Risk Profiling by Law Enforcement Agencies in the Big Data Era: Is There a Need for Transparency?

Sascha Van Schendel

Risk Profiling by Law Enforcement Agencies in the Big Data Era: Is there a Need for Transparency?

Sascha van Schendel[1]

[1] Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University, Tilburg, the Netherlands
s.vanschendel@tilburguniversity.edu

Abstract. This paper looks at the use of risk profiles by law enforcement in the age of Big Data. First, the paper discusses different use-types of risk profiling. Subsequently, the paper deals with the following three categories of challenges of risk profiling: a) false positives (and to some extent false negatives) as well as incorrect data and erroneous analysis, b) discrimination and stigmatization, c) and maintaining appropriate procedural safeguards. Based on the hypothesis of risk profiling creating challenges, this paper addresses the question whether we need transparency of risk profiling by law enforcement actors, from the perspective of protecting fundamental rights of those affected by the use of risk profiles. The paper explores tackling these challenges from the angle of transparency, introducing Heald's varieties of transparency as a theoretical model.

Keywords: Risk Profiling, Transparency, Law Enforcement, Procedural Safeguards, False Positives, Discrimination, Data Protection, Criminal Law, Explanation.

1 Introduction

Risk assessment has become very popular in all sectors of society, including in the prevention against crime. Over the last years, the term 'Big Data' has taken flight and has increasingly received much attention in government policies and practices.[1] The use of Big Data analysis is in part the reason for a strong emphasis on preventing and minimizing risk in society. Having the tools to analyze huge volumes of data and extract information from them, possibly completely by automated means, facilitates processes such as the creation and analysis of risk profiles.[2] The use of profiles grows as they can be constructed and applied more easily, while at the same time the construction, analysis and application of the profiles become more complicated and opaque.

The use of risk profiles to find suspects or determine if someone poses a risk to society has traditionally been an important tool to national law enforcement agencies to efficiently make use of their powers. Some scholars have described the emphasis on risk in criminal justice as entering into an era of actuarial justice[3] in which we focus on analyzing risk in a mathematical way, the rise of 'the logic of risk'[4], or 'the new paradigm of criminal law'[5]. While there are arguments to make in favor of law enforcement agencies making their practices more efficient by using risk profiles[6], this development is not without its issues and raises issues towards those affected by this practice. This leads to the first hypothesis of the paper: risk profiling in the Big Data

era creates challenges. Based on this hypothesis of risk profiling creating challenges, this paper addresses the question whether we need transparency of risk profiling by law enforcement actors, from the perspective of protecting fundamental rights of those affected by the use of risk profiles. This research question also contains the second hypothesis of this paper, namely that transparency could be an interesting angle to tackle the challenges. The aim of this paper is to shed light on the challenges of risk profiling. Exploring whether transparency is a way to approach these challenges is intended as a starting point of a discussion. This paper does not provide an analysis of how transparency will solve the challenges of risk profiling, nor does the author outline what transparency should look like in this context. This is the topic of future research of the author.

Section 2 of this paper briefly maps risk profiling by law enforcement actors in practice. One specific example is taken as a case study to be explored in more detail. This example is SyRI (System Risk Indication), a Dutch risk profiling system. This example was chosen as it is currently under review in a national court case. SyRI is a good example of risk profiling that presents the starting point of a criminal investigation. Some parallels are drawn to the USA in Section 2, as some of the types of use of risk profiles are still very minimal in the European Union but might become more prominent following the USA's example. Section 3 describes the main challenges of the use of risk profiling, grouping them under three main, non-exhaustive headers: errors, discrimination and stigmatization, and lack of procedural safeguards or outdated safeguards. Section 4 describes why transparency might be an interesting angle to approach the challenges. For this purpose, Section 4 introduces and briefly describes Heald's 'varieties of transparency'[7] as a theoretical model. Subsequently, Section 4 narrows transparency down to foster further discussions, as transparency in itself is a very broad concept. For this purpose a bottom-up approach to the issues is chosen, focusing on explanations as a means of transparency. The focus on explanations is all the more relevant after the introduction of the General Data Protection Regulation[8] ('GDPR'), as it contains references to explanations in the context of automated decision making. Section 4 will therefore also briefly mention transparency and explanations under the GDPR and the Law Enforcement Directive[9] ('LED').

2 Risk Profiling in Practice

2.1 What is Risk Profiling?

Risk profiling, for the purpose of this paper, is categorizing or ranking individuals or groups, sometimes including automated decision making, using correlations and probabilities drawn from combined and/or aggregated data, to determine the level of risk that is posed to the security of others or national security by those individuals or groups.[1] The most prominent type of risk here is the likelihood of an individual or group (re)committing crime.

