Privacy in the Post-NSA Era: Time for a Fundamental Revision?

van der Sloot, B.

Publication date
2014
Document Version
Final published version
Published in
Journal of Intellectual Property, Information Technology and Electronic Commerce Law

Privacy in the Post-NSA Era: Time for a Fundamental Revision?

by **Bart van der Sloot,** Institute for Information Law (IViR), University of Amsterdam[1]

Abstract: Big Brother Watch and others have filed a complaint against the United Kingdom under the European Convention on Human Rights about a violation of Article 8, the right to privacy. It regards the NSA affair and UK-based surveillance activities operated by secret services. The question is whether it will be declared admissible and, if so, whether the European Court of Human Rights will find a violation. This article discusses three possible challenges for these types of complaints and analyses whether the current privacy paradigm is still adequate in view of the development known as Big Data.

Keywords: NSA, Human Rights, ECHR, Big Data, Privacy, Right of Complaint, Right to Privacy

Recommended citation: Bart van der Sloot, Privacy in the Post-NSA Era:Time for a Fundamental Revision?, 5 (2014) JIPITEC 2, para 1

A. Introduction

1 The data collection by the NSA and other secret service organizations is part of a broader trend also known as Big Data,[2] in which large amounts of personal data are being collected by means of cameras, telephone taps, GPS systems and Internet monitoring, stored in large databases and analysed by computer algorithms. These data are then aggregated, used to create group profiles and analysed on the basis of statistical relationships and mathematical patterns. Subsequently, the profiles are used to individualize persons that meet a certain pattern or group profile.[3] This technique, called profiling, is used for a growing number of purposes, such as in the fight against terrorism, in which a person may be monitored or followed when he (in whole or in part) meets a certain profile (for example, male, Muslim, Arab origin and frequent trips to Yemen). Similarly, banks and insurance companies rely on risk profiles of customers to take certain decisions, and Internet companies like Google and Facebook use such profiles for advertising purposes. For example, if a person fits the profile "man, university degree, living in London", he might get an advertisement for the latest Umberto Eco book or for an apartment in one of the richer suburbs.[4]

2 In such processes, there is basically no demarcation in person, time and space, as simply everyone could be subjected to them. Data collection and processing do not start after a particular ground or reason has arisen, but the value and use of the information will only become apparent at a later stage. The gathered data are often meta-data – regarding the length of and participants to a telephone call, for example – but this often does not regard the content of the communication. Meta-data can be compared to the information visible on an envelope in the ordinary mail, such as the addressee, the size and the weight and possibly the sender. These data traditionally do not fall within the realm of privacy and the secrecy of communication. Still, through the use of modern techniques, these data can be used to generate increasingly detailed profiles.[5] Thus although they are not privacy-sensitive data initially, they may become identifying data at a later stage. In addition, the collected data are not linked directly to one person, but they are used to generate

general group profiles and statistical correlations. These profiles may be applied to an individual if he meets one or several of the elements contained in the group profile. Finally, in these processes, no reasonable suspicion is needed to individualize someone. Even a 1% chance that someone will buy an expensive luxury product or will engage in terrorist activities may provide sufficient grounds to do so. Consequently, the individual element and the interests of specific persons are moved to the background in such systems.

3 Although it is clear that European citizens cannot challenge the activities of the US National Security Agency (NSA) as unveiled by Edward Snowden, Big Brother Watch and others have filed a complaint against the United Kingdom for similar practices by its secret services under the European Convention on Human Rights (ECHR),[6] specifically Article 8, which holds as follows:

> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

4 In a reaction, the European Court for Human Rights has asked the parties to respond to three questions: (1) Can the applicants claim to be victims of a violation of their rights under Article 8 ECHR? (2) Have the applicants done all that is required of them to exhaust domestic remedies? (3) If so, are the acts of the United Kingdom intelligence services in relation to the collection and processing of data in accordance with the law and necessary in a democratic society? This article will try to answer questions (1) and (3) by assessing three general points. Does the complaint fall under the scope of Article 8 ECHR *ratione personae,* meaning have the applicants suffered from any personal damage? Does the complaint fall under the scope of Article 8 ECHR *ratione materiae,* meaning do the practices complained of constitute an infringement with the right to privacy? And if so, what would the likely outcome be in relation to whether the infringement was necessary in a democratic society; that is, how will the Court balance the right to privacy with the need for security? Not discussed are the questions related to the exhaustion of domestic remedies and to the matter of whether the governmental practices are "in accordance with the law".

5 Although this complaint functions as the central theme, the findings will be extrapolated to the current development of Big Data. The general conclusion will be that, currently, the right to privacy is based on the individual and his interests in a threefold manner: (1) It provides the individual with a right to submit a complaint about a violation of his privacy. (2) It provides him with protection of his personal interests, related to human dignity and personal autonomy. (3) In concrete circumstances, a privacy infringement will be judged on its legitimacy by balancing the individual with the societal interest, for example related to security. Subsequently, it will be argued that the new developments of Big Data, of which the NSA affair is a shining example, bring the following results: (1) it is increasingly difficult to demonstrate personal damage and to claim an individual right, (2) the value at stake in this type of process is a societal rather than an individual one and (3) the balance of different interests no longer provides an adequate test to determine the outcome of cases. Finally, some modest alterations of the current paradigm will be proposed.

