Surveillance & Society

Article

How to Watch the Watchers? Democratic Oversight of Algorithmic Police Surveillance in Belgium

Rosamunde van Brakel

Vrije Universiteit Brussel, Belgium
rosamunde.van.brakel@vub.be

Abstract

In the last decade and more recently triggered by the COVID-19 pandemic, algorithmic surveillance technologies have been increasingly implemented and experimented with by the police for crime control, public order policing, and as management tools. Police departments are also increasingly consumers of surveillance technologies that are created, sold, and controlled by private companies. They exercise an undue influence over police today in ways that are not widely acknowledged and increasingly play a role in the data capture and processing that feeds into larger cloud infrastructures and data markets. These developments are having profound effects on how policing is organized and on existing power relations, whereby decisions are increasingly being made by algorithms. Although attention is paid to algorithmic police surveillance in academic research as well as in mainstream media, critical discussions about its democratic oversight are rare. The goal of this paper is to contribute to ongoing research on police and surveillance oversight and to question how current judicial oversight of algorithmic police surveillance in Belgium addresses socio-technical harms of these surveillance practices.

Introduction

> *"Surely the most terrible and shameful thing of all is for shepherds to rear dogs as auxiliaries for the flocks in such a way that due to licentiousness, hunger or some other bad habit, they themselves undertake to do harm to the sheep and instead of dogs become like wolves."*
>
> *"Terrible," he said. "Of course."*
>
> *"Mustn't we in every way guard against the auxiliaries doing anything like that to the citizens, since they are stronger than they, becoming like savage masters instead of well-meaning allies?"*
>
> *"Yes," he said, "we must."*
>
> *"And wouldn't they have been provided with the greatest safeguard if they have been really finely educated?"*
>
> *"But they have been," he said.*
>
> *And I said, "It's not fit to be too sure about that, my dear Glaucon. However, it is fit to be sure about what we were saying a while ago, that they must get the right education, whatever it is, if they're going to have what's most important for being tame with each other and those who are guarded by them." (Plato 1968: 95)*

The quotation above comes from Plato's *Republic*. In this passage, but also elsewhere in the book, Socrates reflects on how we should prevent the guardians from abusing their power and proposes philosophy and

van Brakel, Rosamunde. 2021. How to Watch the Watchers? Democratic Oversight of Algorithmic Police Surveillance in Belgium. *Surveillance & Society* 19(2): 228-240.
https://ojs.library.queensu.ca/index.php/surveillance-and-society/index | ISSN: 1477-7487
© The author(s), 2021 | Licensed to the Surveillance Studies Network under a Creative Commons Attribution Non-Commercial No Derivatives license

education to address possible bad behavior. Through philosophy, they will study "the idea of the good" and cultivate a healthy soul. In the same vein, this article aims to address the question of how to prevent abuse of power by algorithmic police surveillance, whereby the power is not completely in the hands of humans anymore. In the last decade and more recently triggered by the COVID-19 pandemic, algorithmic surveillance technologies have been increasingly implemented and experimented with by the police for crime control, public order policing, and as management tools (van Brakel and De Hert 2011; Bennett Moses and Chan 2016; van Brakel 2016; Egbert and Leese 2020; Gandy 2019; Wilson 2019; Babuta and Oswald 2020). Police departments are also increasingly consumers of surveillance technologies that are created, sold, and controlled by private companies. They exercise an undue influence over police today in ways that are not widely acknowledged (Joh 2017) and increasingly play a role in the data capture and processing that feeds into larger cloud infrastructures and data markets (Wilson 2019). These developments are having profound effects on how policing is organized and on existing power relations, whereby decisions are increasingly being made by algorithms. Further, what is becoming increasingly clear is that the deployment of algorithmic surveillance often happens without public debate, transparency, and accountability mechanisms (Broeders et al. 2017; van Brakel 2021).

It is often claimed that the data collected by surveillance technology is anonymized or the practice is compliant with data protection law. However, human rights risks for citizens and social consequences remain. In addition, the way oversight is organized, it primarily concerns the protection of individual rights (van Brakel 2020). As van der Sloot and van Schendel (2021: 2) argue, "a legal regime that addresses incidental data harms only on an individual level runs the risk of leaving unaddressed the underlying causes, allowing structural problems to persist." This is in line with what has been shown repeatedly in the surveillance studies corpus, that consequences of surveillance inherently transcend the individual (Regan 1995, 2011; Lyon 1994; Steves 2008; Bennett 2011) through social sorting mechanisms (Gandy 1993; Lyon 2003).

This paper aims to open the debate within surveillance studies about democratic oversight of algorithmic surveillance. The main goal of the paper is to theoretically explore how judicial oversight practices in Belgium address the social and ethical risks of algorithmic police surveillance. I argue that the current Belgian police oversight constellation pays insufficient attention to what I call socio-technical harms of algorithmic police surveillance and has a judicial bias. I argue that to avoid surveillance infrastructures fading into the woodwork when they are deemed compliant with the law, oversight of algorithmic police surveillance should be approached from a socio-technical perspective. This implies attention to the political, ethical, and social choices that have been made in the development and implementation of surveillance (Bowker et al. 2010) and the social-technical harms that might result from the surveillance.

Currently, much of what has been written not only about algorithmic (police) surveillance but also about police accountability and oversight has been situated in Angel-Saxon countries. This paper aims to contribute to a growing body of literature that involves examples and case studies of algorithmic systems from non-English speaking countries (see, for instance, AlgorithmWatch 2020). To do this, the paper will explore how oversight is organized in Belgium. While some aspects of the Belgian case may not be generalizable because of characteristics inherent to the Belgian political system, the conclusions may inform our understanding of how democratic oversight of algorithmic police surveillance is conducted in Europe and also critically assess the data protection paradigm that is inspiring countries around the world (Schwartz 2019).

The paper is structured as follows: In the first part, I will give an overview of the main discussions in the literature with regards to external police oversight and, more specifically, external oversight of the use of surveillance by law enforcement. In the second part, I will discuss how external oversight of algorithmic police surveillance in Belgium is organized. In the final part, I will explore how external oversight practices in Belgium address the risk of socio-technical harms from algorithmic police surveillance.

