Information Polity 27 (2022) 219–232
DOI 10.3233/IP-211538
IOS Press

The sensitive nature of facial recognition: Tensions between the Swedish police and regulatory authorities[1]

Marie Eneman[a,*], Jan Ljungberg[a], Elena Raviola[b] and Bertil Rolandsson[c,d]
[a]*Applied IT, University of Gothenburg, Sweden*
[b]*Academy of Art and Design, University of Gothenburg, Sweden*
[c]*Sociology and Work Science, University of Gothenburg, Sweden*
[d]*Sociology, Lund University, Sweden*

Abstract. Emerging technologies with artificial intelligence (AI) and machine learning are laying the foundation for surveillance capabilities of a magnitude never seen before. This article focuses on facial recognition, now rapidly introduced in many police authorities around the world, with expectations of enhanced security but also subject to concerns related to privacy. The article examined a recent case where the Swedish police used the controversial facial recognition application Clearview AI, which led to a supervisory investigation that deemed the police's use of the technology illegitimate. Following research question guided the study: How do the trade-offs between privacy and security unfold in the police use of facial recognition technology? The study was designed as a qualitative document analysis of the institutional dialogue between the police and two regulatory authorities, theoretically we draw on technological affordance and legitimacy. The results show how the police's use of facial recognition gives rise to various tensions that force the police as well as policy makers to rethink and further articulate the meaning of privacy. By identifying these tensions, the article contributes with insights into various controversial legitimacy issues that may arise in the area of rules in connection with the availability and use of facial recognition.

Keywords: Surveillance, facial recognition, privacy, affordances, legitimacy, police authority, regulatory authorities, institutional dialogue, qualitative document analysis

Key points for practitioners:

- The study contributes to the public debate by highlighting how trade-offs between privacy and security unfold in the police use of facial recognition.
- The study shows how the police's use of facial recognition gives rise to various tensions that force the police as well as policy makers to rethink and further articulate the meaning of privacy.
- The study highlights the urgent need for the police to establish organizational routines to evaluate efficiency of new technologies as well as a model to assess impact.

1. Introduction

Emerging technologies with developments in artificial intelligence (AI) and machine learning (Kitchin, 2017) are laying the foundation for surveillance capabilities of a magnitude never seen before, creating a

[1]This article received a correction notice (Erratum) post publication with DOI 10.3233/IP-229012, available at http://doi.org/10.3233/IP-229012.

*Corresponding author: Marie Eneman, Applied IT, University of Gothenburg, Sweden. E-mail: marie.eneman@ait.gu.se.

paradigm shift in surveillance referred to as "algorithmic surveillance" (Kosta, 2022; Murphy, 2017). Significant changes in today's surveillance system are that they have become more powerful, pervasive, automated and large-scale in the collection, analysis, storage and sharing of data (Lyon, 2014, 2019; Eneman et al., 2020). These surveillance capabilities have emanated from early discreet surveillance technologies into a growing assemblage of devices, digital infrastructure, cloud-based personal data and surveillance practices that provide real-time monitoring of citizens' whereabouts (Richards, 2013; Ball & Snider, 2020). As a consequence, surveillance has become ubiquitous, providing data on and insights into all aspects of human life, and thus conditioning human action in far-reaching ways (Flyverbom, 2019). Recent technological advances are providing previously unseen opportunities to extend the scope of surveillance, making it increasingly powerful and embedded in our daily lives (Kosta, 2022; Lyon, 2014; 2018).

In this article, we address the implications of one of the latest innovations in surveillance, namely, facial recognition technology, which is now rapidly introduced within police authorities around the world, justified by the need to enhance public security (Smyth, 2019; Bragias et al., 2021). However, facial recognition is also associated with concerns about far-reaching risks and threats to important democratic values as individuals' privacy (Ball & Webster, 2020; Madiega & Mildebrath, 2021; McSorley, 2021). Privacy is closely connected and intertwined with surveillance and, in line with previous research, we recognize that the term privacy in today's society is often defined as the right to control information about oneself (Véliz, 2020; Hildebrandt, 2020). One of the main challenges with the term privacy is, however, its vagueness (Solove, 2006; Richards, 2013).

Facial recognition refers to automated systems for identifying human biometrics (Smyth, 2019). Human facial images constitute biometric data that are more or less unique, that cannot be changed naturally and that cannot be easily hidden in society. Therefore, they are easy to capture in public spaces, in contrast to other forms of biometrics such as fingerprints or DNA (Smith & Miller, 2021).

In view of their sensitive nature, the European Commission (EC) has recognized facial images as a "special category of personal data" or "sensitive data", where the most relevant legal instrument is the Data Protection Law Enforcement Directive (Dir. EU2016/680). The EC recently (April 2021) presented a proposal for a new regulation on AI systems with the aim to benefit from emerging technologies while safeguarding fundamental rights and values. In the proposal, facial recognition was defined as "a high-risk technology" and suggested harmonizing regulations of AI technologies in the European Union (COM (2021) 206 final). In addition, the European Parliament recently (October 2021) called for a ban on police use of facial recognition in public places, as well as of private facial recognition databases such as Clearview AI (Heikkilä, 2021). This further illustrates the technology's intrusive properties and the risk of purpose slippage once the technology is implemented, further eroding police legitimacy (Bradford et al., 2020; Brayne, 2021).

