7 THE INDIVIDUAL IN THE BIG DATA ERA: MOVING TOWARDS AN AGENT-BASED PRIVACY PARADIGM

Bart van der Sloot

The current human rights framework in general and the privacy paradigm in particular is based on the individual in a threefold manner: (1) it provides him with a subjective right, (2) to protect his personal interest and (3) the outcome of a court case is determined by balancing the individual against a societal interest. Big Data processes, however, do not revolve around individuals; they focus on large groups and have an impact on society in general. Consequently, the focus on the individual and his interests is becoming increasingly obsolete. To remedy this fact, privacy scholars have suggested to reformulate privacy either as a group right, a societal interest or a precondition for a democratic society. Focusing on other than individual interests obviously has an impact on the way rights and legal claims are attributed, how rules are enforced and how the outcome of legal cases is determined. This contribution discusses the different suggestions that have been put forward and determines in how far they might ameliorate the current privacy paradigm.

7.1 INTRODUCTION

Privacy has been declared dead ever since it was conceived. Already in the sixties of last century, books appeared that proclaimed the end of privacy. Mostly, such eschatological visions point either to the young, who supposedly no longer care about privacy, or to newly emerging technologies, which enable large-scale data collection, whether it be photography, telephone records, data bases, the internet or Big Data. At the same time, scholars have always claimed to 'reinvent' privacy, either by introducing new ways of emphasizing the interests at stake, arguing for a different way of protecting privacy (for example, through commodity rights or through technological regulation) or by introducing new concepts, such as informational privacy and data protection.

Perhaps this is because privacy is about boundaries, boundaries between the private and the public, between the individual and society, between individual autonomy and public rules, etc. Boundaries change over time, and the types of boundaries thought necessary differ per person, per culture and per epoch. Still, what has unified most privacy theories so far is that they focused on the protection of the individual against the collective, of the private against the public. It is exactly this presumption that is wavering in the age of Big Data: it appears to be

increasingly difficult to relate the effects of Big Data processes back to individual interests. Increasingly, recourse is taken to the use of metaphors to capture what is at stake in these types of data flows.

The classic metaphor is that of the Panopticon, after the prison model of Bentham, who proposed the design of a prison in which the guard could see the prisoners but the prisoners could not see the guard (Bentham 1791). Foucault suggested that this model is archetypical for current Western society, in which everyone might be watched but is never sure about it (Foucault 1975). This will result in citizens curtailing their behaviour out of precaution, which is also known as the chilling effect. These types of theories do not focus on actual and concrete harm, but on future and hypothetical effects of current surveillance techniques.

Other theories have used metaphors to capture the increased focus on groups and categories in data processing techniques. Those pointing to the Mathew effect argue that Big Data may increase the inequality between groups in society. The use of profiles may have a stigmatizing effect: people living in certain neighbourhoods may have more trouble getting loans, people with a certain ethnic or religious background may be checked and surveilled more often, etc. Others have suggested the metaphor of a Filter Bubble (Pariser 2012), which captures the fear that people will be profiled in a particular category and will get stuck in it because they will only get news, search results and advertisements that fit that profile. These types of theories try to address the fact that the use of data is increasingly moving from the individual to the group.

Reference is also made to environmental protection (Galetta and De Hert 2014). Data is called the new oil (Kuneva 2009) and privacy the canary in the coal mine (Thatcher 2014). Others have likened privacy violations following from Big Data processes to the environmental pollution resulting from the industrial revolution (Hirsch 2014). There are certain similarities between environmental pollution and privacy violations following from Big Data. Both may have an impact on the individual as well as the environment in general. It is not for nothing that environmental laws not only allow claims by specific individuals who have suffered from personal harm, but also facilitate claims regarding damage to the environment as such. Consequently, individual rights and individual interests are complemented by class actions and general interests. With regard to individual impact, it should be noted that it is often very difficult to prove the causal relationship between, for example, air pollution and a specific health condition.

Similarly, Big Data may have an impact on both specific individuals and on the world we live in. Moreover, in individual cases, it is often difficult to determine the direct link between individual harm and Big Data processes. That is why some have argued that, in privacy laws, there should also be room for class actions in the

general interest and that privacy regulators could learn something from the more relaxed requirements in environmental laws regarding the causality between incidents and individual harm. Finally, the metaphor of Kafka's *The Trial* has often been proposed (Solove 2008). Here the idea is simply that citizens are unsure why the government is acting in certain ways and how this might impact them. The point is not so much that it has a negative impact on them, but simply that there is no way of finding out whether this is the case and that there are no safeguards against the abuse of power by the government. Again, similarities are drawn to Big Data processes, which are often vague and incomprehensible to ordinary citizens, even if the outcome of these processes may have a serious impact on their lives.

What has prompted these theories is that it is increasingly difficult to determine what is exactly at stake in Big Data processes. Although everyone agrees that, for example, there is something problematic about the NSA's data collection, it is hard to point out what that really is, besides mere technical points of whether the activities were prescribed by law and whether Parliament or even president Obama knew about them. What impact, for example, has the NSA data collection had on ordinary American or European citizens? How and in what way did it harm them? It is also increasingly difficult to focus on individual rights, quite simply because these large data gathering processes do not revolve around individuals. While the legal domain focuses on the individual level, on the particular, technical reality revolves around structural developments and focuses on the general level. Scholars are increasingly trying to develop privacy theories that solve this discrepancy, by focusing on societal interests, group interests, etc., rather than on individual interests. This chapter will discuss and evaluate these theories.

Section 7.2 will discuss the original privacy paradigm, which focused on the individual, his/her rights and his/her interests only in part. It will take as an example the European Convention on Human Rights (ECHR). Section 7.3 will briefly show that the current paradigm, by contrast, focuses on individual rights and interests almost exclusively. Section 7.4 will argue why it might prove problematic to maintain this focus because Big Data does not revolve around individuals. The transition between the 'original' and the 'current' paradigm has been discussed in greater detail in other publications (Van der Sloot 2014a, 2014b, 2014c, 2015a, 2015b, 2016a, 2016b); it is important to stress that the discussion here is idealized and that reality is far muddier and more complex than a few pages can describe. There is neither a linear process nor an exact moment in time when the transition from the 'original' to the 'current' paradigm took place, and it is important to stress that one may still find elements of the 'original' paradigm in current case law. Still, generally speaking, there has been an enormous change in how cases are approached under the European Convention on Human Rights. The two idealized models will be contrasted in sections 7.2 and 7.3.

After section 7.4, the chapter will continue by discussing the theories that have been proposed to solve this problem. They will be loosely divided in four sections, though there is certainly some overlap. Section 7.5 will focus on theories that argue that privacy is constitutive for societal institutions, such as the healthcare sector, the legal system and journalism. Section 7.6 will discuss the aggregated, group and collective interests that relate to privacy protection. Section 7.7 will discuss theories that focus on potential and future harm, including the chilling effect. Section 7.8 will discuss theories that revolve around the (ethical) evaluation of agents, or potential privacy violators. These theories let go of the requirement of individual harm altogether and instead focus on the moral responsibilities and ethical duties of agents gathering and processing data. Finally, section 7.9 will evaluate these theories and argue that these last theories in particular might prove to be fruitful for privacy protection in the age of Big Data.

