Layout: T1 Standard SC | Book ID: 346872_1_En | Book ISBN: xxx-x-xxxx-xxxx-x
Chapter No.: 15 | Date: 31 October 2015 2:16 PM | Page: 1/26

# Is the Human Rights Framework Still Fit for the Big Data Era? A Discussion of the ECtHR's Case Law on Privacy Violations Arising from Surveillance Activities

Bart van der Sloot

**Abstract** Human rights protect humans. This seemingly uncontroversial axiom might become quintessential over time, especially with regard to the right to privacy. Article 8 of the European Convention on Human Rights grants natural persons a right to complain, in order to protect their individual interests, such as those related to personal freedom, human dignity and individual autonomy. With Big Data processes, however, individuals are mostly unaware that their personal data are gathered and processed and even if they are, they are often unable to substantiate their specific individual interest in these large data gathering systems. When the European Court of Human Rights assesses these types of cases, mostly revolving around (mass) surveillance activities, it finds itself stuck between the human rights framework on the one hand and the desire to evaluate surveillance practices by states on the other. Interestingly, the Court chooses to deal with these cases under Article 8 ECHR, but in order to do so, it is forced to go beyond the fundamental pillars of the human rights framework.

**Keywords** Human rights · Big data · Mass surveillance · Individual harm · Societal interest · Conventionality

Bart van der Sloot is a researcher at the Institute for Information Law (IViR), University of Amsterdam, the Netherlands. This research is part of the project "Privacy as virtue", which is financed by the Dutch Scientific Organization (NWO).

B. van der Sloot (✉)
Instituut Voor Informatierecht (IViR), Room B1.16, Korte Spinhuissteeg 3, 1012 CG
Amsterdam, Netherlands
e-mail: b.vandersloot@uva.nl



S. Gutwirth et al. (eds.), *Data Protection on the Move*,
Law, Governance and Technology Series 24, DOI 10.1007/978-94-017-7376-8_15

Layout: T1 Standard SC | Book ID: 346872_1_En | Book ISBN: xxx-x-xxxx-xxxx-x
Chapter No.: 15 | Date: 31 October 2015 2:16 PM | Page: 2/26



# 1 Introduction

Human rights are designed to protect humans. Whether one accepts the philosophical idea that they are innate to man even in the state of nature,[1] the theological belief that God has bestowed these rights uniquely onto man,[2] the Habermasian theory of the internal correlation between human rights and democracy,[3] or any other theory, human rights have a unique position in legal discourse. They stand apart from other doctrines and rights in that they are conceived as fundamental, sometimes even non-derogable, and protect the most basic personal needs and interest of every human being, regardless of legal status or background. This focus on the individual is even stronger with regard to the right to privacy, Article 8, than with many other human rights as protected under the European Convention on Human Rights (ECHR). This focus on individual rights of natural persons and their personal interests is quite understandable, as privacy is the most 'private' and 'personal' of all human rights. It should also be recognized that this focus has worked very effectively for decades; it has allowed the European Court of Human Rights (ECtHR) to deal not only with the more traditional privacy violations, such as house searches, wiretapping and body cavity searches, but also with the right to develop one's sexual,[4] relational[5] and minority identity,[6] the right to protect one's reputation and honour,[7] the right to personal development,[8] the right of foreigners

[1]Among others: Thomas Hobbes, *Leviathan* (Cambridge: Cambridge University Press, 1996 [1651]). Thomas Paine, *The rights of man: for the benefit of all mankind* (Philadelphia: Webster, 1797 [1791]).

[2]Even in Locke, one might find references to this view: John Locke, *Two treatises of government* (Cambridge: Cambridge University Press, 1988 [1689]).

[3]Jurgen Habermas, 'On the Internal Relation between the Rule of Law and Democracy', *European Journal of Philosophy* 3 (1995).

[4]ECtHR, I.G. v. Slovakia, appl. no. 15966/04, 13 November 2012. ECtHR, V.C. v. Slovakia, appl. no. 18968/07, 08 November 2011. ECtHR, Evans v. the United Kingdom, appl. no. 6339/05, 10 April 2007. ECtHR, Dickson v. the United Kingdom, appl. no. 44362/04, 04 December 2007.

[5]ECtHR, Phinikaridou v. Cyprus, appl. no. 23890/02, 20 December 2007. ECtHR, Mikulic v. Croatia, appl. no. 53176/99, 07 February 2002. ECtHR, Gaskin v. the United Kingdom, appl. no. 10454/83, 07 July 1989.

[6]ECmHR, Lay v. the United Kingdom, appl. no. 13341/87, 14 July 1988. ECmHR, Smith v. the United Kingdom, appl. no. 14455/88, 04 September 1991. ECmHR, Smith v. the United Kingdom, appl. no. 18401/91, 06 May 1993. ECmHR, G. and E. v. Norway, appl. no. 9278/81, 03 October 1983. ECtHR, Chapman v. the United Kingdom, appl. no. 27238/95, 18 January 2001. ECtHR, Aksu v. Turkey, appl. nos. 4149/04 and 41029/04, 27 July 2010.

[7]ECtHR, Pfeifer v. Austria, appl. no. 12556/03, 15 November 2007. ECtHR, Rothe v. Austria, appl. no. 6490/07, 04 December 2012. ECtHR, A. v. Norway, appl. no. 28070/06, 09 April 2009.

[8]ECmHR, X. v. Iceland, appl. no. 6825/74, 18 May 1976. ECtHR, Frette v. France, appl. no. 36515/97, 26 February 2002. ECtHR, Varapnickaite-Mazyliene v. Lithuania, appl. no. 20376/05, 17 January 2012. See further: ECtHR, Biriuk v. Lithuania, appl. no. 23373/03, 25 November 2008. ECtHR, Niene v. Lithuania, appl. no. 36919/02, 25 November 2008. ECtHR, Goodwin v. the United Kingdom, appl. no. 28957/95, 11 July 2002. ECtHR, B. v. France, appl. no. 13343/87, 25 March 1992.

Layout: T1 Standard SC | Book ID: 346872_1_En | Book ISBN: xxx-x-xxxx-xxxx-x
Chapter No.: 15 | Date: 31 October 2015 2:16 PM | Page: 3/26



to a legalized stay,[9] the right to property and even work,[10] the right to environmental protection[11] and the right to have a fair and equal chance in custody cases.[12] Although some say that the broadened scope of the ECHR in general and the right to privacy in particular has gone too far,[13] one thing is clear: the current privacy paradigm under the European Convention on Human Rights works very well when it is applied to cases that revolve around individual rights and individual interests of natural persons.

However, the current developments known as Big Data might challenge this approach.[14] Big Data, for the purpose of this study, is defined as gathering massive amounts of data without a pre-established goal or purpose, about an undefined number of people, which are processed on a group or aggregated level through the use of statistical correlations.[15] The essence of these types of cases is thus that the individual element is lost, although data may originally be linked to individuals and the results of Big Data processes may be applied to individuals or groups of

[9]ECtHR, Moustaquim v. Belgium, appl. no.12313/86, 18 February 1991. ECtHR, Cruzvaras and others v. Sweden, appl. no. 15576/89, 20 March 1991. ECtHR, Sen v. the Netherlands, appl. no. 31465/96, 21 December 2001. ECtHR, Slivenko v. Latvia, appl. no. 48321/99, 09 October 2003. ECtHR, Sisojeva and others v. Latvia, appl. no. 60654/00, 15 January 2007. ECtHR, Nasri v. France, appl. no. 19465/92, 13 July 1995.

[10]ECtHR, Karner v. Austria, appl. no. 40016/98, 24 July 2003. ECtHR, Sidabras and Dziautas v. Lithuania, appl. nos. 55480/00 and 59330/00, 27 July 2004. ECtHR, Coorplan-Jenni GMBH and Hascic v. Austria, appl. no. 10523/02, 24 February 2005. ECtHR, Ozpinar v. Turkey, appl. no. 20999/04, 19 October 2010.

[11]ECtHR, Moreno Gomez v. Spain, appl. no. 4143/02, 16 November 2004. ECtHR, Villa v. Italy, appl. no. 36735/97, 14 November 2000. ECtHR, Kyrtatos v. Greece, appl. no. 41666/98, 22 May 2003. ECtHR, Morcuende v. Spain, appl. no. 75287/01, 06 September 2005. ECtHR, López Ostra v. Spain, appl. no. 16798/90, 09 December 1994. ECtHR, Ledyayeva, Dobrokhotova, Zolotareva and Romashina v. Russia, appl. nos. 53157/99, 53247/99, 56850/00 and 53695/00, 26 October 2006.

[12]ECtHR, B. v. the United Kingdom, appl. no. 9840/82, 8 July 1987. See similarly: ECtHR, R. v. the United Kingdom, appl. no. 10496/83, 8 July 1987. ECtHR, W. v. the United Kingdom, appl. no. 9749/82, 8 July 1987. ECtHR, Diamante and Pelliccioni v. San Marino, appl. no. 32250/08, 27 September 2011.

[13]Janneke Gerards, "The prism of fundamental rights", *European Constitutional Law Review*, 8 (2012): 2.

[14]See further: Antonella Galetta & Paul De Hert, 'Complementing the Surveillance Law Principles of the ECtHR with its Environmental Law Principles: An Integrated Technology Approach to a Human Rights Framework for Surveillance', *Utrecht Law Review*, 10-1, 2014. Thérèse Murphy & Gearóid Ó Cuinn, 'Work in progress. New technologies and the European Court of Human Rights', *Human Rights Law Review*, 2010.