External Oversight of Law Enforcement Uses of Surveillance Technologies

In this section, I will introduce some of the main discussions in the literature with regards to external police oversight and, more specifically, external oversight of the use of surveillance by law enforcement. Police accountability implies that police activity is not only open to scrutiny by a variety of oversight institutions but also by the public. The powers of democratically embedded police forces should be checked and controlled by the public through designated processes. Procedural justice is regarded as one of the most important building blocks in guaranteeing police legitimacy (Den Boer 2018; Feys and Verhage 2019). More specifically, in Europe, the Council of Europe proposed a European Code of Police Ethics in 2001 that:

> provides a general organisational framework for the police, their place in the criminal justice system, their objectives, performance and, with regard to oversight mechanisms, their accountability. The Code specifically sets out principles of external accountability of the police as well as those exercised internally, within police services. The Code affirms that: "The police shall be accountable to the state, the citizens and their representatives. They shall be subject to efficient external control." (Byrne and Priestly 2017)

Oversight and control are seen as ways to ensure the quality of policing and police services (Terpstra et al. 2015).

Devroe et al. (2020) provide an overview of the risks of external oversight measures identified in the literature. A first risk is regulatory capture as the result of a lack of critical attitude by the external oversight body in relation to those subject to oversight and/or too much dependence on the information that is given by those that are subject to oversight. This risk can be higher if there is a lack of time, money, and technical expertise and if the external oversight body is located (organizationally) closer to the police. A second risk is the oversight paradox. After something negative happens, the call for increased and better oversight is strong; however, after time goes by without any incidents, these calls fade away and the calls for less oversight take over (Havinga, Verbruggen, and de Waele 2015).

A third risk highlighted was the limited focus of the oversight framework. A research report that evaluated external oversight mechanisms in the Netherlands by the Scientific Council for Government Policy (WRR 2013) concluded that external oversight of the police was mainly geared toward the reduction of costs, compliance, and enforcement of the law, as well as the political-managerial function of oversight. According to the WRR (2013), this framework is too narrow. The dominant orientation on compliance and enforcement of the law means an impoverishment of oversight, and they argue for a broader approach to oversight that starts from the protection of public interests.

Devroe et al. (2020) also identify several solutions: (1) That several actors and institutes are necessary to ensure accountability, each with their own role to ensure that the police acts in the public interest and that there is one independent body that oversees this whole and has full discretion without supervision by a minister (United Nations Office on Drugs and Crime 2011). (2) The body should be accountable to the Parliament and not the executive body responsible for the police. (3) There should be sufficient funding. (4) Representatives of the oversight body should be free to bring unwelcome messages without fear of losing their job. (5) The results of investigations and the recommendations that follow from them should be transparent. (6) There should be good communication and information-exchange between external and internal oversight bodies.

In addition, according to the United Nations Office for Drugs and Crime (2011), effective police accountability implies that all police activities (from the conduct of individual police officers to police structures, policy, and funding) are not subject to internal judicial controls and oversight by public authorities only. Civilian oversight is needed for this accountability to be effective.

Historically, oversight of the police has focused on the prevention of corruption and misconduct by police officers via complaints procedures (Prenzler and Roncken 2001). Considering the potential risks of surveillance technologies, police oversight needs to encompass significantly more than merely responding to complaints about police misconduct and preventing corruption.

A research report by the European Union Agency for Fundamental Rights (2017), which explores the fundamental rights implications of surveillance practices by intelligence services, shows that all EU Member States have at least one independent body in their oversight framework. The findings, however, also identified that some of these oversight bodies remain strongly dependent on the executive: the law does not grant them binding decision-making powers, they have limited staff and budget, or their offices are in government buildings. Cayford, Pieters, and Hijzen (2019), looking at the oversight of intelligence agencies in the United States and United Kingdom, conclude that oversight mechanisms typically have a mandate concerned with one of three elements: effectiveness, cost, or proportionality. Oversight bodies were found to minimally treat the question of strict effectiveness and instead rely on the intelligence agencies to perform evaluations of effectiveness. In their study of intelligence agencies in fourteen countries, Korff et al. (2018) conclude that most countries lack effective checks and balances on mass surveillance powers. In countries where oversight systems are in place, such as the US, UK, and Germany, they have proved to be ineffective. They argue that accountability and oversight must be accompanied by consequences for any failures to meet the relevant standards: rule of law, transparency and oversight, and accountability (Korff et al. 2018).

Apart from questions of independence, a too-limited focus, and too little accountability and transparency, other research shows that oversight of surveillance practices by intelligence agencies lacks the expertise and tools to deal with new technologies. For instance, Raab (2017), who also looks at the US and UK, points out that government agencies have trouble keeping up with information and communication technology developments, and this raises issues for the effectiveness of legislation and oversight. Vieth and Wetzling (2020) argue that modern data analysis entails numerous risks in terms of data abuse and circumventing legal requirements. A lack of up-to-date tools, resources, and technical expertise serves to further undermine effective oversight. Oversight bodies need an update. They need to adopt tech-enabled instruments to respond to the technological advancements driving the intelligence field.

Although the above authors do highlight several important issues and limits of oversight models in relation to covert (algorithmic) surveillance by intelligence agencies, algorithmic surveillance used by the police can be both overt and covert and implies other types of surveillance technologies from video surveillance to predictive policing.

Broeders et al. (2017), looking at law enforcement agencies in general, argue that the current oversight of data processing by security agencies leaves a lot to be desired, even more so in view of developments in big data. Data Protection Authorities (DPAs) and the various forms of oversight on data collection and processing of security and intelligence agencies do not appear to be properly equipped to face the challenges of the big data era in terms of powers, expertise, and financial resources. Babuta and Oswald (2019) highlight, looking at police use of predictive analytics in the UK, that there is a lack of coordination and clarity regarding the delineation of responsibilities as regards scrutiny, oversight, and regulation. This lack of national coordination results in the duplication of efforts, unnecessary overspending, and a lack of compatibility and interoperability between local, regional, and national information systems. They further highlight the lack of minimum standards for the scientific validity and relevance of algorithmic outputs, which would enable the police to judge the level of confidence to assign to a prediction. The authors argue for a role for ethics committees that could test proposals against the "public good" and provide the benefit of a "fresh" pair of eyes (Babuta and Oswald 2020). Finally, when it comes to predictive policing, Mathys and Niculescu-Dinca (2020), in their study of the oversight constellation of the CAS system in the Netherlands, conclude that the current oversight constellation is lacking. They argue that it would be better to frame predictive policing as a flexible social-technical process because this leaves room for intervention in the oversight constellation and for a more a priori transparency.