[1] This definition of risk profiling is the author's own and is a working definition.

Risk profiling can take many forms in the law enforcement context. Risk profiling can be used in concrete criminal investigations where there is already an identified suspect or perpetrator and a profile is applied to this person. A first instance is to make decisions about which police powers to employ. Brkan gives the example of automated decision making to determine whether to seize a mobile device.[10]

Risk profiling of an identified individual can also be targeted towards future behavior. This can be risk profiling to determine whether someone is allowed bail or probation specifically whether that person is at risk of reoffending, or risk profiling in sentencing determining the duration of incarceration. The most famous example is from the USA, namely COMPAS. COMPAS is an algorithm used by judges and probation- and parole officers to assess a criminal defendant's likelihood of reoffending.[11]

There are types of risk profiling where the target is a location. These are often types of predictive policing drawing from various sources of data, ranging from non-personal data such as the distance to the highway to different forms of personal data pertaining to inhabitants of that area such as the history of criminal records. Algorithms can in this way pinpoint the level of risk for areas, so that police officers can be deployed accordingly. This type of risk profiling is very popular in the USA, but also exists in Europe.[12] Such as in the Netherlands, where the Crime Anticipation System is used, creating a grid that is updated every 14 days which shows for each square what crime is likely to take place and on which time of day. This system was at first only applied in the capital, Amsterdam, but is now being used in various other cities. While such a system is targeted at the risk level of a location, it indirectly profiles the residents of that area. This is where discussions on stigmatization and self-fulfilling prophecies come in: by attaching a risk label to a certain area and sending police patrols there accordingly, this can impact the view residents and outsiders have of this area plus lead to an increase in crime detection further increasing patrols and measures taken against residents of this area. Indirectly the residents are also profiled as high risk. Of course this means that there is an assumption that the suspects or perpetrators would reside in this area, while this does not have to be reality.

Besides the above described type where law enforcement applies profiles to an already identified individual or area, risk profiles are also used to detect individuals -or groups- that fit the profile. In these cases an algorithm finds individuals that fit the risk profile in a haystack of data. These individuals are likely to commit a crime or are likely to have committed an undetected crime. This type of profiling does not take place within the boundaries of a specific criminal investigation but rather leads to the starting point of one. Risk profiling to detect individuals can take the form of 'heatlists', similar to the heatmapping or area profiling described above. An example from the USA is the system Intrado Beware, which is a mobile, cloud-based application, sold to the police, that gathers contextual information from social media, commercial data and criminal data, creating a risk score –green, yellow, red- for individuals.[12] Intrado Beware is slightly different from the standard model of detecting people who have committed a crime, as it is more targeted towards providing police information about the person they are about to encounter and identifying whether they are a risk in the sense of posing a risk to the security of the police officer. Another example of finding individuals that

match the risk profile comes from the Netherlands, which is described in the section below.

2.2 The SyRI Case

An example of risk profiling can be found in the Netherlands in the SyRI ('System Risk Indication') program. SyRI was officially launched in 2014 and is employed by the Dutch Ministry of Social Welfare & Employment. It is a system in which many databases are combined –ranging from tax data and data about social benefits to data about integrating in Dutch society and education-, creating a large data pool to detect fraud.[13] SyRI targets three types of fraud: unlawful use of social benefits, taxation fraud, and fraud with labor laws.[13] Due to the broad scope and large governmental database, almost every citizen of the Netherlands is present in the database. Using a predetermined risk model, the system searches for correlations in the database flagging a potential case of fraud based on the model used for that specific search.[14] The individual is given a risk indication, which is forwarded to the Dutch National Police and/or prosecuting office, who then decide whether to investigate further. The risk indication is stored in a register which relevant public bodies can access.[13] So even though SyRI is not a specific risk profiling program of law enforcement solely, law enforcement is one of the parties that can be included in a cooperation to use SyRI and the risk score of SyRI can be the data point that starts a criminal investigation.