B. Right of complaint

6 When drafting the ECHR, the authors of the Convention chose to link the right to petition only to a limited extent to the individual and the protection of his interests. Under the ECHR, there are two complaint procedures, one for inter-state complaints and another for individual complaints. In an inter-state procedure, it is not the personal interest of the applicant that is assessed, as the applicant state is not itself harmed in any way, nor that of anyone else, but the general quality of the actions and laws of the government accused of a violation of the Convention as such. In such cases, the applicant state brings an action against another state out of the general interest of the country's population, often related to abuse of power; although the citizens of that country may obviously be affected by the policies and/or laws, their individual injury is not central to the Court's assessment.

7 Moreover, the individual right of complaint may be invoked not only by natural persons, but also by legal persons (excluding governmental organizations) and groups. Typical of the latter two categories is that again, no personal harm needs to be demonstrated. A legal person may be hindered in its (business) activities but cannot suffer personal injury or complain about a violation of its autonomy or dignity, among others. Again, in such complaints, it is usually the unlawful conduct of or the abuse of power by the government as such that is at the center of the Court's assessment. In addition, the legal capacity of groups to submit a case to the Court must be understood against the backdrop of the Second

World War, in which groups were systematically discriminated against and stigmatized.[7] The authors of the Convention opened up the right to petition to a person or a group of people who want to stand up for the interests of a particular group without necessarily having suffered individually and specifically from the targeted practice that affect the group as a whole.[8]

8 Finally, given the serious fear of an excessive flow of complaints by individuals,[9] the authors of the Convention decided to introduce a two-step system, in which the admissibility of applications is first reviewed by the European Commission of Human Rights (a task which has been reassigned to a separate chamber of the Court since 1998), and is only afterwards assessed by the Court on the substance of the matter. Characteristically, individuals initially were allowed only to bring complaints before the Commission but not before the Court, even if their case was declared admissible by the Commission. Only the Commission itself or a Member State could decide to send the case for substantive assessment to the Court if they felt this was in the public interest.

9 The practice of the Court has however increasingly focused on complaints of individuals who can demonstrate their personal interest in a case. First, individuals have gradually been allowed to bring complaints directly before the Court.[10] In addition, the other modes of complaint have been of (almost) no value. Since the entry into force of the Convention, only about 20 inter-state complaints have been filed.[11] The possibility of a group complaint has been limited by the Court to the opportunity of different individuals, all of whom have directly and individually suffered from a certain practice, to join their cases, and the Court has ruled that, in principle, legal persons cannot rely on Article 8 ECHR. 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 [].*[12]

10 Although in recent case law, a less restrictive line may be discerned,[13] in principle, the Court still requires the complainant to demonstrate that he has an individual interest and has suffered from personal injury, so that legal persons cannot rely on the right to privacy, or only to a limited extent.

11 A consequence of the emphasis on the individual interests and the personal injury of the complainant is that *in abstracto* claims, in which an applicant complains about a practice or a law as such, without it being applied or otherwise having an impact on the applicant himself, are declared inadmissible. This also holds true for the *actio popularis* or class action, in which a societal organization challenges a law or policy not from a personal perspective, but with an eye on the public interest. Finally, hypothetical complaints and *a priori* applications, in which the case regards a potential, future violation by the state, without any damage having occurred yet, are also declared inadmissible.[14]

12 This brings an obvious problem with it for complaints related to large-scale data collections, whether they are initiated by secret services or by big Internet companies, since persons are often unaware that they have been filmed, followed by cookies or subjected to Internet monitoring and accordingly only few will file a legal complaint. Those who do will have trouble demonstrating any individual harm. In addition, the personal element in this type of data processing is increasingly moved to the background, as not one individual or a particular group is affected by the large-scale data system, but an unquantified number of people, and the information often regards meta-data. Moreover, whereas in classic privacy issues, such as a house search, the individual interest is fairly clear and delineated and is causally linked to the infringement, the individual damage resulting from data collection practices is often rather hypothetical, as the collection itself usually has little impact on the personal autonomy or dignity of an individual and the damage that could arise stems from the hypothetic possibility of, for example, a data breach or the abuse of the data by a future and malicious regime. Consequently, claims regarding Big Data processes will often have an abstract and hypothetical character.

13 To overcome these problems, the Court has been willing to accept a slight relaxation of the requirement of individual damage and personal interest. Regarding a presumed surveillance practice about which no insight was given by the secret services, the Court held that it is unacceptable that "the assurance of the enjoyment of a right guaranteed by the Convention could be thus removed by the simple fact that the person concerned is kept unaware of its violation".[15] Similarly, in some cases the Court has also been prepared to adopt a broader interpretation with regard to complaints about legislation authorizing surveillance practices, which is drafted in very broad and general terms. In these cases, the Court has determined that

> *[t]he mere existence of the legislation entails, for all those who might fall within its reach, a menace of surveillance; this menace necessarily strikes at freedom of communication between users of the postal and telecommunications services and thereby constitutes an "interference by a public*

authority" with the exercise of the applicants' right to respect for correspondence.[16]