The above discussion about the oversight of (algorithmic) surveillance by law enforcement paints a troubling picture of the ineffective oversight of law enforcement agencies and their use of surveillance in several countries.

Oversight of Algorithmic Police Surveillance in Belgium

In this section, I will first provide a description of algorithmic surveillance and how it has been deployed by the police in Belgium, followed by an overview of how the oversight of algorithmic surveillance is organized. Then, I will discuss one example where the oversight body stepped in and stopped a pilot test of facial recognition software by the federal police at Brussels airport.

Algorithmic surveillance is not new; twenty-six years ago, Norris (1995: 7) already wrote about algorithmic surveillance in the context of policing: "cameras coupled to sophisticated computer software allow the images to be converted into numerical data and analysed by complex algorithms. This enables the software to automatically read numberplates, calculate vehicle speed and even match facial features against a pictorial database of known offenders." Introna and Murakami Wood (2004: 181) write more generally about algorithmic surveillance and define it as "surveillance technologies that make use of computer systems to provide more than the raw data observed. This can range from systems that classify and store simple data, through more complex systems that compare the captured data to other data and provide matches, to systems that attempt to predict events based on the captured data." Although a good definition at the time, the definition could use an update that includes big data and machine learning. I propose to rephrase the definition as follows: algorithmic surveillance ranges from systems that make use of traditional algorithms to classify, store, combine, and search structured and unstructured data, compare captured data to other data, and provide matches to systems that use machine-learning algorithms to find patterns and actionable knowledge in big data sets and attempt to predict events based on the patterns found in the captured data.

In the last decade, the use of algorithmic surveillance in Belgium has expanded significantly. Since 2013, Automatic Number Plate Cameras (ANPR) have been installed and, in December 2015, the Federal Government decided to invest thirty-five million Euros to build a national shield of ANPR cameras in 260 locations in Belgium in response to the terrorist attack in Brussels in March 2015. Partly the result of smart city developments, the last couple of years have seen an expansion of the implementation of algorithmic video surveillance.[1] The COVID-19 pandemic has further accelerated the implementation of algorithmic video surveillance in Belgium (Verbergt 2021). Corona cameras, as they are being called in the Flemish press, have been installed as COVID-19 measures at the Belgian coast and in several cities in Belgium such as Ghent and Antwerp. The purpose of these cameras is to monitor busy places such as shopping streets. Other types of cameras used included heat-cameras mounted on drones to identify if people were staying in their second homes at the Belgian coast while these stays were not allowed (Belpaeme and Mariën 2020). Apart from algorithmic video surveillance, since 2016, local police have started experimenting with predictive policing (van Brakel 2020). In response to a parliamentary question about the predictive policing project of police zone Zennevallei on June 5, 2020, the former Belgian minister of Security and Home Affairs, Pieter De Crem stated that:

> different police zones are developing a methodology of predictive policing. In that respect police zone Antwerp developed such a tool in collaboration with the University of Antwerp. The Federal Police also has ambitions to optimize its analysis capacity with an eye on predictive policing. I have no direct access to the results of these studies and

[1] Since 2019, the local police in the cities of Kortrijk, Kuurne, and Lendelde (VLAS) have been using a "smart" video surveillance system developed by an American company called Briefcam. The system stores all "objects" (for example, people, small and large vehicles, and animals) that appear in the video images. An algorithm then decides what category each object belongs to, and, after this first categorization, a sub-categorization is made. The system is also able to implement facial recognition (PZVlas 2019).

> experiences. Nevertheless, my administration, the general direction Security and Prevention, is supporting the development of such a methodology, in so far it connects to the twelve recommendations that have been drafted by the European Crime Prevention Network and has been presented to the European authorities.[2] (De Crem 2020b)

The European Union's approach to dealing with algorithmic police surveillance has been to regulate the collection and processing of personal data by law enforcement in what is known as the Law Enforcement Directive (LED).[3] Oversight is the responsibility of Data Protection Authorities (DPA), who assess if collection and processing practices comply with mentioned regulation and more specific stipulations in police law and national data protection laws of member states. In response, Belgium has created a separate data protection authority that specifically oversees compliance with the Belgian translation of the LED into its data protection and police laws: Supervisory Body of Police Information (COC). Apart from the COC, the already existing police oversight body Comité P also plays a role in the oversight of new technologies, focusing specifically on compliance with national police law. Police oversight in Belgium is characterized by judicial oversight. No other forms of oversight or policy instruments or bodies exist that are specifically concerned with the use of new surveillance technology such as, for example, ethics committees or standardized evaluation procedures (van Brakel 2020).

The COC was initially established in 2015 as part of the Belgian Privacy Commission and had the responsibility for the oversight of the processing of information and data that have been stored in the General National Database, which contains information that is necessary for police services to conduct their duties. The body was reformed and became independent from the Privacy Commission as the result of the implementation of new Belgian data protection law. The new body is responsible for making sure the local and federal police agencies are compliant with the GDPR and EU law enforcement directive, the new Belgian data protection law (Belgian Ministry of Justice 2018), and the camera law (Ministry of Home Affairs 2018). The three main goals of the body are efficiency, effectiveness, and legality of police information management. In addition, they provide advice to police and policy makers, investigate complaints, and proactively conduct investigations. The body has coercive powers and can take corrective action if necessary (Schuermans 2020). Corrective measures can range from an official warning that the processing is unlawful to the suspension of a certain data flow to a temporary or permanent ban on data processing (COC 2020). The COC team consists of nine statutory staff members, which include the direction committee that consists of two magistrates and one data protection expert, the research team that consists of three members (of which two should come from the police), and a secretariat that consists out of a direction-assistant, two lawyers, and an ICT expert (Schuermans 2020).

