Accountability for the Use of Algorithms in a Big Data Environment

Anton Vedder and Laurens Naudts, KU Leuven Center for IT and IP Law

Accountability is the ability to provide good reasons in order to explain and to justify actions, decisions, and policies for a (hypothetical) forum of persons or organizations. Since decision-makers, both in the private and in the public sphere, increasingly rely on algorithms operating on Big Data for their decision-making, special mechanisms of accountability concerning the making and deployment of algorithms in that setting become gradually more urgent. In the upcoming General Data Protection Regulation, the importance of accountability and closely related concepts, such as transparency, as guiding protection principles, is emphasized. Yet, the accountability mechanisms inherent in the regulation cannot be appropriately applied to algorithms operating on Big Data and their societal impact. First, algorithms are complex. Second, algorithms often operate on a random group-level, which may pose additional difficulties when interpreting and articulating the risks of algorithmic decision-making processes. In light of the possible significance of the impact on human beings, the complexities and the broader scope of algorithms in a big data setting call for accountability mechanisms that transcend the mechanisms that are now inherent in the regulation.

Keywords: algorithms, accountability, privacy, data protection, non-discrimination

1. Introduction

Algorithms have been defined as finite, abstract, effective, compound control structures, imperatively given and accomplishing a given purpose under given provisions (Hill, 2016), or even more concisely, as encoded procedures through which input data is being transformed into a usable, and therefore desired, output (Gillespie 2012). Within the information society, algorithms perform a key function: by following a logical and mathematical sequence, algorithms can structure and find additional meaning in a Big Data environment. Although no single definition of Big Data exists, we agree with the definition posited by boyd and Crawford who refer to Big Data as the cultural, technological and scholarly phenomenon, in which technology is used to aggregate, analyse, link and compare large data sets with the aim of identifying patterns to make economic, social, technical and legal claims (boyd and Crawford 2012). Whereas Big Data symbolizes the challenges raised by the explosive growth of data, algorithms, for instance, in the form of data mining techniques, represent their solution. Algorithms embody the techniques and software that are to be deployed if we wish to make sense of the data that is continuously being collected and produced, both offline and online (Colonna 2013, 330). In combination with data, they provide us with the knowledge we desire and the knowledge that we do not yet desire because we simply do not even have a clue before the algorithms do their work.

Algorithms are already omnipresent: They serve a broad variety of purposes, in an equally broad variety of contexts, ranging from seemingly innocent kitchen-sink applications to highly critical societal endeavours. They can offer, for instance, personalised shopping advice or suggestions to improve one's lifestyle; but they can also be deployed to determine potential job offers and positions, creditability, or being a suspect for the police or criminal investigations authorities. Even when algorithms are delegated daily tasks or processes, their deployment can impact the things, individuals and processes they interact with (Wilson 2016, 3). In their performance of daily chores, for instance, they can provide the corporations that exploit them with information about the persons for whom the chores are performed. Many authors claim that algorithms impact identities, and as a consequence, opportunities granted in life, in various unobtrusive ways. The analytics within Big Data environments may thus cause a "fundamental

shift in our understanding of ourselves and our individual, social, cultural and political life" (Nerurkar et al. 2016, 3).

Algorithms are powerful procedures. Consequently, there is a growing need to evaluate the claims, decisions, actions, and policies that are being made on the basis of them. This evaluation requires gauging the reasons for an algorithmic decision, its components, and the weight assigned to them. The assessment of algorithms is becoming increasingly difficult, however. As we will explain in the subsequent section, algorithms are complex. They seem to function behind an impermeable veil, not allowing of attempts to analyse the decision-making process and its outcomes. Algorithms are often perceived as a black box, and the environment they populate as a 'black box society' (*Pasquale* 2015).

Ever since the large-scale introduction of personal computers and information technology, there has been a tendency to consider the social impact of data to fall within the scope of privacy and data protection laws and regulation. In Europe, data protection laws and regulations and – especially – the new General Data Protection Regulation (hereafter referred to as GDPR or "Regulation") [1], emphasize the accountabilities of data controllers. As we will explain in section 4, in many cases these accountability mechanisms cannot be meaningfully applied to data processing with the help of algorithms in a Big Data context. What form is this accountability to take when highly complicated algorithms are used and when the outcomes sometimes refer to other or more people than those involved in the input data? In this paper, we cannot answer this question in any detail yet. After a careful analysis of the specific complexities of algorithms in a Big Data context and of the accountability mechanisms explicitly and implicitly present in the GDPR we will, however, be able to come up at least with rudimentary contours of starting points for such an answer. In doing so, we try to stay close to the conceptual and normative basic assumptions of the Regulation. In particular, we try to cling to its predominant tendency not to close off useful options for the use of (personal) data from the outset, but to enable meaningful use in a responsible way with the help of accountability mechanisms.

In this paper, we will concentrate on algorithms that process or produce data and information directly or indirectly referring to persons, either as individuals or groups. This does not at all mean that we assume that only those algorithms can have ethically relevant consequences. We strongly believe that the use of algorithms in Big Data contexts using and producing merely data or information about non-human entities, such as seeds, foods, medicine, meteorological circumstances et cetera can bring about important transformations in societies, cultures and societal practices, which in turn might affect the lives of humans significantly. Although we think that much of what we will say about algorithmic accountability also applies to algorithms used on data about things, focussing on the direct or indirect use of personal data enables us to make our points with regard to algorithmic accountability all the more clearly.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Hereafter referred to as GDPR. Accessed 28 July 2016 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

2. The Complexity of Algorithms in a Big Data Context

Providing an account of an automated decision and assessing its social desirability will include an explanation and justification of the various elements that may have influenced the algorithmic outcome, and ultimately, the algorithmic decision. One of these elements can be the bias of an algorithm's designer. As Wilson (2016, 3) noted, algorithms are human constructs and therefore the algorithmic process will almost necessarily assume, perhaps unwillingly, certain values. Whilst it is true that algorithms are often value-laden due to design choices, the desirability of algorithmic decisions can often not be assessed through the evaluation of these choices alone. The assessment of algorithmic decision-making is also difficult due to their complex nature. Algorithms are complex in at least two ways: technically and contextually. These complexities are related to the nature of algorithms as such, i.e. mathematical constructions operating within a given context, of which the human factor of the possible bias of the designer is only one type of element to be taken in consideration.