7.2 ORIGINAL PARADIGM

The European Convention on Human Rights originally focused on laying down duties and prohibitions for the states who acceded to the Convention. The ECHR provides absolute prohibitions, such as those regarding abuse of power, enacting retrospective legislation, torture and degrading treatment; it lays down rules that may only be curtailed in a state of emergency, such as the right to a fair trial, the right to petition and the right to liberty and security; and it provides conditions under which a number of rights, such as the right to privacy, the right to freedom of expression and freedom of religion, may be curtailed under the rule of law, namely if they are prescribed by law and necessary in a democratic society for the protection of national security or public order, among other things.

The main goal of the Convention was to curtail the actions of governments, to prevent abuse of power and to sanction those states that did not abide by the rules of the ECHR (Robertson 1975-1985). Consequently, its main focus was on the duties of states and only marginally on the subjective rights of individuals. Hence, not only individuals could complain before European institutions, but also states could submit inter-state complaints (Art. 24 original ECHR), and groups as well as non-governmental organizations could invoke the rights under the convention (Art. 25 original ECHR). The main focus was on protecting the general interest of a society, relating to the good and appropriate use of power by the state; this interest could be invoked by everyone, not only by direct victims of practices and laws.

It should also be noted that individuals, groups and legal persons only had the right to submit a case before the European Commission on Human Rights, whose only task it was to declare cases admissible or inadmissible. Cases declared admissible could only be brought before the Court, which did have the authority to assess the substance of the case if either the Commission or a state decided to

pursue them (Art. 48 original ECHR). This allowed them to shift between cases that addressed only the particular interests of the individual complaint and those cases that addressed a wider issue, impacting society in general. Individuals did not have the right to bring a case before the Court, even if their case was declared admissible by the Commission.

The Convention aimed to protect the general interest by focusing on the integrity of the rule of law and the democratic process; these guarantees ensured a form of negative freedom for citizens, groups and legal persons alike. Of all articles contained in the Convention, the rationales of negative obligations for the state and negative freedom for individuals are most prominent in the right to privacy under Article 8 ECHR. Already under the Universal Declaration of Human Rights, on which the ECHR is largely based, it was this provision that was originally plainly titled 'Freedom from wrongful interference' (UN document: E/HR/3). Likewise under the Convention, the right to privacy was originally only concerned with negative liberty, contrasting with other qualified rights in which positive freedoms are implicit, such as a person's freedom to manifest his/her religion or beliefs (Art. 9 ECHR), freedom of expression (Art. 10 ECHR) and freedom of association with others (Art. 11 ECHR). Likewise, the wording of Article 8 ECHR does not contain any positive obligation, such as, for example, under Article 2, the obligation to protect the right to life, under Article 5, to inform an arrested person of the reason for arrest and to bring him or her promptly before a judge, under Article 6, the obligation to ensure an impartial and effective judicial system, and under Article 3 of the First Protocol, the obligation to hold free elections (Tomlinson 2012: 2).

Finally, the way in which cases should be resolved, according to the Convention authors, was by assessing the behaviour of the state as such. Hence the absolute and relative prohibitions in the Convention, and hence the conditions for restricting the qualified rights, such as the right to privacy. Article 8 ECHR holds in paragraph 1 that everyone has the right to private and family life, home and communications. Paragraph 2 specifies the conditions for curtailing this right:

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

A state, therefore, may curtail the right to privacy if this is prescribed by law, necessary in a democratic society and aimed at one of the goals specified in paragraph 2.

Note that this is a binary test: an infringement is either necessary or it is not, it is either prescribed by law or it is not and it serves either a legitimate goal or not. Take as an example the sanctity of one's home: if the police enters a person's house

for a good and legitimate reason, because, for example, they have reason to believe that this person has committed a murder and they want to search this house for a murder weapon, this is necessary for the protection of public order and is, therefore, legitimate. If the police enter a person's home without a legitimate reason, because the person is a famous football player, however, it is not. No balancing of interests takes place; the test is simply whether an infringement is necessary or not.

7.3 CURRENT PARADIGM

These pillars of the original paradigm have undergone significant changes over time. First, the right to complaint has been reduced to natural persons who have suffered as direct or indirect victims of a certain policy or law. Groups are not allowed to complain (only individuals who have all individually suffered from a certain practice are allowed to bundle their complaints); in principle, legal persons are prohibited from invoking the right to privacy (Van der Sloot 2015a); and so far there have only been some 20 inter-state complaints, contrasting sharply with the tens of thousands of individual complaints (Dijk et al 2006: 50). Furthermore, natural persons are only allowed to invoke the right to privacy if they are a victim and have sustained considerable harm.

This means that a number of complaints are principally rejected by the Court. So-called *in abstracto* claims are declared inadmissible in principle. 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 (Lawlor). *A-priori* claims are rejected as well, as the Court will usually only receive complaints about injury which has already materialized. Claims about future damage will not be considered in principle (Tauira et al.). Hypothetical claims regard damage which might have materialized but about which the claimant is unsure. The Court usually rejects such claims because it is unwilling to provide a ruling on the basis of presumed facts. Applicants must be able to substantiate their 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, to protect not their own interests but those of others or society as a whole. These types of cases are better known as class actions (Asselbourg et al.). Finally, the Court has held that applications are rejected if the injury sustained from a specific privacy violation is not sufficiently serious, even if the matter may fall under the material scope of Article 8 ECHR. For example, a case regarding the gathering and processing of a small amount of ordinary personal data will usually not be declared admissible (see also the *de minimis* rule, Article 35

paragraph 3 (b) ECHR and Trouche, Glass and Murray). Consequently, the right to complain has been narrowed down to natural persons who have directly and significantly been affected by a certain practice.

Second, Article 8 ECHR seems to have shifted from a right to privacy, laying down negative obligations for the state and providing protection to the negative freedom of citizens, to a full-fledged personality right (Van der Sloot 2015c). The element of positive liberty was adopted quite early in a case from 1976:

> "For numerous Anglo-Saxon and French authors the right to respect for 'private life' is the right to privacy, the right to live, as far as one wishes, protected from publicity. [H]owever, the right to respect for private life does not end there. It comprises also, to a certain degree, the right to establish and to develop relationships with other human beings, especially in the emotional field for the development and fulfillment of one's own personality" (X. v. Iceland).

Likewise, from very early on, the Court has broken with the strictly limited focus of the authors of the Convention on negative obligations and has accepted that states may, under certain circumstances, be under a positive obligation to ensure respect for the Convention. This has meant an enormously widened material scope of the right to privacy: it has allowed the European Court of Human Rights to deal not only with the more traditional privacy violations, such as house searches, wire-tapping and body cavity searches, but also with the right to develop one's sexual, relational and minority identity, the right to protect one's reputation and honour, the right to personal development, the right of foreigners to a legalized stay, the right to property and even work, the right to environmental protection and the right to have a fair and equal chance in custody cases. Consequently, the right to privacy has shifted from a doctrine prohibiting the state to abuse its powers, to a right of the individual to develop his/her personality and flourish to the fullest extent; and with this, it has shifted from a doctrine protecting general interests to one in which the core focus is on individual interests.