[15]See further: Viktor Mayer-Schönberger and Kenneth Cukier, *Big data: a revolution that will transform how we live, work, and think* (Boston: Houghton Mifflin Harcourt, 2013). Terence Craig and Mary E. Ludloff, *Privacy and Big Data: The Players, Regulators, and Stakeholders* (Sebastopol: O'Reilly Media, 2011). Kate Crawford and Jason Schultz, "Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms", *Boston College Law Review* 55 (2014): 93.

Layout: T1 Standard SC | Book ID: 346872_1_En | Book ISBN: xxx-x-xxxx-xxxx-x
Chapter No.: 15 | Date: 31 October 2015 2:16 PM | Page: 4/26



individuals. Data are not gathered about a specific person or group (for example those suspected of having committed a particular crime), rather, they are gathered about an undefined number of people during an undefined period of time without a pre-established reason. The potential value of the gathered data becomes clear only after they are subjected to analysis by computer algorithms, not on beforehand.[16] These data, even if they are originally linked to specific persons, are subsequently processed by finding statistical correlations. It may appear, for example, that the data string—Muslim + vacation to Yemen + visit to website X—leads to an increased risk of a person being a terrorist.[17] The data are not based on personal data of specific individuals, but processed on an aggregated level and the profiles are formulated on a group level.[18]

Given this constellation of facts, it becomes more and more difficult for an individual to point out his specific personal interest and personal harm (defined by Feinberg as a setback to interests) in Big Data processes.[19] It should be acknowledged that in the field of privacy, the notion of harm has always been problematic as it is often difficult to substantiate the harm a particular violation has done, e.g. what harm follows from entering a home or eavesdropping on a telephone conversation as such when neither objects are stolen nor private information disclosed to third parties? Even so, the more traditional privacy violations (house searches, telephone taps, etc.) are clearly demarcated in time, place and person and the effects are therefore relatively easy to define. In the current technological environment, however, the individual is often simply unaware that his personal data are gathered by either his fellow citizens (e.g. through the use of their smartphones), by companies (e.g. by tracking cookies) or by governments (e.g. through covert surveillance). Obviously, people unaware of the fact that their data are gathered will not invoke their right to privacy in court.

But even if a person would be aware of these data collections, given the fact that data gathering and processing is currently so widespread and omnipresent,

[16]See further: Rob Kitchin, *The Data Revolution: Big Data, Data infrastructures & their consequences* (Los Angeles: Sage, 2014). Andrew McAfee and Eerik Brynjolfsson, "Big Data: The management Revolution: Exploiting vast new flows of information can radically improve your company's performance. But first you'll have to change your decision making culture", *Harvard Business Review* October 2012. Mark Andrejevic, "The Big Data Divide", *International Journal of Communication* 8 (2014).

[17]See for literature on profiling: Toon Calders & Sicco Verwer, "Three Naive Bayes Approaches for Discrimination-Free Classification", *Data Mining and Knowledge Discovery 21(2),* (2010). Bart H. M. Custers, *The Power of Knowledge; Ethical, Legal, and Technological Aspects of Data Mining and Group Profiling in Epidemiology* (Tilburg: Wolf Legal Publishers, 2004). Mireille Hildebrandt & Serge Gutwirth (eds.), *Profiling the European Citizen Cross-Disciplinary Perspectives* (New York: Springer, 2008). Daniel T. Larose, *Data mining methods and models* (New Yersey: John Wiley & Sons, 2006). Tal Z. Zarsky, "Mine your own business!: making the case for the implications of the data mining of personal information in the forum of public opinion", *Yale Journal of Law & Technology (5),* 2003.

[18]See further: Chris J. Hoofnagle, "How the Fair Credit Reporting Act Regulates Big Data", <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2432955>.

[19]Joel Feinberg, *Harm to others* (New York: Oxford University Press, 1984).

Layout: T1 Standard SC | Book ID: 346872_1_En | Book ISBN: xxx-x-xxxx-xxxx-x
Chapter No.: 15 | Date: 31 October 2015 2:16 PM | Page: 5/26



and will become even more so in the future, it will quite likely be impossible for him to keep track of every data processing which includes (or might include) his data, to assess whether the data controller abides by the legal standards applicable, and if not, to file a legal complaint. And if an individual does go to court to defend his rights, he has to demonstrate a personal interest, i.e. personal harm, which is a particularly problematic notion in Big Data processes, e.g. what concrete harm has the data gathering by the NSA done to an ordinary American or European citizen? This also shows the fundamental tension between the traditional legal and philosophical discourse and the new technological reality—while the traditional discourse is focused on individual rights and individual interests, data processing often affects a structural and societal interest.

This chapter will discuss how the Court deals with privacy violations by the state through the use of (mass) surveillance under Article 8 ECHR. These are, so far, the only cases under the ECHR that concern mass data gathering, storage and processing (it should be remembered that the Convention can only be invoked against states and not against companies). Section 2 will briefly outline the dominant approach of the Court when it deals with cases under Article 8 ECHR. Sections 3– 5 will point out that the Court is willing to relax its focus on individual rights and interests when cases regard surveillance activities. It does so in three distinct ways. Section 3 will present the cases in which the Court focusses not on actual and concrete harm, but on hypothetical harm through the use of the notion of 'reasonable likelihood'. Section 4 describes under which circumstances the Court is willing to accept a 'chilling effect', or future harm, as basis for a claim. Section 5 discusses the Court's third and final approach to these cases, which is also the most controversial one. Sometimes, it is willing to accept *in abstracto* claims, complaints about the legality and legitimacy of laws or policies as such.

Finally, Sect. 6, containing the analysis, will discuss what this last approach implies for the significance of human rights in the age of Big Data. Given the fact that the notions of individual harm and personal interest are so difficult to uphold in Big Data practices, the abstract assessments of Big Data practices may have a high potential, as the specific characteristic of *in abstracto* claims is that the complainant is not required to show any personal interest. Rather, the complaint regards a general or societal interest and addresses a law or policy as such. However, if it is true that human rights protect humans and their most essential needs and interests, the question is how this type of complaints can be reconciled with the basic pillars of the human rights framework. The more fundamental question is perhaps: can the problems following from mass surveillance activities and Big Data practices by states be qualified as human rights violations or do they rather regard general principles of good governance and due process? And, is it proper to assess the mere legality and legitimacy of governmental policies, without any human right being at stake, under a human rights framework? The main conclusion of this chapter is that it is impossible to address certain problems following from Big Data processes in general and mass surveillance activities in particular under human rights frameworks.

Layout: T1 Standard SC | Book ID: 346872_1_En | Book ISBN: xxx-x-xxxx-xxxx-x
Chapter No.: 15 | Date: 31 October 2015 2:16 PM | Page: 6/26



## 2 The Right to Privacy (Article 8 ECHR)

The right to privacy under the European Convention on Human Rights, Article 8, is focussed on the individual in many ways. To successfully submit an application, a complainant must of course have exhausted all domestic remedies, the application should be submitted within the set time frame and it must fall under the competence of the Court. But more importantly, the applicant needs to demonstrate a personal interest, i.e. individual harm following from the violation complained of. This is linked to the notion of *ratione personae*, the question whether the claimant has individually and substantially suffered from a privacy violation, and in part to that of *ratione materiae*, the question whether the interest said to be interfered falls under the protective scope of the right to privacy. This focus on individual harm and individual interests brings with it that certain types of complaints are declared inadmissible by the European Court of Human Rights, which means that the cases will not be dealt with in substance.[20]

So called *in abstracto* claims are in principle declared inadmissible. These are claims that regard the mere existence of a law or a policy, without them having any concrete or practical effect on the claimant. 'Insofar as the applicant complains in general of the legislative situation, the Commission recalls that it must confine itself to an examination of the concrete case before it and may not review the aforesaid law *in abstracto*. The Commission therefore may only examine the applicant's complaints insofar as the system of which he complains has been applied against him.'[21] *A priori* claims are rejected as well, as the Court will usually only receive complaints about injury which has already materialized. A-contrario, claims about future damage will in principle not be considered. 'It can be observed from the terms "victim" and "violation" and from the philosophy underlying the obligation to exhaust domestic remedies provided for in Article 26 that in the system for the protection of human rights conceived by the authors of the Convention, the exercise of the right of individual petition cannot be used to prevent a potential violation of the Convention: in theory, the organs designated by Article 19 to ensure the observance of the engagements undertaken by the Contracting Parties in the Convention cannot examine—or, if applicable, find—a violation other than a posteriori, once that violation has occurred. Similarly, the award of just satisfaction, i.e. compensation, under Article 50 of the Convention is limited to cases in which the internal law allows only partial reparation to be made, not for the violation itself, but for the consequences of the decision or measure in question which has been held to breach the obligations laid down in the Convention.'[22]

Hypothetical claims regard damage which might have materialized, but about which the claimant is unsure. The Court usually rejects such claims because it is

[20] <http://www.echr.coe.int/Documents/Admissibility_guide_ENG.pdf>.

[21] ECmHR, Lawlor v. the United Kingdom, application no. 12763/87, 14 July 1988.

[22] ECmHR, Tauira and others v. France, application no. 28204/95, 04 December 1995.