Technical Complexity

Algorithms are encoded by a programmer in an algorithmic language before being translated into a machine-readable binary sequence. Algorithmic language is a language that is especially designed to express mathematical or symbolic computations and thus to express algebraic operations in a notation, reminiscent of logic and related to mathematics.[2] In order to understand an algorithm, and in order to assess its decision-making capabilities, expert knowledge of the mathematical or system language used to build the algorithm is thus required. The general public to be affected by the algorithm will mostly not be in possession of this knowledge. Even computer experts, however, might have difficulty in understanding the algorithm's actual behaviour in a Big Data setting although a computer system's source code might be legible for them (Kroll et al, 2017, 6). Regardless of whether or not the language can be read, algorithms in a Big Data setting might still behave in unpredictable ways. Neither does the unpredictability depend on whether or not the algorithm as such is designed to be 'predictive' or 'descriptive'. Some algorithm's decision-making processes, for instance, rely – sometimes in an essential manner – on randomization techniques (Kroll et al 2017, 22-24). Randomization, however, can severely limit the predictability of outcomes. In addition, algorithms are not necessarily used individually. Rather, ensemble approaches, where multiple algorithms are applied to a data set, can be used in order to determine the best solution or explanation to make sense of a given data set in varying industrial applications, such as credit scoring or Netflix ranking (Seni and Elder 2010, 7; Siegel 2013, Kitchin 2014, 2).

The complexity of algorithms in a Big Data setting on a technical level is not restricted to the mathematical sequence. The technical context, in which the algorithms are ultimately deployed, is equally important. This complexity is of a structural nature. Algorithms do not operate in isolation, but perform functions as part of a larger structure. The primary constituents of a computer system are the underlying algorithms and data structures (Manovich 1999, 84). As such, algorithms are inert and without meaning; they need to be paired with databases (Gillespie 2012). Before algorithms can produce results, information must have been collected, prepared, i.e. formalized in a manner that the algorithm can act on it automatically, and sometimes excluded or demoted, by subtly removing information through other algorithmic equations (*Ib.*). Algorithmic accountability does not only require the examination of algorithms or the

[2] Encyclopedia Brittanica, *Computer Programming Language.* Accessed 28 July 2016. *https://www.britannica.com/technology/computer-programming-language.*

code as such but also an examination of how algorithms are deployed within different areas and what the tasks are that they perform (Kitchin, 2016). The potential interconnectedness of algorithms and of algorithmic decisions also seriously restricts the means of algorithmic decision-makers to give an account of the decisions they make. If, for instance, an algorithmic decision builds upon the decisions made by a previous algorithm, the individual accountable for the latter decision, might not be aware of the decision-making process of the former. Consequently, he will only be able to provide an account of the logic applied during the later decision-making stage, but not the one applied during the preceding processes that may have influenced or affected that later decision.

Complexity due to contextual dependence

The complexity of algorithms is not restricted to the purely technical realm. Part of their complexity also arises at what perhaps is best perceived as the intersections of the arithmetic or logic of algorithms on the one hand and their application to the real world of human beings on the other. Algorithms are contextual and relational as they perform tasks in collaboration with data, technologies, *and* people under varying conditions. Furthermore, the Big Data environment, in which algorithms are deployed, is in itself, relational and flexible.[3] (Kitchin 2013). Consequently, the effects of algorithms "unfold in contingent and relational ways, producing localised and situated outcomes," as Kitchen notes (Kitchin 2016, 12).

Algorithms can affect individuals (or groups of individuals) based on how the data suggest they might behave or should behave on the basis of patterns in the past, rather than based on the actual behaviour of the individuals (Ramirez 2013; Citron and Pasquale 2014; Zarsky 2014). Whereas the individual's perception is influenced by his experience, emotions and values, algorithms are generally considered to start from available data and, therefore, to provide "sheer facts and truths". Unfortunately, the widely shared view that "computer knows best" overlooks both the fact that data and algorithms may in many ways be biased or value-laden and the fact that algorithms always operate with a function that is itself value-driven, i.e. done for a purpose (although the outcomes are not always in conformity with that purpose). Put differently, algorithms are shaped by meanings and in turn construct new meaning (Roberge and Melancon 2016, 3; see also Ananny 2016, 10).

Take, for instance, random-group level operations. Random-group level operations are just one example of a type of complexities that is both due to the logic or technicality of algorithms and to their application to the real world, in this case of individuals and random groups of people. Algorithms search for patterns, correlations and commonalities hidden within large datasets (Fayyad, Piatetsky-Shapiro and Smyth 1996). Algorithms prioritise, associate, classify, and filter information (Diakopoulos 2016). The new information found can serve as an immediate differentiation ground between individuals and between groups of individuals. Algorithms, however, can group together individuals on a random-group level and find currently undefined strata of society based upon, yet to be discovered, shared commonalities found within large data sets. The groups that have been thus created, might not be easily definable, nor in reality easily recognizable, due to their seemingly random nature.

[3] According to Kitchin, Big Data is relational and flexible in nature, as a) Big Data contains common fields that "enable the conjoining of different data sets" and b) Big Data is both extensional and scalable, meaning new fields can be added easily, and the size of a dataset can expand rapidly (Kitchin, 2013).

Of course this already in itself makes it difficult to perceive the function of the algorithm and to predict its output and impact, but where random groups are involved, the *outcomes* can confront us with additional difficulties, since they will often be non-distributive. This means that they contain statements about *average* characteristics and patterns of behaviour or, in any case, about the individuals as members of the random group, rather than statements about the individuals in their own right. Both types of statements can be true, but they can be contradictory. Whereas a person may, as a member of a random group, run a statistically high risk of developing lung cancer, she may as an individual in her own right be the healthiest person on earth with a health prognosis for which many would envy her. Although both statements are true *in a way*, their meaning and function may be contraries. Their actual use will depend on the context and the perspective of the user. (Vedder 1999, 258). Grasping these outcomes will be difficult. As was already noted before, the commonalities of random groups are often not easily discernible. The groups can often only be identified by those who defined them for a specific purpose and not by the individuals affected by the statements. The latter might even consider the definition of the group as 'arbitrarily chosen' (*ib*.).

