Maynooth University School of Law and Criminology

Declaration on Plagiarism

I hereby certify that this material, which I now submit for assessment on the programme of study leading to the award of MA in Comparative Criminology and Criminal Justice is entirely my own work and has not been taken from the work of others save and to the extent that such work has been cited and acknowledged within the text of my work.

Student Name: Caoimhe McKeon

Student Number: 18351973

Date: 22/09/2023

Student Signature: Caoimhe McKeon

Challenging the pixels of power: A critical inquiry into police use of facial recognition technology through the lens of surveillance studies

Caoimhe McKeon

18351973

Research Supervisors:

Dr. Cian Ó Concubhair & Dr. Ciara Bracken-Roche

A dissertation submitted in partial fulfilment of the requirements for the degree of

MA in Comparative Criminology and Criminal Justice.

Maynooth University

School of Law and Criminology

Abstract

The increasingly prevalent roll out of surveillance-focused technological tools by law enforcement worldwide has the ability to alter the practice of policing as we know it. Therefore, understanding the potential ramifications of implementing such technology into the criminal justice space is imperative. This dissertation employed a comparative case study analysis to examine the adoption of facial recognition technology by police agencies and its possible implications via the assistance of a surveillance studies lens. The study focused on two distinct police agencies located in different jurisdictions, these were: New York City Police Department (United States) and the London Metropolitan Police (United Kingdom). The examination of FRT use in these separate law enforcement organisations addresses key questions surrounding the technology's justification and surveillance motivations underpinning its explosion amongst law enforcement organisations. An extensive analysis of secondary sources was conducted, including existing policies and regulations, media and news articles, academic journals and when available, governmental, civil liberty and other interest group publications. The results of this research reveal the multifaceted dynamics that influence the adoption and operation of facial recognition technology by the police and provides a critical insight into the tensions between security objectives, the safeguarding of civil liberties and the relationships between corporations and law enforcement. The findings of this study contribute to the already existing research on the complexities of facial recognition technology in the policing context and underscores the need for transparent and informed dialogue as societies navigate the evolving landscape of technology-driven surveillance.

Acknowledgement

First and foremost, I would like to acknowledge the continuous support I have received from my amazing Mam and Dad, who have been my backbone since the beginning of my studies and who have given me the strength to keep going this year when I felt like giving up.

Of course, a huge thank you also to my incredible partner, extended family and friends, who have done nothing but give me the encouragement and motivation I needed to get to this stage in my studies and listened to me when I felt overwhelmed with the workload.

I would like to extend my deepest thanks to my supervisors Dr. Cian Ó Concubhair and Dr. Ciara Bracken-Roche for their knowledge and expertise on the topics of policing and surveillance, which were crucial to this project and is so greatly appreciated. I would also like to thank them both for their patience and support throughout my dissertation journey.

Finally, I would also like to thank all the staff of the Maynooth School of Law and Criminology for their continued support and guidance over the last year and throughout the three years of my undergraduate degree in civil law and criminology. I would like to thank Dr. Ian Marder in particular, who is truly a credit to Maynooth University and who was there for all of us this year when things got difficult.

Table of Contents

Chapter 1
Introduction

"It is imperative that An Garda Síochána can utilise modern technology with appropriate safeguards to increase efficiencies within the organisation and ensure that policing expertise is utilised in the most effective and strategic manner. That is why I firmly believe that facial recognition Technology is also vital to ensuring that Gardai can do their jobs most effectively" (Helen McEntee, Department of Justice, 2023).

Since the invention of the first recorded technological tools during the stone age approximately two million years ago, technology and its capabilities have advanced considerably (The British Museum, n.d.; Rajesh, 2017). For instance, the period of time between the years 1990 and 2000 has been frequently referred to as the "digital wave" in the history of society where we witnessed seminal technological developments such as the revolution of the mobile phone, the release of the first ever MP3 portable music player, in addition to the official launch of the world wide web (Verganti, 2009, Reller *et al*, 2009; Ring, 2023). However, recent decades, more than ever, have proven to be significant in the world of technological innovation and progression. A growing interest in exploring the various ways that technology can be used, applied and refined has been ignited, which has led to the creation of the multitude of devices and programmes we now use on a day-to-day basis such as the modern smartphone, Google's online search engine, and electric cars (Hammond, 2020).

In tandem with this burgeoning technological curiosity, there has been an evolving fascination with the concept of artificial intelligence (AI). Defined by Boden (1996) as "the study of how to build or program computers to enable them to do what minds can do", conversations around AI and machine-learning have flooded 21st century mainstream media tenfold in recent years and has become a focal point of attention for many (Waltl & Vogl, 2018; Thrall *et al*, 2018; Pierce *et al*, 2021; Bareis & Katzenbach, 2022). Amidst this spotlight on AI advancements and the technologies that fall under its umbrella, so to speak, biometric facial

recognition technology has stood as a notable component (Smith & Miller, 2022). With the capacity to identify individuals based on the automated comparison of their unique facial features, this technology has introduced an unprecedented way of shifting the long-standing power of identification decision-making from human to computer (Mohammad, 2020).

Whilst facial recognition technology (FRT) is not an entirely new concept, with its initial roots dating back as far as the 1960's, the technology has recently found its way into numerous facets of everyday life (Tucker, 2014). Notwithstanding its connection to futuristic ideologies, the technology has surpassed the realm of science fiction and entered the realm of reality, exhibiting its many functionalities by providing us all with an alternative and convenient way of unlocking our smartphones, for example, along with many other capabilities such as allowing us to apply entertaining filters to our faces when taking pictures and videos, in addition to suggesting friends to tag from recently uploaded pictures on well-known social media platforms such as 'S*napchat'* and ;*Facebook'* (Hamann & Smith, 2019; Petrescu, 2019; Pujianto, 2023). Additionally, just like the operation of a personal identification card, FRT in today's world can also serve as proof of identity, allowing for individuals to be free from the grips of ample amounts of documentation and successfully cross borders and pass through airports (Israel, 2020; Santana & Gentilo, 2023). The technology has also been in high demand, if not already adopted, in various other areas such as retail, as a means of identifying thieves (Chivers, 2019; Hill, 2023).

This evident spread of FRT in contemporary society has also gained significant traction amongst police agencies worldwide as an investigative tool, with countless law enforcement organisations globally demonstrating a rapid uptake of the technology (Tedeneke, 2021). Its recent explosion in popularity within the policing space has been coupled with a plethora of declared benefits to its use, namely the ability it would give to law enforcement officers to locate and identify potential suspects or people of interest (i.e terrorists) in a more straightforward and timely efficient manner, ultimately enhancing public safety (Klum *et al*, 2014; Carter, 2018; Galterio *et al,* 2018; Hamann & Smith, 2019; Nestrova, 2020). Further to this assertion that FRT could become a promising crime-fighting tool, assisting police officers to catch and apprehend criminals quicker and more easily, additional benefits have also been put forward alongside this

rationale. To name a few, it has been continuously expressed that if implemented into the investigative apparatus of police forces, FRT could aid in identifying trafficked or missing people, as well as being able to identify sexually exploited children (Carter, 2018; Galterio *et al*, 2018; Russell, 2020). Thus, scholars such as Carter (2018, p.49) have suggested that FRT has the ability to further the reach of limited police resources and "act… as a force multiplier". Moreover, advocates in support of the technology's use by the police have also argued that FRT has the capability of reducing problematic police discretion by eliminating the subjective opinion of an officer when decision-making in investigations, and placing it on to an 'objective algorithm', presumably free of preconceptions and prejudices and subsequently improving the accuracy of suspect identification (Joh, 2015; Kotsoglou and Oswald, 2020).

However, these articulated benefits of FRT in policing have not come without their critiques. In fact, as noted by Hill *et al* (2022), voices of concern surrounding the overall use of FRT, particularly in the context of policing, have become increasingly louder and have presented a host of risks and disadvantages of the technology ranging from its initial development and foundation to the ramifications that have arisen post-implementation. Its deployment has sparked an array of issues in relation to human rights and civil liberty violations, concerns in regards to the accuracy and bias of the technology, in addition to its governing regulations and the potential it has to create power imbalances and conduct mass surveillance.