Finally, in most cases, the necessity test has been replaced by a balancing test, in which the societal and the personal interests involved in a specific privacy violation are balanced and weighed against each other.

> "Establishing that the measure is necessary in a democratic society involves showing that the action taken is in response to a pressing social need, and that the interference with the rights protected is no greater than is necessary to address that pressing social need. The latter requirement is referred to as the test of proportionality. This test requires the Court to balance the severity of the restriction placed on the individual against the importance of the public interest" (Ovey and White 2002: 209).

The provisions under the European Convention on Human Rights and the right to privacy in particular, therefore, are no longer seen primarily as minimum principles which the state must take into account, but as relative interests of individuals which can always be overridden if a particularly weighty societal interests is at stake.

7.4 BIG DATA

Consequently, the current privacy paradigm focuses largely on the individual, his/her interests and his/her subjective right to protect those individual interests. In the field of privacy, the notion of harm has always been problematic as it is often difficult to substantiate what harm has been caused by a particular violation; what harm, for example, follows from entering a home or eavesdropping on a telephone conversation when neither objects have been stolen nor private information has been disclosed to third parties? Even so, the 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, with developments such as Big Data, however, the notion of harm is becoming increasingly problematic. An individual is often simply unaware that his or her personal data are gathered by either fellow citizens (e.g., through the use of smart phones), by companies (e.g., by tracking cookies) or by governments (e.g., through covert surveillance). Obviously, people who are unaware of their data being gathered will not invoke their right to privacy in court.

Even if people were 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 them to keep track of every data processing which includes (or might include) their data, to assess whether the data controller abides by the legal standards applicable, and if not, to file a legal complaint. And if individuals go to court to defend their rights, they have to demonstrate a personal interest, i.e. personal harm, which is a particularly problematic notion in Big Data processes: what concrete harm has data gathering by the NSA done to ordinary American or European citizens? This also shows the fundamental tension between the traditional legal and philosophical discourse and the new technological reality: while the traditional discourse focuses on individual rights and individual interests, data processing often affects a structural and societal interest and, in many ways, transcends the individual.

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, wire-tapping someone's telephone because they are suspected of committing a murder, is weighed against the harm the wire-tapping does to their 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 in a particular case is hard to substantiate, but also because the societal interest at the other end is increasingly difficult to specify. It is mostly unclear, for example, 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, that is, how the collection of the personal data of this individual (as a non-suspected person) has ameliorated national security. The same holds true for CCTV cameras hanging on the corners of almost every street in some cities; the problem here is not that one specific person is being recorded and that data about this identified individual is gathered, but rather that everyone in that city is being monitored and controlled. Perhaps more important is the fact that, with some of the large-scale data collections, what appears to be at stake is not a relative interest, which can be weighed against other interests, but an absolute interest. For example, the NSA data collection is so large, has been conducted over such a long time span and includes data about so many people that it may be said to simply qualify as abuse of power. Abuse of power is not something that can be legitimated by its instrumentality towards a specific societal interest; it is an absolute minimum condition of having power.

7.5 CONSTITUTIVE INTERESTS

Many authors have struggled to find an exact definition and description of privacy. Most authors agree that the value and meaning of privacy differs over cultures, epochs and persons. Still, the right to privacy is generally linked to underlying values such as human dignity (Benn 1984), individual autonomy (Roessler 2005) or personal freedom (Mill 1989). This means that, in contrast to those values, the right to privacy is commonly viewed as an instrumental and not an intrinsic value. Solove, for example, holds that the problem with theories that ascribe an intrinsic value to privacy is that they tend to sidestep the difficult task of articulating why privacy is valued.

> "The difficulty with intrinsic value is that it is often hard to describe it beyond being a mere taste. Vanilla ice cream has intrinsic value for many people, but reasons cannot readily be given to explain why. Individuals like vanilla ice cream, and that is about all that can be said. Privacy's value is often more complex than a mere taste, and it can be explained and articulated. Although it is possible that some forms of privacy may have intrinsic value, many forms of privacy are valuable primarily because of the ends they further" (Solove 2008: 84).

Privacy is generally described as an instrumental value, as a relative value (contrasting with absolute values, such as the prohibition of torture) and a personal value. On this last point, there is a contrast with, among other things, freedom of

speech, which is generally said to be instrumental to individual expression and the possibility of personal development, but also to the search for truth in the marketplace of ideas and to the well-functioning of the press, which, in its turn, may be described as a precondition of a vital democracy.

Because of the points discussed in section 7.4, scholars have increasingly argued that privacy is not only instrumental towards personal values, but also constitutive of general institutions. Constitutiveness, in contrast to instrumentality, signals a necessary relationship: privacy is described as a necessary precondition for societal institutions. An example here is Spiros Simitis, who argued that privacy should be seen as a constitutive element of a democratic society (Simitis 1987). Ruth Gavison, in similar vein, held that:

> "In the absence of consensus concerning many limitations of liberty, and in view of the limits on our capacity to encourage tolerance and acceptance and to overcome prejudice, privacy must be part of our commitment to individual freedom and to a society that is committed to the protection of such freedom. Privacy is also essential to democratic government because it fosters and encourages the moral autonomy of the citizen, a central requirement of a democracy" (Gavison 1980: 455).

Of course, reference can also be made to Habermas, who argues that democracy and human rights are mutually constitutive (Habermas 1994). In these types of theories, privacy is a necessary precondition for democracy, the rule of law or a free and equal society.

Similarly, a connection between privacy and specific institutions is often made. Many of the court cases revolving around mass surveillance by secret services, for example, are initiated not only by civil society organizations protecting the right to privacy in general, but also by professional organizations protecting the specific interests of lawyers and journalists. These organizations point to the fact that both professions can only function properly if a degree of secrecy and confidentiality is guaranteed. Without secrecy between lawyers and clients, clients might not feel free to speak about sensitive issues, which leaves lawyers only partially informed and unable to defend their clients' case. This might undermine the right to a fair trial and, ultimately, the rule of law as such. Similarly, the argument is made that journalists cannot function without a form of secrecy of sources being guaranteed. Sources will not feel free to discuss sensitive matters with journalists or leak secret documents, which might ultimately undermine the position of the press as watchdog or fourth estate. The same might apply to the secrecy of ballot, a quintessential element of democratic elections (Lever 2015). Finally, a similar argument has been made with regard to patient-doctor confidentiality. Anita Allen, for example, holds:

> "First, confidentiality encourages seeking medical care. Individuals will be more inclined to seek medical attention if they believe they can do so on a confidential basis. It is reassuring to believe others will not be told without permission that one is unwell or declining,

> has abused illegal drugs, been unfaithful to one's partner, obtained an abortion, or enlarged one's breasts. […] Second, confidentiality contributes to full and frank disclosures. Individuals seeking care will be more open and honest if they believe the facts and impressions reported to health providers will remain confidential. It may be easier to speak freely about embarrassing symptoms if one believes the content of what one says will not be broadcast to the world at large" (Allen 2011: 112).

