substantially negative impact on the reputation of that person [the person under surveillance], even if the investigation did not have any judicial consequence for the person as such'[55]. When following this argument, the missing notification duty would have as a consequence that the notification is excluded in particular in sensitive cases in which the state never enacted judicial proceedings (and thus in cases in which the person under surveillance is innocent).

This however would run against the basic idea of principle 2.2 of Recommendation R (87) 15 which intends to enable individuals subjected to surveillance measures to enact infringement proceeding challenging the lawfulness such measures, at least retrospectively. As a result, every form of ex post control would be excluded in such cases. EU agencies such as Eurojust or Europol could therefore in various cases enact surveillance measure against persons without ever fearing that their measure will be subject to independent control in the future.

While in 1987 principle 2.2 of Recommendation R (87) 15 should be limited to situations in which the police decides to keep the collected data[56], it is interesting to evaluate whether this restriction stipulated in the 1980s was upheld by the ECtHR in its following case-law.

2.3. Confirmation of the Klass findings: Weber and Saravia v. Germany

In June 2006, almost 30 years after the *Klass* judgment, an amendment of the G-10 Act was again subject-matter before the ECtHR. In the case *Weber and Saravia v. Germany*, the applicants impugned the legality of four amendments which extended the powers of the secret service, referring to extended strategic monitoring, the transmission and use of personal data to the Federal Government including the Offices for the Protection of the Constitution and other authorities, the destruction of personal data as well as the failure to give notice of restrictions on the secrecy of telecommunications[57]. The ECtHR examined in detail the applicant's complaints and established important basic principles of general application with which states have to comply when extending the powers of their secret services[58]. To be in accordance

[54] Compare recital 14 and Article 27 of the Europol Decision and recital 20 of the Decision establishing the second generation of the Schengen Information System.

[55] Alonso Blas, 'Ensuring data protection in the field of police and judicial activities: some considerations to achieve security, justice and freedom', *ERA Forum* (2010), 233-250, in particular 243.

[56] Point 44 of the explanatory memorandum of Recommendation R (87) 15 clarifies that 'this procedure will be unnecessary if the police has decided to delete the data collected unbeknown to the individual'.

[57] *Weber and Saravia v Germany*, Application No 54934/00, Admissibility, 29 June 2006.

[58] The ECtHR uses the principles outlined in *Weber and Saravia v Germany* in subsequent cases as a standard of reference when it comes to the assessment of safeguards and guarantees against abuse, see for instance *Kennedy v the United Kingdom* Application No 26839/05, Merits, 18 May 2010 at para 158, and

with Article 8 ECHR specific and particular minimum requirements have to be fulfilled. The Court observes that before enacting strategic monitoring, a series of restrictive conditions have to be satisfied. Detailed safeguards against abuse have to be established. Examples are: the restriction of monitoring measures to a short period of time (for instance three months), immediate interruption of the measures if the conditions set out in the monitoring order were no longer fulfilled or the measures themselves were no longer necessary, as well as the destruction of data as soon as they were no longer needed to achieve the purpose pursued[59]. Additionally, independent supervision (in this case a parliamentary board and a special commission) empowered with substantial power in relation to all stages of interception and the establishment of reporting duties, at least for the Federal Minister authorising monitoring measures, have to be provided[60]. Detailed provisions must regulate storage and destruction of data[61].

Concerning the subsequent notification of surveillance measures, the ECtHR referred to the findings of the *Klass* case and emphasised again that this question is closely linked to the effectiveness of remedies before the courts and therefore to the existence of effective safeguards against the abuse of monitoring powers[62] Reminiscent of the *Klass* case, the Court however stressed that 'the fact that persons concerned by secret surveillance measures are not subsequently notified once surveillance has ceased cannot by itself warrant the conclusion that the interference was not 'necessary in a democratic society', as it is the 'very absence of knowledge of surveillance which ensures the efficacy of the interference'[63]. By referring to the risk that the notification 'might reveal the working methods and fields of operation of the Intelligence Service', the ECtHR nonetheless adds 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 be provided to the persons concerned[64].

The Court observed that this requirement was fulfilled by the amended G-10 Act and found that the German Constitutional Court moreover strengthened the safeguards against abuse by hindering the obligation of notification from being circumvented[65]. The possibility of not notifying the individual in cases in which the data were quickly destroyed after the surveillance measure, only applied in situations in which the data had not been used during the retention period.

Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria Application No 62540/00, Merits, 28 June 2007 at para 86.

[59] *Weber and Saravia v Germany* Application No 54934/00, Admissibility, 29 June 2006 at para 114.

[60] Ibid. at para 115.

[61] Ibid. at para 116.

[62] 'since there is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively', *Weber and Saravia v Germany* Application No 54934/00, Admissibility, 29 June 2006 at para 135.

[63] Ibid. at para 135.

[64] Ibid.

[65] Ibid. at para 136.

In addition, the independent G-10 Commission[66], supervising the application of the G-10 Act, had the power to decide whether the notification of an individual being monitored was necessary. These safeguards led the ECtHR to the conclusion that the G-10 Act sufficiently ensured that the individuals being monitored were notified in cases in which the notification could be reasonably carried out. In conclusion, the ECtHR found that adequate and effective guarantees existed against abuses of the State's strategic monitoring powers in the G-10 Act[67].

The case *Weber and Saravia v. Germany* clearly shows a confirmation of the principles established in *Klass*. The Court even goes beyond Principle 2.2. of Recommendation R (87) 15, which only requires information in cases the data were kept by the police. In *Weber and Saravia*, the person concerned had to be informed in all cases in which the data were used by the police.

2.4. Recognition of the notification duty as an important safeguard against abuse: Ekimdzhiez v. Bulgaria

Notification as a requirement to guarantee effective safeguards against abuse in the framework of surveillance activities also played an important role in the case *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria.* In this case in 2007 the ECtHR set limits to restrict sprawling powers of governmental secret surveillance. The ECtHR was faced with the Bulgarian 'Special Surveillance Means Act' (SSMA) which granted far reaching surveillance rights to the police and the Bulgarian secret service[68]. The ECtHR compared the Bulgarian legislation with the German G-10 Act, subject-matter in *Weber and Saravia v. Germany* as well as in *Klass v. Germany*, and found that Bulgarian law did not comply with basic safeguards against the risk of abuse[69]. The Court primarily based itself on four main arguments:

Above all, no external independent control assured compliance with the rules of the SSMA. There was no independent review of the implementation of secret surveillance measures or compliance with warrants authorising the use of such means. Nor was there any control over whether the secret service faithfully reproduced the original data in the written record or whether the data were destroyed within the legal time limit if surveillance has proved fruitless[70]. Solely the Minister of Internal Affairs – who was directly involved in the commissioning of special means of surveillance and whose competences of control were not set out in the law – was entrusted with a certain overall control. Moreover, the ECtHR identifies an apparent lack of regulations precisely specifying the manner of screening the intelligence obtained through surveillance, the procedures for preserving its integrity and confidentiality and the procedures for its destruction[71]. In addition, the ECtHR refers

[66] The G 10 Commission consists of a president who is qualified to hold judicial office and three additional members who are appointed by the Parliamentary Supervisory Board for the duration of one legislative term and who are independent in the exercise of their functions, compare *Weber and Saravia v Germany* Application No 54934/00, Admissibility, 29 June 2006 at para 25.

[67] *Weber and Saravia v Germany* Application No 54934/00, Admissibility, 29 June 2006 at para 137.

[68] Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria Application No 62540/00, Merits, 28 June 2007.

[69] Ibid. at para 93.

[70] Ibid. at para 85; to the lack of supervision, see also: Volokhy v Ukraine Application No 23543/02, Merits, 2 November 2006 at paras 42-54.

[71] Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria Application No 62540/00, Merits, 28 June 2007 at para 86.

to the transmission of data to third parties. It compares the Bulgarian legislation with the German G-10 Act and criticises the SSMA for not providing strict rules regulating the transmission of intelligence to other services, nor independent monitoring of those rules[72].