Layout: T1 Standard SC | Book ID: 346872_1_En | Book ISBN: xxx-x-xxxx-xxxx-x
Chapter No.: 15 | Date: 31 October 2015 2:16 PM | Page: 7/26



unwilling to provide a ruling on the basis of presumed facts. The applicant must be able to substantiate his claim with concrete facts, not with beliefs and suppositions. The ECtHR will also not receive an *actio popularis*, a case brought up by a claimant or a group of claimants, not to protect their own interests, but to protect those of others or society as a whole. These types of cases are better known as class actions. 'The Court reiterates in that connection that the Convention does not allow an *actio popularis* but requires as a condition for exercise of the right of individual petition that an applicant must be able to claim on arguable grounds that he himself has been a direct or indirect victim of a violation of the Convention resulting from an act or omission which can be attributed to a Contracting State.'[23]

Furthermore, the Court has held that applications are rejected if the injury claimed following from a specific privacy violation is not sufficiently serious, even although it does fall under the scope of Article 8 ECHR. This can also be linked to the more recent introduction of the so called *de minimis* rule in the Convention, which provides that a claim will be declared inadmissible if 'the applicant has not suffered a significant disadvantage'.[24] With environmental issues, for example, it has been ruled that if the level of noise is not sufficiently high, it will not be considered an infringement on a person's private life or home.[25] Similarly, although data protection partially falls under the scope of Article 8 ECHR, if only the name, address and other ordinary data are recorded about an applicant, the case will be declared inadmissible, because such 'data retention is an acceptable and normal practice in modern society. In these circumstances the Commission finds that this aspect of the case does not disclose any appearance of an interference with the applicants' right to respect for private life ensured by Article 8 of the Convention.'[26] Moreover, an interference might have existed which can be substantiated by the applicant and which was sufficiently serious to fall under the scope of Article 8 ECHR. Still, if the national authorities have acknowledged their wrongdoing and provided the victim with sufficient relief and/or retracted the law or policy on which the violation was based, the person can no longer claim to be a victim under the scope of the Convention.[27]

Then there is the material scope of the right to privacy, Article 8 ECHR. In principle, it only provides protection to a person's private life, family life, correspondence and home. However, the Court has been willing to give a broader interpretation. As discussed in the introduction, it has held, inter alia, that the right to

[23]ECtHR, Asselbourg and 78 others and Greenpeace Association-Luxembourg v. Luxembourg, application no. 29121/95, 29 June 1999.

[24]Article 35 paragraph 3 (b) ECHR.

[25]ECmHR, Trouche v. France, application no. 19867/92, 01 September 1993. ECmHR, Glass v. the United Kingdom, application no. 28485/95, 16 October 1996.

[26]ECmHR, Murray v. the United Kingdom, application no. 14310/88, 10 December 1991.

[27]Dean Spielmann, *Bringing a case to the European Court of Human Rights: a practical guide on admissibility criteria* (Oisterwijk: Wolf Legal Publishers, 2014). Theodora A. Christou & Juan Pablo Raymon, *European Court of Human Rights: remedies and execution of judgments* (London: BIICL, British Institute of International and Comparative Law cop. 2005).

privacy also protects the personal development of an individual, it includes protection from environmental pollution and may extend to data protection issues.[28] Still, what distinguishes the right to privacy from other rights under the Convention, such as the freedom of expression, is that it only provides protection to individual interests. While the freedom of expression is linked to personal expression and development, it is also connected to societal interests, such as the search for truth through the market place of ideas and the well-functioning of the press, a precondition for a liberal democracy. By contrast, Article 8 ECHR, in the dominant interpretation of the ECtHR, only protects individual interests, such as autonomy, dignity and personal development (in literature, scholars increasingly emphasize a public dimension of privacy). Cases that do not regard such matters are rejected by the Court.[29]

This focus on individual interests has also had an important effect on the types of applicants that are able to submit a complaint about the right to privacy. The Convention, in principle, allows natural persons, groups of persons and legal persons to complain about an interference with their rights under the Convention. Indeed, the Court has accepted that, under certain circumstances, churches may invoke the freedom of religion (Article 9 ECHR), that press organisations may rely on the freedom of expression (Article 10 ECHR) and that trade unions are admissible if they claim the freedom of assembly and association (Article 11 ECHR). However, because Article 8 ECHR only protects individual interests, the Court has said that in principle, only natural persons can invoke a right to privacy. For example, when a church complained about a violation of its privacy by the police in relation to criminal proceedings, the Commission found that '[t]he extent to which a non-governmental organization can invoke such a right must be determined in the light of the specific nature of this right. It is true that under Article 9 of the Convention a church is capable of possessing and exercising the right to freedom of religion in its own capacity as a representative of its members and the entire functioning of churches depends on respect for this right. However, unlike Article 9, Article 8 of the Convention has more an individual than a collective character [].'[30] This led the Commission to declare the complaint inadmissible, a line which has been confirmed in the subsequent case law of the Court and which it is willing to leave only in exceptional cases.[31] Groups of natural persons claiming a Convention

[28]See among others: ECtHR, Leander v. Sweden, application no. 9248/81, 26 March 1987. ECtHR, Amann v. Switserland, application no. 27798/95, 16 February 2000. EctHR, Rotaru v. Roemenia, application no. 28341/95, 04 May 2000. See also: <http://www.echr.coe.int/Documents/FS_Data_ENG.pdf>.

[29]See for one of the earliest examples of the broadening scope of Article 8 ECHR: ECmHR, X. v. Iceland, application no. 6825/74, 18 May 1976.

[30]ECmHR, Church of Scientology of Paris v. France, application no. 19509/92, 09 January 1995.

[31]See among others: ECtHR, Stes Colas Est and others v. France, application no. 37971/97, 16 April 2002. See in more detail: Bart van der Sloot, "Do privacy and data protection rules apply to legal persons and should they? A proposal for a two-tiered system", *Computer Law & Security Review* 31 (2015): 1.

right are also principally rejected by the Court and the possibility of inter-state complaints (Article 33 ECHR) is seldom practiced.[32] This leaves only the individual to submit a complaint about a breach of the right to privacy.

The problem is that this focus on natural persons and individual harm is difficult to uphold in cases that concern practices that do not revolve around specific individuals, but affect large groups in society or potentially everyone. Mass (covert) surveillance is the example par excellence, but Big Data practices in general pose a problem for the victim-requirement of the Court. Given the trend of increasingly big data collection and aggregation systems, the relevance of these types of cases is likely to increase. In these types of cases, the Court is often faced with the choice between sticking to its strict interpretation of the victim-requirement and declaring the cases inadmissible or accepting that the cases fall under its jurisdiction and leaving or stretching its focus on individual harm. The Court typically chooses the latter option in three instances: (1) when there is a reasonable chance that the applicant has been harmed, (2) when it is likely that the applicant will be affected by the practice in the future and (3) when the mere existence of a law or policy as such leads to a violation of Article 8 ECHR. These three approaches will be briefly discussed in the following three sections.

## 3 Reasonable Likelihood (Hypothetical Harm)

Obviously, a discussion about the victim-requirement and surveillance activities by the state has to start with *Klass and others v. Germany*,[33] which revolved around the claim by the applicants that the contested German legislation permitted surveillance measures without obliging the authorities in every case to notify the persons concerned after the event. They also complained about the lack of remedy before the courts against the ordering and execution of such measures. This led, according to them, to a situation of potentially unchecked and uncontrolled surveillance, as those affected by the measures were kept unaware and would, consequently, not challenge them in a legal procedure. In essence, the case revolved around hypothetical harm, as the applicants claimed that they could have been the victims of surveillance activities employed by the German government, but they were unsure as the governmental services remained silent on this point. The claimants were judges and lawyers, professions which cannot function without respect for secrecy of deliberations or of contacts with clients. Moreover, by virtue of their profession, they are more likely to be affected by the measures than ordinary citizens, at least so the applicants claimed. The government, to the contrary, pointed

[32] See further: Bart van der Sloot, "Privacy in the Post-NSA Era: Time for a Fundamental Revision?", *Journal of intellectual property, information technology and electronic commerce law*, 5 (2014a): 1.

[33] ECtHR, Klass and others v. Germany, application no. 5029/71, 06 September 1978.

Layout: T1 Standard SC | Book ID: 346872_1_En | Book ISBN: xxx-x-xxxx-xxxx-x
Chapter No.: 15 | Date: 31 October 2015 2:16 PM | Page: 10/26



out that the applicants could not substantiate their claim that they were victims of the contested surveillance activities and consequently, that they were bringing forth an *in abstracto* claim.

The Commission, deciding on the admissibility of the case, referred to Article 25 ECHR, the current Article 34 ECHR, which specifies: 'The Court may receive applications from any person, nongovernmental organisation or group of individuals claiming to be the victim of a violation by one of the High Contracting Parties of the rights set forth in the Convention or the Protocols thereto. The High Contracting Parties undertake not to hinder in any way the effective exercise of this right.' It argued that under this provision 'only the victim of an alleged violation may bring an application. The applicants, however, state that they may be or may have been subject to secret surveillance, for example, in course of legal representation of clients who were themselves subject to surveillance, and that persons having been the subject of secret surveillance are not always subsequently informed of the measures taken against them. In view of this particularity of the case the applicants have to be considered as victims for purposes of Art. 25.'[34]

Before the Court, which dealt with the case in substance, the Delegates of the Commission considered that the government was requiring a too rigid standard for the notion of 'victim'. They submitted that, in order to be able to claim to be the victim of an interference with the exercise of the right to privacy, 'it should suffice that a person is in a situation where there is a reasonable risk of his being subjected to secret surveillance.'[35] The Court took it even one step further and held that 'an individual may, under certain conditions, claim to be the victim of a violation occasioned by the mere existence of secret measures or of legislation permitting secret measures, without having to allege that such measures were in fact applied to him.'[36] In this case, the Court thus accepted an *in abstracto* claim, instead of a hypothetical claim, as the 'mere existence' of a law may lead to an interference with Article 8 ECHR.[37] This contrasts with the test proposed by the Delegates, namely whether there is a 'reasonable likelihood' that the applicants were affected by the measures complained of. In the latter test, the requirement of personal harm remains, though it is not made dependent on actual and concrete proof, but on a reasonable suspicion; in the abstract test, the requirement of personal harm is abandoned, as the laws and policies are assessed as such.