Bearing these concerns in mind and in reference to the quote at the beginning of this section, the Irish police force, An Garda Síochána, are currently in the wake of possibly implementing FRT into the Irish Jurisdiction by virtue of the the recommended legislative bill 'Garda Síochána (Digital Management and Facial Recognition Technology) Bill 2023' (Irish Legal News, 2023).. In light of this, the aim of this research is to highlight the implications that may follow the adoption of such technology for Irish law and policy-makers and establish whether the use of FRT by An Garda Síochána would be justified and therefore, necessary.

To achieve this objective and contribute to the already existing literature on the topic, the two research questions I intend to answer in this study are as follows: 1) Is the use of FRT by the police as an investigative tool justified? and 2) To what extent can the lens of surveillance studies

aid in explaining the drive to adopt FRT within law enforcement? This is completed via the use of a comparative case study analysis of two distinct police agencies in separate jurisdictions, whose use of FRT has been a source of controversy. The lens of surveillance studies is then applied, in order to enhance and deepen our understanding of the motivations underpinning the technology's ever-growing prevalence in policing. In terms of importance, this study and others of the same nature, are pivotal to prevent ill-considered adoptions of FRT by law enforcement organisations. By presenting the downfalls and harmful effects that FRT can have when used within the criminal justice system, this research illustrates what factors need to be considered if FRT is to be introduced into Irish jurisdiction.

The following chapter will examine the existing literature in the area of FRT more broadly, and will explore previous research on the concerns that have been raised regarding the technology in addition to its use by police. Additionally, it will also examine relevant and available surveillance studies literature in order to situate the theoretical lens that will be used to analyse the findings of this research. In Chapter 3, an in - depth methodology will detail my overall approach to gathering and analysing the chosen case studies relevant to my research. Chapter 3 also includes the methods and techniques that were used and the justifications for their selection. Following this, chapter 4 will present the key information from each chosen case study to support my research questions. Chapter 5 will discuss the findings in the context of the current state of FRT use in the jurisdictions and police agencies considered in this study, existing literature and the conceptual framework of surveillance studies. The concluding chapter of this paper will provide a concise summary of my research and will include future suggestions and considerations for Irish law and policy - makers to take into account when contemplating FRT roll-out within the Irish law enforcement sphere.

Chapter Two
Literature Review

Introduction

This literature review synthesises key findings from existing research in the area of FRT to provide a comprehensive understanding of the operation, concern and current applications of the technology. It will firstly begin by evaluating and dissecting how FRT functions as an AI tool. Following this, it will explore FRT's popularity, growth and expansion into everyday life in realms of society outside of the law enforcement sphere and will then concentrate on police uptake and adoption of the technology specifically. Subsequent to this, the scrutiny, criticism and debates that have been raised in relation to the use of FRT in the context of policing will be examined, along with the public's attitude and perceptions of law enforcement organisation's use of the technology. Lastly, it will situate the theoretical lens of the study and will discuss the existing surveillance studies literature that will be used to analyse the research findings. This will include the outlining of surveillance studies concepts and theoretical frameworks that I believe are most relevant to addressing the research questions put forward in this dissertation.

What is FRT and how exactly does it operate?

Before we can delve into the existing studies and literature surrounding the utilisation of FRT, one must clearly understand how the technology works. FRT seeks to identify and match a face that it encounters with a face it has stored in its database via the assistance of a computer-generated algorithm (Qinjun *et al*, n.d). Once a face is captured by FRT, whether that be in real-time or from an existing picture, the FRT transforms that facial image into mapped biometric measurements and numerical expressions, which record and make note of the various unique facial features of that specific person through the use of computerised filters (Crumpler & Lewis, 2021). Once prompted by the FRT, the underlying algorithm compares and contrasts the recorded facial measurements against what is already there in its database in order to determine similarity, focusing on distinctive characteristics such as the width of a person's nose or the depth of their eye sockets, for example, and subsequently finding what it thinks to be a few or one potential matches based on these measurements (Crumpler & Lewis, 2021; Simerman, 2023). In the event that a match can not be identified, this data can then be stored as a 'biometric template'

for comparisons in the future and can thus be used to name or identify possible criminal suspects images that come to the attention of the police, for example (Simerman, 2023).

Additionally, in the same way that it is important to fully comprehend how FRT works as a technological tool, it is also equally vital to know how the underpinning algorithms function that allow FRT to complete its task of identifying individuals. Extensively used throughout both the IT and AI industries in today's technological world, algorithms are often referred to as the 'building blocks' of present-day computers and programmes as they are the component that allows and facilitates websites, smartphones and computers to have the capability of making decisions (Gillis, 2022; GCFGlobal, n.d.).

To put it simply, an algorithm is a step-by-step set of instructions designed to solve a specific problem or perform a certain task, which essentially serves as a 'blueprint' upon which multiple modern technologies operate (Brogan, 2016; University of York, 2022; Corbo, 2022). Once data is received or entered into an algorithm, it will process and analyse that data and execute the job that it has been engineered to do, providing an outcome (University of York, 2022). In the context of FRT, this process would involve an algorithm taking the facial measurement 'data' taken from either a still image or real-time image of a person's face, examining that and ultimately producing possible match results due to its engineering configuration to identify. Algorithms have this ability because at their core, an algorithm is a computer programme itself, with a coded formula that when activated, orders the technology to do something constructive to address a particular issue (University of York, 2022). Further to this, algorithms are designed to ensure the correct information is provided in the outputs it gives, which is ultimately achieved by the computing system applying an assortment of filters such as mathematics, decision-making and repetition to build "if x, then y" equations (Corbo, 2022).

Prevalence of FRT in modern society

Whilst the concept of FRT has long been contained within the world of science-fiction novels and a frequently covered topic by popular media outlets, it has, in recent years, broken through the barrier of futuristic and dystopian ideologies into many areas of contemporary daily-life (Benson, 2017). Its use has gained significant popularity in almost all areas of society

and has been adopted by both the public and private sectors, finding versatile applications across various industries (Seng, Al-Ameen & Wright, 2021). As a result, FRT has now become a part of everyday existence for an alarming number of us, as asserted by Bischoff (2022). In the realm of retail, for instance, businesses are leveraging FRT to enhance customer experiences. Through personalised interactions, customers can receive tailored recommendations and advertisements based on their previous purchases and preferences (Cheshire, 2017; Güven, 2019). Moreover, this technology facilitates streamlined payment processes, allowing for secure and convenient transactions without the need for physical cards or cash (Dang *et al,* 2022).

FRT is also making significant strides in the healthcare sector. It is being employed to improve patient care by enabling swift and accurate patient identification, reducing the risk of medical errors, and ensuring that individuals receive the appropriate treatments (Mishra *et al,* 2023). In particular, as noted by Qiang *et al* (2022), has been introduced into the medical arena on a large-scale to assist healthcare teams in diagnosing diseases that involve "facial abnormalities". Additionally, FRT can aid in monitoring and analysing patients vital signs and expressions, assisting medical professionals in assessing pain levels and emotional well-being (De Sario *et al,* 2023; Rebelo *et al,* 2023).

The entertainment industry is also embracing FRT to enhance user engagement. Amusement parks, for instance, are utilising it to create personalised experiences for visitors, such as customised character meet-and-greets or interactive attractions that react to visitors expressions (Forbes Technology Council, 2023). Similarly, other entertainment venues such as sports stadiums have introduced FRT to improve fan experiences and participation by creating smartphone applications that can allow fans to generate keep-sake memories and have their time on the stadium jumbotron (Cohen, 2023). Thus, this innovation heightens the sense of immersion and enjoyment for guests.

In the cybersecurity space, FRT is being employed as an advanced form of biometric authentication. An application of FRT in this sector that has become so familiar to us in recent times is the technology's use to unlock devices such as smartphones and tablets (Davis *et al*, 2022; Dauvergne, 2022). Indeed, as noted by Andrechienko and Kolisnyk (2022), the vast majority of companies that produce these technological items in today's digitally ridden society

incorporate FRT as one of the main features of their products. In the same vein, FRT is also being used to as a means of identification verification to grant people access to guarded spaces and when logging into private and confidential bank accounts, adding an extra layer of protection against unauthorised access (Katsanis et al, 2021; Luo & Guo, 2021; AL-Aadamy & AL-Dulaimi, 2023). This method is often more convenient and secure than traditional passwords or PINs, which can easily be forgotten or compromised.