Finally, with regard to the notification of the individuals the ECtHR underlines that safeguards must not only exist during the authorization procedure of surveillance, but also beyond the surveillance activities itself, in particular when they have ended[73]. As a marked contrast to what the ECtHR postulated in former cases, Bulgarian law did not provide for any notification of the individual[74]. It even explicitly prohibited the disclosure of information that a person had been subjected to surveillance, or that warrants had been issued for this purpose:

> Finally, the Court notes that under Bulgarian law the persons subjected to secret surveillance are not notified of this fact at any point in time and under any circumstances. According to the Court's case-law, the fact that persons concerned by such measures are not apprised of them while the surveillance is in progress or even after it has ceased cannot by itself warrant the conclusion that the interference was not justified under the terms of paragraph 2 of Article 8, as it is the very unawareness of the surveillance which ensures its efficacy. However, as soon as notification can be made without jeopardising the purpose of the surveillance after its termination, information should be provided to the persons concerned '…'. Indeed, the German legislation in issue in the cases of Klass and Others and Weber and Saravia, '…', did provide for such notification '…'[75].

The Court concludes that as a consequence of the Bulgarian SSMA, persons concerned of surveillance measures only discovered that they were subject of surveillance measures if they were subsequently prosecuted on the basis of the information collected during the surveillance or if there was a leak of information[76]. It follows that they were unable to seek redress for interferences with their rights stemming from Article 8 ECHR.77 As a result, according to the ECtHR, 'Bulgarian law thus eschews an important safeguard against the improper use of special means of surveillance'[78].

For the first time in its case-law related to the notification of individuals of a surveillance measure, with reference to the German legislation in *Klass* and in *Weber and Saravia*, the ECtHR directly requires that after the termination of surveillance, 'as soon as notification can be made without jeopardising the purpose of the measure', information should be provided to the persons concerned[79]. Whereas in both German cases the Court was satisfied with the German notification duty, but did not directly require it, in *Ekimdzhiev v. Bulgaria*, it explicitly requests the Bulgarian authorities to provide for a similar instrument.

In addition to the violation of Article 8 ECHR caused by the missing notification duty, the Court also found an infringement of a procedural right for the purpose of Article 13 ECHR. Due to the lack of information of the surveillance measure, the applicants were deprived of the possibility to challenge the violation of their rights before a court. With regard to Article 13 ECHR, the court stipulated:

---

[72] Ibid. at para 89.
[73] Ibid. at para 84.
[74] Ibid. at para 90.
[75] Ibid.
[76] Ibid. at para 91.
[77] Ibid.
[78] Ibid.
[79] Ibid. at para 90.

> It is obvious that when surveillance is ordered and while it is under way, no notification of the persons concerned is possible, as such notification would jeopardise the surveillance's effectiveness. They are therefore of necessity deprived of the possibility to challenge specific measures ordered or implemented against them. However, this does not mean that it is altogether impossible to provide a limited remedy – for instance, one where the proceedings are secret and where no reasons are given, and the persons concerned are not apprised whether they have in fact been monitored – even at this stage[80].

Although the ECtHR recognizes the difficulty of notifying a person during a pending surveillance measure, it clearly insists on the possibility to seek redress in respect of the use of secret surveillance measures in their aftermath[81].

As the applicant was unable to claim his rights in front of courts because Bulgarian law excluded the notification of the surveillance measure, the ECtHR additionally found a violation of Article 13 ECHR:

> As regards the availability of remedies after the termination of the surveillance, the Court notes that, unlike the legislation in issue in *Klass and Others*, and *Weber and Saravia*, '…', the SSMA does not provide for notification of the persons concerned at any point in time and under any circumstances. On the contrary, in two judgments of 12 February and 15 May 2004 the Supreme Administrative Court held that the information whether a warrant for the use of means of secret surveillance had been issued was not to be disclosed. The second judgment stated that such information was classified '…'. It thus appears, that, unless criminal proceedings have subsequently been instituted or unless there has been a leak of information, a person is never and under no circumstances apprised of the fact that his or her communications have been monitored. The result of this lack of information is that those concerned are unable to seek any redress in respect of the use of secret surveillance measures against them[82].

In brief, the Court held in the *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria* case that the missing notification of the individual after surveillance has ended does not only violate Article 8 ECHR, but also Article 13 ECHR. The legal protection of the individual in surveillance cases and the obligation to be notified is thus considerably strengthened by the possibility to invoke Article 13 ECHR in addition to Article 8 ECHR. Due to the status of Article 13 ECHR as a procedural right, this possibility remains however limited to cases where the individuals concerned started subsequent legal proceedings.