[34]ECmHR, Klass and others v. Germany, application no. 5029/71, 18 December 1974.

[35]ECtHR, Klass and others v. Germany, application no. 5029/71, 06 September 1978, § 31.

[36]ECtHR, Klass and others v. Germany, application no. 5029/71, 06 September 1978, § 34.

[37]There is also a discussion about the question whether surveillance in itself entails enough injury to bring a case under the scope of Article 8 ECHR. See among others: ECmHR, Herbecq and the Association Ligue Des Droits de L'Homme v. Belgium, application nos. 32200/96 and 32201/96, 14 January 1998. ECtHR, Perry v. the United Kingdom, application no. 63737/00, 17 July 2003. There is also discussion about in how far redress should go to render claims inapplicable. ECtHR, Rotaru v. Romania, application no. 28341/95, 04 May 2000.

Layout: T1 Standard SC | Book ID: 346872_1_En | Book ISBN: xxx-x-xxxx-xxxx-x
Chapter No.: 15 | Date: 31 October 2015 2:16 PM | Page: 11/26



Both approaches have played an important role in the Court's subsequent case law.[38] The abstract test was adopted in *Malone v. the UK*[39] and in *P.G. and J.H. v. the UK*,[40] among other cases. In *Mersch and others v. Luxembourg*, the Commission carefully distinguished between the two tests, applying them to two different types of complaints. The case was declared incompatible with the provisions of the Convention in so far as it regarded a violation of the Convention's provisions on account of measures taken under a legal instrument, as the claimants had not been subjected to surveillance measures. Likewise, the Commission stressed that legal persons, one of the applicants being a legal person, could not complain about such matters as they could not be subjected to monitoring or surveillance ordered in the course of criminal proceedings because legal persons had no criminal responsibility. However, it continued to point out that another part of the claim regarded laws as such, allowing for surveillance not confined to persons who may be suspected of committing the criminal offences referred to therein. With regard to this abstract claim, the Commission accepted all applicants in their claim and declared the case admissible.[41] Vice versa, in *Hilton v. the UK*, the Commission stated that 'the Klass case falls to be distinguished from the present case in that there existed a legislative framework in that case which governed the use of secret measures and that this legislation potentially affected all users of postal and telecommunications services. In the present case the category of persons likely to be affected by the measures in question is significantly narrower. On the other hand, the Commission considers that it should be possible in certain cases to raise a complaint such as is made by the applicant without the necessity of proving the existence of a file of personal information. To fall into the latter category the Commission is of the opinion that applicants must be able to show that there is, at least, a reasonable likelihood that the Security Service has compiled and continues to retain personal information about them.'[42]

Section 5 will explore the use of the abstract test by the Court in more detail. What is important to note with regard to the reasonable likelihood test[43] is that two

[38]ECtHR, Case of Association "21 December 1989" and others v. Romania, application nos. 33810/07 and 18817/08, 24 May 2011. ECmHR, Spillmann v. Switzerland, application no. 11811/85, 08 March 1988.

[39]ECmHR, Malone v. the United Kingdom, application no. 8691/79, 13 July 1981. See further: ECtHR, Leander v. Sweden, application no. 9248/81, 26 March 1987. ECtHR, Huvig v. France, application no. 11105/84, 24 April 1990. ECtHR, Kruslin v. France, application no. 11801/85, 24 April 1990.

[40]ECtHR, P.G. and J.H. v. the United Kingdom, application no. 44787/98, 25 September 2001.

[41]ECmHR, Mersch and others v. Luxembourg, application nos. 10439/83, 10440/83, 10441/83, 10452/83, 10512/83 and 10513/83, 10 May1985.

[42]ECmHR, Hilton v. the United Kingdom, application no. 12015/86, 06 July 1988.

[43]ECtHR, Stefanov v. Bulgaria, applicaiton no. 65755/01, 22 May 2008. ECmHR, Nimmo v. the United Kingdom, application no. 12327/86, 11 October 1988.

Layout: T1 Standard SC | Book ID: 346872_1_En | Book ISBN: xxx-x-xxxx-xxxx-x
Chapter No.: 15 | Date: 31 October 2015 2:16 PM | Page: 12/26



aspects can lead to the establishment of a reasonable likelihood.[44] First, if the applicant falls under a group or category that is specifically mentioned in the law on which the surveillance activities are based. In these types of cases, the Court is willing to accept that applicants who fall under these categories can demonstrate a reasonable likelihood that they had been affected by the matters complained of. Second, the Court takes into account specific actions by the applicants which make them more likely to be affected by surveillance measures. In *Matthews v. the UK*, for example, the Commission decided that the assumption of the applicants that they were wiretapped was not substantiated by their argument that they heard mysterious clicking noises when telephoning. 'However, in view of the fact that the applicant was active in the campaign against Cruise (nuclear) missiles in the United Kingdom, the Commission will assume for the purposes of this decision that the applicant has established a reasonable possibility that her telephone conversations were intercepted pursuant to a warrant for the purposes of national security.'[45]

## 4 Chilling Effect (Future Harm)

The chilling effect principle is mostly connected to the freedom of speech and the Court uses it to explain that certain actions by the government, although not directly limiting the freedom of speech of its citizens, may lead to self-restraint: a chilling effect in the lawful use of a right. The chilling effect is the effect which exists when people know that they are watched of know that they might be watched. Afraid of the potential consequences, people will restrain their behavior and abstain from certain acts which they perceive as possibly inciting negative consequences.[46] However, the Court is also willing to accept this doctrine in

[44]ECtHR, Senator Lines GmbH v. Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, the Netherlands, Portugal, Spain, Sweden and the United Kingdom, application no. 56672/00, 10 March 2004. ECtHR, Segi and others and Gestoras Pro-Amnistia and others v. 15 states of the European Union, application nos. 6422/02 and 9916/02, 23 May 2002. ECmHR, Tauira and 18 others v. France, application no. 28204/95, 04 December 1995. ECtHR, C. and D. and S. and others v. the United Kingdom, application nos. 34407/02 and 34593/02, 31 August 2004. ECtHR, C. v. the United Kingdom, application no. 14858/03, 14 December 2004. ECtHR, Berger-Krall and others v. Slovenia, application no. 14717/04, 12 June 2014. ECmHR, Esbester v. the United Kingdom, application no. 18601/91, 02 April 1993. ECmHR, Hewitt and Harman v. the United Kingdom, application no. 20317/92, 01 September 1993. ECmHR, Redgrave v. the United Kingdom, application no. 20271/92, 01 September 1993. ECmHR, T.D., D.E. and M.F. v. the United Kingdom, application nos. 18600/91, 18601/91 and 18602/91, 12 October 1992.

[45]ECmHR, Matthews v. the United Kingdom, application no. 28576/95, 16 October 1996. ECtHR, Halford v. the United Kingdom, application no. 20605/92, 25 June 1997, § 48.

[46]Jeremy Bentham, *Panopticon; or The inspection-house* (Dublin, 1791). Michel Foucault, *Surveiller et punir: naissance de la prison* (Paris, Gallimard, 1975).

Layout: T1 Standard SC | Book ID: 346872_1_En | Book ISBN: xxx-x-xxxx-xxxx-x
Chapter No.: 15 | Date: 31 October 2015 2:16 PM | Page: 13/26



certain cases relating to Article 8 ECHR, primarily when they regard surveillance measures, but also in relation to laws that discriminate or stigmatize certain groups in society. Here, the Court is willing to accept that although no harm has been done yet to an applicant, he may still be received in his (a priori) claim if it is likely that he will suffer from harm in the future, either because he is curtailed in his right to privacy by the government or because he will resort to self-restraint in the use of his right.

An example may be the case of *Michaud v. France*, in which the applicant complained that because lawyers were under an obligation to report suspicious operations, as a lawyer he was required, subject to disciplinary action, to report people who came to him for advice. He considered this system to be incompatible with the principles of lawyer-client privilege and professional confidentiality. The government maintained, however, that the applicant could not claim to be a 'victim' as his rights had not actually been affected in practice, highlighting that he did not claim that the legislation in question had been applied to his detriment, but simply that he had been obliged to organize his practice accordingly and introduce special internal procedures. This would qualify as an *in abstracto* claim, according to the government. It continued to stress that if the Court accepted his status as a 'potential victim', this would open the door for class actions.

The Court pointed out that, indeed, in order to be able to lodge an application in pursuance of Article 34 of the Convention, a person must be able to claim to be a 'victim' of a violation of the rights enshrined in the Convention: to claim to be a victim of a violation, a person must be directly affected by the impugned measure. The ECHR does not envisage the bringing of an *actio popularis* for the interpretation of the rights set out therein, the Court continued, or permit individuals to complain about a provision of national law simply because they consider, without having been directly affected by it, that it may contravene the Convention. Referring to *Marckx v. Belgium*, *Johnston and others v. Ireland*, *Norris v. Ireland* and *Burden v. the UK*, it stressed, however, that it is 'open to a person to contend that a law violates his rights, in the absence of an individual measure of implementation, and therefore to claim to be a "victim" within the meaning of Article 34 of the Convention, if he is required to either modify his conduct or risk being prosecuted, or if he is a member of a class of people who risk being directly affected by the legislation.'[47]

The Court pointed out that if the applicant failed to report suspicious activities as required he would expose himself by virtue of the law to disciplinary sanctions up to and including being struck off. The Court also considered credible the applicant's suggestion that, as a lawyer specialising in financial and tax law, he was even more concerned by these obligations than many of his colleagues and exposed to the consequences of failure to comply. In fact he was faced with a dilemma comparable, mutatis mutandis, to that which the Court already identified in *Dudgeon v. the UK* and Norris: either he applies the rules and relinquishes his

[47]ECtHR, Michaud v. France, application no. 12323/33, 06 December 2012, § 51.