Furthermore, both the transportation and educational sectors have also acquired FRT. In terms of transportation, the technology has been employed in an effort to increase passenger safety and efficiency. Airport and other transport hubs such as border and custom crossings between countries are deploying this technology to expedite security checks and boarding procedures (U.S Customs and Border Protection, n.d.; Ó Conghaile, 2018; United States Government Accountability Office, 2022; Van Cleave, 2023; Bakshi, 2023). In fact, it was reported by Bischoff (2022) that sixty percent of countries now have FRT deployed in a variety of their respective airports. A major rationale underpinning FRT's use in this industry has been that by analysing traveller's faces when they pass through transport domains such as airports and border control, authorities can compare these faces against their respective FRT databases to identify potential threats and manage passenger flow more effectively (NEC, 2019; Khan & Efthymiou, 2021).

In the realm of schooling and education, FRT has been introduced in an attempt to address a range of matters. According to Andrejevic and Selwyn (2019), these have largely included issues related to school campus security in countries where school shootings are a risk, emotional detection in relation to individual student engagement and learning, as well as automated student registration. Attendance tracking in particular has emerged as a popular use of FRT in educational settings, which aims to eliminate the gaps and omissions that often occur when human teachers are burdened with the calling of names of big student groups (Puthea *et al*, 2017). Further to this, FRT has also been deployed in the contexts of exam and online course integrity, controlling access to online course content in addition to monitoring the presence of students throughout the duration of computer-based examinations (Montegomery & Marais, 2014; Hernández *et al,* 2008; Apampa *et al*, 2010). Similarly, there have also been attempts made

to incorporate FRT into webcams that are used in conjunction with frequently accessed third level educational platforms such as 'moodle' (Guillén-Gámex *et al,* 2014).

Thus, it is clear that the spread and expansion of FRT use continues to reshape diverse industries by offering convenience, personalisation, and efficiency. This is evidently observable across various facets of society, from its ability to revolutionise retail experiences and improve healthcare service to bolstering cybersecurity, streamlining transportation processes and both enhancing and monitoring entertainment and student engagement. Its application in today's world appears to be endless, with various other niche industry adoptions of FRT also available such as its ability to impose age restrictions in relation to the online viewing of pornography and its capacity to limit gambling addiction, to name but a few (O'Mallon, 2019; Robson, 2011).

Police use of FRT

The ever-growing integration of FRT into law enforcement investigative apparatus around the globe, is an application of the technology that has engendered much discourse within both the academic and public domains. Scholars have extensively explored the potential benefits of police use of FRT, with the technology's capacity to expedite criminal investigations and enhance public safety being a prominently voiced advantage. As acknowledged by Dauvergne (2022), advocates in favour of the technology have noted how the technology may recognise a photo of a missing person, identify a human trafficking victim or a perplexed and lost elderly person. Further, Dauvergne (2022) notes that supporters of FRT have also made reference to the technology's capability of solving cold cases by identifying unknown witnesses or suspects from historical crime scene footage and photographs. Indeed, these potential asserted benefits to police use of the technology have been illustrated in various cases. For instance, FRT was successfully used in the search for hurricane Dorian victims in the Bahamas in 2019 and has been documented as being useful in the identification of children that have gone missing in both India and China (Corum, 2019; Feng, 2019; Nagaraj, 2020). Additionally, the department of homeland security have reported that FRT allowed them to identify and assist 311 children who had been the victims of child sexual exploitation (Roeloffs, 2023). Further, it has been suggested by academics that FRT could mitigate police bias in traditional identification decision-making (Lunter, 2020).

However, by the same token, others have argued that the inherent inability of FRT to accurately identify individuals of certain ethnic descent, among other physiological characteristics, will not solve this issue. Rather, scholars such as Johnson *et al* (2022) argue that based on their research, it will simply exacerbate racial inequalities in policing and worsen this phenomenon. Fussey *et al* (2021) have also disagreed with this purported benefit to FRT. Instead, they note that although the decision-making aspect of policing is somewhat "algorithmically framed" by FRT use, it still requires that police officers choose whether or not to apprehend a person that the FRT has identified as a possible suspect. Fussey *et al* (2021) state that contrary to what people may assume, FRT in street policing simply guides an officers decision-making and does not, "wholly determine it". Therefore, Fussey *et al* (2021) argue that the discretionary power given to police that has been witnessed since the inception of police agencies is not taken away by FRT, it is merely "assisted" and still requires that individual officers make the final call on who to approach when provided with one or many potential matches by the FRT algorithm.

A significant area of contention associated with the unfettered implementation of FRT by police pertains to issues of privacy and civil liberties. For instance, critics argue that the expansive surveillance potential of FRT infringes upon individual rights to privacy and anonymity in public spaces (Naker & Greenbaum, 2017). Scholars such as Turley (2020) highlight the idea of a "fishbowl society", noting how although numerous literary and cinematic works have, for decades, depicted worlds where privacy is a foreign concept and throughout, there is a continual and omnipresent surveillance. Whilst considered a source of entertainment and fiction for many, Turley (2020) suggests that FRT could very well be modern democracy's ticket to that dystopia. Moreover, though spoken in greater detail further on in this section, scholars such as Garvie *et al* (2016) have exposed the technology's potential to magnify racial bias, as some systems exhibit higher error rates for individuals with darker skin tones, reinforcing existing disparities in the criminal justice system.

The ethical dimensions of facial recognition technology's police deployment have also drawn substantial scrutiny. The notion of "function creep" emerges from discussions around technological intent and actual application. As outlined by Koops (2021), this term "function

creep" refers to when technologies that have been initially introduced for specific purposes gradually expand into other domains without due democratic deliberation. In other words, data and information obtained originally for one particular reason is then used in circumstances that have not been consented to (Mann & Smith. 2017). In the context of policing, Camplin (2022) asserts that whilst FRT may be introduced firstly into police agencies for the purposes of identifying individuals that have a warrant out for their arrest, for example, this may gradually expand and ultimately be used for a myriad of reasons. This tendency for FRT to "function creep" into areas it was not originally adopted for, Selwyn *et al* (n.d.) note, has already been evident in regard to state authority and government implementation of the technology. For instance, Selwyn *et al* (n.d.) refer to the 2018 FIFA world cup in Moscow and the 175,000 FRT enabled cameras that were deployed under the guise of visitor safety with the underpinning rationale being to identify anti-war protestors that attended. Nonetheless, Selwyn et al (n..d) state that when the COVID-19 pandemic became inescapable and measures were put in place to prevent the spread of the virus, the boundary between why the FRT was initially introduced for and alternative applications of the technology was blurred, leading to the creeping of FRT use into the domain of monitoring adherence to these regulations. Thus, Selwyn *et al* (n.d.) argue that the notion of "function creep" in the context of FRT and other surveillance technologies that involve the tracking and profiling of individuals can ultimately intensify controlling, authoritarian and manipulative tendencies.

Inaccuracies, discrimination and biases

One of the primary concerns in relation to FRT and indeed its use by the police within the criminal justice system is the technology's ability to accurately and correctly identify an individual and the subsequent racial disparities that have occurred as a result of the technology failing to do so.

Countless studies have demonstrated that FRT can produce high error rates depending on the colour of a person's skin, their age and their sex. A landmark study in this space conducted by Grother, Ngan and Hanaoka (2019) and produced by the National Institute of Standard and Technology (NIST) discovered after testing 189 commercially available algorithms, many displayed high error rates for African and Asian faces in comparison to Caucasian faces. In fact,

the study confirmed that individuals of either African American or Asian ethnicity were 100 times more likely to be misidentified than their Caucasian counterparts (Harwell, 2019). These findings are congruent with another leading study in this area known as 'Gender Shades' which was conducted by Buolamwini and Gebru (2018). In this study, both Buolamwini and Gebru used 6 datasets (3 African countries and 3 European countries) to assess the ability of 3 FRT technology algorithms in detecting, recognising and classifying people's faces. The overall result of the study was that the three algorithms used exhibited a lower accuracy rate when it came to detecting if a person was female and also appeared to perform better on individuals with lighter skin than it did on the participants that were considerably darker in complexion.