The clear recognition of an (active) notification duty after surveillance measures have ended in the *Ekimdzhiev v. Bulgaria* case constitutes a remarkable development in the framework of the safeguards against abuse which are necessary in surveillance cases.

2.5. Specifications of the notification duty - The Kennedy case

The question of whether another possibility to obtain an effective remedy, apart from the notification of the individual, satisfies the requirements of Article 8 ECHR was recently discussed in the case *Kennedy v. the United Kingdom*. The applicant, *Kennedy*, who suspected to be the subject of secret telephone tapping, challenged the alleged surveillance measures in front of the responsible British authority, the independent

[80] Ibid. at para 100.
[81] Ibid. at paras 100-101.
[82] Ibid. at para 101.

Investigatory Powers Tribunal (IPT)[83]. The IPT examined his case and came to the conclusion that 'no determination had been made in his favour in respect of his complaints', which left the question unanswered of whether there had been no interception or whether an interception took place but was lawful[84]. In contrast to the German notification system in the cases of *Klass* and *Weber and Saravia*, the jurisdiction of the IPT did not depend on the notification of the individual. The IPT was obliged to examine every allegation brought by individuals assuming to be the subject of wrongful interference with their communications[85]. The tribunal had, inter alia, access to secret material, the power to annul an interception order, require destruction of intercepted material and order compensation to be paid in cases of abuse[86]. As the Court already indicated in *Klass*, the notification of the individual may represent one of several possibilities to guarantee an effective safeguard against abuse and an effective remedy:

> '…' In the present case, the Court highlights the extensive jurisdiction of the IPT to examine any complaint of unlawful interception. Unlike in many other domestic systems (see, for example, the G 10 Law discussed in the context of *Klass and Others* and *Weber and Saravia*, '…'), 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[87].

The establishment of an independent and accessible authority vested with considerable powers responsible for the review of surveillance measure may also satisfy these requirements:

> The Court emphasises that the IPT is an independent and impartial body, which has adopted its own rules of procedure. The members of the tribunal must hold or have held high judicial office or be experienced lawyers '…'. In undertaking its examination of complaints by individuals, the IPT has access to closed material and has the power to require the Commissioner to provide it with any assistance it thinks fit and the power to order disclosure by those involved in the authorisation and execution of a warrant of all documents it considers relevant '…'. 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 '…'. The publication of the IPT's legal rulings further enhances the level of scrutiny afforded to secret surveillance activities in the United Kingdom '…'[88].

Considering these arguments, the ECtHR specifies the details of the requirement to notify individuals subjected to surveillance measures. While the Court seems to be favourable of an active notification duty (the authority carrying out the surveillance must inform the persons concerned ex-post of the measure) such as in the cases *Klass*, *Weber and Saravia* and *Ekimdzhiev*, the *Kennedy* case shows that also an alternative to

---

[83] The Investigatory Powers Tribunal (IPT) was established under section 65(1) Regulation of Investigatory Powers Act 2000 (RIPA) to hear allegations by citizens of wrongful interference with their communications as a result of conduct covered by RIPA. Members of the tribunal must hold or have held high judicial office or be a qualified lawyer of at least ten years` standing. Any person may bring a claim before the IPT and, save for vexatious or frivolous applications, the IPT must determine all claims brought before it (sections 67(1), (4) and (5) RIPA), compare *Kennedy v the United Kingdom*, Application no. 26839/05, judgement of 18 May 2010, at para 75.

[84] *Kennedy v the United Kingdom* Application No 26839/05, Merits, 18 May 2010.

[85] Ibid. at para 75.

[86] Ibid. at para 167.

[87] Ibid.

[88] Ibid.

the notification duty is possible. The establishment of an independent tribunal responsible for examining every allegation brought by individuals assuming to be the subject of wrongful interference with their rights, satisfies also the requirements of Article 8 ECHR. In the view of the ECtHR, it is essential that the individual has the possibility, in one way or another, to obtain information on possible surveillance measures ordered against him.