Layout: T1 Standard SC | Book ID: 346872_1_En | Book ISBN: xxx-x-xxxx-xxxx-x
Chapter No.: 15 | Date: 31 October 2015 2:16 PM | Page: 14/26



idea of the principle of lawyer-client privilege, or he decides not to apply them and exposes himself to disciplinary sanctions and even being struck off. Therefore, the Court accepted that the applicant was directly affected by the impugned provisions and could therefore claim to be a 'victim' of the alleged violation of Article 8. In conclusion, the Court accepted a victim status, not because the applicant had actually suffered from any concrete harm, but because he was likely to be affected by it in the future, either because he would restrict or limit his behaviour or because he would not and face a legal sanction.

The references to the cases of, inter alia, Marckx, Dudgeon and Norris, are particularly telling. The Court is also willing to relax its strict focus on individual harm when cases regard potential discrimination and stigmatization of weaker groups in society. For example, it has accepted that where the national legislator had adopted a prohibition on abortion and the applicant neither was pregnant, nor had been refused an interruption of pregnancy, nor had been prosecuted for unlawful abortion, the claimant could still be received.[48] Likewise, in Marckx, the inheritance laws complained of had not yet been applied to the applicants and presumably would not be applied for a certain period of time, but the Court argued nonetheless that they had a legitimate interest in challenging a legal position, that of an unmarried mother and of children born out of wedlock, which affected them—according to the Court—personally.[49] In Dudgeon and Norris, the case regarded a claim by an applicant about the regulation of homosexual conduct. The Court held that the applicant could be received even without the law being applied to him and without there being any reason to believe that it might be, as 'the very existence of this legislation continuously and directly affects his private life: either he respects the law and refrains from engaging—even in private with consenting male partners—in prohibited sexual acts to which he is disposed by reason of his homosexual tendencies, or he commits such acts and thereby becomes liable to criminal prosecution.'[50]

This approach is becoming increasingly important in cases revolving around surveillance activities by the state, in which the Court is also willing to accept potential future harm and chilling effects. A good example may be the case of *Colon v. the Netherlands*, in which the applicant complained that the designation of a security risk area by the Burgomaster of Amsterdam violated his right to respect for privacy as it enabled a public prosecutor to conduct random searches of people over an extensive period in a large area without this mandate being subject to any judicial review. The government, to the contrary, argued that the designation of a security risk area or the issuing of a stop-and-search order had not in itself

[48]ECmHR, Brüggemann and Scheuten v. Germany, application no. 6959/75, 19 May 1976.

[49]ECtHR, Marckx v. Belgium, application no. 6833/74, 13 June 1979, § 27.

[50]ECtHR, Dudgeon v. the United Kingdom, application no. 7525/76, 22 October 1981, § 41. See further: ECtHR, S.A.S. v. France, application no. 43835/11, 01 July 2014. ECtHR, Mateescu v. Romania, application no. 1944/10, 14 January 2014. ECtHR, Ballianatos and others v. Greece, application nos. 29381/09 and 32684/09, 07 November 2013.

constituted an interference with the applicant's private life or liberty of movement. Since the event complained of, several preventive search operations had been conducted; in none of them had the applicant been subjected to further attempts to search him. This was, according to the government, enough to show that the likelihood of an interference with the applicant's rights was so minimal that this deprived him of the status of victim.

The Court stressed again, that in principle, it did not accept *in abstracto* claims or an *actio popularis*. 'In principle, it is not sufficient for individual applicants to claim that the mere existence of the legislation violates their rights under the Convention; it is necessary that the law should have been applied to their detriment. Nevertheless, Article 34 entitles individuals to contend that legislation violates their rights by itself, in the absence of an individual measure of implementation, if they run the risk of being directly affected by it; that is, if they are required either to modify their conduct or risk being prosecuted, or if they are members of a class of people who risk being directly affected by the legislation.'[51] It went on to stress that it was 'not disposed to doubt that the applicant was engaged in lawful pursuits for which he might reasonably wish to visit the part of Amsterdam city centre designated as a security risk area. This made him liable to be subjected to search orders should these happen to coincide with his visits there. The events of 19 February 2004, followed by the criminal prosecution occasioned by the applicant's refusal to submit to a search, leave no room for doubt on this point. It follows that the applicant can claim to be a "victim" within the meaning of Article 34 of the Convention and the Government's alternative preliminary objection must be rejected also.'[52]

Like with the laws prohibiting homosexual conduct, the applicant was left only the choice between two evils: either he avoided traveling to the capital city of the Netherlands or he risked being subjected to surveillance activities. This is enough for the Court to accept a victim-status, which it has reaffirmed in later jurisprudence.[53] Right now pending before the Court is a case regarding mass surveillance activities by the British government and its intelligence services.[54] It will be interesting to see whether in the future, the Court is willing to content that, if governments engage in data retention practices[55] or wiretap all telecommunication coming in or going out of their country, echoing Colon, citizens are left only with the choice either to abstain from legitimately using the internet or other common (electronic) communication channels or face the risk of being subjected to surveillance activities.

[51]ECtHR, Colon v. the Netherlands, application no. 49458/06, 15 May 2012, § 60.

[52]Colon, § 61.

[53]ECtHR, Ucar and others v. Turkey, application no. 4692/09, 24 June 2014.

[54]ECtHR, Big Brother Watch and others v. the United Kingdom, application no. 58170/13, 07 January 2014.

[55]ECJ, Digital Rights Ireland, C–293/12 and C–594/12, 8 April 2014.

Layout: T1 Standard SC | Book ID: 346872_1_En | Book ISBN: xxx-x-xxxx-xxxx-x
Chapter No.: 15 | Date: 31 October 2015 2:16 PM | Page: 16/26



## 5 In Abstracto Claims (No Individual Harm)

Although in the cases discussed in the foregoing a relaxation takes place, the Court still holds on to the victim requirement. There are, however, cases, which have been briefly touched upon in Sect. 3, in which the Court allows *in abstracto* claims, regarding laws or policies as such, without them having been applied to the claimant or otherwise having a direct effect on him.[56] Sometimes, the Court, rather artificially, holds on to the victim requirement by holding that everyone living in a certain country is affected by a certain law. For example, in *Weber and Saravia v. Germany*, the applicants claimed that certain provisions of the Fight against Crime Act violated Article 8 ECHR. The Court reiterated that the mere existence of legislation which allows a system for the secret monitoring of communications entails a threat of surveillance for all those to whom the legislation may be applied. 'This threat necessarily strikes at freedom of communication between users of the telecommunications services and thereby amounts in itself to an interference with the exercise of the applicants' rights under Article 8, irrespective of any measures actually taken against them.'[57] In similar fashion, the Court recalled in *Liberty and others v. the UK* its findings 'in previous cases to the effect that the mere existence of legislation which allows a system for the secret monitoring of communications entails a threat of surveillance for all those to whom the legislation may be applied. This threat necessarily strikes at freedom of communication between users of the telecommunications services and thereby amounts in itself to an interference with the exercise of the applicants' rights under Article 8, irrespective of any measures actually taken against them.'[58] The fact that everyone may claim to be a victim means that everyone may submit a claim before the Court, a situation which it hoped to prevent by introducing the prohibition on class actions.

Although in these cases, the Court still holds onto the victim requirement, in most cases revolving around *in abstracto* claims, such as Klass, Malone, P.G. and J.H. and Mersch, the victim requirement is simply abandoned. This fact has had a large influence on the admissibility of cases and complainants more in general. While typical cases under Article 8 ECHR revolve around individual interests such as human dignity, individual autonomy and personal freedom, cases in which the Court accepts *in abstracto* claims revolve around societal interests, such as the abuse of power by the government. Abandoning the victim-requirement means that other hurdles for invoking Article 8 ECHR are also minimized. A number of

[56]See further: ECmHR, M.S. and P.S. v. Switserland, application no. 10628/83, 14 October 1985. ECtHR, Tanase v. Moldova, application no. 7/08, 27 April 2010. ECtHR, Hadzhiev v. Bulgaria, application no. 22373/04, 23 October 2012. See further: ECtHR, Goranova-Karaeneva v. Bulgaria, application no. 12739/05, 08 March 2011.

[57]ECtHR, Weber and Saravia v. Germany, application no. 54934/00, 29 June 2006, § 78.

[58]ECtHR, Liberty and others v. the United Kingdom, application no. 58243/00, 01 July 2008, § 56–57.

examples may be provided, three of them will be touched upon here briefly. First, the rejection of the Court of legal persons invoking the right to privacy, second the obligation to exhaust all domestic remedies before submitting a claim under the system of supra-national supervision and third, the requirement that a case must be brought before the European Court of Human Rights within six months after the final decision has been made on the national level.