Finally, under the label of contextual dependence, we should perhaps also mention proprietary or ownership aspects. Computer systems are often not the product of a single individual, but are developed as part of a corporate culture, being produced by teams (Nissenbaum 1994, 75). Corporations and professionals within those corporations who develop the algorithms belong to the context of algorithms. Corporations will often want to keep those algorithms secret for commercial reasons. Burrell therefore ranks trade secrets among the main causes of opacity of algorithms, together with what he refers to as technical illiteracy, and opacity that arises from the characteristics of machine learning and the scale required to apply them usefully (Burrell 2016). Of course, ownership is different from the other factors of complication. It is not so much an intellectual difficulty, but rather an impediment for understanding. Without having access to the algorithm, or the context in which the algorithm is deployed, it is difficult to assess whether or not algorithmic decision-making is desirable in a given situation. Yet the decision to maintain algorithmic secrecy is, other than technical or contextual complexity, a man-made decision, and thus not inherent to the functioning of algorithms.

3. Accountability in Data Protection Legislation

Algorithms process data, sometimes personal data. Data protection legislations, therefore, seem to be appealing candidates for regulating the responsible deployment of algorithms especially where human beings are affected by the data involved. Data protection legislation often has a broad material scope. The EU Data Protection framework, for instance, will apply as soon as a) there is a processing activity, i.e. any operation or set of operations performed on data and b) the processing activity concerns personal data, i.e. any information relating to an identified or identifiable natural person.[4] Since algorithms operate on data sets and many algorithms function through the use of personal data, algorithmic decision-making easily enters the ambit of the EU data protection framework.[5] Algorithmic operations should respect the fundamental right to data protection and the deployment of algorithms should be in accordance with the fundamental

[4] Art. 4 (1) GDPR.
[5] Art. 4 (2) GDPR.

principles related to the protection of personal data, such as fairness, transparency and accountability. Accountability, and closely related concepts such as transparency, are becoming even more important as guiding protection principles in the upcoming European General Data Protection Regulation ('GDPR'). We have nonetheless some reservations concerning the sufficiency of these principles to safeguard the responsible deployment of algorithms.

Accountability has often been considered as an important privacy and data protection enhancing principle (Bennett 2014; Guagnin et al. 2014; Zimmermann and Cabinakova 2015). The GDPR's accountability principle reminds of the 1980 OECD privacy principles. These principles postulated accountability as a central privacy-enhancing principle stating that a data controller should be accountable for complying with measures, which give effect to the OECD's privacy principles (OECD 1980). The OECD principles remain relevant and have shaped subsequent privacy and data protection legislation. The principles appoint for instance the data controller as the responsible party for ensuring compliance. The controller shall also have the responsibility of complying with measures that give effect to data protection principles (Alhadeff, 2012). The Regulation imposes upon the data controller the obligation to "be responsible for, and be able to demonstrate compliance with the principles relating to processing of personal data.[6] Thus, within an algorithmic context, the data controller is to be held responsible and accountable for algorithmic decision-making.

The principle of accountability as such is only mentioned explicitly twice in the GDPR; yet the principle permeates throughout the Regulation. In 2010 the Article 29 Working Party (hereafter: WP29) favoured the introduction of accountability and stated that the expected results of accountability mechanisms would "include the implementation of internal measures and procedures putting into effect existing data protection principles, ensuring their effectiveness and the obligation to prove this should data protection authorities request it"(WP29 2010). The WP29 also provided an illustrative list of potential measures, including an internal review and assessment, setting up binding data protection policies which should be made available to data subjects, mapping data processing operations and maintaining an inventory thereof, the appointment by the controller of a data protection officer, providing training and education to staff, setting up procedures to manage the subjective rights of data subjects, the implementation and supervision of verification procedures, et cetera. In the current GDPR text, many of these 'accountability' measures have been introduced. According to the European Data Protection Supervisor (EDPS 2016), following the GDPR, accountability in personal data processing involves transparent internal policies, training employees, responsibility at the highest level for the monitoring of the implementation, assessment and demonstration to external parties of the implementation's quality and procedure for redressing poor compliance and data breaches (EDPS 2016). Other examples of accountability obligations considered by the EDPS are: obligations to keep processing documentation, to install data security measures, to make a data protection impact assessment and to provide for data protection by design and default.

[6] Art. 5 §2 GDPR. The principles relating to the processing of personal data and for which the data controller shall demonstrate compliance state that personal data shall be a) processed in a lawful fair and transparent manner; b) collected for specified explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; c) adequate, relevant and necessary to what is necessary in relation to the purposes for which they are processed; d) accurate and, where necessary, kept up to data; kept in a for which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed and f) processed in a manner that ensures appropriate security of the personal data (Art. 5 §1 GDPR).

Therefore, and even though the GDPR only refers explicitly to accountability when imposing the obligation on the controller, to *"be responsible for, and be able to demonstrate compliance with data quality principles",* other – rather implicit – accountability mechanisms have been put in place, which in principle could enhance responsibility with regard to algorithmic decisions. Although accountability is not often explicitly and expressly mentioned, the regulation therefore seems to acknowledge and assert the underlying principles and starting points latently in various ways. In the subsequent subsection, we will discuss some of the guises of accountability in the GDPR.

Self-Assessing Mechanisms of Accountability

The primary notion of accountability as mentioned above, clearly requires the data controller to put in place specific mechanisms of accountability: the controller will have to assess whether or not the intended processing activities are in accordance with the law. Since this is primarily a responsibility for the controller, the controller himself should ensure that regulatory compliance is achieved. One of the main reasons the controller has been attributed more responsibility concerning the implementation of accountability measures under the GDPR was to increase the trust of individuals in the protection of their personal data in a digital environment (European Commission 2012, 42). In addition, increased accountability measures could also be considered a cost-reducing mechanism for ex-post, regulatory supervision requirements (European Commission 2012, 109). Some of these self-assessing mechanisms existed already under previous data protection frameworks. Nevertheless, under the GDPR, they have been expanded.