Even though SyRI has been used for a couple of years now, its use has not been without resistance. There have been parliamentary debates centered on the question whether SyRI met proportionality demands and whether its legal basis was not too broad. The program raises issues of transparency, mainly awareness and contestability. Most citizens are not aware that their data is in this system nor that they might be flagged. Most people are confronted with the existence of the system when they receive an administrative fine or encounter another negative consequence. Besides possible privacy and data protection issues that follow from a system that uses so much data, there are serious issues with possibilities to contest the system and correct errors. In March 2017, several NGOs and two citizens took up the initiative to launch a court case, which is still ongoing, to test whether SyRI is compliant with EU data protection legislation, the fundamental right to privacy and the right to fair trial under article 6 of the European Convention on Human Rights.[15] One of the points that is debated is the secrecy of the risk models, but also the lawfulness of the automated decision making and the broadness of the legal basis.[15] In this sense the problematic aspects of SyRI illustrate the challenges following from data driven policing or policing in the Big Data era, such as risk profiling.

3 Risk Profiling: Challenges

This section groups the challenges of risk profiling under three main headings: errors, discrimination and stigmatization, and lack of procedural safeguards or outdated safeguards. This is a non-exhaustive list but aims to give an oversight of the main challenges

based on literature about profiling, algorithms, predictive analysis and data analysis in the law enforcement domain.

3.1 Errors: Relying on Statistics and Probabilities

Most profiles are probabilistic, describing the chance that a certain correlation will occur.[16] In most cases the individuals included under the profile do not share all the attributes or characteristics of the group profile.[16] This is especially true for non-distributive profiles, which are framed in terms of probabilities and averages, comparing members within a group or category, or comparing those groups or categories to each other.[17] This means that there is always an inherent risk of errors in the use of profiles, as it might include people erroneously within a profile or might miss certain individuals, leaving them out of scope. The first category is false positives, the second situation is false negatives.[18] In case of false positives, people would be incorrectly classified in a group or profile. This in turn could have consequences for decisions taken to the disadvantage of these persons, or they could be erroneously subjected to police powers. In the case of a false negative, we encounter the more traditional problem of law enforcement, namely overlooking someone who should be a suspect or miscalculating the risk of recidivism. Especially in the context of terrorism threats, risk profiles aim at minimizing false negatives, as the societal consequences are a lot graver when allowing for a false negative than a false positive.[19] Mittelstadt et al. talk about these issues in terms of 'inconclusive evidence', meaning that algorithms often draw from statistics and in doing so create only probable outcomes that are focused more on actionable insights than causal relations.[20] Algorithms become increasingly complex and autonomous, which makes it harder for law enforcement to be transparent about why they receive a certain outcome. Mittelstadt et al. refer to this complexity and opaqueness as 'inscrutable evidence', where humans have trouble interpreting which data points lead to the conclusion.[20] Risk profiling in the Big Data era relies heavily on algorithms and statistics. Statistics offer insight into numbers, for example how many people re-offend within an amount of years. Algorithms can be used to combine statistics, mine them for patterns, and make a prediction about an individual's behavior by applying this information to their situation. This does not mean however that this person acts according to the statistics nor that the conclusion based on combining statistics is right. If the process becomes more complex and opaque it can become harder for law enforcement agencies to demonstrate why they received this outcome.

3.2 Discrimination & Stigmatization

The trend of risk management combined with the strong focus in politics on terrorism prevention can push law enforcement to target specific groups, especially with the pressure to fully use technologies such as algorithms and Big Data analysis. The technology, to a large extent, takes over tasks that were not fully automated before. Now algorithms take over the task of detecting the patterns, creating the profiles and finding correlations.[5] As these technologies are not foolproof –just as police officers' instincts and human observation and logic are not foolproof- this does pose a threat of