As has been discussed, in *Mersch and others v. Luxembourg*, the Court was willing to accept a legal person in its claim for the part of the case that regarded the mere existence of laws or policies as such. Besides Mersch, the Court accepted the complaint of a legal person in Liberty and in the case of the Association for European Integration and Human Rights and *Ekimdzhiev v. Bulgaria*. The latter case regarded the authorities' wide discretion to gather and use information obtained through secret surveillance. The applicants suggested that, by failing to provide sufficient safeguards against abuse, by its very existence, the laws were in violation of Article 8 ECHR. The government disputed that the applicants could be considered victims (as they did not claim to be specifically harmed by the matter) and that legal persons should not be allowed to claim a right to privacy in general and in particular in this case because the legal person could not have been harmed itself. The Court, however, pointed to the statutory objectives of the association and found that the 'rights in issue in the present case are those of the applicant association, not of its members. There is therefore a sufficiently direct link between the association as such and the alleged breaches of the Convention. It follows that it can claim to be a victim within the meaning of Article 34 of the Convention.'[59] Essentially the same was held in *Iordachi and others v. Moldova*.[60] This means that legal persons who have statutes that incorporate references to the general protection of privacy and other human rights may have direct access to the court in the future when cases regard mass surveillance activities by the state.

As a second example, reference can be made to the requirement to exhaust all domestic remedies before submitting a claim before the ECtHR, which is also relaxed with *in abstracto* claims. The European Convention on Human Rights, Article 35, regarding the admissibility criteria, specifies that the Court may only deal with a matter after all domestic remedies have been exhausted, according to the general recognized rules of international law. This is connected to the principle that the Court dismisses cases in which the national authorities have acknowledged their mistake and have remedied their misconduct, either by providing compensation and/or by revoking the law or policy on which the abusive practices were based. If the national courts would be passed over by the claimant, national states would be denied this chance. However, the problem with *in abstracto* claims is that, especially when linked to mass surveillance by secret services, the national oversight on surveillance activities is often quite limited. In particular, *in abstracto*

[59]ECtHR, Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, application no. 62540/00, 08 June 2007, § 59.

[60]ECtHR, Iordachi and other v. Moldova, application no. 25198/02, 10 February 2009, § 33–34.

Layout: T1 Standard SC | Book ID: 346872_1_En | Book ISBN: xxx-x-xxxx-xxxx-x
Chapter No.: 15 | Date: 31 October 2015 2:16 PM | Page: 18/26



claims can often not be brought forward by citizens or legal persons on the domestic level. Moreover, the courts and tribunals often simply lack the power to annul laws or policies and can only assess specific individual cases. That is why the ECtHR is often willing to accept claimants which have not exhausted all domestic remedies if the claim regards the mere existence of laws or policies as such.

For example, in *Kennedy v. the UK*, the Court concluded that the applicant had failed to raise his arguments as regarded the overall Convention-compatibility of the Regulation of Investigatory Powers Act 2000 (RIPA) provisions before the Investigatory Powers Tribunal (IPT). However, it also stressed that where the government claimed non-exhaustion it must satisfy the Court that the remedy proposed was an effective one available in theory and in practice at the relevant time, that is to say, that it was accessible, was capable of providing redress in respect of the applicant's complaints and offered reasonable prospects of success. However, if 'the applicant had made a general complaint to the IPT, and if that complaint been upheld, the tribunal did not have the power to annul any of the RIPA provisions or to find any interception arising under RIPA to be unlawful as a result of the incompatibility of the provisions themselves with the Convention. [] Accordingly, the Court considers that the applicant was not required to advance his complaint regarding the general compliance of the RIPA regime for internal communications with Article 8 § 2 before the IPT in order to satisfy the requirement under Article 35 § 1 that he exhaust domestic remedies.'[61] The Court held essentially the same in *M.M. v. the UK*.[62] This means for *in abstracto* claims, that the ECtHR is willing to rule as court of first instance.

To provide a final example, the Convention specifies certain time-restricting principles, which are also put under pressure with *in abstracto* claims, as these do not revolve around specific violations, but the existence of laws or policies as such and are thus not linked to a specific moment in time. The principle of *ratione temporis*, which means that the provisions of the Convention do not bind a national state in relation to any act or fact which took place or any situation which ceased to exist before the date of the entry into force of the Convention or the accession of a state to the ECHR. This means that, for example, if the right to privacy of an individual had been violated by a state before that state entered the Convention, this case will be declared inadmissible by the Court. Obviously, this principle does not apply to *in abstracto* claims, as the infringement continues to exist. The Convention, Article 35, also requires applicants to submit their application within a period of six months from the date on which the final decision on the national level was taken. This principle is also very difficult to maintain with regard to *in abstracto* claims, and the ECtHR has often adopted a flexible approach with this respect.

For example, in *Lenev v. Bulgaria*, the Court made a sharp distinction between the complaint regarding individual harm and the part of the application revolving

[61]ECtHR, Kennedy v. the United Kingdom, application no. 26839/05, 18 May 2010.

[62]ECtHR, M.M. v. the United Kingdom, application no. 24029/07, 13 November 2012.

around the mere existence of the law. It stressed that the applicant complained 'more than six months later, on 12 September 2007. The fact that he did not have knowledge of the exact content of the recording is immaterial because the lack of such knowledge could not prevent him from formulating a complaint under Article 8 of the Convention in relation to the secret taping of his interrogation. Nor can the Court accept that the criminal proceedings against the applicant constituted an obstacle to his raising grievances in this respect. It follows that the complaints concerning the secret taping of the applicant's interrogation have been introduced out of time and must be rejected in accordance with Article 35 §§ 1 and 4 of the Convention. By contrast, the concomitant complaints concerning the mere existence in Bulgaria of laws and practices which have established a system for secret surveillance relate to a continuing situation—in as much as the applicant may at any time be placed under such surveillance without his being aware of it. It follows that his complaints in that respect cannot be regarded as having been raised out of time.'[63] Consequently, claims revolving around the mere existence of laws or policies are not bound by the time-limits specified by the Convention. In conclusion, abandoning the victim-requirement has the effect that many threshold for invoking a right under the Convention dissolve.

## 6 Analysis

To summarize briefly, the following has been shown. The Court focusses on individual harm by natural persons when assessing the admissibility of cases under Article 8 ECHR. According to the Court, this provision guarantees protection only to individual interests such as human dignity, individual autonomy and personal freedom. Cases are declared inadmissible if they do not revolve around individual harm. Examples are: *in abstracto* claims, a priori claims, hypothetical complaints, class actions, claims about minimal harm, claims about harm which has been remedied, claims by legal persons and claims that do not regard strictly personal interests. However, it has also been explained that in certain types of cases, mostly revolving around surveillance activities, the Court is willing to relax its standards. It is sometimes willing to allow for hypothetical complaints if a reasonable likelihood exists that the applicant has been harmed, it is occasionally willing to accept a priori claims, when the applicant is forced to restrict its legitimate use of his right to privacy in order to avoid legal sanctions, and it is even willing to accept claims that revolve around the mere existence of laws and policies as such.

The reason why the Court is willing to relax its stance in these cases specifically is clear. With (mass) surveillance activities, either by secret services or other governmental institutions, the citizen is mostly unaware of the fact that he is being followed or that his data are being gathered, why this is done, by whom, to what

[63] ECtHR, Lenev v. Bulgaria, application no. 41452/07, 04 December 2012.

Layout: T1 Standard SC | Book ID: 346872_1_En | Book ISBN: xxx-x-xxxx-xxxx-x
Chapter No.: 15 | Date: 31 October 2015 2:16 PM | Page: 20/26



extent, etc. Likewise, especially with regard to laws allowing for mass surveillance and data retention, the fact is that the potential violations do not revolve around a specific person, but affect everyone living under that regime or at least very large numbers of people. Mostly, the issue is simply the presumed abuse of power by national authorities. This is a societal interest, related to the legitimacy and legality of the state.

The reason for discussing these matters in such detail is that these characteristics are shared to a large extent by privacy infringements following from Big Data initiatives. Often, an individual is simply unaware that his personal data are gathered by either his fellow citizens (e.g. through the use of their smartphones), by companies (e.g. by tracking cookies) or by governments (e.g. through covert surveillance). Even if a person would be aware of these data collections, given the fact that data gathering and processing is currently so widespread and omnipresent, and will become even more so in the future, it will quite likely be impossible for him to keep track of every data processing which includes (or might include) his data, to assess whether the data controller abides by the legal standards applicable, and if not, to file a legal complaint. And if an individual does go to court to defend his rights, he has to demonstrate a personal interest, i.e. personal harm, which is a particularly problematic notion in Big Data processes.[64]

Finally, under the current privacy and data protection regimes, the balancing of interests is the most common way in which to resolve cases. In a concrete matter, the societal interests served with the data gathering, for example wiretapping a person's telephone because he is suspected of having committed a murder, is weighed against the harm the wiretapping does to his personal autonomy, freedom or dignity. However, the balancing of interests becomes increasingly difficult in the age of Big Data, not only because the individual interest involved with a particular case is so difficult to substantiate, the societal interest at the other end is also increasingly difficult to specify.[65] For example, it is mostly unclear in how far the large data collections by intelligence services have actually prevented concrete terrorist attacks. This balance is even more difficult if executed on an individual level, i.e. how the collection of personal data of a particular non-suspected person

[64]See further: David Bollier, "The Promise and Peril of Big Data", <http://www.emc.com/collateral/analyst-reports/10334-ar-promise-peril-of-big-data.pdf>. Danah Boyd and Kate Crawford, "Six Provocations for Big Data", <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1926431>. Lawrence Busch, "A Dozen Ways to Get Lost in Translation: Inherent Challenges in Large Scale Data Sets", *International Journal of Communication* 8 (2014). Neil M. Richards & Jonathan H. King, "Three Paradoxes of Big Data", *Stanford Law Review online* 66 (2013): 44.