The fear is that surveillance in general and certain IT projects in the healthcare sector in particular might undermine the confidentiality required for a well-functioning healthcare sector. Reference is sometimes made to underdeveloped countries, where the fear of others finding out about a certain disease or condition is often greater than the wish to be cured, but also to the United States, where there are many fears about the influence of commercial parties and insurers.

7.6 GROUP AND COLLECTIVE INTERESTS

There are also theories that focus on the connection between individual harm and harm to others. The loss of privacy for one individual may have an impact not only on the privacy of others, but also on other important interests. It is stressed by some that a loss of privacy may undermine social relationships between individuals, which often consist of the very fact that certain information is disclosed between them and not to others. This is called the social value of privacy (Roessler and Mokrosinska 2013). But the loss of privacy for one individual may also have an impact on the privacy of others. This is commonly referred to as the network effect. A classic example is a photograph taken at a rather wild party. Although the central figure in the photograph may consent to posting the picture of him or her at this party on Facebook, it may also reveal others attending the party. This is the case with much information: people's living conditions and the value of their home does not only disclose something about them, but also about their spouse and possibly their children. Perhaps the most poignant example is that of hereditary diseases: data about such diseases might reveal sensitive information not only about a specific person, but also about their direct relatives.

Alternative theories look not only to one specific individual, but to all individuals affected by a specific violation. These theories focus on aggregated harm and primarily aim against the common practice in the legal domain of focusing on the specificities of a case, in combination with the fact that only individual victims can successfully file a complaint. What follows from this approach, according to some scholars, is a situation in which the effects of a certain law or policy are only measured and assessed with regard to its effects on the situation of a specific claimant. In reality, however, the law or policy has an effect on many, sometimes millions of people. In contrast with the individual interest at stake, the general interest, such as that relating to national security, is often assessed at a general and societal level. The question is not how the monitoring of a specific individual (the claimant) has benefited the fight against terrorism, for example, but how the mass surveillance

system as such aids this goal. It might be worthwhile, consequently, to assess the negative consequences of a particular law or policy in terms of privacy on a collective level as well.

These theories, though they broaden the scope of individuals being affected, still focus on individual harm. More recent theories have proposed to transcend the focus on the individual when it comes to assessing privacy violations. Generally speaking, this might be done by focusing either on the privacy of a group or on the privacy of larger collectives and the value of privacy for society as a whole. With regard to group privacy (Taylor et al. 2016), there are generally two lines of thinking. First, much in line with the ideas of social privacy, it might be said that groups depend on a form of privacy or secrecy for their existence. Consequently, if the right to privacy is undermined, this might have an effect on the group and its existence. Second, there is an increasing trend to use group profiles not only with regard to crime fighting and the war against terrorism, but also when banks use risk profiles when deciding about loans or health insurers when deciding who to insure, against what price, etc. The fact is that decisions are increasingly made on the basis of these profiles, which might lead to discrimination and stigmatization, as well as loss of privacy. The problem is not so much that this or that specific individual is affected by being put in a certain category, whether rightly or wrongly, but that policies are based on stigmatizing or discriminating group profiles as such, and it has been suggested, therefore, that it might be worthwhile to look into the possibility of granting groups a right as such. Finally, as to the rights of future generations, it is not only a healthy living environment that may be in their best interest, but a good privacy environment may possibly be included in those interests too.

There are also those who have argued that privacy should be regarded as a public good (Fairfield and Engel 2014) or a societal interest (Van der Sloot 2014a) rather than as an individual interest or in addition to it. For example, many of the current privacy violations are taking place on such a large scale and are affecting so many people that this might qualify simply as abuse of power, undermining citizens' trust in the government and in democratic institutions. Others have stressed, in reference to the Panopticon, that the fear following from mass surveillance curtails the scope of their unfettered experimentation and their development, which is detrimental not only to those specific individuals, but also to society as a whole (Richards 2013). When discussing privacy and the common good, Priscilla Regan distinguishes between three types of values.

> "Privacy has value beyond its usefulness in helping the individual maintain his or her dignity or develop personal relationships. Most privacy scholars emphasize that the individual is better off if privacy exists; I argue that society is better off as well when privacy exists. I maintain that privacy serves not just individual interests but also common, public, and collective purposes. If privacy became less important to one individual in one particular context, or even to several individuals in several contexts, it would still be

> important as a value because it serves other crucial functions beyond those that it performs for a particular individual. Even if the individual interests in privacy became less compelling, social interests in privacy might remain. [...] I suggest that three concepts provide bases for discussing a more explicitly social importance for privacy – privacy as a common value, privacy as a public value, and privacy as a collective value. The first two concepts are derived from normative theory, while the latter is derived from economic theory; the styles of analysis, therefore, are different, with the first two being conceptual and the third more technical" (Regan 1995: 211).

There is a common interest in privacy, Regan suggests, because individuals who have privacy become more valuable not only to themselves, but also to society as a whole. Privacy as public value is the idea that privacy is not just valuable in itself, but is also instrumental towards other values, such as freedom of speech. Finally, the idea of privacy as a collective value is derived from the economists' concept of collective or public goods, which are those goods that are defined as indivisible or non-excludable: not one member of society can enjoy the benefit of a collective good without others also benefiting. Clean air and national defence, she suggests, are examples of public or collective goods.

> "Currently a number of policies and policy proposals treat privacy as a 'private good' and allow people to buy back or establish the level of privacy that they wish. For example, when you subscribe to a magazine, you can indicate that you do not want your name and information about you incorporated in a mailing list and sold for direct-mail purposes. Similarly, one policy proposal concerning Caller ID is that individuals be given the ability to 'block' the display of their numbers. Such examples suggest that you can indeed 'divide' privacy into components and allow people to establish their own privacy level. But three factors limit the effectiveness of this individual or market-based solution for privacy: the interests of third-party record holders; the nonvoluntary nature of many record-keeping relationships; and computer and telecommunication technologies" (Regan 1995: 228).

7.7 POTENTIAL HARM

There is a third branch of privacy theories that focuses not on actual and concrete harm at the individual level, but on potential harm. This might be either hypothetical harm or potential future harm. Hypothetical harm can exist when people might be affected by a certain privacy violation but are unsure about this. The classic example is the potential privacy violation following from the mass surveillance activities of secret services. As those services usually remain silent about their practices, victims are often unaware of the fact that they might be affected by these practices. Normally, people who cannot substantiate their claim that they have been harmed by a certain practice will not be able to successfully submit a complaint. However, the European Court of Human Rights has stressed that it will make an exception in these types of cases because it will not accept that the mere fact that someone is kept unaware of his or her victim-status will result their remaining powerless to challenge those practices and policies. It has stressed that if people fit a category specifically mentioned in a law or policy or if people engage in certain activities which give them reason to believe that they might be subjected to surveillance activities, this might be enough to accept their victim status (Van der

Sloot 2016a). Besides hypothetical harm, increasing attention is being paid to future harm. This again may be divided into two lines of thought: the one focusing on potential future harm and the other focusing on harm following from self-restraint, also known as the chilling effect. The first category focuses on the possibility that certain harm might occur in the future. Although data, power or techniques may not be abused right now, for example, they may be abused in the future, especially if there are insufficient safeguards. Ultimately, the Second World War hypothesis is applied: imagine that a Nazi-like regime were to seize power; would it not, so the argument goes, be rather simple for such a regime to execute its evil policies if it had access to all the data gathered and stored right now, including racial data? The same argument may be applied to companies such as Facebook and Google, who may do no evil right now but might do so in the future, if their owners or board members change.