14 In similar fashion, the Court has stated in a case that

> *the authorities were authorised to capture communications contained within the scope of a warrant issued by the Secretary of State and to listen to and examine communications falling within the terms of a certificate, also issued by the Secretary of State. Under section 6 of the 1985 Act arrangements had to be made regulating the disclosure, copying and storage of intercepted material. The Court considers that the existence of these powers, particularly those permitting the examination, use and storage of intercepted communications constituted an interference with the Article 8 rights of the applicants, since they were persons to whom these powers might have been applied.*[17]

15 Consequently, cases in which the plaintiff does not know whether he was subjected to a particular surveillance practice and has no chance to determine whether this was so, and cases in which a complainant is merely affected by a law by way of its all-encompassing scope, may be declared admissible by the Court under certain circumstances. Yet here, too, it must be plausible that someone was affected by a particular practice, that the applicant was part of a specific group of people designated in the law or had engaged in activities that could lead to monitoring and surveillance. Inter alia, no right to petition under the Convention is accepted on the basis of vague assumptions and references to mysterious clicking noises during phone calls, but it is accepted when the complainants are members of a group actively campaigning against nuclear missiles, from which a reasonable fear of active monitoring may be deduced.[18] The Court therefore recognizes as matter of principle that to be granted a right of complaint, a "reasonable likelihood" must exist that the applicant has been subjected to a surveillance or monitoring practice.[19] In such instances, the Court is prepared to hold

> *that the applicants, even though they were members of a group of persons who were likely to be affected by measures of interception, were unable to demonstrate that the impugned measures had actually been applied to them. It reiterates, however, its findings in comparable 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.*[20]

16 In conclusion, it is uncertain whether claims about Big Data, such as the application of Big Brother Watch, will be declared admissible. In principle, there not only remains the requirement for an individual to demonstrate his personal interest, or at least the plausibility of individual damage; there also is a practical threshold for citizens who do not know whether they have been targeted by a particular practice, since, if there is no evidence indicating so, few people will take a matter to court. Even if this knowledge existed, and even if personal damage could be convincingly demonstrated, the practical use of such an individual right of complaint is still questionable. In a world where not only secret services and governmental organizations, but also large companies like Google and Facebook and even ordinary citizens, assisted by their smart-phones, can gather and process large amounts of personal data, it is likely that it will simply become undoable for a person to keep track of everyone who is in possession of his personal data, to assess whether they are using that data legitimately and if there is reason to believe this is not so, to seek justice through a legal procedure. With such structural and societal tendencies, it seems that the individual is as powerless as King Canute trying to turn the tide.

C. Scope of the right to privacy

17 Article 8 ECHR protects everyone's private and family life, home and correspondence – in short, the right to privacy. However, in principle, it does not apply to large-scale data processing, which falls under what is called the right to data protection. To clarify the difference, reference can be made to the Charter of Fundamental Rights of the European Union from 2000, of which Article 7 provides that everyone has the right to respect for his private and family life, home and communications, and Article 8 holds as follows:

> 1. Everyone has the right to the protection of personal data concerning him or her.
>
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
>
> 3. Compliance with these rules shall be subject to control by an independent authority.'

18 This right to data protection is separated from the right to privacy and is regulated primarily by the Data Protection Directive.[21]

19 The Council of Europe, not to be confused with the European Union, has also issued an instrument for data protection: the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.[22] Mostly, the Convention and the Directive run along the same lines, the latter being

somewhat more elaborate. The Court has referred to both instruments in its jurisprudence[23] and similarly, the Court has referred to the Charter of the EU to overthrow its earlier jurisprudence, from before 2000, on a number of important points.[24] Since the accession of the EU to the European Convention of Human Rights, more and more synthesis has been created between the two fundamental rights instruments.[25] This article will mainly refer to the Data Protection Directive, as it is seen as the more important of the two documents, though it must be stressed that most of the rules contained therein are also present in the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

20 Although on a number of points there is a clear overlap between the right to privacy and the right to data protection, there are also important differences. First, the background of both rights is quite different. Privacy in the sense of a separation between the private and the public sphere, the integrity of the body and the secrecy of communications has been a part of the constitutional order for ages. Privacy is mostly linked to the protection of private interests of the individual related to personal autonomy or human dignity, among others. Data protection, in contrast, is of more recent origin and was created primarily in relation to the use of large databases by governmental agencies. The rules were not so much linked to the protection of private interests, but to the fairness and quality of the data processing. Most of the rules could be qualified as principles of good governance: collect data only when necessary, store them in a safe and confidential manner, be transparent about it and make sure that the personal data are kept correct and up to date. With the latter principle, a clear demarcation between privacy and data protection can be drawn. These principles of fair and legitimate data processing may require gathering more, not less, personal data, a rule which is difficult to reconcile with privacy rights.[26] As another difference, reference can be made to the fact that data protection is predominantly directed at private parties and horizontal relationships; especially security-related data processing by state and governmental agencies is often excluded from the scope of data protection acts.[27] This is different for the protection of privacy, especially under the European Convention of Human Rights, with regard to which citizens can only complain about the conduct of states.