The data controller should implement appropriate technical and organisational measures to ensure and to be able to demonstrate that the processing is performed in accordance with the GDPR.[7] In doing so, the controller shall take into account "the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons".[8] In this way, the GDPR encourages data protection by design and privacy by default, both at the time of determining the means for processing, as well as during the processing itself.[9] The Regulation for instance refers to pseudonymization as a data protection by design mechanism to ensure data minimisation.[10]

Article 30 requires the data controller to maintain a record of processing activities under its responsibilities.[11] In this record, the controller has to provide information on amongst others the name and contact details of the controller or joint controllers[12], the purposes of the processing activities[13], a description of the categories of data subjects and of the categories of

[7] Art. 24 §1 GDPR
[8] Ibid.
[9] Recital 78 GDPR and Art. 25 GDPR
[10] Art. 25 §1 GDPR
[11] Recital 82 GDPR and Art. 30 GDPR
[12] Art. 30 §1 (a) GDPR
[13] Art. 30 §1 (b) GDPR

personal data[14], the recipients of data disclosure and possible data transfers[15]. Finally, the data controller should install internal data protection policies, assign responsibilities, raise awareness and train staff.[16]

Another, and potentially stronger, accountability mechanism introduced by the GDPR, is the data protection impact assessment. A data controller is required to carry out an impact assessment of the intended processing operations on the protection of personal data where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons involved.[17] This applies in particular to the use of new technologies.[18] Such an assessment is specifically required in the case of a systematic and extensive evaluation of personal aspects of natural persons, which is based on automated processing, including profiling, and which is to serve as a basis for decisions that produce legal effects concerning the natural person or affect the natural person significantly in a similar manner.[19] This assessment must contain a systematic description of the intended processing activities, the purposes for the processing and the legitimate interest lying at its basis, the necessity and proportionality of the processing operations in relation to the purposes. An assessment of the necessity and proportionality of the processing operations in relation to the purposes and an assessment of the risks to the rights and freedoms of data subjects and the measures envisaged to address the risks of the processing activity, must also be included in the impact assessment.[20] The impact assessment is a form of accountability as it necessitates the data controller to make an analysis of the desirability of his actions and their impact in a high risk context.

The right not to be subject to automated decision-making

The right not to be subject to automated decision-making targets the involved individual directly.[21] Article 22 GDPR states that the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. Moreover, as it covers automated decision-making, it also covers algorithmic processing activities. Indeed, automated decisions have an algorithmic underpinning. Therefore, this subjective right might also be considered an eminent mechanism to address undesirable effects of algorithmic decision-making. The nature of this right is inherently limited however as it only relates to 'solely

[14] Art. 30 §1 (c) GDPR. The categories chosen by the data controller should be necessary in order to achieve the defined data processing purposes. Although no concrete definition of "category" is provided, the term seems to refer to the overall category to which the specific types of information of the data subject processed by the controller would belong. Categories could be 'name' or 'address'. The name and address of the data subject would then belong to these respective categories. The GDPR does refer to 'special categories of data'. These data reveal information concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetics, health, sex life, etc.

[15] Art. 30 §1 (d) GDPR

[16] Art. 24 and 39 GDPR

[17] Recitals 89, 90, 91, 92, 93, 94, 95 and 96 GDPR and Art. 35 GDPR

[18] Art. 35 §1 GDPR

[19] Recital 91 GDPR and Art 35 §3 (a) GDPR. A data protection impact assessment also has to be performed when a) processing activities take place on a large scale of special categories of data, e.g. personal data revealing racial or ethnic, political or religious beliefs or genetic information and b) there is a systematic monitoring of a publicly accessible area on a large scale.

[20] Art. 35 §7 (b) and (c) GDPR.

[21] Recital 71 GDPR and Art. 22 GDPR

automated' processes and not to algorithmic processes in general. In other words, once there is a human in the loop guiding the algorithm, the decision-making process might no longer be considered to be a 'solely' automated one. Furthermore, the article's wording suggests that it is not simply meant to serve as a safeguard for merely an individual's data protection; it also sees to other interests and rights. Regardless of whether personal data are adequately protected, if the automated process produces legal effects concerning the individual or significantly affects the individual, the right can be asserted. Further clarification on what a 'legal effect' or 'significant impact' on the individual could be, is missing. The GDPR considers an automatic refusal of an online credit application or e-recruiting practices without any human intervention as having a 'significant' impact on the individual,[22] but it remains unclear what other decision-making processes could be categorised as such.

Although not mentioned explicitly, the exercise of the right not to be subject depends upon strong accountability mechanisms towards the individual. The effective exercise of this right requires that the data subject is adequately informed, i.e. the data subject must receive an account of the automated decision, the underlying algorithmic processes and the ultimate impact of the decision. The right does not apply however, when the automated process is necessary for entering into, or performance of, a contract between the data subject and a data controller; authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or when the individual has given explicit consent for the automated decision.[23] In these cases, the GDPR stipulates that the data subject should be informed about the existence of the automated decision and should receive meaningful information about the logic involved, as well as the consequences and the significance of the processing for the data subject.[24] The GDPR even provides additional safeguards if the data subject is not granted the right not to be subject: the data controller must then implement suitable measures to safeguard the data subject's rights, freedoms and legitimate interests, and the data subject shall have at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.[25] This means that the controller is accountable for the automated decision and that the data subject should receive an account by the data controller on how the decision will be made and what the impact might be.

Transparency

Transparency is often considered to be a key component of efficient accountability frameworks: "An actor's conduct can only be compared to some standards if the conduct if its consequences can be observed by a forum"(Zimmermann and Cabinakova, 2015). Thus transparency should ensure that the algorithmic process can be observed and information regarding its future behaviour is provided. Transparency is also an integral principle within data protection frameworks, and especially within the GDPR. The GDPR requires data processing activities to be transparent, which entails that any information and communication concerning the processing of personal data should be easily accessible, easy to understand and conveyed

[22] Recital 71 GDPR.
[23] Recital 71 GDPR and Art. 22 §2 (b). GDPR.
[24] See Recital 63 GDPR and Art. 4 (1) GDPR, Art. 13 §2 (f) GDPR, Art. .14 §2 (g) GDPR and Art. 15 §1 (h) GDPR.
[25] Recital 71 and Art. 22 § 3 GDPR

through clear and plain language.[26] The transparency required is concerned with the identity of the data controller, the purposes for which processing activities are performed, but also the data that are being processed, the duration of data storage,[27] or as mentioned above, the logic of the automata underlying the processing activities.[28]

Transparency defined in this manner, could pave the way towards algorithmic accountability. It should also be noted that transparency as a data protection enhancing measure is aimed towards everyone: data processing activities should be conveyed to the general public in a transparent manner in order for the public to be able to make informed decisions.