There is also increasing attention being paid to future harm in the legal domain, for example, in the proposed General Data Protection Regulation. This will presumably contain rules on privacy impact assessments, which specify that where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. This is so when data controllers process privacy-sensitive data. The idea of privacy impact assessments has been borrowed from the domain of environmental law, where such assessments have already been introduced. Such impact assessments may pertain to potential future harm on an individual level or on a societal level and on legal, social or ethical consequences alike.

There is a slight difference with regard to the type of harm that is at the heart of these types of assessments. The Second World War argument stresses that, although there may be no reason now to believe that harm may take place or that power has been abused, you never know for sure. Impact assessments, by contrast, focus on the type of harm that is reasonably foreseeable but ignores the unknown unknowns.

Second, future harm might lie in self-restricting behaviour, that is, when people know that they might be surveilled and possibly punished for their behaviour or face other negative consequences. If people know that confidential information may fall into the hands of third parties, they may feel restrained to experiment freely as they know that they might be confronted with their 'mistakes' in the future. Obviously, this fear also underlies the introduction of the hotly debated right to be forgotten. What proponents of this doctrine argue is that children and adolescents may want to experiment freely in life with hairstyles, alcohol or sex, without them being haunted for the rest of their lives by a certain Facebook tag,

Instagram photo or Youtube video. Not only would this limit their future social, societal and financial perspectives, but they might also choose not to experiment altogether if they know that it is impossible to keep those experiments secret.

This is known in legal terms as the chilling effect, which is also increasingly accepted by the European Court of Human Rights as regards data processing. 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 privacy as it enabled a public prosecutor to conduct random searches of people in a large area over an extensive period without this mandate being subject to any judicial review. The government, on the contrary, argued that the designation of a security-risk area or the issuing of a stop-and-search order had not in itself constituted an interference with the applicant's private life or liberty of movement. After the event the applicant complained of, several preventive search operations had been conducted, and 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 being a 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" (Colon v. Netherlands § 60).

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" (Colon v. Netherlands § 61).

Consequently, the Court accepted that the chilling effect in itself may be enough to meet the victim requirement under the Convention. No concrete harm is required in those instances.

7.8 ABSTRACT TESTS

There is a fourth and final branch of privacy theories that proposes to leave the focus on harm altogether. Scholars have increasingly proposed to move away from classic liberal theories focusing on (individual) harm, because to stay within this paradigm, theories are stretching the notion of harm to the point where it becomes forced and far-fetched. A Second World War scenario is perhaps the most poignant target of such critiques, but the focus on hypothetical and future harm serves the point all the same. The problem with Big Data programmes appears to be not individuals and their interests, but the fact that companies, states or even individuals have certain powers, have access to certain techniques, are in possession of certain types of data, as such. The fourth branch of theories, therefore, suggests not to focus on the 'patient' – the individual being acted upon and potentially violated in his or her privacy – but on the 'agent', the one acting upon the individual and potentially violating his or her privacy.

These types of theories are called agent-based theories. They focus on the behaviour and the character of agents and evaluate them on the basis of either legal or ethical principles. Theories that have been proposed focus, for example, on the existence of power rather than its abuse (real or potential), on the possession of certain data rather than its link to specific individuals, and on the access to certain techniques rather than their actual use or application.

First, with regard to abuse of power, it should be noted that there are certain doctrines in the legal realm that seek to prevent such abuse. Article 18 ECHR, for example, 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." This is a restriction on abuse of power by states. The curious thing, however, is that the European Court of Human Rights has said that this doctrine can only be invoked by an individual claimant if he or she is curtailed in exercising one or more of his or her individual rights, such as the right to privacy or freedom of expression. The article cannot, however, be invoked independently, to address abuse of power that has had no direct impact on specific individual rights.

It is interesting to see that the Court has made one prominent exception to its strict focus on individual rights and interests: cases that revolve around mass surveillance activities by governmental institutions (see more in detail Van der Sloot 2016a). In such cases, the Court accepts *in abstracto* claims, which revolve around the conduct of states as such, without any harm needing to be demonstrated. Consequently, not only individuals, but also legal persons and civil society organizations may submit a complaint. Because there is no individual harm, the Court cannot determine the outcome of the case by balancing the different interests

involved. Rather, it determines whether the surveillance activity was prescribed by law. As these activities are often prescribed by law, the Court has introduced an additional requirement, namely that the law must provide for sufficient safeguards against abuse of power. These safeguards may entail rules on transparency and oversight by either a judge, parliament or an oversight committee. States can be held in violation of the ECHR not only if they have abused their powers, negatively impacting individuals, but also if they have insufficient safeguards in place to prevent such abuse.

In a similar vein, it has been argued that not only the possession of power as such requires certain safeguards, but also the possession of certain types of data. Currently, legal instruments in principle only provide protection to private, privacy-sensitive and personal data: these types of data have a direct link to individuals and can be used to directly affect them. Sensitive data, such as relating to health and sexual or political preferences, are protected to a greater extent because they can be used in a way that has an even greater impact on the individual (Article 8 DPD). In the current technological environment, however, the direct connection of data to an individual is becoming less evident. Data increasingly have a circular life cycle: they may begin as individual data, then be linked to other data so they become sensitive data, then be aggregated and anonymized in a group profile and then a specific individual may finally be linked to the group profile. Consequently, the status of the data and the question of whether they can be linked to an individual at one specific moment is becoming less important. More important is the quality of the data as such, without them necessarily being linked to specific individuals. It has been suggested, therefore, that the sensitivity of the data or dataset itself should be the main determinant for data regulation (Van der Sloot 2015a: footnote 114).

Finally, a similar argument has been made with regard to technology. It has been argued, for example, that it is not so important how a specific technology is used in practice, but rather the capacity of the technology itself. Such theories argue that the core question should be:

> "whether an investigative technique or technology has the capacity to facilitate broad programs of indiscriminate surveillance that raise the specter of a surveillance state if deployment and use of that technology is left to the unfettered discretion of government. We think that the Fourth Amendment and the privacy issues at stake, as we have described them here, suggest taking a different tack. There are a number of ways that the Fourth Amendment status of a surveillance technique or technology could be determined. The most obvious would be for anyone who knows that he or she has been subject to surveillance by a novel technology, or dramatically improved existing technology, to file a civil suit seeking equitable relief or even damages. In such an action, a court would first need to determine whether the technology at issue should be subject to Fourth Amendment regulation. Among the important factors that a court would need to consider are: (1) the inherent scope of a technology's surveillance capabilities, be they narrow or broad; (2) the technology's scale and scalability; and (3) the costs associated with deploying and using the technology. If a court finds that a challenged technology is capable of broad and indiscriminate surveillance by its nature, or is sufficiently inexpensive

> and scalable so as to present no practical barrier against its broad and indiscriminate use, then granting law enforcement unfettered access to that technology would violate reasonable expectations of quantitative privacy" (Gray and Citron 2013: 101-102).