21 Perhaps the most important difference lies in the material scope of the right to privacy under Article 8 ECHR, which is linked to the protection of personal interests such as human dignity, individual autonomy and personal freedom, and consequently, its scope does not extend to the collection of non-private and non-sensitive data: "[P]rivate life does not necessarily include all information on identified or identifiable persons. However, data protection covers exactly this information. This wider scope results from the definition of personal data in the Data Protection Convention and the Data Protection Directive".[28] The term "personal data", central to the Data Protection Directive, is not limited to private or sensitive information but extends to any data with which someone could potentially be identified. "Even ancillary information, such as 'the man wearing a black suit' may identify someone out of the passers-by standing at a traffic light."[29] Consequently, the Data Protection Directive not only regards the protection of personal interests of specific individuals, but also, and perhaps primarily, lays down procedural safeguards and duties of care for data processers.

22 Despite the significant differences between the two rights, the Court has increasingly recognized a number of the principles underlying the Data Protection Directive under the ECHR, specifically the right to privacy, by stressing (among other things) that the collection of personal data, such as transcripts of telephone conversation, photographs, hospital records and bodily material, also falls under the scope of the right to privacy. In addition, the Court has determined that there should be a legitimate ground for processing personal data, that processors should be cautious about transferring personal data to third parties and that where possible, personal data should be deleted when they are no longer relevant to the purpose for which they were collected.[30] Every one of these principles are core values underlying the Data Protection Directive. Finally, the Court has determined that the Member States to the Convention have a positive obligation to lay down adequate data protection rules in their national legislation.[31]

23 Nevertheless, the Court retains the position that for a case to fall under the scope of the right to privacy, there should be a link to personal interests, such as an infringement of an individual's dignity or autonomy. Consequently, if a limited amount of personal data is stored, if a dataset contains only trivial information such as names and addresses, or if the data collection must be regarded as a common and standard practice in the European Union, it is usually declared to fall outside the scope of the right to privacy.[32] Moreover, the Court has held that if data are collected in public and are not stored, or are stored but are made inaccessible, this does not fall under the scope of the right to privacy.[33] Not surprisingly, privacy experts suggest that the guarantee of data protection principles under Article 8 ECHR is quite limited and argue that the distinction between private data and non-sensitive data, which is no longer at work in the Data Protection Directive, is still a leading principle in the case law of the Court.

> *A closer reading shows that the old distinction between "data that merits protection" and "data that does not" is still at work and that processing of data is excluded from the privacy scope when (1) the data as such are not considered as private, (2) when there are no systematically stored images or sound recordings, or other data, (3) when the data are not systematically stored with the focus on the data subject, and (4) when the data subject could reasonably expect the processing.*[34]

24 Consequently, there seems to be a number of thresholds for applying Article 8 ECHR on matters related to Big Data processes. (1) Much of the data collected are not private but public; additionally, processing often regards so-called meta-data, such as data on the length of and the participants to a call, but not the content of communication itself.[35] (2) In addition, the personal data themselves are not always recorded, but they are often used for creating aggregated datasets and group profiles.[36] (3) The essential characteristic of this type of large-scale data systems is that they have no focus on any specific subject, but that they regard an unquantified group of people, potentially everyone.[37] (4) In a sense, large-scale data processing may already be described as an everyday practice, and it is highly likely that in the future, this will even be more so.

25 In conclusion, it seems questionable whether the right to privacy under the ECHR provides adequate protection in relation to Big Data systems and data processing such as revealed with regard to the NSA. This may be the fundamental question: Is a doctrine focussed on the protection of the individual interest – related to human dignity, individual autonomy or personal freedom – still feasible in a world that is increasingly engulfed by large-scale data processing techniques, which, by their very nature, are not focused on the individual?

D. Balance of interests

26 Even if the NSA data processing were to fall under the scope of Article 8 ECHR, and even if a right of complaint were to be accepted, it is still highly questionable whether the Court would rule in favour of the complainants. Article 8, paragraph 2 specifies as follows:

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

27 Consequently, privacy limitations are allowed when they are prescribed by law and necessary in a democratic society in connection to, among others, national safety, public health and economic prosperity.

28 The authors of the Convention had in mind that the outcome of a case should be determined by an assessment of the necessity of an infringement, inter alia by determining the effectiveness, proportionality and subsidiarity of a particular measure. Although this 'intrinsic test' has not been completely abandoned by the Court, it has been moved to the background and is increasingly supplemented by a 'balancing test'. "This test requires the Court to balance the severity of the restriction placed on the individual against the importance of the public interest."[38] Consequently, to determine the outcome of a case, the Court balances the damage a specific privacy infringement has done to the individual interest of a complainant against its instrumentality towards safeguarding a societal interest, such as national security.

29 The problem with a balancing test in relation to Big Data systems is twofold. First, the necessity test seems a far better tool to assess the problems posed by, among others, the NSA affair and similar cases. The question here seems simply whether such large data sets regarding so many people and collected over such a large time span is at all necessary and proportionate in the light of public safety, even apart from any individual interest, and whether there are no less intrusive means at the disposal of the government. In addition, it might be asked how effective such data processing systems really are.