[65]See further: Kevin Driscoll and Shawn Walker, "Working Within a Black Box: Transparency in the Collection and Production of Big Twitter Data" *International Journal of Communication* 8 (2014). Theresa M. Payton & Theodore Claypoole, *Privacy in the age of Big Data: recognizing threats, defending your rights, and protecting your family* (Rowman & Littlefield: Plymouth, 2014). Cornelius Puschmann and Jean Burgess, "Metaphors of Big Data", *International Journal of Communication* 8 2014. Omer Tene & Jules Polonetsky, "Big Data for All: Privacy and User Control in the Age of Analytics", *Northwestern Journal of Technology and Intellectual Property* 11 (2013): 239.

has ameliorated the national security.[66] Perhaps more important is the fact that with some of the large scale data collections, there seems not a relative interest at stake, which can be weighed against other interests, but absolute interests. For example, it has been suggested that the data collection by the NSA is so large, is conducted over such a long time span and includes data about so many people that this simply qualifies as abuse of power.[67] Abuse of power is not something which can be legitimated by its instrumentality towards a specific societal interest—it is an absolute minimum condition of the use of power.

The same problems with applying the current privacy paradigm also count for data protection rules. They too are dependent for their applicability on the material and personal scope, which, like the right to privacy, is linked to the natural person. For example, the Data Protection Directive defines personal data as 'any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity'.[68] However, if data are processed on an aggregated level and turned into group profiles, it is often impossible to directly identify one particular person on the basis of it. Moreover, like the right to privacy, data protection revolves to a large extent around individual rights, such as the right to access personal data and correct them, the right to be forgotten and the right to a legal remedy. The same problems signaled with regard to individual privacy rights consequently apply to the data protection regime.[69]

All notions connected to the victim-requirement, such as the *de minimis* rule, the prohibition on hypothetical, future and abstract harm, the prohibition of class actions and of legal persons instituting a complaint, and the focus on individual interests, seem to be put under pressure by the developments known as Big Data. What seems most suitable for claims regarding privacy infringements following from mass surveillance and Big Data practices is claims about the potential chilling effect (e.g. users being afraid to use certain forms of communication), about hypothetical harm and even abstract assessments of the policies and practices as such. Not the individual seems to be best equipped to file a complaint, but civil

[66]See further: Pierre-Luc Dusseault, "Privacy and social media in the Age of Big Data: Report of the Standing Committee on Access to Information, Privacy and Ethics", <http://www.parl.gc.ca/content/hoc/Committee/411/ETHI/Reports/RP6094136/ethirp05/ethirp05-e.pdf>.
Neil M. Richards & Jonathan H. King, "Big Data Ethics", *Wake Forest Law Review* 49 (2014).
Ira Rubinstein, "Big Data: The End of Privacy or a New Beginning?", *NYU School of Law, Public Law Research Paper* No. 12–56. Drury D. Stevenson & Nicholas J. Wagoner, 'Bargaining in the Shadow of Big Data', *Florida Law Review*, 66 (2014): 5.

[67]Bart van der Sloot, "Privacy in the Post-NSA Era: Time for a Fundamental Revision?" *Journal of intellectual property, information technology and electronic commerce law* 5 (2014): 1.

[68]Article 2 sub (a) 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.

[69]See also: <http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf>.

Layout: **T1 Standard SC** Book ID: **346872_1_En** Book ISBN: **xxx-x-xxxx-xxxx-x**
Chapter No.: **15** Date: **31 October 2015 2:16 PM** Page: **22/26**



society groups and legal persons. Not individual interest are at stake in these types of processes, but general and societal interests. Thus, in order to retain the relevance of the rights to privacy and data protection in the modern technological era, the victim-requirement and all its sub-requirements should be relaxed.

And this is exactly what the ECtHR is willing to do in cases that revolve around surveillance activities. It does accept claims about future harm and potential chilling effects, about hypothetical harm, it does receive class actions, abstract claims and legal persons and it does take into account abstract and societal interests. The question is, however, at what price this comes. What is left for the Court, particularly with *in abstracto* claims, to assess in these types of cases is the mere quality of laws and policies as such and the question is whether this narrow assessment is still properly addressed under a human rights framework. The normal assessment of the Court revolves around, roughly, three questions: (1) has there been an infringement of the right to privacy of the claimant, (2) is the infringement prescribed by law and (3) is the infringement necessary in a democratic society in terms of, inter alia, national security, that is, does the societal interest in this particular case outweigh the individual interest. Obviously, the first question does not apply to *in abstracto* claims because there has been no infringement with the right of the claimant. The third question is also left untouched by the Court, because it is impossible, in the absence of an individual interest, to weigh the different interests involved. This means of course that another principle by the Court, namely that it only decides on the particular case before it, is also overturned.

Even the second question is not applicable as such as there is no infringement that is or is not prescribed by law. Although the Court regularly determines in cases, inter alia, whether the laws are accessible, whether sanctions are foreseeable and whether the infringement at stake is based on a legal provision, this does not apply to *in abstracto* claims. There *is* often a law permitting mass surveillance (that is exactly the problem) and these laws *are* accessible and the consequences *are* foreseeable (in the sense that everyone will be affected by it). Rather, it is the mere quality of the policy as such that is assessed—the content of the law, the use of power as such, is deemed inappropriate. The question of abuse of power can of course be addressed by the Court, though not under Article 8 ECHR, but under Article 18 of the Convention, which specifies: 'The restrictions permitted under this Convention to the said rights and freedoms shall not be applied for any purpose other than those for which they have been prescribed.' But as the Court has stressed, this provision can only be invoked if one of the other Convention rights are at stake. Reprehensible as the abuse of power may be, it is only proper to address this question under a human rights framework if one of the human rights contained therein will or have been violated by the abuse. The Court cannot assess the abuse of power as such (a doctrine which it also applies to, inter alia, Article 14 ECHR, the prohibition of discrimination).

However, what is assessed in cases in which *in abstracto* claims regarding surveillance activities have been accepted is precisely the use of power by the government as such, without a specific individual interest being at stake. This is a test of legality and legitimacy, which is well known to countries that have a constitutional court or body, such as France and Germany. These courts can assess the 'constitutionality' of national

Layout: T1 Standard SC | Book ID: 346872_1_En | Book ISBN: xxx-x-xxxx-xxxx-x
Chapter No.: 15 | Date: 31 October 2015 2:16 PM | Page: 23/26



laws in abstract terms. Not surprisingly, the term 'conventionality' (or 'conventionalité' in French) has been introduced in the cases discussed.[70] For example, in Michaud, the government argued that with a previous *in abstracto* decision, the Court had 'issued the Community human rights protection system with a "certificate of conventionality", in terms of both its substantive and its procedural guarantees.'[71] Referring to the Michaud judgment, among other cases, in his partly concurring, partly dissenting opinion in *Vallianatos and others v. Greece*, judge Pinto De Albuquerque explained: 'The abstract review of "conventionality" is the review of the compatibility of a national law with the Convention independently of a specific case where this law has been applied.'[72]

He argued that the particular interest of the Vallianatos and others case, which revolved around the fact that the civil unions introduced by a specific law were designed only for couples composed of different-sex adults, is that the Grand Chamber performs an abstract review of the "conventionality" of a Greek law, while acting as a court of first instance. 'The Grand Chamber not only reviews the Convention compliance of a law which has not been applied to the applicants, but furthermore does it without the benefit of prior scrutiny of that same legislation by the national courts. In other words, the Grand Chamber invests itself with the power to examine *in abstracto* the Convention compliance of laws without any prior national judicial review.'[73] As explained earlier, when discussing *Lenev v. Bulgaria*, the Court is likewise willing to pass over the domestic legal system and act as court of first instance in cases revolving around mass surveillance. Subsequent to Michaud and Vallianatos, the term 'conventionality' has been used more often,[74] as well as the term 'Convention-compatibility', for example in the case of *Kenedy v. the UK* discussed earlier,[75] and most likely will only gain in dominance as the Court opens up the Convention for abstract reviews of laws and policies.

[70]See for the use of the word also: ECtHR, Py v. France, application no. 66289/01, 11 January 2005. ECtHR, Kart v. Turkey, application no. 8917/05, 08 July 2008. ECtHR, Duda v. France, application no. 37387/05, 17 March 2009. ECtHR, Kanagaratnam and others v. Belgium, application no. 15297/09, 13 December 2011. ECtHR, M.N. and F.Z. v. France and Greece, application nos. 59677/09 and 1453/10, 08 January 2013.

[71]Michaud, § 73. See also: ECtHR, Vassis and others v. France, application no. 62736/09, 27 June 2013.

[72]ECtHR, Vallianatos and others v. Greece, application nos. 29381/09 and 32684, 07 November 2013.

[73]Ibid.

[74]See among others: ECtHR, S.A.S. v. France, application no. 43835/11, 01 July 2014. ECtHR, Avotins v. Latvia, application no. 17502/07, 25 February 2014. ECtHR, Matelly v. France, application no. 10609/10, 02 October 2014. ECtHR, Delta Pekarny A.S. v. Czech Republic, application no. 97/11, 02 October 2014.

[75]See among others: ECtHR, Animal Defenders International v. the United Kingdom, application no. 48876/08, 22 April 2013. ECtHR, Emars v. Latvia, application no. 22412/08, 18 November 2014. ECtHR, Kennedy v. the United Kingdom, application no. 26839/05, 18 May 2010. ECtHR, Mikalauskas v. Malta, application no. 4458/10, 23 July 2013. ECtHR, Sorensen and Rusmussen v. Denmark, application nos. 52562/99 and 52620/99, 11 January 2006. ECtHR, Bosphorushava Yollari Turizm ve Ticaret Anonim Sirketi v. Ireland, application no. 45036/98, 30 June 2005. ECtHR, Lunch and Whelan v. Ireland, application nos. 70495/10 and 74565/10, 18 June 2013. ECtHR, Interdnestrcom v. Moldova, application no. 48814/06, 13 March 2012.