Following this line of thinking, access to the technology and the scope and reach of the technology or technical infrastructure become the main points for a regulatory approach.

Two theories have been put forward that try to give such privacy theories an ethical foundation: the republican theory and the virtue ethical theory. Both are agent-based theories that focus on the capacities or the character of the agent as such. Republicanism, in contrast to liberalism, does not view matters as problematic if they affect a specific individual, but it does if an agent possesses power without there being sufficient checks and balances. Roberts, for example, notes that:

> "republicans are concerned about interference, but not interference per se. Concern is reserved for others' capacity to interfere in an agent's choices on an arbitrary basis. The individual who suffers such interference is at the mercy of the agent or agency that has power to interfere. But while such interference will always constitute domination – to a greater or lesser extent, depending on the nature of the interference – a person need not interfere with another's choices in order to exercise dominating control. If an agent or agency has the power to interfere arbitrarily in an individual's choices, freedom is diminished even if the power is never exercised" (Roberts 2014: 6).

What is at the core here is the idea that others should never have the capacity to interfere arbitrarily in another person's choices. This is wrong even without power being actually abused. Virtue theory also proposes to evaluate the ethical conduct of agents such as states, but it goes a step further. It not only stresses that states should not abuse their powers and have sufficient safeguards in place against abuse, but it also provides that states must use their powers in such a way that the lives of citizens are facilitated in their potential to grow on a personal, social or professional level. There is not only a negative obligation to abstain from harming individuals or a positive obligation to prevent harm, but also a positive obligation to help individuals to flourish to an optimum extent (Van der Sloot 2014c).

It should come as no surprise that ethical theories have gained in prominence, given the fact that there is increasing doubt whether legal rules as such, or at least black letter law, could effectively regulate Big Data. Ethical codes, codes of conduct, self-regulation and soft law are more and more proposed as viable alternatives. As has been stressed, many of the problems following from Big Data processes concern general, systemic and societal issues, larger trends that impact society as a whole and potentially have an impact on future generations. These matters are a combination of legal and ethical concerns, and it often proves to be difficult to capture those concerns in legal rules because these questions belong to the political rather than the legal realm.

This ties up with the fact that the enforcement of legal rules is becoming increasingly difficult, because it is increasingly difficult to pinpoint which types of data should be regulated, because it is difficult in Big Data processes to determine who is responsible for what types of data processing activities, because of the territoriality principle, which is difficult to uphold, etc. As the data processing domain is increasingly transnationalizing, this brings with it that different types of norms are endorsed: privacy norms differ largely between different regions and continents. This is why many scholars and privacy advocates have promoted non-legal solutions and codes of conducts, focusing on agreement over underlying ethical principles rather than hard legal rules.

7.9 ANALYSIS

This chapter has argued that the original privacy paradigm focused only partially on the individual, his or her interests and the subjective rights of natural persons. The current privacy paradigm, however, focuses almost exclusively on protecting individual interests; it grants subjective rights to individuals, and the outcome of cases is determined by balancing the individual with the societal interest at stake. This paradigm is wavering because Big Data processes do not revolve around individuals but affect large groups and potentially society as a whole. It is increasingly difficult to link the effects of such processes back to individual interests; it is increasingly difficult for individuals to claim their subjective right in a world where data processing is so endemic; and the balance of interests is difficult to maintain because both the individual and the societal interests at stake are increasingly difficult to capture. This chapter has subsequently discussed several theories that try to find a solution for the discrepancy between the legal domain, which focuses on the individual, and technical reality, which focuses on general and systemic data collection and processing. These have been loosely divided into four categories.

Those theories focusing on the constitutive nature of privacy argue that confidentiality is a necessary precondition for certain societal institutions, such as the medical sector, the legal professions and (investigative) journalism. Those focusing on group and social or societal interests try to reformulate the right to privacy and raise it to a higher level, that is, to an aggregated, a group or a societal level. There are also theories that focus on hypothetical harm, i.e. situations in which people may have been harmed by a certain practice but are unsure of it, on potential future harm, which may be prevented and forestalled through impact assessments, and on chilling effects, the idea that people will restrain their behaviour beforehand if they know that they might be watched or controlled. Finally, there are theories that do not focus on citizens or the person affected by Big Data processes, but on the agent or the one executing the Big Data process. The question is

simply whether the agent has power, has access to certain data or is in the position to use certain techniques. If so, certain rules and conditions, checks and balances should be installed.

Each of these theories has appealing facets, but they also have specific downsides. With theories focusing on the constitutionality of privacy towards societal institutions, the downside is twofold. First, the value of privacy is primarily explained in relation to the value of societal institutions, and the value of privacy itself is moved into the background. Second, these theories do not focus on privacy as such but rather on confidentiality. There is an obvious overlap between the two concepts, but privacy is far wider than the mere right to keep things secret.

Theories focusing on group rights and societal interests run into a number of practical problems in terms of granting rights: who should protect the interests at stake and invoke, for example, a group right to privacy? This is problematic because a group formed through group profiles is generally unstable; the group is mostly unaware of the very fact that it is a group; there is no hierarchy or leadership nor a legal representative of the group; and there is no way to determine what is in the interest of the group, as the interests may differ from group member to group member.

Theories focusing on hypothetical and potential future harm have the problem that they tend to become too hypothetical, unrealistic and far-fetched; particularly the Second World War scenario faces this criticism. However, also the chilling effect and future and hypothetical harm are in a way forced attempts to stay within the liberal paradigm, focusing on (individual) harm, while the strength of this approach is waning. In agent-based theories, finally, the concept of privacy is moved into the background and is replaced by a focus on power and safeguards against abuse. It runs the risk, therefore, of no longer being a privacy theory.

Still, the latter type of theories may provide the most fruitful ground for future privacy regulation. In agent-based theories, the focus is no longer on concrete individual interests, but on the general interest of being protected against abuse of power and on the positive obligation of states to use their power to facilitate human flourishing. No balancing of interests takes place, but an intrinsic assessment is applied to evaluate the behaviour, power and actions of states, companies or even citizens, and this requires checks and balances to be in place against abuse of power. An intrinsic assessment could address many of the current privacy and data protection issues, without having to link them back to individual interests. Under an agent-based privacy paradigm, there is no need to attribute privacy claims to natural persons; rather, it facilitates claims in the general interest (class actions) and *in abstracto* claims. This model has the further advantage of lending itself to non-legal forms of regulation, such as codes of conduct.

It should be stressed that agent-based theories do not require a totally new approach to privacy; rather they resemble in many ways the original privacy paradigm as designed by the authors of the European Convention on Human Rights. It should also be pointed out that the European Court of Human Rights is already willing to relax its focus on individual rights and individual harm when exceptional circumstances apply; in such circumstances, it takes into account chilling effects, future harm, hypothetical harm and *in abstracto* claims. Whether the current paradigm still stands and marginal exceptions are made or whether it is slowly developing into its third phase is still unsure.

What is important, however, is that there are leads in European jurisprudence for national regulators to develop an alternative privacy paradigm that is based on an agent-based instead of a patient-based approach (Van der Sloot 2016a). Obviously, this 'new' or alternative paradigm would need to co-exist with the current paradigm. The current paradigm is very suitable for tackling traditional privacy violations targeting individuals or small groups. The new or alternative paradigm should be installed next to the current paradigm in order to be able to tackle the new privacy challenges following from new technological realities, especially in connection with Big Data.