2.6. The use of a Global Positioning System (GPS) and the notification of the individual in Uzun

As was outlined above, the ECtHR seems to proceed increasingly often on the assumption that, as a matter of course, the notification of the individual of the surveillance measure constitutes an important safeguard against abuse. Therefore, the notification of the individual plays an important role, in particular as regards the use of new techniques for surveillance. Information technologies permit the surveillance of individuals in a faster and more efficient way than the traditional surveillance measures relying on the physical presence of undercover agents.

In the recent case *Uzun v. Germany*, the question arose whether the use of a Global Positioning System (GPS)[89] to track the movements of suspects in the public sphere interferes with Article 8 ECHR and, if it interferes, whether the subsequent notification of the targeted individual was necessary[90]. The applicant, Mr. *Uzun*, was suspected of having participated in bomb attacks for which an organisation pursuing the armed combat of the Red Army Fraction had claimed responsibility. For surveillance purposes, a GPS receiver had been built into the car of the applicant's suspected accomplice to observe his and *Uzun's* movements. The data collected via GPS surveillance were later used in trial against both. The Court argues that, although the 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', the systematic collection and storage of data disclosing the whereabouts and movements of a person, amounted nonetheless to an interference[91]. The data were further used to establish patterns on the applicant's movements. The Court however accepts that, in contrast to visual or acoustical means of surveillance, the foreseeability requirement in cases in which the authorities made use of a GPS is less strict. Therefore, the requirement to have the surveillance measure previously ordered by a judge was found not to be necessary when using a GPS for surveillance purposes for a short time (less than one month). In this case, the Court agrees that it was sufficient if only the prosecution ordered a suspect's surveillance via GPS[92]. As the interference provoked trough the GPS monitoring was found less infringing with the rights of an individual as other means of surveillance, the question

[89] GPS is defined as 'a radio navigation system working with the help of satellites. It allows the continuous location, without lapse of time, of objects equipped with a GPS receiver anywhere on earth, with a maximum tolerance of 50 metres at the time. It does not comprise any visual or acoustical surveillance. As opposed to transmitters, its use does not necessitate the knowledge of where approximately the person to be located can be found.', compare *Uzun v Germany* Application No 35623/05, Merits, 2 September 2010 at para 13.

[90] *Uzun v Germany* Application No 35623/05, Merits, 2 September 2010 at paras 41-53.

[91] Ibid. at para 52.

[92] Ibid. at para 71.

arose whether the person concerned had to be nonetheless informed of the surveillance measure.

In this regard, the Court however notes that other 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, must have been in place before the surveillance via GPS can be ordered[93]. In this context, the Strasbourg Court refers to the German Criminal Code which provided for the information of the person under surveillance 'as soon as this is possible without endangering the purpose of the investigations, public safety, life and limb of another person or the possible further use of an undercover agent involved in the measure' and concludes that this provision constituted a sufficient protection against abuse:

> 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. '…' Moreover, Article 101 § 1 of the 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 '…'[94].

In conclusion, although the Strasbourg Court deems the surveillance via GPS to be a rather small infringement of Article 8 ECHR, it does not abstain from the notification requirement.

2.7. Limitations of the notification duty - the Mosley case

Another interesting aspect of notification duties after having been the victim of secret recording was recently subject to the case *Mosley v. the United Kingdom*. The newspaper *News of the World* published clandestinely filmed video footage and photos in their print issue as well as on their webpage showing the applicant, Mr. *Mosley*, during sexual activities. The article alleged that his activities were related to sexual Nazi role-plays. He claimed damages in front of domestic UK courts for the privacy infringements and obtained GBP 60,000. However, the applicant brought legal proceedings before the ECtHR, claiming that despite the money granted to him, he remained a victim of the violation of Article 8 ECHR, because the UK did not provide for a legal duty of the press to inform persons concerned in advance of the publication of material concerning their private life. A pre-notification by the newspaper of the planned publication would have given him the possibility to ask for an interim injunction and prevent the publication.

Thus, the main question of this case was whether Article 8 ECHR entails a positive obligation requiring a pre-notification duty in order to ensure effective protection of the right of respect for private life[95]. This right, enshrined in Article 8 ECHR, had therefore to be balanced against the right to freedom of expression stipulated in Article 10 ECHR. The Court first considered that damages in general represent an effective remedy for violations of the right to respect for private life by the press:

> The Court further observes that, in its examination to date of the measures in place at domestic level to protect Article 8 rights in the context of freedom of expression, it has

[93] Ibid. at paras 64-74, in particular at para 72.
[94] Ibid. at para 72.
[95] *Mosley v the United Kingdom* Application No. 48009/08, Merits, 10 May 2011 at para 121.

implicitly accepted that *ex post facto* damages provide an adequate remedy for violations of Article 8 rights arising from the publication by a newspaper of private information '…'[96].