In this article we set out to examine how the police use of facial recognition technology is shaped by the interplay between the regulatory authorities and the mandate to determine how technological affordances can be materialized. More precisely, the article examines a recent case where the Swedish police used the controversial facial recognition technology Clearview AI, which led the supervisory authority, the Swedish Authority for Privacy Protection (IMY), to conduct a supervisory investigation. They concluded that the police's use of the technology was unlawful, and issued a penalty of 2,500,000 SEK (ca. 250,000 Euro). The police appealed the IMY's decision to a higher court, the Administrative Court, and the Court recently announced that they rejected the police's appeal. According to Rezende (2020), the police in several countries have used facial recognition technology for a while now; however, as emphasized by Rezende, the Clearview AI application goes far beyond other traditional facial recognition technologies.

By using this recent case we are able to empirically analyze the institutional dialogue between the three authorities, and show how the Police Authority, the IMY and the Court reason and negotiate in interaction with each other about technological, organizational and legal aspects of the police use of facial recognition. In this article we recognize the importance of controversies surrounding these issues, and aim to unpack and nuance the trade-off between security and privacy that emerges in relation to new powerful surveillance technologies. Our research question was: How do the trade-offs between privacy and security unfold in the police use of facial recognition technology?

2. Theoretical foundation

The article draws on institutional theory (Thornton et al., 2012; Raviola & Norbäck, 2013) and sociomateriality (Orlikowski & Scott, 2008) which allows us to address and focus on the relation between technological possibilities and their institutional embeddedness (Kallinikos et al., 2013). We address the impact that the regulatory dimension (Black & Murray, 2019) has on how police authorities are able to organize surveillance practices conditioned by emerging digital technologies (Schatzki, 2019). Surveillance therefore is shaped by the interplay between digital technologies affording surveillance practices (Brayne, 2021; Lyon, 2018), and institutional forces that condition the realization of those affordances in practice. The analysis focuses on the trade-offs in the use of facial recognition technology between enhancing public security and, at the same time, protecting the individual's right to privacy (Solove, 2006; Richards, 2013), forging logics of action that underpins the recognition of police surveillance as legitimate. Thus, the notions of *technological affordances* and *legitimacy* emerge as especially important here.

Technological affordances can be understood as sociomaterial assemblages that are made meaningful as parts of organizational and individual contexts and are enacted in practice. In this context, affordance refers to the co-constitutive relation between technology and humans that offers a set of potential actions for the user of the technology (Norman, 1999; Faraj & Azad, 2012). Advancements in AI and machine and deep learning algorithms have changed surveillance methods in a fundamental way (Kosta, 2022; Murphy, 2017). Facial recognition technologies afford great potential for surveillance, enabling personal identification by using universal, unique, constant, recordable and measurable data on individuals (Smith & Miller, 2021). These emerging technologies draw on the vast amount of data that are generated from digital services, social media, and devices designed for purposes other than surveillance, but that can feed into surveillance processes. Data collection can also be done by specific devices such as cameras, sensors, and Global Positioning System (GPS) devices, either to be analyzed in batches, in real time, or to be used to train machine learning algorithms for later automatic monitoring. When put to use, the functionality and reach of a machine learning algorithm are not only hidden in its formula, or in the code that implements it, but are also found in the wider assemblage of hardware, data, and different groups of users (Kitchin, 2017). Over the last two decades we have witnessed a convergence of earlier discreet surveillance technologies into a ubiquitous surveillance assemblage that operates by "abstracting human bodies from their territorial settings and separating them into a series of discrete flows [...] reassembled into distinct 'data doubles' which can be scrutinized and targeted for intervention" (Haggerty & Ericson, 2000, p. 606).

This transformation of discreet surveillance technologies into a ubiquitous surveillance assemblage is strongly linked to privacy concerns, (Solove, 2006). This article analyses how regulatory conditions for maintaining privacy (Hildebrandt, 2020) depend on the interplay between the emergence of digital technologies affording an assemblage of surveillance practices (Lyon, 2018), and the institutional forces that condition the realization of those affordances. In the analysis, we recognize that this interplay is

characterized by a tense struggle over privacy and we discuss trade-offs between security and privacy. In doing so, we scrutinize how involved government actors in their construction of privacy encounter different legitimacy issues (Bradford et al., 2020), revolving around an act of balance between risks and benefits of surveillance that can be framed as appropriate in a contemporary democracy (Ball & Webster, 2020).

Legitimacy refers to the generalized perception or assumption that the actions of an entity are desirable, proper, or appropriate within some socially constructed system of norms, values, beliefs and definitions (Suchman, 1995). Based on doctrines and norms in terms of which the use of emerging technologies such as facial recognition is justified, legitimacy depends on whether and how the police are able to call upon sufficient other authorities, or centres of power, to facilitate the recognition of the police's authority and enhancing police effectiveness (Stinchcombe, 1968). To minimize the consequences of criticism and continue using surveillance, realizing technological affordances the way they were set out to be realized, the police have to gain recognition and legitimacy from other actors in the field. In analyzing the dynamic that unfolds, this article therefore examines how the police, in an institutional dialogue (Tremblay, 2005) with other regulatory actors, recognize how different surveillance technologies can afford measures that both enhance public security and facilitate police responsibility for citizens' security by improving police efficiency (e.g. when enforcing the law) (Brayne, 2021).