> *Some agency insiders now believe that NSA is only able to report on about 1 percent of the data that it collects, and it is getting harder every day to find within this 1 percent meaningful intelligence. Senior Defense and State Department officials refer to this problem as the "gold to garbage ration," which holds that it is becoming increasingly difficult and more expensive for NSA to find nuggets of useful intelligence in the ever-growing pile of garbage that it has to plow through.'*[39]

30 On the other hand, it is increasingly difficult to make a proper balance of interests in this kind of Big Data systems. A balancing test provides an adequate tool when reviewing classic privacy issues – for example, a house search in the context of a criminal investigation – in which the infringement is clearly delineated in person, time and space, and both the resulting individual interest and the public interest – for example related to solving a murder case – have a clearly defined character. With Big Data systems, however, both the public and the individual interest are rather hypothetical and abstract, as it is often unclear whether a particular data set will contribute to the national security and how; and, as indicated earlier, the individual element in these processes is often moved to the background and the presumed damage arises from potential future data leaks or the abuse of the data by malicious regimes. Both interests are consequently very vague and therefore difficult to balance.

31 To address these problems, in data processing cases the Court is prepared to focus predominantly on the intrinsic qualities of legal frameworks and governmental activities. Among others, the "Court must be satisfied that, whatever system of surveillance is adopted, there exist adequate and effective guarantees against abuse".[40] It has also stipulated that where possible, persons have to be informed of the fact that they have been subjected to monitoring, that there must be proper democratic control by parliament to assess the activities of the secret services and that there should be effective legal remedies open to individuals who believe they have been subjected to monitoring and surveillance.[41]

32 Although the Court's case law does leave some room for assessing cases without directly balancing the individual with the public interest, this seems to provide only meagre safeguards with regard to Big Data systems. First, it should be noted that the Court is willing to focus on procedural conditions, such as with regard to access to a court and the existence of democratic control, but not on the necessity, proportionality and subsidiarity of the measures as such.[42] If the national court or legislature were to decide that the practices are indeed necessary and proportionate, the Court would in principle follow their judgment. The Court has also stated that in the case of intelligence and surveillance systems, "the margin of appreciation available to the respondent State in assessing the pressing social need [] and in particular in choosing the means for achieving the legitimate aim of protecting national security, [is] a wide one".[43]

33 Moreover, the Court accepts that both confidentiality regarding the nature and purpose of the intelligence activity and reluctance in informing specific persons about the fact that they have been subjected to eavesdropping, in principle, must be deemed legitimate since confidentiality is part of the effectiveness of the activities by secret services. Finally, it should be noted that although the requirement that a privacy infringement must be prescribed by law also applies to the practices of intelligence organizations, it is precisely with regard to secret services that a separate and rather limited legal framework exists, so that usually neither the ordinary citizens nor the ordinary parliamentarian will know exactly what activities are conducted and with which specific purpose. In any case, the fundamental point remains that, apart from the specific context of secret services, the balancing test seems simply unsuitable for Big Data systems. Another fundamental question may be whether the privacy interests at stake should still be considered relative, to be balanced against other values such as security. If it is true that incidents such as the NSA affair challenge the basic legitimacy and effectiveness of the state, it could be argued that these are absolute minimum principles to be respected by every democratic order respecting the rule of law.

E. Analysis

34 The current privacy doctrine under Article 8 ECHR is based on three characteristics: it is the right of a natural person; it protects his personal interests related to, among others, autonomy and dignity; and the outcome of a case will be determined primarily by weighing the private against the public interests, such as those related to national security. Developments in the field of Big Data and profiling challenge each of these principles. Although the Court is willing to adopt a certain amount of flexibility to meet these challenges, the question remains whether this is sufficient to provide adequate protection. Even if the Court were willing to compromise the three fundaments so as to ensure adequate protection, there remains a fundamental tension between the focus on the individual and his interests on the one hand and the current technological developments on the other. With regard to the claim of *Big Brother Watch and others v. the United Kingdom*, it is questionable whether they will be successful in their claim. This article has signalled three potential hurdles.[44]

35 First, the applicants would have to prove that they have been subjected to monitoring practices, or at least demonstrate that this is likely, as *in abstracto* claims are declared inadmissible. More importantly, the Court's case law makes clear that there is a prohibition on an *actio popularis* or class action, in which a civil society organization or group complains about a matter not out of personal interest, but in the interest of the society as a whole. The first complainant, Big Brother Watch, is a limited company, not in any way directly affected by the presumed practices of the British secret services, and the second and third applicants are a charity and a limited company, for which the same holds true. The only natural person is the fourth and last applicant, Constanze Kurtz, but she works and lives in Berlin and is thus highly unlikely to have been a victim of the practices complained of.

36 Second, it is questionable whether the matter falls under the material scope of Article 8 ECHR.

> *The applicants allege that they are likely to have been the subject of generic surveillance by GCHQ [The Government Communications Headquarters] and/or the United Kingdom security services may have been in receipt of foreign intercept material relating to their electronic communications, such as to give rise to interferences with their rights under Article 8 of the Convention. [] The applicants further contend that the generic interception of external communications by GCHQ, merely on the basis that such communications have been transmitted by transatlantic fibre-optic cables, is an in-*

herently disproportionate interference with the private lives of thousands, perhaps millions, of people.[45]

37 If it is recalled that to fall under the scope of Article 8 ECHR, (1) the data must be considered private, (2) they must be systematically stored, (3) with a focus on the data subject and (4) the possessing could not be reasonably expected, it seems that at least point three will provide a threshold, as the data are not stored with the focus on a particular subject, but are aggregated for the use of making group profiles and determining statistical correlations.