discrimination and stigmatization of certain groups. The technology might 'over target' specific groups. It has been shown already that risk-based policing targets certain societal groups within different EU countries, such as North African youths, soccer supporters, Roma, and Muslims.[19] The technology might increase racial or ethnical profiling especially. For example, in the Netherlands, the existence and possible condoning of ethnic profiling by police officers has been a topic of societal debate for years.[21] While these types of debates were mainly targeted at racial profiling based on 'police instinct', automated profiling possibly increases racial profiling.[19, 20] As Van Brakel explains: "*Predictive mapping can potentially lead to ethnic profiling. If arrest rates are a measure for predicting in which areas most crime occurs, for instance, and if it is clear that arrest rates are disproportionately higher in particular population groups as a result of ethnic profiling there is a clear bias in the prediction, and the mapping can lead to even more ethnic profiling*".[12] Referring back to the example of the Dutch predictive policing application CAS, ethnic profiling has already been demonstrated to be an issue.[21]. When using automated means, all the data analysis is scaled up, increasing the scale of the problematic aspects. Profiling in itself is a discriminatory process, which is not illegal in itself, but can become illegal discrimination if based on factors such as race or religion.[22] Article 11 of the Law Enforcement Directive prohibits the use of sensitive data –officially called 'special categories of data'[2]- unless suitable safeguards are in place to protect the interests of the data subject. So when using sensitive data such as ethnicity or religion extra safeguards might need to be put into place. However, provisions that forbid the use of these types of factors or require extra safeguards, do not prevent the use of proxies. The use of proxies could nonetheless be discriminatory, such as using zipcodes or income as a proxy for ethnicity. Discrimination following directly from automated decision making is forbidden as far as the special categories of data go. Profiles that focus on other characteristics –or proxies for those characteristics-, such as age can also be deemed illegal. Recently, a court in the Netherlands ruled that the use of a risk profile –of single men of 55 years or older– was in violation of the right not to be discriminated against.[23] It is extremely hard, however, to tackle illegal discriminatory profiling if the impacted individuals are not aware that they are placed in a certain profile. As Leese states: "*as datadriven profiles produce artificial and non-representational categories rather than actual real-life social groups, the individual is likely to not even notice when he or she becomes part of a 'risky' category*".[19] Besides individuals not being aware, the actors operating the algorithm might also be unaware of illegal discrimination happening in their dataset or algorithm, or they might be unaware that their use of proxies has the same result as the illegal discrimination based on certain characteristics. These problems are only more difficult to detect and address as systems get more complex.

---

[2] Special categories of data under the GDPR and LED are data that are deemed especially sensitive and therefore receive more protection. The set categories are: data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

3.3 Procedural Safeguards

Automated risk profiling works in a different way than the more traditional policing, creating challenges in the way in which safeguards are set up. First, risk profiling is a form of proactive or even preventive policing. This forms a contrast to the more traditional reactive policing. Koops has referred to a shift in paradigm in criminal law which for example contains a focus on prevention, risk, groups, profiling, and statistics.[5] An issue is that safeguards might be linked to the prosecution phase, leaving out the opaque pre-investigation practices where a lot of data is already analyzed.[5] In reactive policing the focus for checks and balances is traditionally on the judge, who comes in at the later investigation stages or only at the trial. However with risk profiling someone might be arrested erroneously and released shortly after. Similarly, with risk profiling used in general policing, a lot of data is analyzed and privacy infringements could take place there as a consequence, but go undetected because there is no criminal investigation of a specific suspect yet. Second, in the information society decisions are increasingly made based on group profiles.[18] In literature on data protection and privacy there are increasingly more debates on the possibilities for collective procedures to address types of data processing such as Big Data analytics and group profiling.[24] Vedder, in his work on KDD (Knowledge Discovery in databases), already signaled a tendency of treating people based on group characteristics.[17] This tendency has only grown with modern risk profiling, as risk profiling requires statistics and categorizing or ranking of people. Vedder discusses data that for example used to be personal data but during time has become part of a broader set of anonymous data, at some stage the data became part of aggregate data and individual identifiers were replaced with group identifiers.[17] As Vedder precisely states, using generalizations and categorizations based on profiles can be highly problematic when they are used as a basis for policy and people are treated as a member of a group instead of on their own merits.[17] However, safeguards and rights are often linked to individual decision making. Automated decision making under article 11 of the Law Enforcement Directive, which produces an adverse legal effect concerning the data subject or significantly affects him or her, is prohibited unless authorized by national law and provided with appropriate safeguards. Profiling is concerned with creating a set of correlations on the aggregate level and subsequently applying it to individuals or groups. One could argue that only the application of a profile to an individual situation is regulated here. Brkan gives the example of a group being the target of profiling by making an automated decision to patrol certain areas, affecting the lives of the people who live in such an area.[10] Again, reference could be made to the Dutch predictive policing system, CAS, indicating where and when which crimes are likely to take place. Based on those risk indications police officers are deployed, but it is not clear whether the decision to target areas as high risk areas meets the criteria of article 11 of the Law Enforcement Directive to require further safeguards.

4 Transparency

4.1 Using Transparency to Address Challenges

Having presented the most prominent challenges of risk profiling by law enforcement agencies, the issue is how to address these challenges. I propose to look at the concept of transparency for solutions to these challenges.