Compromises and trade-offs constitute a central empirical unit in this analysis. The realization of legitimacy is, then, related to how the advancements of technology emerge as such, but even more importantly, to how technological affordances are embedded and addressed in the different societal institutions, regulations and policies. Concretely, this means that we will look into the logic underpinning the recognition of legitimate forms of digital surveillance by examining how police and other regulatory actors address trade-offs between, on the one hand, society's desire to enhance security and, on the other, privacy protection for individuals. By pointing to the incompleteness of digital technology, showing that it is "perpetually in the making" (Kallinikos et al., 2013, p. 357), we do then also recognize the ambivalent ontology of digital materiality, salient in technologies such as AI and machine learning. Kallinikos et al. (2013, p. 357) formulated this as follows: "They are objects yet they lack the plentitude and stability afforded traditional items and devices."

3. Research design

3.1. Setting

This study focuses on a recent case where the Swedish Police Authority was subject to sanctions for their illegitimate use of Clearview AI's facial recognition application. Clearview AI received a lot of attention in January 2020, when the *New York Times* published an internationally acclaimed article, "The secretive company that might end privacy as we know it", which revealed Clearview's business model (Hill, 2020). Prior to that, Clearview AI had deliberately worked in silence, while offering its product to law enforcement agencies in various countries as well as to private security companies. While police authorities in several countries have been using different types of facial recognition technologies for a while now, Clearview's facial recognition application goes far beyond traditional facial recognition technologies (McSorley, 2021; Rezende, 2020). The company uses an automated image scraper to scrape facial images from the open Internet (Campbell, 2019), not least from social media platforms such as Facebook, Instagram and Twitter. The images are being used by the company to build a giant biometric database that currently contains more than three billion images. Clearview sells access to this database to

law enforcement agencies and private security companies. The application can be used free of charge during a test period of two weeks. When Clearview's customer list was leaked (Buzzfeed, 2020), it was revealed that authorities in several Western countries outside the USA, including Sweden, have used the application. The list also showed that several authoritarian regimes were customers of Clearview, which has further contributed to the debate on Clearview AI as a highly controversial technology. The EC has pointed out that the ability of Clearview AI to protect data is highly questionable and has not been tested by an independent party, further pointing to the risk that millions of EU citizens sharing personal photos on social media platforms will now likely exist in the company database (Rezende, 2020).

In early 2020, the Swedish national media (e.g. Carlsson & Rosén, 2020) drew the public's attention to Clearview AI and revealed that the Swedish police was using Clearview's facial recognition application. The IMY reacted quickly to the media reporting and initiated the abovementioned supervisory investigation (Dnr DI-2020-2719) early in March 2020. The investigation consisted of the IMY formally asking the Police Authority to describe and clarify past, present and planned future use of Clearview AI by any part of the police organization, the details of this use in terms of purpose, time and scope, and any organizational and technical routines in place in relation to the facial recognition technology. Based on this investigation, the IMY concluded, in their decision on 10 February 2021 (Dnr DI-2020-2719), that the police's use of Clearview AI was illegitimate, and that the Police Authority must pay a sanction fee of SEK 2,500,000 for violations of the Criminal Data Act. In addition, the Police Authority was instructed to train its staff to ensure that they did not handle personal data in violation of the applicable law, that they inform the persons whose images had been entered into Clearview AI, and that they ensure that the personal data entered in the Clearview AI application to be deleted. In March 2021, the Police Authority appealed this decision to the Administrative Court. The Court's verdict, however, completely rejected the police's appeal and found that the processing of biometric data was in itself of a sensitive nature and involved special risks, which made the violation of privacy very serious in this case. This case has provided us with a rich material illustrating how the three authorities negotiated in what we view as an institutional dialogue (Tremblay, 2005) about the police's use of a facial recognition technology.

3.2. Document collection and analysis

The empirical material collected and analysed for this article consists of public documents from the three authorities: the IMY, the Police Authority and the Administrative Court in Stockholm. Access to public documents in Sweden is regulated by the "Principle of public access to information", a basic principle that is regulated by one of Sweden's fundamental laws – the Freedom of the Press Act (1949:105). This principle gives the public the right to access public documents unless they are covered by confidentiality. In Sweden, documents are defined as public if they are: held by a public authority; and considered under specific rules to have been received or drawn up by such an authority. We contacted the three authorities via e-mail and formally requested the public documents, stating that we wanted access to all documents regarding the Swedish police's use of Clearview AI, as our inclusion criteria. The documents were sent to us by e-mail within two-five days.

Previous research (Bowen, 2009; King & Brooks, 2019) has highlighted that document can be a rich source of data. Gross (2018, p. 2) states that document analysis is a "viable independent" method that should not only be seen as a complement to other methods. Bowen (2009) emphasizes that it is important for researchers to read documents through a critical lens, i.e. not to regard formal documents as "neutral" but to show awareness that the documents were created and conditioned for a specific purpose. The documents collected in this study were created by lawyers, which means that what is expressed in the

Table 1
Overview of the collected documents

Authority	Type of document
The Swedish Authority for Privacy Protection (IMY)	*Investigation into the use of Clearview AI* (Dnr DI-2020-2719, date: 2020-03-05) *Request for supplementation* (Dnr DI-2020-2719, date: 2020-03-30) *Decision after the inspection* (Dnr DI-2020-2719, date: 2021-02-10)
The Swedish Police Authority	*Investigation into the use of Clearview AI* (Dnr A126.614/2020, date: 2020-03-19) *Request for supplementation* (Dnr A126.614/2020, date: 2020-05-07) *Appeal regarding the IMY's decision* (Dnr A126.614/2020, date: 2021-03-01) *Completion of previously filed appeal regarding the IMY's decision* (Dnr A126.614/2020, date: 2021-03-05)
The Administrative Court in Stockholm	*Decision of the Administrative Court* (Cnr 4756-21, date: 2021-09-30)

documents is largely based on lawyers' perceptions and reasoning about the use of an emerging facial recognition technology.