38 Finally, even if it is accepted that the applicants may successfully claim their right to privacy and that the matter complained of does fall under the scope of Article 8 ECHR, it is questionable whether the ECtHR will judge in their favour. Although the applicants claim that there has been "an inherently disproportionate interference with the private lives of thousands, perhaps millions, of people", it remains unclear how exactly they have been affected by the practices and how this influences their daily lives, their autonomy or their dignity. The individual interest is thus highly abstract and hypothetical. It seems that the British parliament has simply determined the need for such practices necessary with an eye on the national security and has felt that this outweighs the particular interests of private individuals. If the European Court of Human Rights were to conclude that the matter complained of is "in accordance with the law", as laid down by the British parliament, a question not assessed in this article, it is highly likely that it would accord a wide margin of appreciation to the British legislator and respect its decision in this regard.

39 The question arises whether the current approach of the Court and the chosen interpretation of Article 8 ECHR is still feasible in a world in which technological developments and data processing techniques rapidly succeed each other. Not only does it not give a satisfactory outcome for cases regarding NSA-like data processing systems, it must be recalled that the NSA affair is part of a bigger and structural change in society. Two possible approaches are possible. First, the Big Data processes and the resulting problems may simply be said not to qualify as privacy issues but to fall under other doctrines, such as the abuse of power, anti-discrimination provisions and general procedural doctrines. However, this seems an unsatisfactory solution because the problems are indeed related to and partly derived from classic privacy issues, such as the monitoring of private individuals, placing wiretaps and generating large dossiers about possible suspects. In addition, the right to privacy, both in legal and in societal discourse, is the doctrine which is referred to when it comes to these issues. However, if the right to privacy under the European Convention of Human Rights is to retain its relevance in the changing environment, some fundamental revisions seem necessary.[46]

40 First, it may be questioned whether the requirement of personal injury should be maintained. The problem with this principle is that complaints about data collection processes often have a hypothetical and abstract nature, but that does not mean that they are of less importance. Although the chance of an 'evil' regime seizing power and abusing the collected data for malicious purposes is extremely small, the possible negative consequences dwarf the importance of ordinary privacy cases related to a house search, for example. Moreover, the background of this principle lies in ensuring that the Court is not flooded with complaints and that only those can file an application who have suffered individually and directly from the matter complained of. However, it is questionable whether the abandonment of the principle of personal injury will indeed result in an increased flow of complaints. Allowing an *actio popularis* may in fact ensure that potential damage arising from structural problems is addressed so that individual damage and myriad claims can be prevented or at least bundled. Likewise, allowing for *in abstracto* claims may ensure that potential future damage is prevented and would also ensure that the judgment of the ECtHR would be substantially more concise as there is no need for a description and analysis of the particular circumstances of the case, the personal situation of the complainant and the causal link between the act or practice complained of and the harm to the individual interest. The decision would merely regard the necessity, proportionality and effectiveness of the measures themselves.

41 Second, it may be questioned whether the right to privacy should be focused solely on protecting the personal interest of the complainant in relation to, among others, his dignity, autonomy or freedom, or that the underlying value and the related material scope of the right to privacy could also be formulated as or connected to a public interest. For example, under the Universal Declaration of Human Rights, on which Article 8 ECHR is based, the right to privacy was initially simply formulated as the 'freedom from wrongful interference' and specified as such: "Freedom from unreasonable interference with his person, home, reputation, privacy, activities, and property is the right of every one."[47] Privacy, as it was originally understood by the authors of both the Declaration and the Convention, was primarily a duty of the state and was connected to a societal interest, namely the prevention of abuse of governmental power and the disproportionate and unnecessary meddling in the private sphere of citizens. It regarded primarily the quality of legislation and governmental practices as such and not or only to a limited extent the protection of specific individual interests, related to their autonomy or dignity. Possibly, renewed emphasis could be placed on this

approach, which would also dovetail with dropping the injury requirement, because the prime norm-addressee of the privacy doctrine would be the state, which has an obligation to respect it independently of any subjective right or individual interest.

42 Third, this might also facilitate the reintroduction of an 'intrinsic' test, in which the outcome of a case is determined by assessing the necessity, proportionality, subsidiarity and effectiveness of the measures or laws. This focus could not only be adopted to large data collection processes but perhaps also be applied to more traditional privacy issues regarding house searches and wiretaps, in which the primary question is also whether a certain interference is necessary and proportionate, irrespective of the individual interests involved. In relation to cases related to national security, this method seems reasonable: if a house search, telephone-tap or data collection is necessary and effective in the context of national security, it is often simply irrelevant whether and to what extent a citizen is affected, as the public interest will almost always outweigh the individual interest.[48] It would therefore be worthwhile to assess whether the subjective element in this respect could be substituted for a more objective and intrinsic-based test.

1 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). Parts of this research will also appear in Dutch: B. van der Sloot, "Privacy in het post NSA-tijdperk: tijd voor een fundamentele herziening?", NJB, to be published.

2 V. Mayer-Schonberger & K. Cukier, "Big data: A revolution that will transform how we live, work, and think", Boston, Houghton Mifflin Harcourt, 2013.