Similarly, a 2018 study conducted by the Garvie, Bedoya and Frankle (2018) in the Georgetown Law Centre on Privacy and Technology found that some FRT systems were less accurate for women and people with darker skin tones. In the police context specifically, Fussey and Murray (2018) found that out of the 42 generated matches that the Metropolitan Police Department algorithm identified, only 8 of these were verifiably correct. These studies echo the findings of earlier research such as the work done by Phillips *et al (*2010), Klare *et al* (2012), Abdurrahim *et al* (2018) and Cook *et al* (2019). Thus, scholars such as Reinbold (2020) argue that FRT's inability to correctly identify individuals based on their unique characteristics such as their sex, ethnicity and age can further the discrimination of people of black descent, for example, identifying them as suspected offenders when indeed, they are not.

On the other hand, academics such as Najibi (2020) have also noted that even if the technology was accurate in terms of its identification capabilities, FRT has the potential to further perpetuate racial discrimination within the criminal justice system that has long been highlighted across criminological research, thus widening already existing inequalities.

Regulatory frameworks governing FRT

In terms of regulatory frameworks that govern use of FRT, there is significant variation across jurisdictions. As noted by Almeida *et al* (2022), despite being significant users of FRT, there exists no federal law governing the use of FRT in the United States, with its use largely left up to individual states and localities to regulate. Some states, such as Illinois, have enacted laws

regulating the use of FRT which has given legal standing for private individuals to recover damages and sue for the improper access and/or usage of their biometric data while others have no regulations at all (Chabinsky and Pittman, 2020). In the European Union, the use of FRT is regulated currently by the General Data Protection Regulation (GDPR) directive which officially came into force in 2018 and places significant restrictions on the collection and use of personal data, including biometric data (Almeida *et al,* 2022). Contrasingly, in China, the government has implemented a vast and invasive surveillance system that includes the use of FRT, with little regard for privacy or civil liberties (Bischoff, 2021).

However, as can be observed, the regulation of the FRT space is complex and varied with this fragmented mind field of FRT regulation prompting the input and opinion of various scholars. Numerous scholars have called for the temporary mortarium or complete ban of FRT until there is an adequate legal framework that is adopted to regulate its use sufficiently (e.g Crawford, 2019; Selinger and Hartzog, 2020; McSorley, 2021). Others have advocated for policies regulating FRT to be adaptive in nature and not rigid for fear of inhibiting advancements in technology if a blanket ban is issued, whilst others have suggested public engagement in the development stage of FRT policy as they are the parties most effected (Hill *et al,* 2022; Li *et al,* 2023).

Nevertheless, it has been noted by commentators on AI such as Morrison (2018) on the 'internet of things' (Iot) and Pasztor and Wall (2016) on drone usage, that regulations which govern these technologies rapidly become outdated and even when 'thoughtful' legislation and regulation has been implemented, they are unlikely to prevent FRT surveillance tools from creeping overtime into unregulated spaces by way of 'technological mission creep' (Frischmann and Selinger, 2018), 'function creep' (Koops, 2021), 'surveillance creep' (Da Costa, Schulte and Singer, 2006) or 'private to public creep' (Dauvergne, 2022). Additionally, academics such as Dauvergne (2022) have noted that unregulated FRT in countries that do not have an independent judicial system or robust civil liberties like we see in the western hemisphere will be in significant danger as problems that we have experienced in the west with such technology such as algorithmic bias and misidentification will be exacerbated in countries that do not have such structure.

Privacy and Civil Liberty Concerns

In addition to both inaccuracies and the fragmented landscape of regulations addressing the use of FRT, several scholars and civil liberty groups have also raised concerns regarding FRT's ability to greatly impact fundamental human rights and democratic participation.

Unlike other forms of biometric analysis used by law enforcement such as DNA analysis, for example, FRT is what is known as a 'silent technology' and can be installed in various forms of technology (e.g Public CCTV cams), often operating covertly without the consent of the subject and/or subjects that are being surveilled (Introna and Wood, 2004; hill *et al*, 2022). Numerous scholars, commentators and civil liberty advocates have argued that this has the ability to be misused and allow mass surveillance of the public be conducted without their knowledge, resulting in a total invasion of the individual right to privacy and creating the opportunity for people to end up in a virtual line-up of suspected criminals, for example, without any awareness of such (e.g Garvie, Bedoya and Frankle, 2018; American Civil Liberties Union, n.d; Privacy International, n.d; Lively, 2021; Irish council for Civil Liberties, 2022). Thus, it allows for FRT to sweep up personal data in unrestricted ways from large numbers of people regardless of whether a person is suspected of a crime or not, which has been noted by scholars as totally dystopian (Bracken-Roche, Farries and Cronin, 2023).

It has also been argued that FRT has the capability of muzzling the democratic right to protest and political activism, which occurred in the US during the Black Lives Matter protests when tracking down protesters (Devich-Cyril, 2020; Surveillance Technology Oversight Project, 2020; Amnesty International, 2021). The concern surrounding the lack of oversight and transparency in relation to FRT use by the police has also been raised as it is very frequently unclear how law enforcement is using FRT, what exactly happens to the data that is derived from these technologies and whether or not the data that has been gathered is actually secure (Carter, 2018; Ringrose, 2019). Further to this, scholars such as Fan (2018), Mann and Smith (2017) and Slobogin (2017), to name a few, have expressed unease in terms of how police store, use, and search this information due to the sheer volume of highly personal data that is now being stored by police forces that use and operate FRT. In relation to this, multiple scholars and academics

alike have noted that due to the alluring value of facial recognition data, it is very vulnerable to hackers and data breaches which can comprise individual identity and privacy, leading to endless opportunities for malicious individuals to conduct identity theft, robbery, scamming, stalking and the list goes on (Naker and Greenbaum, 2017; Schippers, 2019; Mohsin, 2020 and Perego, 2021).

Public acceptance of FRT use

Numerous studies have highlighted the multifaceted nature of public attitudes towards FRT use both in general and by law enforcement organisations specifically. Horowitz *et al* (2023), for example, refer to what they term the "intricate interplay" between technological familiarity and acceptance, suggesting that individuals tend to exhibit more positive stances toward AI-related technology adoption when they possess a deeper understanding of both their functionalities and capabilities.

Kostka *et al* (2023) completed a study on the public's opinion of FRT use across four different countries, these were: China, the United Kingdom, the United States and Germany. What they found was that across the four separate jurisdictions, the perception and acceptance of FRT varied greatly. They discovered that FRT acceptance was positively linked to trust in governmental institutions and interest in technology and was also influenced by the public's awareness of their individual country's surveillance history in addition to concerns regarding individual privacy. Ultimately, they found that the highest approval rate of FRT use was evident amongst the Chinese participants of the study, who expressed the benefits to the technology. However, this result is not entirely surprising if we consider the fact that China is and has long been an authoritarian digital surveillance state and therefore, this type of monitoring has been somewhat normalised for the country's residents (Huang & Kellee, 2022). In fact, scholars such as Hou (2017) frequently refer to China as the modern-day 'big brother'.

Similar findings have been mirrored in earlier studies on public attitudes of FRT use. For instance, in Steinacker *et al's* cross-country (2020) work on public opinion of FRT use, it was found that individuals in different countries had distinctive thresholds in terms of when they believed FRT was acceptable, with the potential risks and benefits such as the technology's

ability to discriminate and also increase public security, playing a significant role in this decision. Notably, this study revealed that people placed more trust in governmental use of FRT in comparison to private company use. Like Kostka *et al's* (2023) study, the Chinese respondents included in this study had the highest acceptance rates. Additionally, another study conducted by Ritchie *et al* (2021) on the public's opinions of FRT use and adoption across the US, UK, China and Australia also highlighted further nuances to this subject matter. In this piece, the authors found that depending on what the technology was used for and who it would be used by significantly impacted the acceptance of its use by individuals. Trust also appeared to be a deciding factor in terms of support for the technology also, depending on what country the participants were from. For example, respondents from the U.S were more accepting of FRT tracking citizens and private company use of the technology and less trusting of police use of FRT when compared to UK and Australia.