Layout: T1 Standard SC | Book ID: 346872_1_En | Book ISBN: xxx-x-xxxx-xxxx-x
Chapter No.: 15 | Date: 31 October 2015 2:16 PM | Page: 24/26



What is left in these types of cases is thus the abstract assessment of laws and policies as such, without a Convention right necessarily being at stake. Furthermore, the Court is willing to assess the 'Conventionability' of these laws as court of first instance. Desirable as such an abstract test may be,[76] it is questionable whether it should be conducted under a human rights framework. Of course, in the Big Data era, what is needed is not more individual rights protecting individual interests, but general duties to protect general interests.[77] Accepting *in abstracto* claims and assessing the legality and legitimacy of laws and (Big Data) practices as such fits this purpose. But if it is true that human rights protect humans and their interests, it seems that the Court should only have the competence to address human rights violations. Although it does have the power to assess the abuse of power, under a human rights framework, the abuse of power addressed should at least have an impact on concrete individual rights. When this is not the case, like with cases revolving around the abstract assessment of laws permitting mass surveillance and in the future, potentially, cases revolving around Big Data processes, it seems that the human rights framework is simply not the most appropriate instrument to turn to. When the Court does so nevertheless, although for noble reasons, it seems to overstretch its own competence and change the nature of the ECHR from a human rights instrument to a document resembling a constitution, and its position from a supra-national court overseeing severe human rights violations in last instance, to a first instance court for assessing the legality and legitimacy of laws and policies as such.

## Bibliography

Andrejevic, Mark. 2014. The big data divide. *International Journal of Communication* 8.
Bentham, Jeremy. 1791. *Panopticon; or the inspection-house* (Dublin).
Bollier, David. 2010. The promise and peril of big data. http://www.emc.com/collateral/analyst-reports/10334-ar-promise-peril-of-big-data.pdf.
Boyd, Danah and Kate Crawford. (2011) Six provocations for big data. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1926431.
Busch, Lawrence. 2014. A Dozen Ways to Get Lost in Translation: Inherent Challenges in Large Scale Data Sets. *International Journal of Communication* 8 (2014).
Calders, Toon & Sicco Verwer. 2010. Three naive bayes approaches for discrimination-free classification. *Data Mining and Knowledge Discovery* 21(2).

AQ3

[76] Letting go of the personal and material scope of data protection rules could similarly lead to the application of certain principles *in abstracto*, such as the transparency principle, the requirement of having a clear and defined purpose for the processing, the purpose limitation principle and the obligations to process data safely and confidentially and to keep the data correct and up to date. Again, although this abstract test might be in itself desirable, the question is whether it is appropriate to fit this under the regimes protecting personal data.

[77] See further: Bart van der Sloot, "Do data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation", *International Data Privacy Law* 3 (2014b).

Craig, Terence, and Mary E. Ludloff. 2011. *Privacy and big data: The players, regulators, and stakeholders*. Sebastopol: O'Reilly Media.

Crawford, Kate and Jason Schultz. 2014. Big data and due process: Toward a framework to redress predictive privacy harms. *Boston College Law Review* 55: 93.

Custers, Bart H. M. 2004. *The power of knowledge; ethical, legal, and technological aspects of data mining and group profiling in epidemiology* (Tilburg: Wolf Legal Publishers).

Davis, Kord with David Patterson. 2012. Ethics of big data: Balancing risk and innovation. http://www.commit-nl.nl/sites/default/files/Ethics%20of%20Big%20Data_0.pdf.

der Bart Sloot, Van. 2015. Do privacy and data protection rules apply to legal persons and should they? A proposal for a two-tiered system. *Computer Law & Security Review* 31: 1.

Driscoll, Kevin and Shawn Walker. 2014. Working within a black box: Transparency in the collection and production of big twitter data. *International Journal of Communication* 8.

Dusseault, Pierre-Luc. 2013. Privacy and social media in the age of big data: Report of the standing committee on access to information, privacy and ethics. http://www.parl.gc.ca/content/hoc/Committee/411/ETHI/Reports/RP6094136/ethirp05/ethirp05-e.pdf.

Feinberg, Joel. 1984. *Harm to others*. New York: Oxford University Press.

Foucault, Michel. 1975. *Surveiller et punir: naissance de la prison*. Paris: Gallimard.

Galetta, Antonella and Paul De Hert. 2014. Complementing the surveillance law principles of the ECtHR with its environmental law principles: An integrated technology approach to a human rights framework for surveillance. *Utrecht Law Review* 10-1.

Gerards, Janneke. 2012. The prism of fundamental rights. *European Constitutional Law Review* 8: 2.

Habermas, Jurgen. 1995. On the internal relation between the rule of law and democracy. *European Journal of Philosophy* 3.

Hildebrandt, Mireille, and Serge Gutwirth (eds.). 2008. *Profiling the European citizen cross-disciplinary perspectives*. New York: Springer.

Hobbes, Thomas. 1996. *Leviathan*. Cambridge: Cambridge University Press.

Hoofnagle, Chris J. 2013. How the fair credit reporting act regulates big data. <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2432955>.

International Working Group on Data Protection in Telecommunications. 2014. Working paper on big data and privacy. Privacy principles under pressure in the age of big data analytics 55th Meeting, 5–6, Skopje.

Kitchin, Rob. 2014. *The data revolution: Big data, data infrastructures & their consequences*. Los Angeles: Sage.

Larose, Daniel T. 2006. *Data mining methods and models* (New Yersey: Wiley).

Locke, John. 1988. *Two treatises of government*. Cambridge: Cambridge University Press.

Mayer-Schönberger, Viktor, and Kenneth Cukier. 2013. *Big data: A revolution that will transform how we live, work, and think*. Boston: Houghton Mifflin Harcourt.

McAfee, Andrew and Eerik Brynjolfsson. 2012. Big data: The management Revolution: Exploiting vast new flows of information can radically improve your company's performance. But first you'll have to change your decision making culture. *Harvard Business Review*.

Murphy, Thérèse and Gearóid Ó Cuinn. 2010. Work in progress. New technologies and the European court of human rights. *Human Rights Law Review*.

Paine, Thomas. 1797. *The rights of man: For the benefit of all mankind*. Philadelphia: Webster.

Payton, Theresa M., and Theodore Claypoole. 2014. *Privacy in the age of big data: Recognizing threats, defending your rights, and protecting your family*. Plymouth: Rowman & Littlefield.

Puschmann, Cornelius and Jean Burgess. 2014. Metaphors of big data. *International Journal of Communication* 8.

Richards, Neil M. & Jonathan H. King. 2013. Three paradoxes of big data. *Stanford Law Review online* 66: 44.

Richards, Neil M. and Jonathan H. King. 2014. Big data ethics. *Wake Forest Law Review* 49.

Rubinstein, Ira. 2013. Big data: The end of privacy or a new beginning?. *NYU School of Law, Public Law Research Paper* No. 12–56.

Layout: **T1 Standard SC** | Book ID: **346872_1_En** | Book ISBN: **xxx-x-xxxx-xxxx-x**
Chapter No.: **15** | Date: **31 October 2015 2:16 PM** | Page: **26/26**



842 Stevenson, Drury D. and Nicholas J. Wagoner. 2014. Bargaining in the shadow of big data.
843 *Florida Law Review* 66: 5.
844 Tene, Omer and Jules Polonetsky. 2013. Big data for all: Privacy and user control in the age of
845 analytics. *Northwestern Journal of Technology and Intellectual Property* 11: 239.
846 Van der Sloot, Bart. 2014a. Privacy in the Post-NSA Era: Time for a Fundamental Revision?.
847 *Journal of intellectual property, information technology and electronic commerce law* 5: 1.
848 Van der Sloot, Bart. 2014b. Do data protection rules protect the individual and should they? An
849 assessment of the proposed general data protection regulation. *International Data Privacy*
850 *Law* 3.
851 Zarsky, Tal Z. 2003. Mine your own business!: making the case for the implications of the data
852 mining of personal information in the forum of public opinion. *Yale Journal of Law &*
853 *Technology* 5.

# Author Query Form

Book ID: **346872_1_En**
Chapter No: **15**

Springer
the language of science

Please ensure you fill out your response to the queries raised below and return this form along with your corrections

Dear Author
During the process of typesetting your chapter, the following queries have arisen. Please check your typeset proof carefully against the queries listed below and mark the necessary changes either directly on the proof/online grid or in the 'Author's response' area provided

| Query Refs. | Details Required | Author's Response |
|---|---|---|
| AQ1 | Please clarify the meaning of the sentence '[] Accordingly, the Court considers that the applicant was…'. | |
| AQ2 | The closing quotes does not have a corresponding opening quotes in the sentence 'It follows that his complaints in that respect…'. Please insert the quotes in the appropriate position. | |
| AQ3 | Kindly check and confirm the inserted year of publication are correct for References 'Bollier (2013), Boyd and Kate (2011), Davis and David (2012), Dusseault (2013), Galetta and Paul (2014), Hoofnagle (2013), International Working Group on Data Protection in Telecommunications. (2014), McAfee and Eerik (2012), Theresa and Theodore (2014), Rubinstein (2013), Stevenson and Nicholas (2014)'. | |