3 See further: S. Bu (et al.), "Preservation of Patterns and Input-Output Privacy", Proceedings of ICDE2007, 20070. T. Calders, & S. Verwer, "Three Naive Bayes Approaches for Discrimination-Free Classification", Data Mining and Knowledge Discovery 21(2), 2010. J. S. Fulda "Data Mining and Privacy", Alb. L.J. Sci. & Tech. 11, 2000. H. P. Grice, "Logic and conversation". In: P. Cole & J. Morgan (eds.), "Syntax and semantics", New York, Academic Press, 1975. K. Guzik, "Discrimination by Design: Data Mining in the United States's 'War on Terrorism'", Surveillance & Society (7), 2009. M. Hildebrandt & S. Gutwirth (eds.), "Profiling the European Citizen: Cross-Disciplinary Perspectives", New York, Springer, 2008. D. Pedreschi, S. Ruggieri & F. Turini, "Discrimination-Aware Data Mining, KDD, 2008. C. C. Porter, "De-Identified Data and Third Party Data Mining: The Risk of Re-Identification of Personal Information", Shidler i.L. Com. & Tech. (30), article no. 3, (2008). Y. Poullet & A. Rouvroy, "General introductory report", (2008). <http://portal.unesco.org/ci/en/files/27268/12145631033Intro_gen_rapporteur_Y-Poullet_en.pdf/Intro_gen_rapporteur_Y-Poullet_en.pdf>. A. Ramasastry, "Lost in translation? Data mining, national security and the 'adverse inference' problem", Santa Clara Computer & High Tech. L.J. (22), 2006. W. N. Renke, "Who controls the past now controls the future: Counter-terrorism, data mining and privacy", Alta. L. Rev. (43), 2006. C. Westphal, "Data Mining for Intelligence, Fraud & Criminal Detection", Boca Raton, Taylor & Francis Group, 2009. T. 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, 2003 (5).

4 B. Custers, T. Calders, B. Schermer & T. Zarsky (eds.), "Discrimination and privacy in the information society: Data mining and profiling in large databases", Heidelberg, Springer, 2013.

5 See regarding meta-data (with thanks to Matthijs Koot <http://blog.cyberwar.nl/> for these suggestions): <http://www.cs.princeton.edu/~felten/testimony-2013-10-02.pdf>. <http://www.crypto.com/blog/metatapping>. B. Greschbach, G. Kreitz and S. Buchegger, "The Devil is in the Metadata – New Privacy Challenges in Decentralised Online Social Networks", <http://www.csc.kth.se/~bgre/pub/GreschbachKB12_MetadataPrivacyDecentralisedOnlineSocialNetworks.pdf>. <http://www.theguardian.com/technology/interactive/2013/jun/12/what-is-metadata-nsa-surveillance#meta=1111111>.

6 <https://www.privacynotprism.org.uk/assets/files/privacynotprism/letter_from_ecthr_to_uk_gov.pdf>.

7 A. H. Robertson, "Collected edition of the 'travaux préparatoires' of the European Convention on Human Rights. Vol. 1", The Hague, Nijhoff, p. 160-162

8 Robertson, vol. 2, p. 270.

9 Robertson, vol. 2, p. 188-192.

10 An intermediate step: <http://conventions.coe.int/Treaty/en/Treaties/Html/140.htm>.

11 <http://hudoc.echr.coe.int/sites/eng/Pages/search.

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

13 See among others: ECtHR, Stes Colas Est and others v. France, application no. 37971/97, 16 April 2002.

14 See among others: ECmHR, Tauira and others v. France, application no. 28204/95, 04 December 1995.

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

16 ECtHR, Lordachi and others v. Moldavia, application no. 25198/02, 10 February 2009, § 34.

17 ECtHR, Liberty v. Great Britain, application no. 58243/00, 01 July 2008, § 57.

18 ECmHR, Matthews v. Great Britain, application no. 28576/95, 16 October 1996.

19 See among others: ECtHR, Kennedy v. Great Britain, application no. 26839/05, 18 May 2010.

20 ECtHR, Weber and Saravia v. Germany, application no. 54934/00, 29 June 2006.

21 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.

22 <http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm>.

23 Convention: ECtHR, Rotaru v. Romania, application no. 28341/95, 04 May 2000. Directive: ECtHR, Romet v. the Netherlands, application no. 7094/06, 14 February 2012. ECtHR, S. and Marper v. the United Kingdom, application nos. 30562/04 and 30566/04, 04 December 2008. ECtHR, M.M. v. the United Kingdom, application no. 24029/07, 13 November 2012.

24 See for example: ECtHR, Christine Goodwin v. the United Kingdom, application no. 28957/95, 11 July 2002. ECtHR, I. v. the United Kingdom, application no. 25680/94, 11 July 2002.

25 <http://hub.coe.int/what-we-do/human-rights/eu-accession-to-the-convention>.

26 B. van der Sloot, "From Data Minimization to Data Minimummization". In: B. Custers, T. Calders, B. Schermer &

T. Zarsky (eds.), Discrimination and Privacy in the Information Society. Data Mining and Profiling in Large Databases, Springer, Heidelberg, 2012.