This study has been designed as a qualitative document analysis (Gross, 2018) and we have used thematic analysis (King & Brooks, 2019) to identify emerging patterns and themes related to how the various authorities reasoned and negotiated in interaction with each other about technological, organizational and legal aspects of facial recognition technology. We started by reading all the material; next, we discussed our first interpretation within the research group. To formulate a more detailed understanding of what was expressed, we proceeded by reconstructing the process. During this process, we engaged in a first phase of coding, which allowed us to identify how the different actors perceived the police use of facial recognition. By then re-reading the documents in more depth (King & Brooks, 2019) and discussing possible links between coded text segments (Gubrium & Holstein, 2009), we were able to identify three emerging themes as central, they are outlined in the next section.

4. Results

Our analysis of the institutional dialogue around the police use of the Clearview AI facial recognition identified the following three themes, which emerge as tensions, in the unfolding of the trade-offs between the desire to enhance public security and the strive to protect the individual's privacy.

4.1. Effectiveness versus privacy – the sensitive nature of facial recognition technology

The institutional dialogue we analyzed in this article offers different ways of framing the new technological affordances of Clearview AI as legitimate or illegitimate, which are embedded in the institutional mandate and logic of action of the three public authorities. The Swedish Police Authority's mandate is to keep public order and security; the IMY's mandate is to hold the police accountable for respecting individual privacy; finally, the mandate of the Administrative Court, due to the appeal, was to settle the dispute. This relationship between the authorities is worth noting as it represents the institutional context where trade-offs between security and privacy were negotiated. In other words, the mission, logic

of action and relation between the three authorities shape the institutional embeddedness in which the affordances of Clearview AI were used and framed and, finally, ruled as legitimate or illegitimate.

The police expressed an understanding of how the trade-offs between security and privacy are realized by the pervasive nature of facial recognition technology. Responding to the IMY's supervisory investigation, they showed how they, as a public authority, struggled to balance the tempting potential of the new powerful technology, against protecting individuals' privacy. The police argument was:

> *Tools that facilitate the police's criminal investigation activities are always welcome but there needs to be a balance between the authority's need for more effective tools and the consequences for the privacy of individuals.* (A126.614/2020, p. 1)

The police further stated that they continuously strove to maintain a balance. This points at a negotiated compromise that acknowledges an acceptable give and take between "the authority's need for more effective tools" and "the consequences for the privacy of individuals". While the appeal for the protection of individuals' privacy, made by all three authorities, often seems to be treated as a black-box and unquestionable principle, some parts of the institutional dialogue under discussion show the relation between security and privacy as a practically negotiated compromise within the police authority's logic of action and give some glimpses into how such compromise is made. The police acknowledge this "balance" to be part of their daily practical and organizational work, but in the case at hand this is put into question by the new facial recognition technology as it collects and analyses a type of data that is considered particularly sensitive, namely, biometric data. The police argued:

> *Biometric comparisons can be an absolutely necessary investigative measure when investigating specific cases of, for example, sexual abuse of children or to identify persons linked to serious organized crime.* (4756-21, p. 7)

By referring to particularly severe crimes, the police in this case tried to justify their use of biometric data and argued that the use of Clearview AI may be legitimate. In cases where crimes are considered to be very serious and organized, the police claimed that their institutional mandate to fight crime outweighed the controversial nature of data and made their use legitimate. By contrast, considering both the police's institutional mandate to fight crime and the serious risks that the access and use of biometric data implies for individuals' privacy, the Court noted the lack of impact assessment by the police, disagreed with the police on the necessity to use biometric data and therefore judged the police use of Clearview AI as illegitimate.

In the institutional framing of the trade-off between security and privacy, it is important to note that the Court's ruling did not unconditionally deprioritize the security argument, championed by the Police authority, in favor of the privacy argument, championed by the IMY. Biometric data are considered particularly sensitive in terms of privacy, but the institutional dialogue opened up the possibility for this kind of data to be used to the extent that the compromise between security and privacy is in practice considered, controlled and evaluated through "technical and organizational measures". This was also recognized by the IMY:

> *The current processing of biometric data is of a sensitive nature and involves special risks, which means high demands on technical and organizational measures to ensure constitutional processing. The guidelines do not contain any further information on the processing of biometric data or facial recognition. [. . .] The issue is therefore not specifically addressed. Nor has the Police authority shown that information has been provided in any other way about [. . .] how biometric data are to be handled in order to be considered to have been processed in accordance with the Constitution.* (4756-21, p. 6)

Before the police use biometric technology such as facial recognition, an impact assessment must have been carried out in an earlier step where the police has weighed its interest in using the technology against possible risks to the privacy of the individual(s) involved. This was, however, not addressed in the case of using Clearview AI, which the police argued was due to the fact that the use of Clearview AI had not been sanctioned by the Police Authority. Neither had the application been provided by the Police authority. The Administrative Court argued as follows:

> *The current processing of biometric data is in itself of a sensitive nature and involves special risks, which entails high demands on technical and organizational measures in order to ensure constitutional processing. In the present case, it has been a matter of privacy-sensitive data which without prior impact assessment [have] been used in an external application. Furthermore, it has not been possible to clarify what has happened with the personal data used.* (4756-21, p. 9)

4.2. Organizational responsibility versus individual professional discretion

The second theme that reveals the trade-off between security and privacy in the present case is an organizational one. Clearview's application had in fact been used by some police officers in a number of different Swedish police units since 2019. The application had mainly been used in investigations of child sexual abuse and of serious organized crime. The application had been used for the purpose of identifying unknown victims and offenders linked to ongoing investigations. In their responses to the IMY, the Police Authority revealed some details of how individual officers had used a trial version of Clearview AI during the free trial period. Some of them had been informed about Clearview AI during a Europol training course while others had received information about the application from a national central unit within the Swedish Police Authority.

Hence, the institutional dialogue around the Swedish Police use of Clearview AI contains a controversy around how the formally unsanctioned use of the technology could be considered a matter of organizational responsibility or individual choice of professional police officers.

In response to the IMY's demands for clarification, the Police Authority attempted to disentangle its institutionalized responsibility from the police officers' work and to limit it to explicitly sanctioned use of technology. In doing that, this avenue in the Police Authority's argumentation sets aside the question of whether the use of Clearview AI was legitimate or illegitimate and focuses instead on who was responsible for actions by individual police officers who, in the exercise of their professional work, used tools not officially sanctioned to investigate crime. From the Police Authority's view, the use of Clearview AI that had taken place had been prompted by the curiosity and professional motivation of a number of individual police officers from across different departments in the organization, who had tested Clearview AI on a number of occasions since the autumn of 2019.

The Police Authority argued that as an authority it did not encourage employees to use new technologies that it had not itself provided or sanctioned. The Authority emphasized that this case was about the actions of individual police officers, adding that the police organization is large and therefore difficult to have full control over police officers' daily work practices. As a professional organization, the Police Authority works also with a certain degree of discretion, trust and autonomy for individual professionals. The Police Authority nevertheless assured the IMY and the Administrative Court that it had not, as an authority, taken the position that Clearview AI could be used within the police force, and furthermore, that it had reported all possible misconduct.

The lack of formalized organizational knowledge regarding the use of Clearview AI was not only the basis of the Police Authority's attempt to disentangle its organizational responsibility from the

professional judgment and actions of individual police officers, but also to justify the failure of its legal (and therefore institutional) duty to perform an impact assessment, as we have mentioned in the previous theme. Expressed by the Police Authority:

> *As a result of the Police Authority not being aware of the application, no legal assessments have been made. In such circumstances, the Police Authority considers that it cannot be blamed specifically for no impact assessment having been carried out.* (4756-21, p. 8)

The Court, however, argued that neither the legislation nor its preparatory work allowed an exception from the Police Authority's obligation to carry out an impact assessment, in the present case before the processing of biometric data had begun. As the police had failed to carry out an impact assessment, the Court assessed that the Police Authority had violated the Criminal Data Act on this point.

The Police Authority's attempts to discharge itself of responsibility by reducing the case to a matter of a few individual officers' responsibility and referring to emerging demands, failed in the view of both the IMY and the Administrative Court. Both authorities directed the attention back to the use that had already taken place, and realigned the Police Authority and its officers by stating that all use performed in police work was the responsibility of the Police Authority.

4.3. Internal versus external technology

The third theme emerging in the institutional dialogue concerns the control of biometric data processed by the new technology used. From the dialogue, we learn how Clearview AI was used by police officers. Some police officers entered pictures that they described as "cut-out faces" of the victims and offenders they wanted to identify. The application then searched for matches between the uploaded image or part of it (i.e. the face) and the images contained in Clearview AI's database and finally provided the users with a series of links as a result of the search. These links, which may refer to images on social media, in newspaper articles or in other places on the open Internet, were then manually checked by the police. The Police Authority described Clearview AI as follows:

> *Clearview AI presents a number of hits based on similarities between uploaded images and the images in the company's database. Since the algorithm produces similarities on a descending scale, a large number of hits will be quickly rejected after the employee has looked at them. Below the hit result is information about where that particular image [can be found], for example an Instagram account. If a match is similar, you can click on that account and continue searching for information to identify the person you are looking for.* (A126.614/2020, p.2)

According to the Police Authority, images of people, converted into biometric data, had been uploaded to Clearview AI on several occasions as part of ongoing investigation work. The Police Authority did not report how the biometric data uploaded to Clearview AI are processed in the application, e.g. how long the data are stored, how the biometric data are matched, whether the data are transferred to third countries and whether they are disclosed to others in connection with the use.

Given the sensitive nature of biometric data, the IMY emphasized that it was absolutely necessary that they were in accordance with the applicable law. The use of a technology such as Clearview AI meant that individuals' biometric data were matched against large amounts of data obtained unfiltered from the open Internet, which, according to the IMY, was unlikely to meet the strict necessity requirements of the Criminal Data Act and the underlying Criminal Data Directive.