---

[3] Original quote: "*Verschillende politiezones werken aan de ontwikkeling van de methodologie van predictive policing. Zo ontwikkelde de politiezone Antwerpen enkele jaren geleden nog een dergelijke tool met medewerking van de Universiteit Antwerpen. De federale politie ambieert eveneens om haar analysecapaciteit te optimaliseren met het oog op predictive policing. Ik heb geen rechtstreekse toegang tot de resultaten van deze studies en ervaringen. Niettemin ondersteunt mijn administratie, de algemene directie Veiligheid en Preventie, de ontwikkeling van een dergelijke methodologie, mits deze evenwel aansluit op de twaalf aanbevelingen uit het document dat is opgemaakt door het European Crime Prevention Network en dat aan de Europese instanties is voorgelegd*" (De Crem 2020b). The recommendations referred to by the minister have been drafted by the European Crime Prevention Network. The recommendations do not pay attention to legal, social, and ethical issues of predictive policing, nor are they informed by existing research into effectiveness of predictive policing. For instance, one of the recommendations states: "no legislative difficulties as long as you stay away from individuals" (European Crime Prevention Network 2020).

[3] Directive (EU) 2016/680 of the European Parliament and of the Council of April 27, 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, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L0680.

Comité P, the Standing Police Monitoring Committee, was set up in 1991 by the general Belgian law that regulates oversight (Ministry of Justice 1991). According to this law, oversight is intended to protect the rights that safeguard the constitution, the law of the people, and the coordination and efficiency of the police and intelligence agencies. The committee has the following tasks: responding to complaints (from citizens, police officers, police authorities, trade unions, etc.) and drafting reports, preparing and conducting thematic or more general monitoring studies, conducting criminal investigations, and formulating advice and recommendations (Comité P 2019). According to the law, the members of the committee "have to have seven years' experience in the domains of criminal law or criminology, public law, or management skills that have been built up through previous experience, which is similar to the work, activities and organization of the police and intelligence services" (Ministry of Justice 1991: Article 4). Comité P follows up some investigations that concern surveillance technologies. Seeing as not all reports of investigations are public, it is not transparent how many they conduct.

Official policy documents from 2019 about the budget of the COC and Comité P show that there is a significant shortage of personnel and no new people are being recruited. The documents state that the investments are too low to function properly, especially with the increased workload. So, even though Comité P is also responsible for potential investigations, they don't have the budget, staff, or expertise to play a significant role in the oversight of algorithmic surveillance (van Brakel 2020). Even though the COC is a small organization with limited resources, they have been very active and have conducted several investigations,[4] including one related to algorithmic police surveillance that I will discuss more in detail below.

In early 2017, the Belgian Federal Police started a pilot project at Brussels airport to try out a new facial recognition system. The system had four cameras and functioned in two phases. The system continuously individualized the video images through a biometric template of people whereby snapshots are created. These snapshots are stored and linked to blacklists of people who are suspected of a crime. When there is a positive link, a hit is created. During the test phase, the number of false positives was very high. As a result, in March 2017, the testing of this system was stopped. However, during a visit by the Supervisory Body of Police Information (COC), it was found that the system was still partially active. Snapshots of all passengers in the airport were still being taken but without the comparison to a blacklist being performed. To be able to keep testing the system, it had to store the images for a minimum amount of time (COC 2019). The COC launched an investigation in which they concluded that the police had not conducted a data protection impact assessment (DPIA), did not inform the COC about the pilot project, and thus set up an illegal database. As the result of the investigation, they enforced a corrective measure asking for a temporary ban of the pilot project (COC 2019).

As a result of the investigation of the COC, a working group has been launched with legal experts and practitioners from different domains of the federal and local police. The goal is to broaden the discussion to the processing of biometrical data by the police in general. According to the minister, what kind of processing of biometrical data would be interesting for the police and in what way legal texts need to be adjusted to make the processing possible in the future is being investigated, as this can lead to "efficiency profit" for the security services (De Crem 2020a).[5]

---

[4] The website (https://www.controleorgaan.be/nl/publicaties/rapporten) lists seven reports of investigations in 2020–2021. See also the activity report for 2016–2019: https://www.controleorgaan.be/files/Activiteiten-verslag_COC_2016-2019_NL.pdf.

[5] Answer of the former minister of Home Affairs De Crem to a parliamentary question: "*Ondertussen zijn verschillende juristen van de federale politie aan de slag gegaan om een extra juridische analyse uit te voeren. Deze werd mij ondertussen bezorgd en de contacten met het COC hierover zijn lopende. Bovendien werd binnen de geïntegreerde politie ook een werkgroep opgestart met zowel juristen als terreinexperten vanuit de verschillende domeinen van de federale en lokale politie. Dit met de bedoeling om de juridische analyse niet enkel te beperken tot facial recognition maar ze breder open te trekken naar de verwerking van biometrische gegevens in het algemeen. In de eerste plaats werd nagegaan welke verwerkingen van biometrische gegevens in de toekomst wenselijk zouden zijn voor politie. De*

In conclusion, algorithmic police surveillance in Belgium is governed by weak *ex post* judicial oversight, which is not independent from the police or the executive and is underfunded. Although the COC does provide some results with regards to halting illegal practices, the limited scope of their mandate leaves the door open for many of the social and ethical issues of algorithmic police surveillance.

Discussion

As became clear in the previous section, oversight of algorithmic police surveillance in Belgium is *ex post* judicial oversight that is characterized by compliance with data protection regulation. This approach raises two significant issues. First, data protection law applies only to surveillance technologies that collect and/or process personal data, and hence does not apply to algorithmic police surveillance that does not collect or process personal data. An important characteristic of algorithmic police surveillance is that analyses are often conducted on an aggregated level and, therefore, no personal data are processed. Many of the algorithmic surveillance technologies that have been implemented in Belgium are not investigated by the COC as they do not process personal data such as predictive policing. It is not because no personal data are processed that the algorithmic surveillance does not pose any risks for individuals, communities, or society (Broeders et al. 2017; Mann and Metzner 2019; van Brakel, 2020; van der Sloot and van Schendel 2021).[6] Moreover, the narrow focus on regulating the collection and processing of personal data ignores the socio-technical practices that characterize algorithmic police surveillance.