27 See among others, Article 3.2 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.

28 J. Kokott & C. Sobotta, "The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR", p. 89, in: H. Hijmans & H. Kranenborg (eds.), "Data Protection anno 2014: How to Restore Trust? Contributions in honour of Peter Hustinx, European Data Protection Supervisor (2004-2014)", Intersentia, 2014. See in the same book also: C. Docksey, "The European Court of Justice and the Decade of surveillance".

29 Article 29 Working Party, "Opinion 4/2007 on the concept of personal data", 01248/07/EN, WP 136, 20 June 2007, Brussels, p. 13.

30 For the standard cases on data protection among others, see: ECtHR, P.G. & J.H. v. Great Britain, application no. 44787/98, 25 September 2001. ECtHR, Perry v. Great Britain, application no. 63737/00, 17 July 2003. ECtHR, Malone v. Great Britain, application no. 8691/79, 02 August 1984. ECtHR, Copland v. Great Britain, application no. 62617/00, 03 April 2007. ECtHR, Halford v. Great Britain, application no. 20605/92, 25 June 1997. ECtHR, Peck v. Great Britain, application no. 4467/98, 28 January 2003.

31 ECtHR, Köpke v. Germany, application no. 420/07, 05 October 2010.

32 See among others: ECmHR, Murray v. Great Britain, application no. 14310/88, 10 December 1991.

33 ECmHR, Herbecq v. Belgium, application nos. 32200/96 and 32201/96, 14 January 1998.

34 P. De Hert & S. Gutwirth, "Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action", p. 17. In: S. Gutwirth, Y. Poullet, P. De Hert, J. Nouwt & C. De Terwangne (Eds), "Reinventing data protection?", Dordrecht, Springer Science, 2009. Cited from: <http://works.bepress.com/cgi/viewcontent.cgi?article=1009&context=serge_gutwirth>.

35 <http://www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year-documents>.

36 See further: B. 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. J. Jin & C. Clifton, "When do data mining results violate privacy?", in: Proceedings of the 10th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD"04), 2004. D. Skillicorn, "Knowledge Discovery for Counterterrorism and Law Enforcement", Boca Raton, Taylor & Francis Group, 2009. H. T. Tavani, "Genomic research and data-mining technology: Implications for personal privacy and informed consent", Ethics and Information Technology (6), 2004. T. Wang & L. Liu, "Output Privacy in Data Mining", Transactions on Database Systems, 36 2011 (1).

37 See further: A. Evfimievski, R. Srikant, R. Agrawal & J. Gehrke, "Privacy preserving mining of association rules", Proceedings of the 8th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD"02), 2002. P. Kuhn, "Sex discrimination in labor markets: The role of statistical evidence", The American Economic Review, 1987 (77). M. LaCour-Little, "Discrimination in mortgage lending: A critical review of the literature", Journal of Real Estate Literature 1999 (7). D. T. Larose, "Data mining methods and models", New Jersey: John Wiley & Sons, 2006. V. C. Müller, "Would you mind being watched by machines? Privacy concerns in data mining", AI & Soc (23), 2009. S. Ruggieri, D. Pedreschi & F. Turini, "Data Mining for Discrimination Discovery", Transactions on Knowledge Discovery from Data, 4 2010 (2). B. W. Schermer, "The limits of privacy in automated profiling and data mining", Computer law & security review, 2 2011 (7). G. D. Squires, "Racial profiling, insurance style: Insurance redlining and the uneven development of metropolitan areas", Journal of Urban Affairs 25 2003 (4). V. S. Verykios, et al., "State-of-the-art in Privacy Preserving Data Mining", Sigmod Record, 33 2004 (1).

38 C. Ovey & R. C. A. White, "European Convention on Human Rights", Oxford, Oxford University Press, 2002, p. 209.

39 M. M. Aid, "The Secret Sentry: The Untold History of the National Security Agency", New York, Bloomsbury Press, 2009, p. 304.

40 ECtHR, Klass and others v. Germany, application no. 5029/71, 06 September 1978, § 50.

41 See among others: ECtHR, Eimdzhiev v. Bulgaria, application no. 62540/00, 28 June 2007.

42 See further: EHRM, Kruslin/Frankrijk (11801/85), 24/04/1990. EHRM, Huvig/Frankrijk (11105/84), 24/04/1990. EHRM, Uzun/Duitsland (35623/05), 02/09/2010. EHRM, Telegraaf Media e.a./Nederland (39315/06), 22/11/2012. EHRM, Amann/Zwitserland (27798/95), 16/02/2000.

43 ECtHR, Leander v. Sweden, application no. 9248/81, 26 March 1987, § 59.

44 The question of exhausting domestic remedies has not been discussed in this article.

45 <https://www.privacynotprism.org.uk/assets/files/privacynotprism/letter_from_ecthr_to_uk_gov.pdf>.

46 Whether they will replace or complement the current paradigm and how this should be envisaged could be a matter of debate, but these are the points that could be considered.

47 <http://daccess-ods.un.org/TMP/1333278.56659889.html>.

48 It seems like the Court's jurisprudence would allow for such an interpretation: A. McHarg, "Reconciling Human Rights and the Public Interest: Conceptual Problems and Doctrinal Uncertainty in the Jurisprudence of the European Court of Human Rights", The Modern Law Review, Vol. 62, no. 5, 1999.