What is at the center of this controversy is the legitimate boundaries between internal and external control over data and the algorithms. As Clearview AI has been developed and is controlled by a private

commercial company, the Police Authority does not have enough insight, nor does it have control over how the data are handled. Therefore, the Police Authority cannot ensure that the algorithm acts within the legal framework for privacy protection. Finally, it is interesting to note that, while the IMY's decision categorically dismissed the use of Clearview AI as illegitimate, also pointing at the deficient procedures for data protection, the Administrative Court opened for the possibility of use of such technology if an appropriate data protection plan in combination with necessary technical and organizational measures could be put in place, and imagined an internally developed technology as possibly meeting the legal requirements. This clearly shows the authorities' perception of internal versus external technology.

5. Discussion

Facial recognition technology is being widely introduced in many police authorities around the world, based on expectations of enhanced public security (Bragias et al., 2021; Bradford et al., 2020). However, there are also justified critical voices pointing to far-reaching risks and threats to individuals' privacy (McSorley, 2021; Véliz, 2020), which in a broader institutional perspective raises concerns for the legitimacy of police use of facial recognition technology (Stinchcombe, 1968). The recent proposal at European Parliament for a ban of police use of facial recognition technology in public places (Heikkkilä, 2021; Madiega & Midlebrath, 2021) indicates the technology's intrusive and pervasive properties and the risk of purpose slippage once the technology is implemented, further eroding police legitimacy (Bradford et al., 2020).

We analyzed the institutional dialogue (Tremblay, 2005) that took place between the Swedish Police Authority, the IMY and the Administrative Court regarding the police use of the Clearview AI facial recognition technology, in order to articulate the trade-offs between security and privacy in the use of this controversial and powerful technology. We found three major tensions in the unfolding of the trade-offs between security and privacy: (1) *Effectiveness versus privacy – the sensitive nature of facial recognition technology*; (2) *Organizational responsibility versus individual professional discretion*; and (3) *Internal versus external technology*.

This institutional dialogue offers direct insights into how controversial the legitimate use of facial recognition technology such as Clearview AI might be (Rezende, 2020) in the tensions between different institutional framings by the involved authorities (Stinchcombe, 1968). Thus, it shows how they relate and justify their relation to the technology (Richards, 2013). For instance, the police described a powerful technology with the potential to identify previously unknown victims. In addition, it underscored possible efficiency gains, by referring to the enhanced ability to identify and prosecute offenders in extremely complicated cases of child sexual abuse and organized criminality that would otherwise take a long time to solve. It pointed to the importance of understanding such gains in the police's mandate to uphold security in society (Brayne, 2021). It also pointed to the importance of the limited trial of the new technology conducted by the police officers, thus trying to discharge its organizational responsibility and referring instead to individual professional discretion.

Clearview's approach to scrape data from the open Internet is highly controversial, and is considered problematic in terms of privacy (Rezende, 2020; Campbell, 2019). This practice draws entirely on people's willingness to share data online, i.e. practices underpinning what Zuboff (2019) refers to as "surveillance capitalism", not considering people's awareness, or unawareness, of the use of these data for public surveillance processes. Clearview's status as a commercial private company is central to their ability to get away with this. The gigantic database of scraped data is at the very core of the power of their face recognition services and what it can enable police authorities to do (Faraj & Azad, 2012). Their database

consists of more than three billion images (Rezende, 2020), which feed into both the machine learning algorithm (Kitchin, 2017), and the matchmaking of uploaded images with the database. On the material side (Orlikowski & Scott, 2008) both the database and the software are external technologies provided by a market actor. The uploaded images, in the present case, were part of ongoing police investigative material. The IMY and the Court emphasized that, in this case, the use of uploaded images was a question of use of privacy-sensitive (Smyth, 2019) information which, without prior legal assessment, had been entered into, and used in, an external application. It also appears to be highly unclear what has happened to the entered data, i.e. whether these data have now been used to further develop Clearview's database (Campbell, 2019).

In the case analyzed here, although recognizing the difficult trade-offs between security and privacy (Solove & Schwartz, 2020) and using different nuances to frame it, both the IMY and the Administrative Court rejected the Police Authority's justification and deemed their use of the technology illegitimate. For the police officers, this was a technology that effectively identifies previously unknown individuals by using biometric personal data. By making use of images of faces, the technology nevertheless exploits data intrinsically tied to people's identity, and while doing so, enables the police to survey and identify individuals in public without their awareness (Smith & Miller, 2021; Lyon, 2019). It is important to note that the Administrative Court recognized that the new technology may afford new and appealing possibilities for police officers in their investigations (Brayne, 2021). An important implication for the police, here, is the need to identify and institutionalize technological applications affording legitimate potential (Rolandsson, 2020), not only by means of internal policies and other documents, but also by conducting impact assessments and following up how these technologies are used in practice. All these legitimizing practices (Bradford et al., 2020) would contribute to the institutionalization of such technologies as facial recognition, which show a high degree of ambivalence (Kallinikos et al., 2013).

A further implication is that the emerging digital technologies should not merely be understood as tools for practicing certain methods, but rather, should be seen as assemblages consisting of infrastructures that guided by norms or logics, connect a growing number of devices and services that provide data (Flyverbom, 2019, Ball & Webster, 2020). In doing so, this case illustrates the institutional complexity of surveillance assemblages (Haggerty & Ericson, 2000), where both state and private actors (Ball et al., 2015), together with the digital infrastructures, collaborate in an institutional arrangement characterized by an intricate interplay between different institutionalized missions, logics, and practices that shape and determine the affordances of the technology (Faraj & Azad, 2012).