Transparency has possibilities to expose flaws or give insight into decision making. A lot of the challenges relate to processes being opaque. For example, maybe it is not visible that someone is placed in the wrong category or that there is illegal discrimination taking place. Or, because of a lack of procedural safeguards in the early investigation, mistakes do not come to light. In that sense transparency also increases possibilities of awareness. A lot of people are simply not aware that they are being profiled or that a decision about them, for example concerning arrest or deploying investigative measures, is based on a risk profile. A lack of awareness makes it difficult for those affected by risk profiling to check for compliance with their rights when necessary, such as the right to fair trial, equality of arms, privacy, or the principle of non-discrimination. Therefore transparency might be interesting to look further into. However, transparency is a very broad concept and has different meanings even within one discipline. Several authors have already described the relation between transparency and a concept that is often connected to it, namely 'openness'. For example Birkinshaw proposes that transparency and openness are close in meaning but are both broader than merely access to (government) information.[25] Larsson also does not consider openness and transparency to be the same concept, as according to Larsson transparency goes beyond openness and also includes simplicity and comprehensibility.[26] Heald remarks that transparency has become 'the contemporary term of choice' for describing an openness of public actors about actions and decisions they make.[7] However, Heald makes various distinctions within the concept of transparency.[7] These distinctions are helpful to dismantle the broad concept and distinguish which functions or solutions transparency actually offers. Therefore Heald's work on transparency is briefly discussed here as a theoretical framework.

First, Heald makes explicit different directions of transparency. There are two directions of vertical transparency: upwards and downwards. Upwards transparency can be seen in hierarchical terms of allowing the superior to observe behavior or results. Downward transparency can be seen in terms of democracy, allowing the ruled to observe behavior or results of their rulers.[7, p. 27] Second, Heald discusses the two directions of horizontal transparency: outwards and inwards. Transparency outwards occurs when the hierarchical agent can observe behavior outside of its organization or institution, so as to understand the domain it is operating in and observe the behaviour of peers. Transparency inwards occurs when those outside of the organization can observe what is happening within the organization.[7, p. 28]

Next Heald distinguishes different varieties of transparency in general using three dichotomies: event transparency versus process transparency; transparency in retrospect versus transparency in real-time; nominal transparency versus effective transparency. When distinguishing between events and processes, an event can for example

be the input or output data. When providing process transparency one can be transparent about the procedural factors –which rules are followed- or operational aspects –how are the rules applied in this situation-.[7, p 29-32] Another dichotomy is the temporal one, so one can allow for transparency after the fact –in retrospect- or one can continuously allow for transparency so that transparency takes place in real-time.[7, p. 32-33] For the last dichotomy Heald states that there can be a gap between nominal and effective transparency, which he labels the 'transparency illusion'.[7, p. 34] Allowing for transparency does not always mean that it is effective: "*For transparency to be effective, there must be receptors capable of processing, digesting, and using the information*".[7, p. 35] Also, transparency is not effective when it creates an information overload. [7, p. 35]

After having some more insight into the concept of transparency, it is interesting to see how this theory relates to the problem at hand. First, concerning the vertical transparency: in the context of data processing by law enforcement actors, upwards transparency is concerned with transparency towards oversight authorities such as Data Protection Authorities or (investigatory) judges. Downwards transparency is directed towards the people that are the subject of the process, in the case of automated decision making this concerns for example the data subjects. When looking at horizontal transparency, inwards transparency can be offered to oversight authorities, the people affected by the data processing, the democracy or people at large, and so forth. In the context of law enforcement outwards transparency is not so relevant. When distinguishing between events and processes it becomes clear that in the case of risk profiling there is a large variety in what transparency could be given about. Transparency can for example concern events such as the input of new data, or the outcome that the algorithm gives. On the other hand transparency could be given about the process, such as procedural aspects like the decision rules, which in this case could be the algorithm itself. Concerning the process, transparency could also be provided about the operational aspects, focusing on a specific situation, explaining why the decision rules have in this case led to this outcome. With regard to the temporal dimension transparency could be given in retrospect, for example notifying oversight authorities or individuals that a decision has been made based on a risk profile. Or transparency could be offered in real-time, which in the case of law enforcement seems complicated, as this might pose difficulties for ongoing investigations. With regards to the dichotomy between nominal and effective transparency, a lot of issues are left open. To determine the effectiveness of transparency of risk profiling would be quite difficult.

Based on the description above, there is still a lot of variation possible in to whom transparency is offered, about what elements of risk profiling transparency is given, and what constitutes effective transparency. Transparency in risk profiling could have varying functions. However, going back to the research question of this paper, -to determine whether transparency could help with the challenges from the perspective of protecting the rights of those affected by the risk profiling- transparency needs to be narrowed down further along Heald's varieties of transparency. In focusing on those affected by risk profiling, downwards-inwards transparency is the relevant variety. When targeting transparency towards data subjects, and others that might be affected, three steps could be distinguished. The first step is to make data subjects aware that data

processing and risk profiling is taking place. The second step is to explain to data subjects what is going on and how certain decisions are made. These two steps enable the third step, being able to contest profiles and automated decisions and receive due process. Perceiving transparency in this bottom-up way makes it easier to grasp the overall concept of transparency and connects to the challenges. It is after all important in safeguarding the rights of individuals affected that they are not erroneously profiled, illegally discriminated against, or undergoing a process without enough procedural safeguards to protect fundamental rights such as the right to a fair trial.