It has several benefits to let go of the victim requirement, of the notion of harm and of the focus on personal interests. Regulation is now primarily concerned with two phases in which a link with the individual and his or her interests can be made. The first phase is the gathering and storage of personal data. There are numerous data protection rules linked to this moment, for example, the data minimalization principle, the requirement that the data should be correct and up to date, the requirement of a fair and legitimate processing ground and, derived from that, the purpose limitation principle; furthermore, there are rules on storing data safely and confidentially and the obligation to inform data subjects of their data being processed. The second phase is when profiles and correlations drawn from the data analysis process are applied in practice and have an effect on individual citizens. There are rules on automatic decision-making, on fair and non-discriminatory treatment and specific rules regarding redlining, bank loans and health insurance. This approach has three disadvantages that an agent-based approach may tackle:

1. The material demarcation of the right to privacy and data protection is linked to personal interests, namely when private, privacy-sensitive or personal data are processed. However, increasing use is made of metadata, group data and aggregated data; in principle, these types of data fall outside the scope of privacy and data protection laws because they do not identify a particular individual. Still, they can be used to significantly affect a person's life, and even metadata can give a detailed picture of someone's life. Aggregated and non-personal data may also be linked to other data and datasets at a later stage and thus

become personal or even sensitive data. This focus on personal data, consequently, is no longer working in Big Data processes. Letting go of the focus on the individual, an agent-based approach could shift the focus from the question whether data identify a certain person to the question whether possession of data gives an entity a certain type of power. This would allow the inclusion of non-personal data, metadata and group data alike.

2. As has already been stressed several times in this chapter, the focus of current regulations is primarily on effects on the individual, whereas Big Data processes often have an effect on society as such and on societal institutions. An agent-based approach to privacy regulation would take into account these broader and more abstract interests as well.
3. The current regulations focus on the moment when personal data are gathered and the moment when the use of data processing has an effect on concrete individuals. The phase in between, however, when data are analyzed and aggregated, and when algorithms search for patterns and statistical correlations are signalled, is mostly left out of the equation, partly because the individual element and interest is mostly absent from this phase. Data analysis tends to revolve around large quantities of aggregated data, and the group profiles gathered usually depend on characteristics that apply to many persons, for example, 'people using felt under their chair legs are more prone to paying their debts than those who do not', and the statistical correlations usually use categories with a high *n*. This phase, however, is becoming increasingly important because, in reality, this is where the most substantial decisions are made and conclusions are drawn. An agent-based approach to privacy regulation could install a number of rules, such as on the transparency of the process, rules on which algorithms may be used, how datasets may be integrated, what kind of methodology is used for the research, etc.

There are also some other, more practical advantages of the agent-based approach:

4. An agent-based approach could focus on ethical choices that are made by agents as such, without actual, hypothetical or future individual harm needing to be in play. Referring to the previous point, if a bank chooses to use a profile based on race, whether directly or indirectly through redlining, this could be addressed as such because it is an ethically wrong decision and a wrong way to use power. Similarly, if the police primarily gather data around neighbourhoods with a high number of immigrants, it would be wrong for them to draw general conclusions from this data because it is biased. An agent-based theory may also include positive rules on the use of power: that it should be used in a way that promotes the human flourishing of citizens.
5. Currently, citizens are often unaware of the very fact that their data are gathered; it is virtually impossible for ordinary citizens to assess all data-processing initiatives, to check whether they contain any of their personal data, whether the processing of personal data is conducted fairly and legitimately and, if not,

to go to court and find redress; it may be difficult to substantiate individual harm. An agent-based privacy approach would allow for class actions on behalf of specific individuals, groups or society as a whole.

6. Currently, there is a problem in the enforcement of legal instruments that mostly consist of hard rules and black letter law. This has three disadvantages: First, these types of rules tend to become more outdated more quickly than general duties of care. Second, black letter laws can be circumvented more easily because their scope and definition is often more precise than soft law rules. Third, there are enormous differences between black letter laws in different countries and continents, and companies can locate their headquarters in places with the least regulatory burden. The agent-based approach to privacy regulation would allow for an additional focus on soft law, general ethical rules and general duties of care.

REFERENCES

Allen, A.L. (2011) *Unpopular Privacy: What Must We Hide*, Oxford: Oxford University Press.

Andrejevic, M. (2014) 'The Big Data Divide', *International Journal of Communication* 8.

Benn, S.I. (1984) 'Privacy, Freedom, and Respect for Persons', pp. 223-244 in F. Schoeman (ed.) *Philosophical Dimensions of Privacy: an Anthology*, Cambridge: Cambridge University Press.

Bentham, J. (1971) *Panopticon; or the Inspection-House*, Dublin.

Bollier, D. (2010) 'The Promise and Peril of Big Data', available at: www.emc.com/collateral/analyst-reports/10334-ar-promise-peril-of-big-data.pdf.

Boyd, D. and K. Crawford (2011) 'Six Provocations for Big Data', available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1926431.

Busch, L. (2014) 'A Dozen Ways to Get Lost in Translation: Inherent Challenges in Large Scale Data Sets', *International Journal of Communication* 8.

Craig T. and M.E. Ludloff (2011) *Privacy and Big Data: The Players, Regulators and Stakeholders*, Sebastopol: O'Reilly Media.

Crawford, K. and J. Schultz (2014) 'Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms', *Boston College Law Review* 55, 93.

Custers, B. et al. (eds.) (2013) *Discrimination and Privacy in the Information Society: Effects of Data Mining and Profiling Large Databases*, Berlin: Springer.

Davis, D. and D. Patterson (2012) 'Ethics of Big Data: Balancing Risk and Innovation', available at: www.commit-nl.nl/sites/default/files/Ethics%20of%20Big%20Data_0.pdf.

Dijk, P. van, F. van Hoof, A. van Rijk and L. Zwaak (eds.) (2006) 'Theory and Practice of the European Convention on Human Rights',pp. 50 in *Intersentia*, Antwerpen.

Driscoll, K. and S. Walker (2014) 'Working Within a Black Box: Transparency in the Collection and Production of Big Twitter Data', *International Journal of Communication* 8.

Dusseault, P.-L. (2013) 'Privacy and Social Media in the Age of Big Data: Report of the Standing Committee on Access to Information, Privacy and Ethics', available at: www.parl.gc.ca/content/hoc/Committee/411/ETHI/Reports/RP6094136/ethirp05/ethirp05-e.pdf.

Fairfield, J. and C. Engel (2014) *Privacy as Public Good*, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2418445.

Feinberg, J. (1984) *Harm to Others*, New York: Oxford University Press.

Fletcher, G. P. (1979) 'Privacy as Legality', in *Liberty and the Rule of Law*, College Station, Texas A&M University Press.

Foucault, M. (1975) *Surveiller et punir: naissance de la prison*, Paris: Gallimard.

Galetta, A. and P. 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.

Gavison, R. (1980) 'Privacy and the Limits of Law', *Yale Law Journal* 89.