Finally, we may emphasize, that it is important to keep in mind that the analyzed dialogue unfolding in the documents is strongly influenced and framed by the mandate and logic of the three authorities: the Police Authority, whose work aims at keeping public order and security; the IMY which holds the police accountable for not respecting individual privacy; and the Administrative Court whose work was to hear the appeal, and settle the issue. This relationship between the three authorities is worth noting as we interpret it as an explanation for which arguments and perspectives have been at the forefront of the dialogue. By recognizing their mandate and how their assignments influence the different trade-offs that are being made, we may point out that the perspectives that emerge within each of the three themes in this article ultimately also enable us to identify a certain logic of action that eventually shape the institutional context (Thornton et al., 2012; Ravioli & Norbäck, 2013) in which the affordances of Clearview AI are applied, framed and, finally, ruled.

6. Conclusion

This article analyzed the institutional dialogue that took place between the Swedish police and two regulatory authorities, the IMY and the Administrative Court, regarding the police use of Clearview AI facial recognition technology. This facial recognition application has been developed by a private commercial actor and is marketed as a powerful tool for police authorities. In accordance, the study identifies how the technology has potentials (Faraj & Azad, 2012) that can contribute to the police's digital capability. In particular, the technology emerges as a necessary resource in the police's fight against certain serious and organized criminality. At the same time, the article recognizes that the sensitive nature of processing biometric data raised privacy (Smyth, 2019) concerns among all three authorities, urging them to negotiate trade-offs between the police's use of this technology for enhanced security (Solove & Schwartz, 2020) and individuals' privacy (Solove, 2006; Hildebrandt, 2020).

The Police Authority's references to difficulties to control individual police officers' use of the technology imply that this authority was both downplaying its own responsibility and recognizing the existence of misconduct by individual police officers. Still, this did not stop the IMY and Court from holding the Police Authority accountable for the unauthorized use of Clearview AI; a digital capability of the police that is legitimate therefore seems to come with explicit demands for awareness and accountability. Further concerns about the ability of the police to organize and manage a legitimate use of this type of biometric data, respecting demands for privacy, were linked to the fact that the Clearview AI application draws on a broader digital infrastructure. The technology is perceived as controversial and powerful, due to the company Clearview's gigantic database of images created through controversial and unique data scraping practices (Rezende, 2020). However, as Clearview is a private company, the Police Authority does not have insights into or control over how the data are handled; and therefore it could not show that the algorithm acts (Murphy, 2017) within the legal framework for privacy protection. As a consequence, we may also identify tension and controversy over the legitimate boundaries between private and public control of personal data and the algorithms using them (Kosta, 2022) raising further demands on police awareness and accountability (Bragias et al., 2021). At present this tension is linked to serious threats to the privacy (Solove, 2006; Richards, 2013) of individuals, potentially making the use of the technology illegitimate.

This study therefore shows how the police's use of facial recognition technology raises privacy issues as well as directing attention towards a number of legal, organizational and professional implications. These issues manifest themselves as different tensions forcing the police to consider how they are recognized by a set of regulatory actors that are able to legitimize the police's use of facial recognition data (Stinchcombe, 1968). By identifying these tensions, this article provides insights into various controversial legitimacy issues linked to the police's use of facial recognition technologies – technologies which are currently being introduced in many law enforcement authorities around the world. While face recognition technology fosters expectations of a police force's ability to enhance public security, the article shows how privacy issues unfold and condition the institutional recognition of police accountability.

The article has problematized how trade-offs between privacy and security unfold in the police's use of facial recognition in a broader context governed by several different authority logics. In addition, the study shows the urgent need for the police to establish organizational routines for evaluating the effectiveness of new technology and a model for assessing impact. Finally, the article has shown how the police's use of facial recognition gives rise to various tensions that force both the police and decision-makers to rethink and further articulate the meaning of integrity, in order not to remain a vague and black-boxed concept.

Acknowledgments

This research was funded by the Swedish Research Council for Health, Working Life and Welfare (Forte).

The Open Access publication of this paper was supported by the Panelfit project. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.

References

Ball, K., & Snider, L. (2019). *The Surveillance-Industrial Complex: A Political economy of surveillance*, Routledge.

Ball, K., & Webster, W. (2020). *Surveillance and Democracy in Europe*, Routledge.

Black, J., & Murray, A. (2019). Regulating AI and machine learning: Setting the regulatory agenda. *European Journal of Law and Technology*, *10*(3).

Bowen, G.A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal*, *9*(2), 27–40.

Bradford, B., Yesberg, J., Jackson, J., & Dawson, P. (2020). Live facial recognition: Trust and legitimacy as predictors of public support for police use of new technology. *British Journal of Criminology*, *60*, 1502–1522.

Bragias, A., Hine, K., & Fleet, R. (2021). 'Only in our best interest right?' Public perceptions of police use of facial recognition technology. *Police Practice and Research*, *22*(6), 1637–1654.

Brayne, S. (2021). *Predict and surveil: Data, discretion, and the future of policing*, Oxford University Press.

Buzzfeed (2020). *Police In At Least 24 Countries Have Used Clearview AI. Find Out Which Ones Here*, Retrieved on October 7, 2021 from: https://www.buzzfeednews.com/article/ryanmac/clearview-ai-international-search-table.

Campbell, F. (2019). Data Scraping – What are the privacy implications, *Privacy & Data Protection*, 3.