However, there was no uniform approach of the other Member States as regards the pre-notification requirement, nor were there any jurisdiction or legal text requiring such a notification duty and the UK legislation corresponded to the instruments of the Council of Europe enacted so far in this context. Therefore, the margin of appreciation afforded to States was generally a wide one in respect of the measures states must put in place to protect the right to private life[97].

Moreover, although in this particular case the information disclosed was highly private, this could not limit the margin of appreciation of the Member States, given that a pre-notification duty would also affect political reporting and serious journalism[98]. In the UK several other measures to protect the private life had also been in place: a system of self-regulation had been established and persons concerned could institute civil court proceedings to claim damages and interim injunctions, if they were aware of the intended publication concerning their private life.

The Court further analysed the clarity and potential effectiveness of a pre-notification duty. It conducted a hypothetic effectiveness test and considered that even if the pre-notification requirement had existed, it would have required 'some form of public interest'[99], which could have served as an exception from the pre-notification duty to justify publication. In the present case, the newspaper relied on the belief that the sexual activities of Mr. Mosley were related to Nazi role-plays and thus they would have possibly been justified in the public interest[100]. Moreover, even if a pre-notification duty had been in place, the newspaper could have still chosen to circumvent it by publishing the article and the video without notifying Mr. *Mosley* and instead paying a possible sanction ex post[101]. However, the hypothetic effectiveness test regarding the pre-notification duty carried out by the ECtHR raises some doubts on the application of this test in similar cases. Arguing that the notification duty does not represent an effective tool to balance the rights of individuals against the freedom of the press, because the press could circumvent the notification requirement by nonetheless publishing the relevant article and pay a fine subsequently, is not very persuasive. Alleging that a legal rule might not be effective because it is possible to break the rule (and pay a fine ex post) is a circular reasoning and would render any regulative provision unnecessary.

The Court further argues that fines or sanctions could be an effective tool to guarantee compliance with the pre-notification duty, but such fines 'would run the risk of being incompatible with the requirements of Article 10 of the Convention'[102]. In the view of the Court, even if the publication at stake was of entertaining rather than educational nature, it nonetheless profited from the protection offered by Article 10 ECHR[103]. Such protection may only 'cede to the requirements of Article 8 where the

[96] Ibid. at para 120.
[97] Ibid. at paras 81 and 110.
[98] Ibid at paras 122-124.
[99] Ibid. at para 126.
[100] Ibid.
[101] Ibid. at para 128.
[102] Ibid. at para 129.
[103] Ibid. at para 131.

information at stake is of a private and intimate nature and there is no public interest in its dissemination'[104]. The Court concluded:

> However, the Court has consistently emphasised the need to look beyond the facts of the present case and to consider the broader impact of a pre-notification requirement. The limited scope under Article 10 for restrictions on the freedom of the press to publish material which contributes to debate on matters of general public interest must be borne in mind. Thus having regard to the chilling effect to which a pre-notification requirement risks giving rise, to the significant doubts as to the effectiveness of any pre-notification requirement and to the wide margin of appreciation in this area, the Court is of the view that Article 8 does not require a legally binding pre-notification requirement '…'[105].

Thus the Court found that the absence of a pre-notification requirement had not breached Article 8 ECHR.

Although the *Mosley* case is not directly linked to the question of surveillance by the state, it however concerns surveillance by private actors, in this case by journalists. It seems that the ECtHR gets increasingly sensitive as regards the rights of individuals to be informed about infringements of their private life, be it in the context of surveillance measures by the state or in the field of media (law). Comparable to the information requirement in EU law[106], the ECtHR seems to proceed on the assumption that individuals should be in general informed about the information held on them. This information may nonetheless be subject to restrictions. Similar to Article 9 of the Directive 95/46, mentioned above, the Court provides in the *Mosley* case for an exemption for the processing of personal data for journalistic purposes. By doing so, the Court recognises the importance of the freedom of expression in conflicts between the protection of personal data and the freedom of expression and specifies in this way the exemption to the notification duty stipulated in Article 9 of Directive 95/46.