Not only is data protection law limited but the focus of the oversight of the COC is limited as well. As the result of limiting oversight to judicial oversight, there is a lack of attention to the wide-ranging effects of algorithmic police surveillance. Underlying these ideas of judicial oversight is a belief that the government and its agencies are the appropriate instruments to make sure that surveillance is controlled and laws are enforced, even though governments have a history of ineffective and inappropriate use of technology and there are historical-political agendas that are driving government decisions about surveillance (Byrne 1983). In a report titled *Surveillance: Citizens and the State* prepared by the Constitution Committee of the UK House of Lords in 2010, the authors indicate that judicial oversight alone is not sufficient to deal with surveillance:

> 324 We do not believe that the Government should confine themselves to questions of legal authorisation and compliance when seeking to improve surveillance practices. Although proper legal regulation is clearly necessary and important, we believe that the law alone cannot prevent individuals and institutions from abusing their surveillance powers. We agree with the JCHR that concentrating on legal responses is unlikely to generate the required level of commitment to human rights or concern for privacy amongst public sector staff.
>
> 325 In addition, ensuring compliance with the law may not lead to an increase in public trust and confidence. Surveillance and data handling practices that are perfectly legal may nonetheless be undesirable according to other broader ethical or constitutional criteria. (House of Lords Constitution Committee 2010)

---

behoeften werden daartoe ondertussen geïnventariseerd en juristen bekijken momenteel welke teksten dienen aangepast te worden om meer futureproof te kunnen zijn om bepaalde verwerkingen van biometrische gegevens in de toekomst mogelijk te maken voor de politiediensten. Want in dit soort verwerkingen kan efficiëntiewinst geboekt worden bij de veiligheidsdiensten" (De Crem 2020a).

[6] The proposed new EU regulation on artificial intelligence does solve this issue by regulating algorithmic police surveillance that does not collect personal data. See: https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence-artificial-intelligence.

In this respect, Raab (2015: 296) rightly asks if this type of oversight "is strong enough in practice to counter the wide-ranging effects of surveillance." According to Raab (2015: 296), "data protection authorities (DPAs) as external overseers and regulators typically focus upon the privacy-related implications of surveillance and find it difficult or impossible to embrace a wider perspective of values in their regulatory exhortations and enforcement practice. The laws within which they operate do not normally give them a licence to roam across the range of values to invoke when they seek to limit surveillance."

I propose to call these wide-ranging social and ethical effects of algorithmic police surveillance socio-technical harms. They are socio-technical in the sense that the harms are caused by an interplay of existing social structures and technology. It emphasizes that a focus on technological harms ignores the already existing issues and non-technological harms of police policy and practice. There is increasing evidence that police use of algorithmic surveillance is discriminatory towards vulnerable groups in society and poses risks for human rights in general (van Brakel 2016; Lum and Isaac 2016; Ferguson 2017; Buolamwini 2017; Noble 2018; Fussey and Murray 2019; Williams and Kind 2019; Babuta and Oswald 2020; Robertson, Khoo, and Slong 2020). Discrimination and privacy are not the only issues; the right to freedom of expression and association, for instance, has also been indicated as at risk in relation to facial recognition software (see Fussey and Murray 2019).

Good illustrations of the socio-technical harms of algorithmic police surveillance are two recent cases in the United States where black men were wrongfully arrested by Detroit Police as the result of a flawed match made by a facial recognition algorithm. The harms for these individuals in question include stigmatization, humiliation, and diminishment of their life chances. One of the men lost his job and his car as a result. These examples not only raise issues about the faulty algorithms but also about the way in which police rely on them as well as police culture and practice. The harms happened in both cases through an interplay of flawed technology with poor police work. In both cases, the men did not resemble the person they were looking for at all. Even though the police had a picture of the person they were looking for, they did not acknowledge that the algorithm had made a mistake (Hill 2020; O'Neill 2020). This is in-line with findings about the London Live Facial Recognition (LFR) Trials by Fussey and Murray (2019), who conclude that there is a "presumption to intervene" on behalf of human operators assessing the credibility of LFR matches. This tendency of deference to the algorithm also exists despite the computer being either incorrect or not verifiably correct in a large majority of cases.

The lack of attention for socio-technical harms caused by oversight in Belgium can be illustrated by the following recent example. In 2013, in response to the terrorist threat that Europe was facing at the time, Antwerp police installed high-quality cameras in the Jewish Quarter. In March 2021, one of the biggest Flemish newspapers reported that Antwerp police were using these cameras to monitor compliance with COVID-19 measures. Even though this is a classic example of function creep and questions arise about the possible discrimination of a certain religious group, the COC concluded that there was no problem, as the practice was compliant with the law. The purpose limitation of the cameras is that they can be used by the police to fulfill all their administrative and judicial tasks (Bové 2021). Social and ethical risks were not considered. In this case, questions arise as to what extent the lack of independence of the COC played a role, apart from the narrow assessment. As the American writer Audre Lorde ([1984] 2007) famously wrote, "the master's tools will never dismantle the masters' house," and as the United Nations Office on Drugs and Crime (2011) report also underlined, oversight needs to be able to act independently from the police to be effective.

Not only is the lack of attention for socio-technical harms and the COC's lack of independence troubling but also that oversight is primarily organized after investments in surveillance technologies have already taken place. Both discussed Belgian oversight committees have the possibility to launch proactive investigations, but these are conducted when police have already invested in the technology. Similarly, DPIAs are often only conducted after investment. This type of oversight allows investments in surveillance technology, which can cause socio-technical harms and have a significant impact on policing. In addition, there is a lack of minimum standards for the scientific validity and relevance of algorithmic outputs, a lack

of independent evaluations of the surveillance conducted, and a lack of socio-ethical oversight that asks questions about whether the algorithmic surveillance technologies are in the interest of the public.