Carlsson, S., & Rosén, E. (2020). *Polisen bekräftar – har använt kontroversiell app*. Retrieved on October 12, 2021 from: https://sverigesradio.se/artikel/7426017.

Eneman, M., Ljungberg, J., & Rolandsson, B. (2020). Governmental Surveillance – The balance between security and privacy, *Proceedings of the UK Academy for Information Systems*, Oxford, UK.

European Commission (2021). *Proposal for a regulation of the European Parliament and of the council, Laying down harmonised rules on artificial intelligence and amending certain union legislative acts*, COM (2021) 206 final.

Faraj, S., & Azad, B. (2012). The Materiality of Technology: An Affordance Perspective. In Nardi & Kallinikos (eds) *Materiality and Organizing: Social Interaction in a Technological World*. Oxford University Press.

Flyverbom, M. (2019). *The Digital Prism*, Cambridge University Press.

Gross, J. (2018). Document analysis, *The SAGE Encyclopedia of educational research, measurement and evaluation*, SAGE Publications Ltd.

Gubrium, J.F., & Holstein, J. (2009). *Analyzing Narrative Reality*, SAGE Publications. Ltd.

Haggerty, K., & Ericson, R. (2000). The surveillant assemblage. *British Journal of Sociology*, *51*(4).

Heikkilä, M. (2021). *European Parliament calls for a ban on facial recognition*, Retrieved on October 7, 2021 from: https://www.politico.eu/article/european-parliament-ban-facial-recognition-brussels/.

Hildebrandt, M. (2020). *Law for computer scientists and other folk*, Oxford University Press.

Hill, K. (2020). *The Secretive Company That Might End Privacy as We Know It*. Retrieved on October 12, 2021 from: https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

Kallinikos, J., Aaltonen, A., & Marton, A. (2013). The ambivalent ontology of digital artifacts. *MIS Quarterly*, *37*(2).

King, N., & Brooks, J. (2019). Thematic Analysis in Organisational Research. In *The SAGE Handbook of Qualitative Business and Management Research Methods: Methods and Challenges*, SAGE Publications Ltd.

Kitchin, R. (2017). Thinking critically about and researching algorithms. *Information, Communication & Society*, *20*(1).

Kosta, E. (2022). Algorithmic state surveillance: Challenging the notion of agency in human rights. *Regulation & Governance*, *16*, 212–224.

Lyon, D. (2019). State and Surveillance. In *Governing Cyberspace during a Crisis in Trust: An essay series on the economic potential – and vulnerability – of transformative technologies and cyber security*, Centre for International Governance Innovation, pp. 21–25.

Lyon, D. (2018). *The culture of surveillance*, Polity Press.

Lyon, D. (2014). Surveillance, snowden and big data: Capacities, consequences, critique. *Big Data & Society*, *1*(2), 1–13.

Madiega, T., & Midlebrath, H. (2021). *Regulating facial recognition in the EU*, European Parliamentary Research Service (EPRS), PE 698.021.

McSorley, T. (2021). The Case for a Ban on Facial Recognition in Canada. *Surveillance & Society*, *19*(2), 250–254.
Murphy, M. (2017). Algorithmic surveillance: The collection conundrum. *International Review of Law, Computers & Technology*, *31*(2), 225–242.
Norman, D. (1999). Affordance, conventions, and design. *Interactions*, *6*(3).
Orlikowski, W., & Scott, S. (2008). Sociomateriality: Challenging the Separation of Technology, Work and Organization. *The Academy of Management Annals*, *1*(2), 433–474.
Raviola, E., & Norbäck, M. (2013) Bringing technology and meaning into institutional work: Making news at an italian business newspaper. *Organization Studies*, *34*, 1171–1194.
Rezende, I. (2020). Facial Recognition in police hands: Assessing the 'Clearview case' from a European perspective. in *New Journal of European Criminal Law*, *11*(3), 375–389.
Richards, N. (2013). The Dangers of Surveillance, *Harvard Law Review*.
Rolandsson, B. (2020). The emergence of connected discretion: Social media and discretionary awareness in the Swedish police. *Qualitative Research in Organizations and Management*, *15*(3), 370–387.
Schatzki, T. (2019). *Social Change in a Material World*, Routledge Ltd.
Smith, M., & Miller, S. (2021). The ethical application of biometric facial recognition technology. *AI & Society*, *37*, 167–175.
Smyth, S. (2019). *Biometrics, Surveillance and the Law: Societies of restricted access, Discipline and Control*, New York: Routledge.
Solove, D. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, *154*, 3.
Solove (2021). *The Myth of the Privacy Paradox*, GWU Law School Public Law Research Paper No. 2020-10.
Solove, D., & Schwartz, P. (2020). *Privacy, Law Enforcement, and National Security*, Aspen Publishers.
Stinchcombe, A.L. (1968). *Constructing social theories*, University of Chicago Press.
Suchman, M. (1995). Legitimacy: Strategic and institutional approaches. *Academy of Management Review*, *20*(3), 571–610.
Thornton, P., Ocasio, W., & Lounsbury, M. (2012). *The institutional logics perspective: A new approach to culture, structure, and process*, Oxford University Press.
Tremblay, L. (2005). The legitimacy of judicial review: The limits of dialogue between courts and legislatures. *International Journal of Constitutional Law*, *3*(4), 617–648.
Véliz, C. (2020). *Privacy is Power*, Bantam Press.
Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for the Future at the New Frontier of Power*, Profile Books Ltd.