4. Accountability in the GDPR Sufficient for Algorithmic Accountability?

In section 2, we saw that algorithms in a Big Data setting are difficult to understand for a variety of reasons. Algorithms are complex on a technical level due to their language, the manner in which they are programmed, and their dependence on other algorithms and data. They are also complicated due to their contextual dependence because of which they can be both value-laden and produce significant transformations in a latent way. Algorithmic accountability can only be achieved if this algorithmic complexity can be overcome in a manner that enables a clear understanding of the algorithmic decision-making process. Can the accountability mechanisms inherent in the GDPR fulfil this task?

First, *accountability as a data protection enhancing mechanism* as it is described in general terms in the GDPR may only in part be applied in a meaningful way to algorithms in a Big Data context, i.e. only to the degree that the input- and output data are personal data according to the definition of the GDPR. Algorithms in a Big Data context, however, although often relating to human beings, do not necessarily use or produce personal data in the strict sense, as we have seen in the case of random-group operations. These might therefore not be covered by the accountability mechanisms in the GDPR. Second, the accountability mechanisms of the GDPR do not entirely clarify *towards whom* algorithmic decision-makers should be considered to be accountable; they only point out to whom they should be accountable when algorithmic decision-makers process personal data. Algorithmic activities, however, do not necessarily require personal data to be processed in order to have a significant impact. Neither does the application of an algorithmic result to the individual or society imply a necessity for personal data processing. Even though personal data processing might have been required initially, the algorithmic result might be applied in concrete reality, leaving the ultimate decision outside the scope of data protection legislation. The latter might also be the case if anonymized data are used. We will return to the issue of the forum of accountability towards the end of this section.

One might think that *transparency* might be of help. Transparency as such, however, does not constitute accountability (Zimmermann and Cabinakova, 2015, 266-267). [29] Although it certainly facilitates the informed assessment of the desirability of a decision, Kroll et al. have expressed serious doubts regarding transparency as a regulatory mechanism with regard to the

[26] *See inter alia* Recitals 39, 58 and78 GDPR and Articles 5 §1 (a)and 12 GDPR:
[27] Ibid.
[28] See Recital 63 GDPR and Art. 4 (1) GDPR, Art. 13 §2 (f) GDPR, Art. .14 §2 (g) GDPR and Art. 15 §1 (h) GDPR.
[29] Ibid.

technical dimensions of algorithms. First, they deem corporate secrecy to be an un almost insurmountable impediment, and, second, they tend to consider the source code of the algorithms involved eventually unintelligible (Kroll et al, 2017). Although corporate secrecy and the intelligibility of the technical basics of the algorithms certainly raise big problems, they do not exclude the possibility of creating transparency in many other respects completely. Moreover, if the focus is too much on an algorithm's technicity and particularly on the manner in which it is programmed, one might lose sight of the contextual framework in which the algorithm operates. Transparency with regard to contextual factors such as the purpose or functions assigned to algorithms, for instance, can still be created – and, perhaps better, *should* be created. Although information concerning the purposes of data processing activities, and thus algorithms, the envisaged consequences, and the data collected and processed, should be given by the data controller, regardless of his forum (the individual or supervisory authority), this information might still not be enough to ensure algorithmic accountability or an assessment of the algorithm's desirability. A data controller might in complete accordance with the transparency requirements of the GDPR provide information regarding the purpose of the use of algorithmic decision-making, and the amount and categories of data collected for achieving this purpose, but yet leave it unknown how the decision was exactly made, e.g. which component in the decision-making process was assigned most weight. Even though the GDPR rules, for example, now require transparency with regard to the logic involved in algorithmic decision making[30], they do not specify what level of information constitutes compliance: is it the mathematical sequence of the algorithm or the substantial argumentation that could lie at the basis of the decision? It should once again be noticed that in an algorithmic context, the exact purpose for data processing may often remain undetermined too, or might at least be subject to change as algorithms actively search for new purposes to make use of data. Moreover, this purpose-seeking is one of Big Data's main attractions. This is one of the reasons why *a posteriori* accountability is important with regard to the use of algorithms in a Big Data context.

Concerning the mechanisms of *processing records* and *impact assessment*, the legislator stipulates that a supervisory authority, such as the national data protection authority, could gain insight into these records, or in the case where the impact assessment indicates high risk, should gain insight.[31] Where the impact assessment would ultimately indicate that processing would result in a high risk and the controller clearly has not taken measures taken to manage the risk, the controller has an obligation to consult with the supervisory authority prior to the performance of the processing activities. Both the processing records and impact assessment requirements provide a double accountability purpose: they facilitate the controller's self-assessment, whereas they also facilitate the task of the authority in assessing the compliance of the controller's data processing activities. It remains to be seen, however, whether, in practice, algorithmic risks can be adequately mapped. For instance, even though the GDPR recognizes discrimination as a potential risk of processing activities[32], differentiation is often inherent to algorithmic activities, and as we will describe below, it is not always easy to determine whether this differentiation should be considered discriminatory or non-discriminatory, or fair or unfair. It should also be noticed that an impact assessment is an *a priori* mechanism, whereas accountability is usually an *a posteriori* one. In an algorithmic context, however, *a priori*

[30] Art. 14 § 2 (g) GDPR.
[31] Art. 30 §4 GDPR and Art.36 GDPR.
[32] See for instance Recital 75 GDPR, where it is stated that the risk to the rights and freedoms of natural persons, such as the risk of discrimination, may result of data processing.

assessments concerning the potential impact of an algorithm remains difficult due to the possibility of unpredictable outcomes.

The *right not to be subject to automated decision-making* primarily vests power in the individual. The initial accountability and information requirements, however, do relieve the burden that comes along with this power.[33] Accountability towards the individual is appealing. Rather than relying upon the legal framework to determine potentially hazardous processing activities, the individual can decide whether or not to be subject to a processing act, regardless of how the legal framework has qualified that act. This is a form of privacy and data protection as "self-management" (Solove 2012). Grasping the impact of the decision is not an easy task for the individual, however, and neither would it be for the data controller. Moreover, this assessment would have to be made on a regular basis by the data subject, especially if automated decision-making is to become omnipresent. As Obar rightfully comments: "even if the digital citizen had the faculties and the system for privacy self-management, the digital citizen has little time for data governance" (Obar, 2015).