Alternatively, it is interesting to assess in the context of upwards transparency how law enforcement actors will explain their profiling practices and decisions to judges, or other competent authorities, when the analysis becomes more intricate and decisions more data driven. This is, however, a dimension of transparency that will largely take place behind closed doors and very difficult to analyze as researchers.

4.2 Food for Thought: Explanations as a Means of Transparency?

One aspect or means of offering transparency to data subjects, and others affected by risk profiling, is that of providing explanations of the profiling. Explanations of profiling and automated decision making have become very relevant with the reform of EU data protection legislation. To go further into this, a brief description of EU data protection legislation in the context of transparency is needed.

EU data protection legislation consist of several pieces of law. In 2016 the reform package for Data Protection legislation on the European Union level was adopted, introducing the General Data Protection Regulation[8] ('GDPR') and the Law Enforcement Directive[9] ('LED'). Before the introduction of the LED, data protection in this area was left in part to national legislation, partly standardized by Convention 108 of the Council of Europe[27], and in part regulated by a variety of specialist and sector specific instruments, creating a very fragmented landscape.[28] The LED repeals the Council Framework Decision 2008/977/JHA[29], which was very narrow in scope, only applying to cross-border transfers and exchanges of personal data, excluding domestic processing of personal data.[30] As the regulation of the processing of personal data by national law enforcement agencies has been left out of harmonization so far, a wide margin is left to the criminal procedural law of Member States to lay down requirements and safeguards. For data processing in the private sector it is logical to look for requirements and safeguards in the GDPR, but for data processing by national law enforcement agencies the LED needs to be seen together with the safeguards and requirements following from Member States' legislation that arranges the competencies of these actors. The current Law Enforcement Directive does not contain a general principle of transparent processing. Under relevant Council of Europe law this is different. The newest version of Convention 108, which also applies to the law enforcement domain, does contain a principle of transparent data processing under article 5.[3] When

[3] The Convention 108 has recently been modernized. The amending Protocol (CETS No. 223) to Convention 108 was adopted by the Committee of Ministers of the Council of Europe on 18 May 2018.

comparing the GDPR and the LED, a fundamentally different approach with regard to transparency becomes visible. Transparency takes a predominant place within the GDPR in the form of transparent processing[4], combined with various rights towards the data subject. Transparent processing in this sense can mean that data subjects are informed about processing before it takes place, during the processing itself and upon request of the data subject. Besides the principle of transparent processing that applies throughout all types of processing, articles 12 until 14 of the GDPR impose obligations on the side of data controllers as well as rights upon data subjects to request information. In the context of profiling especially article 13 is relevant where, in the context of providing information, it states: "(…)*the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject*." Recital 39 of the GDPR also pays specific attention to transparency, it states: "*The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used*". Thus this principle already implies; first, that information about the processing should be available to the data subject; second, that this information should be easy to access; third, the information itself should be easily understandable. The same aspects of transparency are highlighted in recital 58. Recital 60 underlines the importance of awareness as a component of transparency, by stating that transparency requires the data subject being informed of the *existence* of the processing. In contrast, in the LED the principle of transparent processing is not present. The only relevant reference to transparency is in recital 26. Recital 26 merely mentions that processing should be done in a transparent manner with regard to the persons concerned, while at the same time acknowledging the necessity of some covert operations and surveillance measures. The critical component is "*provided by law and constitute a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the natural person concerned"*. So the requirements for transparency and limits of opaqueness are determined on a case to case basis where practices differ much from country to country. Again, national criminal procedural law also has a role to play here, as regulation is left to the Member States in this area. Some countries might have more provisions on transparency than others.

Transparency in the context of data processing has also become a much debated topic in literature. On the one hand arguments are presented in favor of more transparency of algorithms and algorithmic decision making[31], on the other hand there is a continuously increasing awareness that 'transparency' as such is not an all-encompassing answer for issues with algorithms.[20][32] Transparency more often than not, requires balancing of transparency as a value and other values such as protecting trade secrets, national security, and privacy of others.[19][20] Especially in literature on the law enforcement sector, transparency is discussed in the context of a trade-off or balance between security and transparency –sometimes as an aspect of the right to privacy-.[10]

[4] Under article 5 of the GDPR.