3. Conclusion

Although the analysis of the ECtHR's case-law has revealed a continuous development towards the establishment of a notification duty after surveillance measures have ended, the EU, as well as many Member States, have not yet recognized this obligation in their respective legal frameworks. In ordinary data processing, Directive 95/46 already stipulates a notification requirement for individuals. This article has argued that in view of both, the ECtHR's case-law and the increasing surveillance techniques, the need to establish the notification duty also in a police and secret service context is absolutely essential. To underline this proposition, we conclude with four main theses which clearly illustrate that it is time for the EU and the Member States to recognise the notification duty as part of the ordinary criminal procedure in their respective legal frameworks.

- Notification is a general principle of human rights developed by the ECtHR.

When considering the jurisprudence of the ECtHR in recent years, the Court has determined that it is necessary to establish an active notification duty to comply with

[104] Ibid. at para 131.
[105] Ibid. at para 132.
[106] Article 11 of the Directive 95/46, OJ L 281/31, discussed above.

Article 8 and 13 of the ECHR. Two important results could be observed. First, within the framework of Article 8 ECHR, the notification is seen as an important safeguard against abuse. Second, notification is also considered as an essential tool to guarantee an effective remedy to protect the individual in surveillance cases with regard to Article 13 ECHR.

In particular, the *Ekimdzhiev* case constitutes real progress in terms of the recognition of an active right of notification for individuals in surveillance cases. The Court argues that if the individual is not notified, he is unable to benefit from the protection offered by Articles 8 and 13 ECHR. In this case, the Court seems to have developed a new general principle of human rights derived from the respect of the ECHR. The exceptions from this principle, as formulated in the *Kennedy* and the *Mosley* cases, constitute important specifications. The *Kennedy* case clarifies that if a state does not require the notification, other safeguards enabling the individual to obtain information of surveillance measures have to be in place. *Mosley* establishes an exception for the press.

However, the question needs to be asked whether the *Kennedy* case, in which the ECtHR recognised an alternative to the information duty, is capable of responding to the challenges arising out of the use of new surveillance techniques. Measures such as data retention or 'fishing expeditions' by the police or the secret service increasingly target a greater number of individuals than the 'traditional' surveillance techniques. The storage of personal data in absence of an initial suspicion (for instance at Europol or in the framework of data retention), will also very likely lead to an increasing amount of individuals concerned by surveillance measures. The notification duty appears to be an effective tool to prevent misuse in this fast developing field. Considering these new wide ranging surveillance methods and the number of persons concerned, a tribunal similar to the one described in the *Kennedy* case appears to be nonetheless difficult to implement in practice. If each individual fearing to be subject of surveillance measures makes a complaint before specific tribunals and in each case, these tribunals would have to examine the case, many tribunals with regard to the different surveillance measures in place, would have to be established. In view of these rather practical problems, an automatic and active notification duty seems to be the best solution to comply with the notification requirement following from Articles 8 and 13 of the ECHR.

This understanding is also underlined by one of the first national decisions in Europe interpreting the case law of the ECtHR with regard to notification. The Belgian Constitutional Court in its recent judgement clearly emphasised that the information after the end of surveillance measures 'on request', is not sufficient to comply with Article 8 ECHR (and the Belgian Constitution). According to its understanding, only the active notification of individuals after surveillance measures guarantees compliance with the ECHR and assures that all targeted individuals are able to seek judicial redress after the termination of such measures.

In short, the analysis of the case-law of the ECtHR and its national interpretation has clearly shown the tendency to require the notification of the individual after surveillance has ended. Even if derogations from the notification duty are allowed, the general requirement to notify derives from the respect of Article 8 and 13 ECHR and can be seen as a general principle of human rights developed by the ECtHR in recent years.

- Principle 2.2 of Recommendation R 87 (15) must eventually be applied.