Goffman, E. (1959) *The Presentation of Self in Everyday Life*, Garden City: Doubleday and Company.

Gray, D. and D. Citron (2013) 'The Right to Quantitative Privacy', *Minnesota Law Review* 98, 62.

Habermas, J. (1994) 'Über den internen Zusammenhang zwischen Rechtsstaat und Demokratie' in U.K. Preuß (ed.) *Zum Begriff der Verfassung, Die Ordnung des Politischen*, Frankfurt am Main.

Hirsch, D. (2014) 'The Glass House Effect: Big Data, The New Oil and The Power of Analogy', *Maine Law Review* 66: 373-396.

Hoofnagle, C.J. (2013) 'How the Fair Credit Reporting Act Regulates Big Data', available at: 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 May, Skopje.

Kitchin, R. (2014) *The Data Revolution: Big Data, Data Infrastructures and Their Consequences*, Los Angeles: Sage.

Kuneva, M. (2009) 'Keynote Speech, Roundtable on Online Data Collection, Targeting and Profiling', available at: http://europa.eu/rapid/press-release_SPEECH-09-156_en.htm.

Lever, A. (2015) 'Privacy and Democracy: What the Secret Ballot Reveals', *Law, Culture and Humanities* 11, 2.

McAfee, A. and E. 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* October.

Mill, J.S. (1989) *On Liberty' and Other Writings*, Cambridge: Cambridge University Press.

Mayer-Schönberger, V. and K. Cukier (2013) *Big Data: A Revolution That Will Transform How We Live, Work and Think*, Boston: Houghton Mifflin Harcourt.

Pariser, E. (2012) *The Filter Bubble: What the Internet Is Hiding From You*, London: Penguin Books.

Payton, T.M. and T. Claypoole (2014) *Privacy in the Age of Big Data: Recognizing Threats, Defending Your Rights, and Protecting Your Family*, Plymouth: Rowman and Littlefield.

Ovey, C and R.C.A White (2002) *The European Convention on Human Rights*, Oxford: Oxford University Press.

Richards, N.M. (2013) 'The Dangers of Surveillance', *Harvard Law Review*, available at: http://harvardlawreview.org/2013/05/the-dangers-of-surveillance/.

Richards, N.M. and J.H. King (2014a) 'Three Paradoxes of Big Data', *66 Stanford Law Review* online 44.

Richards, N.M. and J.H. King (2014b) 'Big Data Ethics', *Wake Forest Law Review* 49.

Puschmann, C. and J. Burgess (2014) 'Metaphors of Big Data', *International Journal of Communication* 8.

Regan, P.M. (1995) *Legislating Privacy: Technology, Social Values and Public Policy*, Chapel Hill: University of North Carolina Press.

Roberts, A. (2014) 'A Republican Account of the Value of Privacy', *European Journal of Political Theory* 14, 3: 320-344.

Robertson, G. (ed.) (1985) *Collected Edition of the 'Travaux Préparatoires' of the European Convention on Human Rights/Council of Europe = Recueil des travaux préparatoires de la Convention européenne des droits de l'homme / Conseil de l'Europe*, The Hague: Martinus Nijhoff.

Roessler, B. (2005) *The Value of Privacy*, Cambridge: Polity.

Roessler, B. and D. Mokrosinska (2013) 'Privacy and Social Interaction', *Philosophy Social Criticism* 39, 8.

Roessler, B. and D. Mokrosinska (eds.) (2015) 'Social Dimensions of Privacy: Interdisciplinary Perspectives', Cambridge: Cambridge University Press.

Rubinstein, I. (2012) *Big Data: The End of Privacy or a New Beginning?*, NYU School of Law, Public Law Research Paper 12-56.

Simitis, S. (1987) 'Reviewing Privacy in an Information Society', *University of Pennsylvania Law Review* 135, 3.

Sloot, B. van der (2014a) *Privacy in the Post-NSA Era: Time for a Fundamental Revision?*, JIPITEC, 1.

Sloot, B. van der (2014b) 'Do Data Protection Rules Protect the Individual and Should They? An Assessment of the Proposed General Data Protection Regulation', *International Data Privacy Law*, 4.

Sloot, B. van der (2014c) 'Privacy as Human Flourishing: Could a Shift towards Virtue Ethics Strengthen Privacy Protection in the Age of Big Data?', *JIPITEC* 3.

Sloot, B. van der (2015a) 'Do Privacy and Data Protection Rules Apply to Legal Persons and Should They? A Proposal for a Two-Tiered System', *Computer Law and Security Review* 1.

Sloot, B. van der (2015b) 'How to Assess Privacy Violations in the Age Of Big Data? Analysing the Three Different Tests Developed by the ECtHR and Adding for a Fourth One', *Information and Communication Technology Law* 1.

Sloot, B. van der (2015c) 'Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interests Might Prove Indispensable in the Age of 'Big Data'', *Utrecht Journal of International and European Law* 80.

Sloot, B. van der (2016a) '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' in S. Gutwirth et al. (eds.) *Data Protection on the Move, Law, Governance and Technology*, Series 24.

Sloot, B. van der (2016b) 'Privacy as Virtue: Searching for a New Privacy Paradigm in the Age of Big Data' in *Passau Conference book* (forthcoming).
Solove, D. (2008) *Understanding Privacy*, Cambridge: Harvard University Press.
Stevenson, D.D. and N.J. Wagoner (2014) 'Bargaining in the Shadow of Big Data', *Florida Law Review* 66, 5.
Taylor, L.L. Floridi and B. van der Sloot (eds.) (2016) *Group Privacy*, Springer (forthcoming).
Tene, O. and J. Polonetsky (2013) 'Big Data for All: Privacy and User Control in the Age of Analytics', *Northwestern Journal of Technology and Intellectual Property* 11, 5: 239-273.
Thatcher, J. (2014) 'Big Data, Big Questions. Living on Fumes: Digital Footprints, Data Fumes, and the Limitations of Spatial Big Data', *International Journal of Communication* 8: 1765-1783.
Tomlinson, H. (2012) 'Positive Obligations under the European Convention on Human Rights', available at: http://bit.ly/17U9TDa.

Legal documents and case law

Charter of Fundamental Rights of the European Union (2000/C 364/01).
Convention for the Protection of Human Rights and Fundamental Freedoms, Rome, 4.XI. 1950.
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, *Official Journal L 281 , 23/11/1995 P. 0031-0050*.
ECmHR, Glass v. The United Kingdom, Application no. 28485/95, 16 October 1996.
ECmHR, Tauira and Others v. France, Application no. 28204/95, 4 December 1995.
ECmHR, Trouche v. France, Application no. 19867/92, 1 September 1993.
ECmHR, X. v. Iceland, Application no. 6825/74, 18 May 1976.
ECtHR, Asselbourg and 78 Others and Greenpeace Association-Luxembourg v. Luxembourg, application no. 29121/95, 29 June 1999.
ECtHR, Colon v. The Netherlands, Application no. 49458/06, 15 May 2012.
ECtHR, Lawlor v. the United Kingdom, Application no. 12763/87, 14 July 1988.
ECtHR, Murray v. The United Kingdom, Application no. 14310/88, 10 December 1991.
General Data Protection Regulation, available at: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.