In terms of public perceptions of police use of FRT in particular, on the one hand, some argue that its implementation can lead to enhanced public safety through the efficient identification of suspects and potential criminals and thus emphasise its potential benefits in solving crimes, locating missing people, and preventing acts of terrorism. For instance, research conducted by Raine *et al* (2022) from the pew research centre found that 31% of the American public that took part in the study thought that police use of FRT was acceptable, with the majority of this cohort asserting the aforementioned benefits to investigation timing and capabilities as the reasoning behind their opinion. The intended purpose of FRT use by the police, like in the context of its general use, has also been documented to affect public acceptance. For instance, following the storming of the capitol in America in 2021, there was public advocacy for the use of FRT to identify the suspects that had taken part in the riots (Lyon, 2021). Other studies such as Bragias *et al's* (2021) work in the context of FRT incorporation into police body-worn cameras also demonstrated that the public asserted supportive sentiments regarding police use of FRT due to the ability of the technology to promote officer safety by increasing public accountability.

On the other hand, the research in this area has also underscored a significant level of concern and scepticism amongst the public surrounding FRT use by police agencies. In the

research conducted by Bradford *et al's* (2020), for example, it was found that trust and perceptions of legitimacy of the police played a crucial role in the acceptance of FRT being used in the policing context. They found that participants in their study that vocalised the opinion that FRT should not be used by the police also noted their open distrust in law enforcement and therefore granted police officers less legitimacy and asserted heightened concerns in relation to privacy. This finding has been reflected in a number of other studies. Thus, public acceptance of police use of FRT is intrinsically linked to trust.

Interestingly, in their study assessment of police officers opinions on FRT, Urquhart and Miranda (2022) revealed that officers themselves appear to share some of the same concerns as the general public when it comes to FRT implementation into law enforcement. The authors conducted 26 semi-structured interviews with officers ranging in ages, ranks etc from two separate British police forces in different locations, with the interviews containing questions related to both the current and future use of FRT. What Urquhart and Miranda (2022) found was that five distinctive concerns/themes were voiced by the police officers in relation to FRT use and these were: 1) ineffectiveness 2) Inaccuracy 3) distrust 4) Usefulness 5) Intrusiveness. Urquhart and Miranda's (2022) study not only exhibited that the officers did not believe that FRT is necessary when Fingerprint analysis etc is already available, but they also appeared to be very aware of the various worries expressed by the public and scholars alike, as well as the flaws that have been noted in the research around the area of FRT and expressed distrust and skepticality around its use.

Surveillance studies theories and concepts

Scholars within the surveillance studies space have developed a myriad of theories and concepts that attempt to not only critically examine new and upcoming technologies, such as facial recognition, but also to comprehend the wider social, political and cultural implications of surveillance practices that new technologies have the ability to cause in modern societies. These theories and concepts aim to shed light on the over-reliance placed on surveillance technologies and the ways in which these systems shape power dynamics, enable social control and invade privacy and individual and collective identities. Thus, they seek to encourage individuals and communities to engage in discussions about the risk and benefits of surveillance, the exchange

between security and privacy, the relationships existing between governments and surveillance technology producing corporations and the ways in which surveillance technologies can be ethically and responsibly implemented. In the context of FRT used by the police, which is what this paper intends to critically analyse, I believe the following surveillance studies theories and concepts exhibited in the literature will be the most appropriate to consider in order to aid in evaluating police use of FRT and sufficiently address this study's proposed research questions.

The Janus-face of surveillance technologies

Firstly, for Lyons (2001), societies that are littered with various forms of surveillance are Janus-faced. On the one hand, Lyons (2001) argues that the growth of surveillance-focused technologies can be used to provide a host of benefits to modernity, such as creating convenience and ease when completing everyday tasks as referred to in the introduction of this research paper. They can also, as Lyons (2001) notes, empower both workers and consumers in addition to promoting the rights of citizenship. However, as asserted by Lyons (2001), in their true "double-edged sword" nature, such technologies can also be more concerned with 'control' rather than 'care', which can result in adverse effects of the technologies such as the exacerbation of social inequalities.

Technological Solutionism

Secondly, relevant to the use of FRT by the police, is the concept of 'technological solutionism' which gained significant popularity within the academic space and beyond in 2013, when researcher Evgeny Morozov published his book 'To save everything, click here: The folly of technology solutionism'. The term, as Morozov (2013) describes, refers to the over-reliance placed on new and upcoming technological advancements to solve real-world problems. He argues that there is a growing tendency to see technology as a panacea for complex social, political, and economic issues. This perspective, which he calls 'technological solutionism' posits that with the right app or algorithm, any problem can be fixed.

However, Morozov (2013) raises concerns about the dangers of technological solutionism and argues that it 'oversimplifies' complex issues, reducing them to technical problems with straightforward solutions. In doing so, Morozov (2013) believes that this mindset can result in

the disregard of the underlying societal and ethical aspects of these problems and can lead to a misplaced faith in technology, potentially causing more harm than good. In line with this, Morozov (2013) notes that initiatives that claim to revolutionise societal sectors such as governance or healthcare through the medium of digital innovation, can result in unintended consequences and significant ethical dilemmas.

Central to his argument, Morozov (2013) highlights the importance of preserving what he calls "the moral character of problems". He contends that some problems are inherently moral and require thoughtful, nuanced and often contentious discussions and decisions. Technological solutionism, he argues, can undermine these essential moral debates by providing simplistic, 'one-size-fits-all solutions. Morozov (2013) advocates for a more balanced approach that considers the broader social and ethical dimension of problems, rather than relying solely on technological fixes. Thus, Morozov (2013) urges us to be cautious about embracing the allure of new technologies that on the surface, may seem to be an efficient way to combat a significant societal problem, however, what began as a seemingly good solution, may have detrimental impacts to society.

Political Economy of Surveillance

The surveillance concepts under the umbrella of the 'political economy of surveillance' provide a useful avenue to explore FRT use by the police. This is because the political economy of surveillance allows us, as Munoriyaraw and Mare (2023) put it, to dissect the existing relationship among and between the key stakeholders involved in the investment of advanced surveillance technologies, such as FRT and its use by the police.

The first of these is Shoshana Zuboff's (2015) concept of 'Surveillance Capitalism'. Zuboff (2015) notes that surveillance capitalism refers to the economic system that emerges from the relentless collection and commodification of personal data by corporations. Zuboff (2015) expresses that companies profit by surveilling individuals, capturing their digital activities, and turning them into valuable assets for targeted advertising and behavioural manipulation, often without the knowledge or consent of the individuals being surveilled. In this way, Zuboff (2015) highlights the transformation of surveillance into a profitable business model, where data is seen

as having monetary value, raising concerns about privacy, autonomy, and the power dynamics between individuals and corporations in the digital age.

Second to this is the 'Surveillance-Industrial complex'. Parallel to the theoretical ideologies well-known in the criminological sphere such as the 'military-industrial complex' popularised by the United states president Eisenhower in his 1961 farewell address and the later established 'prison-industrial complex' coined by Davis (1944-1999). She describes the growth and exploitation of prison populations and labour being largely for the purposes of profit for corporations and governments, scholars too have suggested that there is a similar dynamic at play in the case of the rapidly expanding nature of surveillance, such as that provided by FRT (Hooks, 2008).

Scholars in this area, Ball and Snider (2013), suggest that emerging from both of the earlier founded ideologies has come the 'surveillance-industrial complex', a term they use to depict the intersection of interests between the neo-liberal state and capital gain, resulting in the growth and prominence of the surveillance society. The term 'surveillance society' refers to societies wherein a large component of how they function is due to the extensive recording, collection, analysis, storage and application of information on individuals and groups that reside in those societies (Surveillance Studies Network, 2014).