When considering that Recommendation R 87 (15) established the notification duty already in 1987, the very hesitating and slow implementation of this requirement within the Member States and at EU-level is astonishing. If alleging malicious intentions, it seems that this right had been (intentionally) forgotten over the years. Now, considering the emphasis the ECtHR put on the notification duty in its recent case-law, states as well as the EU have to react. At national level, the German legislation and the recent Belgian Constitutional Court decision show that this right can be part of the ordinary criminal procedure and does not hinder successful investigations or surveillance. The qualms of states that this right may in fact help criminals to detect surveillance measures or ongoing investigations is reduced by the precaution that individuals have to be informed only if this information does not jeopardise (ongoing) investigations. But not only the Member States have to implement this principle, the EU must also adhere to the ECHR, in particular in respect of its planned accession. Therefore, the upcoming amendments of the EU-instruments in the former third pillar should be used to establish a general notification right also in the framework of EU law as a form of the normal criminal procedure – only this amendment would bring the EU law in line with the case-law of the ECtHR.

- It is time to recognise the notification duty not only in the framework of Directive 95/46.

As the notification duty exists for all other forms of data processing (compare Directive 95/46) it is essential that the notification is also applicable to police and secret service related activities. The current diversified regulations regarding the notification requirement in the Member States are not adapted to the challenges arising out of the use of new very specific and sophisticated surveillance technologies such as the processing of data in relation to data retention or so called 'fishing expeditions'. Additionally, the general coherence of data protection law in the EU is another strong argument to bring surveillance related activities in line with Directive 95/46. The current revision of Directive 95/46 aims at harmonising the different applicable rules and lays emphasis on the inclusion of the rules on police and judicial cooperation within the scope of the new directive. The consistency of the notification requirement in ordinary, as well as police and secret service related data processing, would be an important contribution to the harmonisation of EU data protection law.

- The *Mosley* case is an important specification of the notification duty.

As every legal rule has its exceptions, the ECtHR has recently increased its efforts to identify and narrow down the scope of this newly recognized notification duty. The non-application of the information requirement in press-related cases is in line with the exceptions as set out in Directive 95/46. This development illustrates how derogations from the notification duty are increasingly better formulated than a few years ago. As a consequence, more detailed exceptions shape the scope of the notification requirement and make room for the implementation of this duty in the EU as well as in the Member States. The latter actors can rely on already established case-law as well as legal acts specifying the concrete application of this right.

To conclude, the notification duty is a key element protecting against the misuse of surveillance techniques and the increasing monitoring of the society. The recognition

of the notification duty by the ECtHR responds to current (and upcoming) challenges arising out of the use of new technologies. Only if individuals are informed about surveillance measures, will they be able to profit from the protection offered by Article 8 and 13 ECHR and only in this case, states comply with their obligation following from the respect of the ECHR.

References (only literature)

[1] Professor Paul DE HERT holds a chair at the Vrije Universiteit Brussel as well as at the Tilburg University; E-mail: paul.de.hert@vub.ac.be.

[2] Dr. Franziska BOEHM is a post-doctoral researcher at the Interdisciplinary Centre for Security, Reliability and Trust (SnT) at the University of Luxembourg; E-mail: franziska.boehm@uni.lu.

[7] Dammann and Simitis (eds), *EG-Datenschutzrichtline*, Commentary to Directive 95/46, Baden-Baden: Nomos Verlag, 1997, Article 10 at para 1; Ehmann and Helfrich (eds), *EG Datenschutzrichtlinie – Kurzkommentar*, Köln: Verlag Dr. Otto Schmidt, 1999, Article 10 at paras 25-28

[13] Dammann and Simitis (eds), *EG-Datenschutzrichtline*, Commentary to Directive 95/46, Baden-Baden: Nomos Verlag, 1997, Article 11 at para 4.

[16] Boehm, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice*, Springer, 2012, p. 231.

[55] Alonso Blas, 'Ensuring data protection in the field of police and judicial activities: some considerations to achieve security, justice and freedom', *ERA Forum* (2010), 233-250, in particular 243.

[107] Damann and Simitis (eds), *EG-Datenschutzrichtline*, Commentary to Directive 95/46, Baden-Baden: Nomos Verlag, 1997, Article 10 at para 1; Ehmann and Helfrich (eds), *EG Datenschutzrichtlinie – Kurzkommentar*, Köln: Verlag Dr. Otto Schmidt, 1999, Article 10 at paras 25-28.