Finally, what becomes clear is that—even though the United Nations Office on Drugs and Crime (2011) emphasized the need for civilian involvement to have effective oversight and article 35(9) in the GDPR states that when conducting DPIAs "where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing" (European Parliament and Council 2018)—in Belgium, there is a complete lack of involvement of the subjects of the algorithmic surveillance in police oversight mechanisms, and public scrutiny is made difficult, as the use of algorithmic police surveillance is not transparent.

Conclusion

In this paper, I explored the emergence of algorithmic police surveillance in Belgium and how the oversight of this surveillance is organized. In the introduction, I raised the question of how judicial oversight deals with the social and ethical risks of algorithmic police surveillance. Looking at Belgium, I conclude the following: (1) algorithmic police surveillance challenges traditional oversight mechanisms; (2) judicial oversight is insufficient to deal with the wide-reaching socio-technical harms that can be the result of algorithmic police surveillance; (3) oversight is not independent and there is no involvement of members of the public; and (4) the oversight is organized *ex post*, which allows socio-technical harms to already happen before the oversight takes place.

Algorithmic police surveillance tends to fade into the woodwork when it gets a data protection stamp of approval or does not (seem to) process personal data. This paper has shown that external oversight of algorithmic surveillance activities by the police in Belgium is concerning. In 2009, Murakami Wood already observed that "most governments do not use any robust methods by which they might be able to assess proposed surveillance technologies, either in themselves or in comparison to other technologies or indeed to non-technological options" (2). We are now twelve years later, and not much seems to have changed. As the Snowden revelations showed, it is easy to violate rights but restoring them and regaining trust takes much longer. Democratic oversight of algorithmic police surveillance should not only be about compliance to the law but also about socio-ethical oversight that includes civil society and the subjects of algorithmic police surveillance and uses different policy instruments such as standards and regular evaluations to ensure the use of these technologies is in the public interest. To be able to address the socio-technical harms of algorithmic police surveillance, a shift is necessary in regulation and policy from a limited focus on technology to socio-technical practices and the power relations that characterize them. This could possibly avoid regulation becoming an enabler and legitimizer for surveillance (Marx 1988; Ericson and Haggerty 1997) and surveillance fading into the woodwork.

Acknowledgments

The author would like to thank Stephanie Garaglia for her proofreading of a draft version of this paper, the guest editors of this special issue, David Murakami Wood and Valerie Steeves, and the two anonymous reviewers from *Surveillance & Society*.

References

AlgorithmWatch. 2020. *Automating Society Report*. https://algorithmwatch.org/en/automating-society-2020/ [accessed March 20, 2021].

Babuta, Alexander, and Marion Oswald. 2020. Machine Learning Predictive Algorithms and the Policing of Future Crimes: Governance and Oversight. In *Policing and Artificial Intelligence*, edited by John L.M. McDaniel and Ken Pease, 214–236. London: Routledge.

Belgian Ministry of Justice 2018. Belgian Data Protection Law. July 30. https://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&table_name=wet&cn=2018073046 [accessed April 10, 2021].

Belpaeme, Leen, and Mathias Mariën. 2020. Politie zet drone met warmtecamera in: "Tweedeverblijvers opsporen in vakantieparken." *Het Laastste Nieuws*, March 28. https://www.hln.be/in-de-buurt/de-haan/politie-zet-drone-met-warmtecamera-in-tweedeverblijvers-opsporen-in-vakantieparken~a242efad/ [accessed April 10, 2021].

Bennett, Colin. 2011. In Defence of Privacy: The Concept and the Regime. *Surveillance & Society* 8 (4): 485–496.

Bennett Moses, Lyria, and Janet Chan. 2016. Algorithmic Prediction in Policing: Assumptions, Evaluation, and Accountability. *Policing & Society* 28 (7): 806–822.

Bové, Lars. 2021. Antwerpse politie mag bewakingscamera's in Joodse wijk inzetten tegen corona-inbreuken. *De Tijd*, March 30. https://www.tijd.be/politiek-economie/belgie/algemeen/antwerpse-politie-mag-bewakingscamera-s-in-joodse-wijk-inzetten-tegen-corona-inbreuken/10294547.html [accessed April 10, 2021].

Bowker, Geoffrey, Karen Baker, Forence Millerand, and David Ribes. 2010. Toward Information Infrastructure Studies: Ways of Knowing in a Networked Environment. In *International Handbook of Internet Research,* edited by Jeremy Hunsinger, Lisbeth Klastrup, and Matthew Allen, 97–117. Dordrecht, NL: Springer.

Broeders, Dennis, Erik Schrijvers, Bart van der Sloot, Rosamunde van Brakel, Josta De Hoog, and Ernst Hirsch-Ballin. 2017. Big Data and Security Policies: Towards a Framework for Regulating the Phases of Analytics and Use of Big Data. *Computer Law & Security Review* 33 (3): 309–323.

Buolamwini, Joy A. 2017. *Gender Shades: Intersectional Phenotypic and Demographic Evaluation of Face Datasets and Gender Classifiers.* PhD Diss., Massachuessettes Institute of Technology.

Byrne, Edmund. 1983. Can Government Regulate Technology? In *Philosophy and Technology*, edited by Paul T. Durbin and Friedrich Rapp, 17–-33. Boston, MA: D. Reidel Publishing Company.

Byrne, Jonny, and William Priestly. 2017. *Report on Police Oversight in the Council of Europe Countries*. Council of Europe Publishing. https://rm.coe.int/police-oversight-mechanisms-in-the-council-of-europe-member-states/168073dd36 [accessed December 20, 2020].

Cayford, Michael, Wolter Pieters, and Constant Hijzen. 2019. Plots, Murders, and Money: Oversight Bodies Evaluating Effectiveness of Surveillance Technology. *Intelligence and National Security* 33 (7): 999–1021.

COC. 2019. Executive summary Tussentijds rapport met corrigerende maatregel betreffende de visitatie bij de Federale Politie van de Luchthaven Zaventem door het Controleorgaan op de Politionele informatie met betrrekking tot het gebruik van gezichtsherkenning op de nationale luchthaven van Zaventem. https://www.controleorgaan.be/files/DIO19005_Onderzoek_LPABRUNAT_Gezichtsherkenning_Publiek_N.PDF [accessed December 20, 2020].