Put simply, what both Ball and Snider (2013) argue is that surveillance is what they term an "organisational control process", which is formulated not to promote interests of the public or other concerned parties for that matter, but to further the voices and desires of specific actors within society and silence and weaken the voices of others. They argue that what comprises the distribution and deployment of surveillance systems today is the strive to gain capital and its subsequent interaction with state agencies, such as the police.

Conclusion

In conclusion, this literature review has shed light on the multifaceted landscape of FRT use by law enforcement agencies. As we navigate the intricate terrain of FRT deployment, several key areas of research have emerged. The prominence of FRT in contemporary society

underscores its significance, and the expansion of its applications warrants comprehensive examination. Police utilisation of FRT introduces complexities ranging from operational enhancements to ethical and societal implications. The concerns surrounding accuracy and bias, coupled with the critical analysis of existing regulatory frameworks, emphasise the urgent need for comprehensive scrutiny. Privacy and civil liberty apprehensions, as well as public acceptance, further contribute to the discourse surrounding FRT.

Finally, the dissertation's foundation in surveillance theories ensures that the forthcoming analysis will be deeply rooted in critical perspectives, allowing for a comprehensive exploration into the intricate web of issues surrounding FRT use within the law enforcement space. This literature review serves as a pivotal precursor, laying the groundwork for a rigorous and insightful investigation into the complexities of FRT's integration into policing and its implications for society at large.

Chapter Three
Methodology

Introduction

This methodology will outline in detail the approach I employed to address my research questions. These were: 1) Is the use of FRT by the police as an investigative tool justified? and 2) To what extent can the lens of surveillance studies aid in explaining the drive to adopt FRT within law enforcement?

In the first section of this methodology I will explain my rationale for selecting a qualitative methodological research approach, outlining the advantages of this approach making reference to academic literature and study. Following this, I will detail my use of cross-case analysis of the two policing agencies included in this study on their use of FRT and I will discuss how I specifically selected and gathered my data from these cases by utilising a purposive sampling strategy, a qualitative research technique that has effectively been employed by a number of researchers.

I include a section outlining the limitations of this research approach that have been identified in academic reports; however, I also include reference to scholars who support this research approach by means of justifying my own selection for investigating my research questions. Further, a section of this methodology is dedicated to any ethical considerations I undertook during my research. The final section is concluded with a brief review of my research methodology.

Research designs and benefits

To achieve the objective of this study and successfully address the proposed research questions mentioned in the introduction, this research paper adopted a qualitative methodological approach, specifically employing a comparative case study analysis. When defining what exactly a case study is, Yin (1990, p.23) asserts that it is “an empirical inquiry that investigates a contemporary phenomenon within its real-life context”. In other words, this form of analysis allows for the examination and real-world illustration of a particular subject matter. They can be

used to examine, explain, and characterise occurrences or phenomena in their natural environments (Yin, 2009). They can, for instance, aid in comprehending and summarising the casual relationships and pathways that come from the creation of a new policy or service (Crowe *et al*, 2011). Case study methodologies are frequently used within the social science field and as George and Bennett (2005, p.151) note, "involve the nonstatistical comparative analysis of a small number of cases…. the study of two or more instances of a well-specified phenomenon that resemble each other" (Zainal, 2007; Crowe *et al,* 2011).

The benefits and advantages of this form of methodology have been extensively documented by scholars over the decades, particularly when applied to social science disciplines such as criminology and/or criminal justice research. For instance, it has been noted that using a case study analysis approach in a a general sense not only facilitates an in-depth exploration and understanding of multi-faceted and complex issues such as FRT use by the police, but also enables a researcher to go beyond the constraints of quantitative research and statistics and understand the behavioural conditions that are at play within a given scenario (Zainal, 2007; Crowe *et al,* 2011). In the same vein, rather than just relying on one source of evidence, which is common to quantitative methods of research, case studies involve numerous sources of evidence which allows for a well-rounded and holistic view of a certain phenomenon or series of events (Gummesson, 1991; Zainal, 2007).

Additionally, case studies enable researchers to pick apart the "how" and "why" certain circumstances are occurring and can clearly depict lessons learned elsewhere, which may be used, compared and applied to future cases (Anderson, 1993; Williams, 2020). Further, the method of case study analysis has been noted as particularly useful within the criminological field, especially in the context of demonstrating the role that theory plays in explaining why certain events or phenomena occur that appear to be, on the surface, unjust and volatile (Quinn *et al*, 1992).

Thus, case study analysis facilitates the bringing to life of criminological theory and concepts, such as those embedded in surveillance studies, by promoting inductive reasoning and highlighting theory's operation in the real world, while simultaneously depicting a more

complete and thorough view of a particular phenomenon (Quinn *et al*, 1992). As Crowe *et al* (2011) put it, findings from case studies may have an impact on both the developing and evaluation of theories and in some cases, may permit theoretical (rather than statistical) generalisation outside of the specific example under study, which is an aim of this study.

When used in conjunction with the comparative method, thus forming a 'comparative case study' analysis as seen in this research paper, this allows for the expansion of the scope of a case study and enables researchers to have the ability to, as Knight (2001) puts it, "assess generalisations that extend across multiple cases".

Further to that, Dammer and Albanese (2014) outline the benefits to the comparative case study approach when using it in the in tandem with criminal justice research and note that it is vital in this context for three reasons, these are: 1) It broadens our understanding of specific topics 2) It allows for us to learn from the experience of others and 3) It allows for us to deal with transnational crime in a more effective manner, making it a very fitting approach for the purposes of this research. In addition, although the research in question does not involve the study of 'transnational crime' per se, the phenomenon of police use of FRT is transnational in that it presently operates across numerous national boundaries.

These outlined benefits and advantages of employing a comparative case study analysis approach underpin the rationale of why this method was chosen for this research paper as the principal aim of this study is to not only provide a detailed and comprehensive account of FRT use by the police in two distinct jurisdictions, but also to demonstrate how surveillance theoretical concepts, influence this.

Case selection and data collection

The cases analysed in this study include a total of two distinct policing organisations located in two separate jurisdictions internationally, whose law enforcement have adopted the use of FRT. These are the Metropolitan Police Service (MPS) in the United Kingdom and the New York Police Department (NYPD) in the United States. These specific cases were chosen by way of a purposive sampling strategy, which is a widely used qualitative research technique that

is employed by researchers in order to both identify and select information-rich cases related to the topic of interest, for the most effective use of limited resources (Patton, 2002; Palinkas *et al*, 2015). It involves finding and choosing the units (i.e organisations, cases, people, events) that have significant experience with or knowledge on a particular phenomenon, the ultimate aim being to enable a researcher to best answer their chosen research question or questions by focusing on specific characteristics of a given population (Cresswell & Plano Clark, 2011; Rai & Thapa, 2015). As a result, the selection of what cases will be included in a particular study relies on a decision made by the researcher, typically based upon the organisations, populations and events that are most suited to the research in question (Rai & Thapa, 2015).

The reasoning and criteria underpinning the decision to choose the above mentioned cases for this research paper is that despite being located in separate jurisdictions and therefore subject to different regulations and policies, each police agencies uptake of FRT has been a source of unease and controversy, which has has given rise to concern by numerous parties such as scholars, civil liberty advocates and other interest groups. Thus, this provides an opportunity to assess the role of surveillance theories in this.

Due to this research being wholly desk-based in nature, data on each police organisations use of FRT was obtained from multiple secondary sources including relevant literature, news and media sources, official government and police organisation documents (when available) and non-profit and interest groups publications on the use of FRT by the chosen police agencies (when available). The process of using several sources of data is otherwise known as 'data triangulation' and has been advocated as a way of promoting a study's internal validity due to the adoption of different angles and its ability of facilitating a comprehensive illustration of a particular phenomenon (Stake, 1995; Mason, 2002; Pinnock *et al*, 2008).