However, that there are arguments in favor of law enforcement agencies operating under a certain level of secrecy, does not mean that there is no room for transparency at all. Requiring law enforcement to explain why someone is profiled in a certain way puts up a safeguard in general against illegal discrimination and errors, as requiring an explanation stimulates checking the analysis to see whether the proper data was used and how the data was weighted to come to this result, as well as the level of probability. Providing explanations also serves a more specific purpose. While the process of profiling becomes more automated and technically complicated, it is important that law enforcement actors can still understand how a profile or decision came about, putting up a safeguard against algorithms that become so opaque and complex that humans cannot understand or justify the outcomes anymore. Law enforcement agencies need to be able to explain their decisions to a judge that checks the legality of, for example, searching a phone or computer; public prosecution needs to be able to explain during a trial why the prosecution authorities started the investigation, meaning why the person in case was suspect according to the risk profiling system. This requirement is inherent in criminal justice systems[33], if law enforcement cannot explain a decision, the judge will probably not accept it. However, giving these sort of explanations might be more challenging in automated processes, or processes with minimal human intervention. Therefore, it would be good to lay down an explicit requirement in national law, whether in data protection legislation or criminal law, for explaining profiling and automated decision making.[33] While the actors using a risk profiling system need to maintain a certain understanding of how it works so that they can be accountable for their decisions, it is equally important that the human actors involved do not over rely on the technology. In literature this has been discussed as 'automation bias', meaning that humans have a tendency to over rely on the accuracy of automated analysis and decisions, the result is assumed to be correct and no counterfactual evidence is sought out.[34] With this risk in mind, explaining the decision also ensures that human actors do not take the outcome for granted but investigate how it came about.

As stated in the introduction, this paper is not the place to develop what explanations of risk profiling in the law enforcement sector should or could look like exactly. It does offer food for thought though, especially with all the new transparency provisions under the GDPR.

5 Conclusion

Preventive and risk based policing is increasingly becoming the new form of policing. However, safeguards might be attuned to more traditional, less data-driven, policing and criminal procedures. This means that now and in the future there will be challenges on this front, such as dealing with probabilities, discrimination, effects on groups and shifting to the pre-investigation phase. This paper proposed to look at transparency for dealing with these challenges. Making the broad notion of transparency more feasible to grasp using Heald's varieties of transparency, it becomes clear that there are a lot of different options regarding to whom transparency could be offered and what the object of this transparency would be. Basing decisions on these risk profiles can have very serious consequences from the perspective of those affected by the risk profiles, for example when it comes to their rights not to be discriminated against or the right to fair

trial and equality of arms in being subjected to complex data analysis that might even concern future behavior. While transparency is prominent in the GDPR and in literature concerning the GDPR, the debate about transparency is not really taking place yet in the literature about the LED and literature about profiling in the law enforcement sector. The increasing use of Big Data and algorithms in policing and in prosecution, such as in the form of profiling and automated decision making will, however, only make transparency more important to discuss. This paper made a first step in discussing why transparency is important, by examining the challenges of risk profiling and the different options of transparency, and why we especially need explanations in the law enforcement domain as a means of transparency. The time has now come to also talk about explanations of profiling in the law enforcement sector to assess what role they could play and what they could look like.

References

1. B. van der Sloot & S. van Schendel, International and Comparative Study on Big Data, Working Paper no. 20, Dutch Scientific Council for Government Policy (WRR) 2016.
2. A. Marks, B. Bowling & C. Keenan, Automatic justice? Technology, Crime and Social Control. In: R. Brownsword, E. Scotford and K. Yeung (eds), The Oxford Handbook of the Law and Regulation of Technology, OUP 2017.
3. H. Kemshall, Understanding risk in criminal justice, Crime and Justice Series, Open University Press UK, 2003; N. Reichman, Managing crime risk: towards an insurance based model of social control, Research in Law and Social Control 8: 151-72, 1986; B. E. Harcourt, Against Prediction Profiling, Policing, and Punishing in an Actuarial Age, The University of Chicago Press 2007.
4. R. V. Ericson & E. Haggerty, Policing the Risk Society, Clarendon Press 1997.
5. E.J. Koops, Technology and the Crime Society: Rethinking Legal Protection, (2009) 1 Law Innovation and Technology.
6. E.T. Zouave & T. Marquenie, An Inconvenient Truth: Algorithmic Transparency & Accountability in Criminal Intelligence Profiling, 2017 European Intelligence and Security Informatics Conference.
7. D. Heald, Varieties of Transparency. In: *Transparency: The Key to Better Governance?* Edited by C. Hood & D. Heald, OUP/British Academy (Proceedings of the British Academy), 2006.
8. 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), L 119/1.
9. Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, L 119/89.
10. M. Brkan, Do algorithms rule the world? Algorithmic decision-making in the framework of the GDPR and beyond (August 1, 2017). Available at SSRN: https://ssrn.com/abstract=3124901.
11. https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm

12. R. van Brakel, Pre-Emptive Big Data Surveillance and its (Dis)Empowering Consequences: The Case of Predictive Policing. In van der Sloot, B. et al (ed.) (2016) *Exploring the Boundaries of Big Data*, Amsterdam: Amsterdam University Press.
13. Besluit SUWI, Staatsblad 2014, 320. Available only in Dutch at: https://zoek.officielebekendmakingen.nl/stb-2014-320.html.
14. https://algorithmwatch.org/en/high-risk-citizens/
15. https://pilpnjcm.nl/en/dossiers/profiling-and-syri/
16. M. Hildebrandt, Defining Profiling: A New Type of Knowledge? In: Profiling the European Citizen, (eds.) M. Hildebrandt & S. Gutwirth, Springer 2008, p. 21-22.
17. A. Vedder, KDD: The challenge to individualism, *Ethics and Information Technology* 1999, 1:275-281.
18. M. Hildebrandt, E.J. Koops, The Challenges of Ambient Law and Legal Protection in the Profiling Era, (2010) *Modern Law Review* 73(3) 428-460.
19. M. Leese, The new profiling: Algorithms, black boxes, and the failure of anti-discriminatory safeguards in the European Union', *Security Dialogue* 2014, Vol. 45(5) 494–511.
20. Mittelstadt et al., The ethics of algorithms: Mapping the debate, *Big Data & Society*, July–December 2016: 1–21.
21. J.P. van der Leun, J.P & M.A.H. van der Woude, Ethnic Profiling in The Netherlands? A Reflection on Expanding Preventive Powers, Ethnic Profiling and a Changing Social and Political Context, *Policing and Society* 21, 4: 444-455; Open Society Initiative (2013) Equality under Pressure: The Impact of Ethnic Profiling, available at: www.opensocietyfoundations.org/sites/default/files/equalityunder-pressure-the-impact-of-ethnic-profiling-netherlands-20131128_1.pdf.
22. B. Schermer, The limits of privacy in automated profiling and data mining, *Computer Law & Security Review* 27 (2011) 45-52.
23. Centrale Raad van Beroep, 21 November 2017, ECLI:NL:CRVB:2017:4068.
24. L. Taylor, L. Floridi & B. van der Sloot (eds.), Group Privacy: New Challenges of Data Technologies, Springer 2017; A. Mantelero, Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection, Computer Law & Security Review, Volume 32, Issue 2, April 2016, P. 238-255.
25. P.J. Birkinshaw, Freedom of Information and Openness: Fundamental Human Rights, *Administrative Law Review* 2006, 58(1), 177–218.
26. T. Larsson, How Open Can a Government Be? The Swedish Experience', in *V. Deckmyn and I. Thomson (eds), Openness and Transparency in the European Union*. Maastricht: European Institute of Public Administration 1998.
27. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.
28. P. De Hert & V. Papakonstantinou, 'The Police and Criminal Justice Data Protection Directive: Comment and analysis', Computers & Law Magazine of SCL 2012, vol. 22, issue 6.
29. Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, L 350/60.
30. T. Marquenie, The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework, *Computer Law & Security Review* 33 (2017) 324-340.
31. T. Zarsky, Transparent Predictions, *University of Illinois Law Review* (2013) 4.
32. M. Annany & K. Crawford, Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability, *New Media & Society*, Vol 20, Issue 3, 2018.

33. Commissie modernisering opsporingsonderzoek in het digitale tijdperk, *Regulering van opsporingsbevoegdheden in een digitale omgeving*, June 2018, available at (only in Dutch): https://www.rijksoverheid.nl/documenten/rapporten/2018/06/26/rapport-commissie-koops---regulering-van-opsporingsbevoegdheden-in-een-digitale-omgeving. This Committee, that reviewed Dutch criminal law in the light of digital developments, also concluded that an explicit requirement for explaining automated data analysis is necessary in national criminal procedural law.
34. M. L. Cummings, Automation Bias in Intelligent Time Critical Decision Support Systems, AIAA 3rd Intelligent Systems Conference 2004.