———. 2020. Activity Report COC 2016-2019**.** https://www.controleorgaan.be/files/Activiteiten-verslag_COC_2016-2019_NL.pdf [accessed March 20, 2021].

Comité P. 2019. *Activiteitenverslag 2018*. https://comitep.be/document/jaarverslagen/2018NL.pdf [accessed March 20, 2021].

De Crem, Pieter. 2020a. Answer to Question by Joy Donné. Integral Report, Belgian Chamber of Representatives, Commission for Home Affairs, Security, Migration and Administrative Matters, CRIV 55 COM 175, 21–22. https://www.lachambre.be/doc/CCRI/pdf/55/ic175.pdf.

———. 2020b. Answer to written question 7-591 of Peter Van Rompuy. Belgian Senate, June 5 https://www.senate.be/www/?MIval=/Vragen/ SchriftelijkeVraag&LEG=7&NR=591&LANG=nl. Den Boer, Monica. 2018. Police Oversight and Accountability in a Comparative Perspective. In *Comparative Policing from a Legal Perspective*, edited by Monica Den Boer, 7–22. Cheltenham, UK: Edward Elgar Publishing.

Devroe, Elke, Joery Matthys, Van den Broeck, and Lodewijk G. Moor. 2020. Editorial: Een algemeen kader voor toetsing van toezicht.Waarom is toezicht op de politie van belang? *Journal of Police Studies* 2: 7–22.

European Crime Prevention Network 2020. *Predictive Policing Recommendations Paper*, https://eucpn.org/sites/default/files/document/files/10._recommendation_paper_predictive_policing_update_0.pdf [accessed December 20, 2020].

European Parliament and Council. 2018. 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). April 27. https://eur-lex.europa.eu/eli/reg/2016/679/oj [accessed April 10, 2021].

Egbert, Simon, and Matthias Leese 2020. *Criminal Futures Predictive Policing and Everyday Police Work*. London: Routledge.

Ericson, Richard V., and Kevin D. Haggerty. 1997. *Policing the Risk Society*. Oxford, UK: Oxford University Press.

European Union Agency for Fundamental Rights. 2017. Surveillance By Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU Volume II: Field Perspectives and Legal Update. https://fra.europa.eu/en/publication/2017/surveillance-intelligence-services-fundamental-rights-safeguards-and-remedies-eu.

Ferguson, Andrew G. 2017. *The Rise of Big Data Policing*. New York: NYU Press.

Feys, Yinthe, and Antoinette Verhage. 2019. Morele dilemma's binnen de politie : legitimiteit onder druk? *Journal of Police Studies (Cahiers Politiestudies)* 53: 31–58.

Fussey, Peter, and Daragh Murray. 2019. *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*. Human Rights and Big Data Project University of Essex, July. https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf [accessed December 20, 2020].

Gandy, Oskar H, Jr. 1993. *The Panoptic Sort: A Political Economy of Personal Information*. Boulder, CO: Westview Press.

———. 2019. The Algorithm Made Me Do It! Technological Transformations of the Criminal Justice System. *The Political Economy of Communication* 7 (2): 3–27.

House of Lords Constitution Committee. 2010. *Surveillance: Citizens and the State*. Available at https://publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/1803.htm.

Haeck, Pieter. 2020. Gsm-signalen en camera's moeten shoppersmassa temmen, *De Tijd*, May 12. https://www.tijd.be/tech-media/technologie/gsm-signalen-en-camera-s-moeten-shoppersmassa-temmen/10226664.html [accessed December 20, 2020].

Havinga Tetty, Paul Verbruggen, and Henri de Waele. 2015 *Toezicht tegen het Licht. Kernwaarden, Kansen en Knelpunten*. Deventer, NE: Kluwer.

Hill, Kashmir. 2020. Wrongfully Accused by an Algorithm. *New York Times*, June 24. https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html [accessed December 20, 2020].

Introna, Lucas, and David Murakami Wood. 2004. Picturing Algorithmic Surveillance: The Politics of Facial Recognition Systems. *Surveillance & Society* 2 (2/3): 177–198.

Joh, Elizabeth. 2017. The Undue Influence of Surveillance Technology Companies on Policing. *New York University Law Review* 97: 101–130.

Korff, Douwe, Ben Wagner, Julia Powles, Renate Avila, and Ulf Buermeyer. 2018. *Boundaries of Law: Exploring Transparency Accountability, and Oversight of Government Surveillance Regimes*. World Wide Web Foundation, January. https://www.statewatch.org/media/documents/news/2017/jan/boundaries-of-law.pdf [accessed March 20, 2021].

Lorde, Audre. (1984) 2007. The Master's Tools Will Never Dismantle the Master's House. In *Sister Outsider: Essays and Speeches*. Berkeley, CA: Crossing Press.

Lum, Kristin, and William Isaac. 2016. To Predict and Serve? *Significance Magazine Royal Statistical Society*, October. https://rss.onlinelibrary.wiley.com/doi/epdf/10.1111/j.1740-9713.2016.00960.x [accessed July 15, 2020].

Lyon, David. 1994. *The Electronic Eye: The Rise of the Surveillance Society*. Minneapolis, MN: University of Minnesota Press.

———, ed. 2003. *Surveillance as Social Sorting. Privacy, Risk and Automated Discrimination*. London: Routledge.

Mann, Monique, and Tobias Matzner. 2019. Challenging Algorithmic Profiling: The Limits of Data Protection and Anti-Discrimination in Responding to Emergent Discrimination. *Big Data & Society* (July–December): 1–11.

Marx, Gary T. 1988. *Undercover: Police surveillance in America*. Berkeley, CA: University of California Press.

Mathys, Joery, and Vlad Niculescu-Dinca. 2020.Overseeing Prediction: The Unavoidable Paradox of Providing Oversight Mechanism for Future-Oriented Predictions. *Journal of Police Studies* 55: 49–64.