It should also be noted that during the course of this study, a freedom of information request for data regarding the future adoption of FRT into the Irish policing space was submitted to An Garda Síochana. Unfortunately, the request was refused on the grounds that the data sought "falls outside the scope" of the Freedom of Information Act 2014 "as it pertains to An Garda Síochana". While this information was not essential for the purposes of this dissertation, the

refusal limits the depth of the analysis conducted in terms of how, if implemented, the Irish police plan to use the technology. Nevertheless, still sufficiently addressing the aim of this research paper, the data and other sources available for the analysis of the two police agencies contemplated in this research paper provide valuable insights into the broader use and implications of FRT.

Data Analysis

The data collected from each case study will be analysed via cross-case comparisons, and will then be followed by a surveillance studies analysis of police use of FRT in order to gain a deeper insight into the phenomenon. This analytical approach will not only enable the examination of the broader social, political and economic factors that can occur through FRT adoption by the police, but it will also facilitate an in-depth investigation into the implementation and subsequent consequences of FRT use in the policing space. This approach will allow for the identification of any emerging similarities and differences exhibited in each country's case, enabling the identification of recurring themes, if present. Drawing on relevant surveillance theoretical frameworks, FRT use by the police will be analysed through this conceptual lens to explore the broader societal implications of FRT. By examining the role of surveillance studies ideologies in the implementation and use of FRT by the police, this analysis will shed light on the power dynamics, interests and implications of such technologies. Through the application of this theoretical framework and cross-case comparisons, key themes and patterns will be identified across the case studies. The data will be carefully analysed to capture these themes and explore the underlying power structures and dynamics at play.

Limitations

It is worth noting that there are several limitations of this study. The application of the surveillance studies conceptual framework is theoretical and relies on the available data derived from the case studies. However, the case study analysis method has received a variety of criticisms from various academics. Firstly, the method has been said to lack sufficient scientific rigour due to the discretion a researcher has in case selection which can facilitate bias, ultimately influencing the subsequent findings of a study (Yin, 1984). Secondly, it has also been critiqued as not reaching the threshold of generalisability as oftentimes case studies are based on a singular

case which can result in questions surrounding the method's reliability and applicability to the world at large (Yin, 1984; Johnson, 1994; Tellis, 1997). As Yin (1984, p.21) notes, "How can you generalise from a single case?". Third and lastly, the case study analysis method has been argued to be difficult to conduct, too long in length, in addition to producing a significant amount of documentation (Yin, 1984).

Despite these negative comments on this form of research approach, Chopard and Przbylski (2021) assert that the case study method is no different to any other research approach in terms of its various strengths and weaknesses, with a selection of highly impactful and valid case studies existing that demonstrate how such a method can produce significantly rigorous results. However, in an effort to address the limitations of the case study analysis method, researchers have moved towards analysing two or more case studies concurrently. Therefore, in contrast to a single case study design, this study employed a comparative case study analysis approach of two police agencies, as similar findings across more than one case study is largely considered to be quite a robust finding (Yin, 1993). Thus, increasing the validity, accuracy and overall generalisability of the findings, enabling the researcher to capture a more comprehensive overview of the subject under study (Noor, 2008). Additionally, drawing on appropriate theoretical frameworks, as exhibited in this study, has also been noted as a way of negating these drawbacks (Crowe *et al*, 2011).

Ethical Considerations

As stated, this research paper adopted a qualitative methodological approach, specifically employing a comparative case study analysis to conduct my research. Given that the data I collected is in the public domain no ethical approval was necessary or required for this section of my paper.

Conclusion

To summarise, I found a qualitative methodological research approach most appropriate to investigate my research questions 1) Is the use of FRT by the police as an investigative tool justified? And 2) To what extent can the lens of surveillance studies aid in explaining the drive to adopt FRT within law enforcement?

The specific research design used was a comparative case study analysis focusing on two countries whose law enforcement have adopted the use of FRT. This included the NYPD in the United States and the MPS in the United Kingdom. The relevant data collected from each of the two case studies will be analysed through the means of cross case comparisons, looking in depth at the use of FRT surveillance by the given law enforcement in the selected countries. Although there are few limitations to this form of research methodology, I have highlighted in this section several examples of academic researchers utilising a cross case comparison research design successfully. Hence, in the following chapter of this paper I will outline my findings from each of the case studies that will aid in answering my research questions.

Chapter Four
Case Study Findings

Introduction

In this chapter, I will present the findings of my research paper which were gathered using the research methods that I described in detail in Chapter 3. The first case study dealt with is the New York city Police Department (NYPD) in the United States (U.S), which is then followed by the second case study of the Metropolitan Police Service (MPS) of London in the United Kingdom (UK).The comparative case study analysis approach that i employed in this study allowed me to make correlations across both police agencies, drawing on similarities and differences between the two.

The New York City Police Department

Background

By virtue of the design and implementation of analytical crime networks such as the Compstat crime statistics system in the early 1990's, the New York City Police Department (NYPD) have been in the business of pioneering technology-led surveillance and policing strategies for the last thirty years (Eterno & Sullivan, 2010). More recently, they have been considered to be the "vanguard" behind the growing push, interest and adoption of sophisticated surveillance technologies in the law enforcement arena, which has become increasingly apparent across police agencies throughout the United States (U.S) (Patel & Price, 2017). This status that has been acquired by the NYPD is linked to the heightened emphasis on security and intelligence measures that came with the tragic aftermath and extensive number of lives lost in the well-known terrorist attack on the world trade centre on September 11th, 2001. What followed was a complete remodel, reform and significant expansion of New York's pre-existing counterterrorism programmes and security intelligence, in order to prevent a similar situation from happening again in the future (Nussbaum, 2012; Apuzzo & Goldman, 2013; Dahl, 2014). Among the steps that were taken to enhance public safety and protection after this event in New York was the deployment of what Landon-Murray and Milliman (2023, p.1) refer to as "more advanced surveillance technologies" by law enforcement.

This development in the NYPD's approach to policing consisted of the rapid uptake of various technological and surveillance-focused tools. For example, with the assistance of Microsoft, the NYPD launched the Domain Awareness Programme (DAS) in 2009, which enabled the NYPD to have quick and easy access to a considerable amount of information like arrest records, licence plate readers, 911 calls and upwards of 3,000 security cameras around the city (Kamali, 2017). Notably, via these sensor systems (i,e licence plates & security cameras), the DAS surveillance network gave the NYPD the ability to both follow and track individuals nationwide, with the system not being limited to suspected criminals or terrorists (Tempey, 2016; Levine *et al*, 2017). Alongside the introduction of systems such as this, a multitude of other surveillance tools were also deployed by the NYPD over the years such as 'cell-site simulators' (Stingrays) that operate to obtain mobile phone data by impersonating a cellular tower, 'x-ray vans' with the capability of examining close by vehicles and buildings for items like drugs and explosives and most importantly for this research, FRT (Friedersdorf, 2015; Long, 2016; Watkins, 2021; Landon-Murray & Milliman, 2023).

Adoption, successes and policy

In the time succeeding the 2001 disaster, the use of these surveillance technologies by the NYPD, FRT in particular, has grown significantly and are no longer just used in the context of anti-terrorism. Formally employed by the police agency in 2011, it has been reported that the NYPD has utilised FRT in 22,000 cases since the year 2017, with half of these occurring in 2019 alone (Amnesty International, 2021; NYPD, 2021). If we delve somewhat deeper, it was documented that in the first 5.5 years of the NYPD using FRT, 2,878 arrests were made in addition to NYPD detectives having used the technology when conducting 7,000 of their searches for suspects in the year 2018 solely (Garvie, 2019; Benedict, 2022).

This clear and continued reliance on FRT by the NYPD, as an investigative tool, has been coupled with the police agency crediting the technology as being successful in an array of cases (NYPD, 2021). For instance, it was reported that in 2019, FRT aided the NYPD in identifying and arresting a suspected terrorist that placed a pair of rice cookers that were believed to be bombs at a subway station, whilst also supplying the NYPD with the means to identify and apprehend an accused rapist within a 24 hour timeframe after his first attack in the same year

(McCarthy, 2019a; McCarthy, 2019b; Parker, 2020). Further to this, the NYPD state on their official website that in 2019, their use of FRT generated an abundance of substantial leads in criminal investigations, with 2,150 possible matches identified for a wide range of crimes from murders and robberies to felony assaults and rapes (NYPD, n.d.).