Furthermore, as was explained in section 3, the right not to be subject cannot always be exercised by the data subject.[34] If the right cannot be exercised, the data controller must implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests and the data subject should, at least, have the right to obtain human intervention from the controller, the opportunity to express his or her point of view and the ability to contest the decision.[35] The exercise of these additional rights however also presupposes a sound understanding of the algorithmic processes and perhaps even the power to have algorithms reconsidered by a human decision-maker. Indeed, the mathematical basis and seemingly rational nature of algorithms might grant the automated decision *de facto* validity against which the human actor might not be inclined to decide negatively.

With regard to the suitable measures to be implemented by the data controller, the GDPR does specify that, in the case of profiling, the controller should use appropriate mathematical or statistical procedures.[36] The technical and organisational measures taken should furthermore be appropriate "to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and that the risk of errors is minimised."[37] Personal data should also be secured and particular attention must be provided to the risks involved for rights and interests of the data subject.[38] Technical and organisational measures should, for instance, serve to prevent the discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or that result in measures having such an effect. Having sound mathematics and statistics however, does not overcome the potential dangers of the algorithm's contextual complexity. Moreover, and even though the recognition of the potentially discriminatory effects of algorithms deserves praise, in an algorithmic context, it is advisable not to exclusively focus on the 'characteristics' or 'salient traits' usually associated with discrimination and anti-discrimination legislation.

[33] According to the CIPL, accountability does not displace the individual's ability to assert his rights, but it serves to relieve the data subject of much of the burden of policing the marketplace for enterprises using data irresponsibly.
[34] Art. 22 §2 GDPR.
[35] Art. 22 §3 GDPR.
[36] Recital 71 GDPR.
[37] Ibid.
[38] Ibid.

Rather, a broad notion of unfair differentiation should be applied, which includes forms of unequal treatment not yet covered by the law. In the case of random group-profiles for example, no 'salient trait', linking all affected individuals, is likely to be detected. The individuals within the group might nonetheless be unfairly judged and treated on the basis of the differentiation of the group in comparison with others (Vedder 1999). We will return to this again towards the end of this section.

It might also be doubted whether a data subject might truly be able to contest a decision. Should the right not to be subject be asserted, the controller should be in a position to provide a verifiable account of how and when automated decision-making might impact the individual. An algorithm, and the resulting decision, must thus first be interpretable for the controller in order for him to effectively render the relevant information to the data subject. The technical and contextual complexity of an algorithm might undermine true understanding, not only for the controller, but also for the algorithm's designer.

In addition, the right not to be subject is of little help to individuals whose data have not been collected, but who are nonetheless affected by the algorithm. Here one may think of algorithmic information, in the form of profiles, used for selection purposes in the real world, such as a job interview or local advertisements. To put it differently: Algorithms sometimes only *inform* decisions affecting individuals, instead of *taking* the decisions directly through automated processes. Consequences such as these might require a rethinking of the power to be allotted to algorithms as a basis for decision-making.

The *forum of accountability* is an issue of concern regarding the GDPR. Within the context of data protection legislation, the Centre for Information Policy Leadership has identified three key parties to whom organisations may be considered to be accountable: individuals, regulators and organisations (CIPL, 2009). In the GDPR, the responsibility of the controller regarding compliance with data protection principles, seems to be targeted towards all three parties, yet due to its scope of protection, the primary subject towards whom accountability should eventually, and considering the scope of protection, perhaps ideally, be given, is the data subject, the individual whose data is being collected. The data subject is defined as an identified or identifiable living natural person, meaning an individual who can be identified, directly or indirectly. As we have seen, however, algorithms do often not only affect data subjects as individuals as such. Of course a group profile can sometimes make the individuals involved directly or indirectly identifiable. It is difficult, however, to uphold a focus on natural persons in cases that affect large groups in society or potentially everyone (Van Der Sloot, 2015, 9). More often than not, that will even more saliently be the case where random groups – even not so large ones – are concerned (Vedder, 1995).

Interestingly, the GDPR mentions the possibility of another forum toward which the processor could be held accountable in addition to the affected data subject. That forum is the European Data Protection Board. The European Data Protection Board can, on its own initiative or, where relevant, at the request of the Commission, issue guidelines, recommendations and best practices for further specification the criteria and conditions for decisions based on profiling pursuant to art. 22 GDPR.[39] Even if the EDPB were to seriously take up this role as a forum of accountability, it should be kept in mind that algorithmic decision-making affects more societal interests than data protection alone. Especially on the basis of their possible roles with regard

[39] Art. 70 §1 (f). GDPR.

to record keeping and data protection risk assessments as stipulated in the GDPR, Mantelero is of the opinion that data protection authorities could play a key role within a Big Data setting (Mantelero, 2016, 252). But can national or even supranational data authorities overcome the complexities of algorithms in a Big Data setting? Can they do justice to all of the interests possibly involved? In order to effectively exercise other autonomous rights and legitimate interests affected by data processing activities, safeguarding multi-stakeholder involvement seems necessary, even though many of the risks involved in Big Data analytics will still remain not assessable *a priori*.[40] The data protection invasive character of a given technology might be discerned; yet, due to algorithms operating on a random-group level, unfair differentiation might not. Differential treatment can be an inherent consequence of the functions algorithms perform. Prioritization, classification, association and filtering algorithms, are known to result in unfair differential treatment and discrimination (see inter alia De Hert, 2012, Barocas and Selbst, 2016; Diakopoulos, 2016; Kroll et al. 2017). Reliance on equality and non-discrimination legislation, however, is also problematic against this algorithmic backdrop. As computational capabilities increase, algorithms will be able to differentiate between individuals and groups on the basis of an increasing number of parameters in an ever increasing variety of contexts. Substantive equality law is built around comprehensively enumerated, pre-defined contexts, e.g. employment or education, or grounds, e.g. gender, race, religion (Le Métayer and Le Clainche, 2012, 325). Algorithms do not merely affect individuals, they also affect the group as a whole and set groups apart from the rest of society (Vedder, 1995, 258, Mantelero, 2016). Yet, as mentioned, the qualification of differential treatment as being unfair should not necessarily be linked to historically disadvantaged groups or types of discrimination already defined within the law as Custers et al.(2013) seem to suggest. The risk of unfair differentiation increases as more classification acts are performed by algorithms, although, of course, the opposite is also true, i.e. that fair differentiation might increase as well (which is not meant to suggest that in an algorithmic environment, fair and unfair differentiation can be simply considered as communicating vessels).