Ministry of Home Affairs. 2018. Updated Camera Law 2018. March 21. http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&table_name=wet&cn=2018032121 [accessed April 10, 2021].

Ministry of Justice. 1991. Belgian Oversight Law 1991. July 18. https://www.ejustice.just.fgov.be/cgi_loi/change_lg_2.pl?language=nl&nm=1991009963&la=N [accessed April 10, 2021].

Murakami, Wood, David. 2009. A New "Baroque Arsenal"? Surveillance in a Global Recession. *Surveillance & Society* 6 (1): 1–2.

Noble, Safiya U. 2018. *Algorithms of Oppression: How Search Engines Reinforce Racism*. New York: NYU Press.

Norris, Clive. 1995. Video Charts. Algorithmic Surveillance. *Criminal Justice Matters* 20: 7–8.

O'Neill, Natalie. 2020. Faulty Facial Recognition Led to His Arrest—Now He's Suing. *Motherboard VICE*, September 4. https://www.vice.com/en_us/article/bv8k8a/faulty-facial-recognition-led-to-his-arrestnow-hes-suing [accessed December 20, 2020].

Plato. 1968. *The Republic of Plato*, 2nd edition. Translated by Allan Bloom. New York: Basic Books.

Prenzler, Tim, and Carol Ronken. 2001. Models of Police Oversight: A Critique. *Policing and Society* 11 (2): 151–180.

PZVlas. 2019. Persnota – woensdag 22 mei 2019. Primeur - Veiligheidscamera's PZ Vlas worden eerste online en offline slimme camera's van Vlaanderen. May 22. https://www.pzvlas.be/fileadmin/MEDIA/website/documenten/nieuwsberichten/20190522_-_Persnota_slimme_camera_s_-_BriefCam.pdf [accessed December 20, 2020].

Raab, Charles. 2015. Effects of Rights and Values on the Oversight of Information Systems. In *Surveillance in Europe*, edited by David Wright and Reinhard Kreissl, 259–267. London: Routledge.

———. 2017. Security, Privacy and Oversight. In *Security in a Small Nation. Scotland, Democracy and Politics,* edited by Andrew W. Neal, 77–102. Cambridge, UK: Open Book Publishers.

Regan, Priscilla. 1995. *Legislating Privacy: Technology, Social Values and Public Policy*. Chapel Hill, NC: University of North Carolina Press.

———. 2011. Response to Bennett: Also in Defense of Privacy. *Surveillance & Society* 8 (4): 497–499.

Robertson, Kate, Cynthia Khoo, and Yolanda Slong. 2020. *To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada*. Citizen Lab and the International Human Rights Program. https://citizenlab.ca/wp-content/uploads/2020/09/To-Surveil-and-Predict.pdf [accessed December 20, 2020].

Schuermans, Frank. 2020. Een (ver)nieuw(d)e actor in het Belgische system van extern politoneel toezicht: het Controleorgaan op de Politionele Informatie (COC). *Journal of Police Studies* 55: 99–124.

Schwartz, Paul. 2019. Global Data Privacy: The EU Way. *New York University Law Review* 94: 101–146.

Steeves, Valerie. 2008. Reclaiming the Social Value of Privacy. In *Lessons from the Identity Trail,* edited by Ian Kerr, 191–208. Oxford: Oxford University Press.

Terpstra, Jan, Alain Duchatelet, Jelle Janssens, Dominique Van Rhijkeghem, and Peter Versteegh. 2015. Verantwoording en politie: een verkenning. *Journal of Police Studies* 4 (37): 91–117.

United Nations Office on Drugs and Crime. 2011. *Handbook on Police Accountability, Oversight and Integrity*. Criminal Justice Handbook Series. New York: United Nations.

van Brakel, Rosamunde. 2016. Pre-Emptive Big Data Surveillance and Its (Dis)Empowering Consequences: The Case of Predictive Policing. In *Exploring the Boundaries of Big Data*, edited by Bart van der Sloot, Dennis Broeders and Erik Schrijvers, 171–141. Amsterdam, NE: Amsterdam University Press.

———. 2020. Een refectie over het huidig toezicht van het gebruik van surveillancetechnologie door de lokale politie in België. *Journal of Police Studies* 55: 139–160.

———. 2021. Rethinking Predictive Policing: Towards a Holistic Framework of Democratic Algorithmic Surveillance. In *The Algorithmic Society: Technology, Power and Knowledge*, edited by Marc Schuilenberg and Rik Peeters, 104–118. London: Routledge.

van Brakel, Rosamunde, and Paul De Hert. 2011. Policing, Surveillance and Law in a Pre-Crime Society: Understanding the Consequences of Technology-Based Strategies. *Journal of Police Studies* 20 (3): 163–192.

Van der Sloot, Bart, and Sasha van Schendel. 2021. Procedural Law for the Data-Driven Society. *Information & Communications Technology Law*. https://www.tandfonline.com/doi/full/10.1080/13600834.2021.1876331.

Verbergt, Mathias. 2021. Ook in andere steden komen er in sneltempo camera's bij. *De Standaard* March 13. https://www.standaard.be/cnt/dmf20210312_98153156 [accessed April 10, 2021].

Vieth, Killian, and Thorsten Wetzling. 2020. Data-Driven Intelligence Oversight: Recommendations for a System Update. SSRN, January 9. http://dx.doi.org/10.2139/ssrn.3505906.

Williams, Patrick, and Eric Kind. 2019. *Data-Driven Policing: The Hardwiring of Discriminatory Policing Practices across Europe*. ENAR. https://www.enar-eu.org/IMG/pdf/data-driven-profiling-web-final.pdf [accessed March 1, 2021].

Wilson, Dean. 2019. Platform Policing and the Real-Time Cop. *Surveillance & Society* 17 (1/2): 69–75.

Wetenschappelijke Raad voor Regeringsbeleid (WRR). 2013. Toezien op publieke belangen. Naar een verruimd perspectief op Rijkstoezicht. WRR Report 89. https://www.wrr.nl/publicaties/rapporten/2013/09/09/toezien-op-publieke-belangen.-naar-eenverruimd-perspectief-op-rijkstoezicht [accessed March 1, 2021].