5. Conclusion

Accountability with regard to algorithms in a Big Data context, can only thrive in a culture in which algorithms are considered as more than mere data processing activities. As the effects of

[40] Though a multi-stakeholder approach seems desirable or even necessary, it does bring along additional difficulties. In particular, multi-stakeholder involvement, must be reconciled with other fields of law, such as competition law. Furthermore, due to conflicting interests, private or public entities might not be willing to participate with other private or public entities. In his interesting contribution to a 2014 study of the French State Council (Conseil D'Etat) concerning Fundamental Freedoms and Digital Technologies and Rights, Pierre Bellanger argues in favour of a single Data Agency. The contribution elaborates upon the collective nature of data, wherein the author argues that data should be governed as a common good. Within this context, Bellanger introduces the Data Agency. He considers that competition among entities should not focus on the ownership of data but its use. This, in turn, would stimulate each company to design the best computer programs to derive meaning and value. However, Bellanger notes that any gathering or processing of personal data should receive authorisation from the Data Agency, before any individual agreement. Although far-going in his approach, it does illustrate that some voices are in favour of a centralised 'data control' agency. Bellanger, Pierre. 2015. «Les données personnelles : une question de souveraineté», *Le Débat* 183:14-25, DOI 10.3917/deba.183.0014.

algorithms transcend the realm of data protection, so must the approach in algorithmic accountability. Accountability by algorithmic decision-makers should not be solely based on data protection principles, nor merely targeted towards a data protection entity as its primary forum. In order to achieve accountability, the controller himself will first have to assess the desirability of algorithmic decision-making, taking into account the larger context in which the algorithms will be deployed. As such, impact assessments could be a first step towards having a more accountable algorithmic culture. Moreover, if risks become apparent, design strategies could be further developed in order to make decision-making more transparent. Yet, given the variety of potential interests affected, the actual impact of algorithms, will often remain undetermined *a priori.* Furthermore, given the technical, relational and contextual nature of algorithms operating within a Big Data environment, the entity towards whom accountability should ultimately be given is not easily determined. An extensive knowledge exchange between technically savvy individuals, ethicists, non-governmental organizations, business corporations and a broad variety of other possible stakeholders is likely to be required in order to overcome the algorithmic complexity described in section 2. If processors are to be held accountable towards one supervisory authority representing specific interests or values, one might run the risk that certain affected interests and potential spill over effects of algorithmic decisions into other decisions or sectors are overlooked. The latter would for instance be the case when an algorithmic decision is taken in a credit-scoring context as a credit score might also affect an individual's other opportunities in life. Therefore, oversight mechanisms are also needed, which enable algorithm intensive industries to be monitored in order to identify future threats to societal values in due time. Perhaps then, and similar to non-discrimination legislation, contexts could be identified in which certain algorithmic risks have become apparent in a more tangible manner and where, in turn, authorities could be established towards which processers can be held accountable in a more effective manner. The GDPR already hints towards such an approach when it encourages associations or other bodies representing categories of controllers or processors to draw up codes of conduct, taking into account the characteristics of the sectors in which they operate.[41] Indeed, the GDPR's preamble specifies that such codes should be drawn up through multi-stakeholder involvement and consultation. The preamble moreover notes that codes of conduct could, in particular, "calibrate the obligations of controllers and processors, taking into account the risk likely to result from the processing for the rights and freedoms of natural persons."[42] Unfortunately, the notions 'stakeholder involvement' and 'obligation calibration', are not mentioned in the GDPR's main body of text nor are they ever further specified.[43] Although codes of conducts do not constitute accountability, they could serve as building blocks for a more accountable algorithmic environment. And as our familiarity with and our knowledge of algorithmic activities increases, so may our ability to translate the risks and effects of algorithms towards the general public.

[41] See *inter alia* Recitals 98, 99 GDPR and art. 40 GDPR.
[42] Recital 98 and 99 GDPR.
[43] See Section 5 GDPR: Codes of Conduct and Certification

Reference List

Alhadeff, Joseph, Brendan van Alsenoy and Jos Dumortier. 2011. "The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions" in Managing Privacy through Accountability, edited by D. Guagnin, L. Hempel, C. Ilten. Palgrave Macmillan, 49-82. DOI: 10.1057/9781137032225

Ananny, Mike. 2016. "Towards an ethics of Algorithms: Convening, Observation, Probability, and Timeliness." Science, Technology, & Human Values 41 (1): 93-117. DOI: 10.1177/0162243915606523

Article 29 Data ProtectionWorking Party. 2010. Opinion 3/2010 on the principle of accountability. Accessed 28 July 2016. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf. Accessed 25 July 2016.

Barocas, Solon and Andrew D. Selbst. 2016."Big Data's Disparate Impact" California Law Review 104 (671). DOI:

Bellanger, Pierre. 2015. "Les données personnelles : une question de souveraineté", Le Débat 183:14-25, DOI 10.3917/deba.183.0014.Bennett, Colin. 2010. "International Privacy Standards: Can Accountability be Adequate?" Privacy Laws and Business International 106

boyd, danah and Crawford, Kate. 2012. "Critical Questions for Big Data: Provocations for a cultural, technological, and scholarly Phenomenon", Information, Communication & Society 15 (5): 662-679. DOI: 10.1080/1369118X.2012.678878

Butin, Denis, Marcos Chicote and Daniel Le Métayer. 2014. "Strong Accountability: Beyond Vague Promises" in Reloading Data Protection, edited by Serge Gutwirth, 343-369. Springer Science+Business Media Dordrecht. DOI: 10.1007/978-94-007-7540-4_1

Burrell, Jenn. 2016. "How the machine 'thinks': Understanding opacity in machine learning algorithms" Big Data & Society (1): 1-12. DOI: 10.1177/2053951715622512

The Centre for Information Policy Leadership. 2009. "Accountability: A Compendium for Stakeholders"; Accessed 28 July 2016 https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/accountability-a_compendium_for_stakeholders__march_2011_.pdf

Citron, Danielle Keats and Frank A. Pasquale III. 2014. "The Scored Society: Due Process for Automated Predictions" Washington Law Review 89: 1

Colonna, Lianne. 2013. "A Taxonomy and Classification of Data Mining", SMU Science and Technology Law Review (16): 309.

Custers, Bart, Toon Calders, Bart Schermer, Tal Zarsky, ed. 2013. Discrimination and Privacy in the Information Society: Data Mining and Profiling in Large Databases. Springer-Verlag Berlin Heidelberg.

Diakopoulos, Nicholas. 2016., "Accountability in Algorithmic Decision Making" Communications of the ACM, February (59) 2: 56-62. DOI: 10.1145/2844110

European Commission. 2012. "Impact Assessment Accompanying the document Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data:" Accessed 28 July 2016. http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf

European Data Protection Supervisor. 2016. "EDPS launches Accountability Initiative". Accessed 28 July 2016.

https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Accountability/16-06-07_Accountability_factsheet_EN.pdf

Fayyad, Usama, Gregory Piatetsky-Shapiro and Padhraic Smyth. 1996. "From Data Mining to Knowledge Discovery in Databases" *AI Magazine* 17 (3): 37-54. DOI: http://dx.doi.org/10.1609/aimag.v17i3.1230

Gellert, Raphaël and Serge Gutwirth. 2012. "Beyond accountability, the return to privacy?" in Managing Privacy through Accountability, edited by D. Guagnin, L. Hempel, C. Ilten. Palgrave Macmillan.

Gillespie, Tarleton. 2012. "The Relevance of Algorithms" in Media Technologies, edited by Gillespie, Tarleton , Boczkowski, Pablo and Foot, Kirsten, (Cambridge, MA: MIT Press). DOI: 10.1057/9781137032225

Hill, Robin K. 2016. 'What an Algorithm Is', Philosophy and Technology 29 (1) :35-59. DOI: 10.1007/s13347-014-0184-5

Le Métayer, Daniel and Julien Le Clainche, 2012. "From the Protection of Data to the Protection of Individuals: Extending the Application of Non-Discrimination Principles". Chap. 15 in European Data Protection: In Good Health?, edited by Serge Gutwirth, Ronald Leenes, Paul De Hert and Yves Poullet, 315-329. Springer Dordrecht Heidelberg London New York. DOI: 10.1007/978-94-007-2093-2_15.

Kitchin, Rob. 2013. "Big Data and human geography: Opportunities, challenges and risks." Dialogues in Human Geography 3(3): 262–267. DOI: 10.1177/2043820613513388

Kitchin, Rob. 2016. "Thinking critically about and researching algorithms" Information, Communication & Society, p. 12. DOI; 10.1080/1369118X.2016.1154087

Kroll, Joshua A, Joanna Huey, Solon Barocas, Edward Felten, Joel R. Reidenberg, David G. Robinson, and Harlan Yu, "Accountable Algorithms" University of Pennsylvania Law Review (165) (Forthcoming 2017)

Manovich, Lev. 1999. "Database as symbolic form." Convergence: The International Journal of Research into New Media Technologies 5 (2): 80-99. DOI: 10.1177/135485659900500206

Mantelero, Allesandro. 2016. "Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection" Computer Law & Security Review 32: 238-255. DOI: 10.1016/j.clsr.2016.01.014

Nerurkar, Michael, Christian Wadephuland Klaus Wiegerling, 2016. "Ethics of Big Data: Introduction" International Review of Information Ethics (5), p.3.

Nissenbaum, Helen. 1996. "Accountability in a Computerized Society" Science and Engineering Ethics 2 (1): 25-42. DOI: 10.1007/BF02639315

Obar, Jonathan. 2015. "Big Data and The Phantom Public: Walter Lippmann and the fallacy of data privacy self-management" Big Data & Society July-December 2015: 1-16. DOI: 10.1177/2053951715608876

Organization for Economic Cooperation and Development. 1980. Guidelines on the protection of privacy and transborder flows of personal data.

Pasquale Frank. 2015., 'The Black Box Society: The Secret Algorithms that Control Money and Information' Harvard University Press: 320.

Postigo, Hector. 2014., "Capture, Fixation and conversation: How the matrix has you and will sell you, part 3/3"; http://culturedigitally.org/2014/04/capture-fixation-and-conversation-how-the-matrix-has-you-and-will-sell-you-part-33/

Ramirez, Edith. 2013. "Keynote Address at the Tech. Policy Inst. Aspen Forum, The Privacy Challenges of Big Data: A View from the Lifeguard's Chair" ; Accessed 28 July 2016 http://www.ftc.gov/sites/default/files/documents/public_statements/privacy-challenges-big-data-view-lifeguard%E2%80%99s-chair/130819bigdataaspen.pdf.

Roberge, Jonathan and Melancon, Louis. 2016. “Being the King Kong of Algorithmic Culture is a tough job after all: Google’s regimes of justification and the meanings of Glass” Convergence: The International Journal of Research into New Media Technologies: 1-19. DOI: 10.1177/1354856515592506

Seni, Giovanni, and John F. Felder. 2010. “Ensemble Methods in Data Mining: Improving Accuracy Through Combining Predictions”. Chapter 1 in Synthesis Lectures on Data Mining and Knowledge Discovery #2, edited by Robert Grossman. Morgan & Claypool Publishers. DOI: doi:10.2200/S00240ED1V01Y200912DMK002

Siegel, Eric. 2013 “Predictive Analytics”. Hoboken: Wiley. As cited by Kitchin, 2014.

Solove, Daniel J. 2013. “Privacy Self-Management and the Consent Dilemma” Harvard Law Review 126: 1880-1903.

Steen,Marc. 2014. “Upon Opening the Black Box and Finding it Full: Exploring the Ethics in Design Practices.” Science, Technology, and Human Values40(3):389–420.doi:10.1177/0162243914547645.

Van der Sloot, Bart. 2015. “”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 & Communications Technology Law. 24(1): 74-103. DOI: 10.1080/13600834.2015.1009714

Vedder, Anton. 1999. “KDD: The challenge to individualism” Ethics and Information Technology 1: 275-281. DOI: 10.1023/A:1010016102284

Wilson, Michele. 2016., “Algorithms and the Everyday” Information Communication and Society 1-14. DOI: 10.1080/1369118X.2016.1200645

Zarsky, Tal. 2014. “Understanding Discrimination in the Scored Society” Washington Law Review 89 (4).

Zimmermann, Christian and Johana Cabinakova. 2015. “A Conceptualization of Accountability as a Privacy Principle” in BIS 2015 Workshops, edited by W. Abramowicz Springer International Publishing Switzerland: 261-272. DOI: 10.1007/978-3-319-26762-3_23