According to the NYPD's (2021, p.3 & 4) revised policy surrounding the operation of FRT, they note that the technology does not perform in real-time, rather, officers run a still image that is otherwise known as a "probe image", which has been obtained from either a photo or video throughout the duration of an investigation, against a pool of photos that have already been previously acquired by the NYPD. In other words, this "pool" contains photos of individuals that have come into contact with NYPD law enforcement before and consists of both arrest and parole photographs, which the NYPD refer to as the "photo repository" (NYPD, 2021, p.3). The NYPD's policy also states that once the FRT has identified a potential match, this merely generates an "investigative lead" and does not give rise to what they term a "stop", "probable cause for arrest", nor does it give the NYPD the ability to "obtain a search warrant" to search that person or their respective dwelling (NYPD, 2021, p.4). Furthermore, the NYPD's (2021, p.5) policy on FRT use explicitly states that it does not use FRT to identify or monitor individuals at political rallies or in crowds and additionally asserts that comparing images to photos outside of the NYPD's photo repository is strictly prohibited unless permission is granted by a superior for an "articulable reason". This policy mirrors what was stated in the earlier published NYPD patrol guide (2020) in regards to FRT use, with the patrol guide also stating that when an officer intends to compare an image against the photo repository, a request must be submitted to the Real Time Crime Center - Facial Identification Section (RTCC-FIS), whom perform the facial analysis and return a match result report to the investigating officer once the analysis is complete. Based on the verdict of this analysis, the investigating officer determines whether further investigation is warranted in order to establish "probable cause" (NYPD, 2020).

Criticisms and Concerns

Notwithstanding its documented investigative achievements and published operational guidelines, the NYPD's use of FRT has generated a host of criticism, scrutiny and legal

challenges put forward by a variety of concerned bodies ranging from government officials and academics to civil liberty advocates and other interest groups.

Inadequate regulation, governance and oversight

A prominent subject of unease that has been raised is the topic of regulation, governance and oversight of the technology. In New York city, the use of FRT by law enforcement is completely legal, with no overarching regulatory body or law to determine how, when, why and where police officers use it (Restrepo, 2023). Thus, the onus of policy-making and procedure development for the technology falls solely on the NYPD, meaning that their own formulated documents, manuals and protocol relating to the use of FRT are the only existing controls (Kofman, 2017). This is facilitated by what Almeida *et al* (2022, p.383) refer to as the "fragmented legislative territory" that has and continues to exist in the United States (U.S) in respect of FRT use by police agencies. Despite being a frequently used and popular tool amongst U.S law enforcement affecting up to what Garvie *et al* (2016) note as 117 million people, there is currently no federal law that deals with the matter (Robinowicz, 2023). Due to this lack of national governance, the decision to regulate and place limits on police use of FRT is dealt with at a state and municipal level, which has enabled several U.S cities such as San Francisco in California, Boston in Massachusetts and Portland in Maine to impose complete bans or similar legal barriers to halt the use of the technology by law enforcement (Dauvergne, 2022b). Nonetheless, whilst New York city legislators and those in congress have the ability and power to alter how the NYPD operate and deploy FRT, the uncontrolled and self-determined legislative terrain has prevailed. In fact, the city's current mayor, Eric Adams, is in full support of the present use of the technology by the police and has asserted his advocacy for its expansion (Goldenberg & Anuta, 2022).

Whilst this limitless FRT use environment has persevered for the NYPD, there have been some attempts made to improve this situation in New York city. The office of the Inspector General for the NYPD (OIG-NYPD) was established in 2013 by the New York city council, allowing an external body to initiate investigations and audits when required on the NYPD, inclusive of its use of surveillance technologies, such as FRT (Kempf, 2020). Additionally, following persistent campaigning by activists and civil liberty groups in New York such as the

Surveillance Technology Oversight Project (S.T.O.P), the New York Civil Liberties Union (NYCLU) and the New York Legal Aid Society, a further effort was made to improve this with the implementation of the Public Oversight of Surveillance Technology (POST) Act in 2020 (Brennan Center for Justice, 2021). By virtue of this Act, the NYPD are under an obligation to publish 'use and impact' policies for both current and future surveillance technologies, which is the NYPD's FRT policy outlined previously in this section (Landon-Murray & Milliman, 2023). Within these published policies, the NYPD are required to cover many aspects of the technology in question such as data security measures, access and usage restrictions and its impact on marginalised groups, to name a few (Landon-Murray & Milliman, 2023). As per their function, the OIG-NYPD are responsible to ensure the NYPD's compliance with the POST Act and report breaches and/or infractions in addition to making suggestions for improvement if necessary (London-Murray & Milliman, 2023). Interestingly, a report conducted by the OIG-NYPD in 2022 discovered that the NYPD had violated the POST Act on a number of grounds (S.T.O.P, 2022). Upon discovery of this, the OIG-NYPD made recommendations to the NYPD to correct this. However, a report published in March of this year revealed that the NYPD declined to implement 14 out of the 15 recommended changes that were made (Claburn, 2023).

Though the establishment of both the OIG-NYPD and POST Act certainly represent significant developments in enhancing the oversight and rules surrounding the NYPD's use of FRT, civil liberty advocates have disagreed with their effectiveness. For example, upon review of the draft 'impact and use' policies that were published by the NYPD, the NYCLU submitted a letter to the NYPD commissioner regarding the "overbroad", "inaccurate" and "inadequate" issues with the policies. Commenting on the FRT policy specifically, Michael Sisitzky and Ben Schaefer of the NYCLU (2021) stated that the policy did not address the extent to which the data being collected on individuals is being shared and collected amongst third parties or how long the NYPD retained said data. Importantly, despite receiving these critiques, the final policies released by the NYPD remained largely the same and were minimally edited (NYCLU, 2021) They also refused to mention anything about machine learning or artificial intelligence, even for technologies that have been previously noted to rely on methods such as this, like FRT, in addition to failing to incorporate the public's criticisms and concerns (NYCLU, 2021). It is also important to notice how neither measures taken combat the ultimate decision-making power that

the NYPD still possess regarding surveillance technologies like FRT. This was echoed in the New York City State Comptroller's (NYCSC) report that was issued in February of this year wherein the key finding was that New York city has an "adhoc and incomplete" approach to AI governance and has allowed for independent city agencies, such as the NYPD, to both create and develop their own "divergent" approaches to the topic with virtually no set rules or limits on the actual use of the AI in question (NYCSC, 2023, p.1). The report further stipulates that this standpoint of New York city on this matter does not combat the issues of transparency, accuracy, bias or disparate impacts (NYCSC, 2023, p.1). The main suggestion made by the report is that New York city needs to implement an "effective AI governance structure", which at the time of writing this research paper, is yet to be addressed (NYCSC, 2023, p.2).

Violations of Privacy, Civil Liberties and Data Misuse

In line with the comments made by the state comptroller (2023), concerning details have emerged regarding how the NYPD use their FRT both before and after the enactment of the POST Act. Following a two year legal struggle to obtain any information from the NYPD relating to their FRT use, researchers from the Georgetown Law Center on Privacy and Technology, led by surveillance technology expert Claire Garvie (2019), uncovered that the NYPD had been using the technology in a variety of questionable ways. Applied in countless routine investigations, it was revealed that the NYPD had tampered with facial images, such as replacing an open mouth with a closed one in order to increase the chance of the FRT finding a potential match (Brandom, 2019). For the same reason, it was also found that to fill incomplete images where the individuals face was not clearly visible, the NYPD used a 3D software to rotate faces in addition to uploading images of celebrities to their database to detect criminals that they believed to be a look-alike of that famous person (Schuppe, 2019; Mejía, 2019; CBS New York, 2019). The researchers also noted that on many occasions, NYPD police officers bypassed long-established investigative techniques to confirm a potential match result (Schuppe, 2019). These instances, as the report (2019) put it, ultimately resulted in the NYPD's "fabrication" of people's facial identity points, leaving the possible misidentification of individuals unavoidable.

The topic of civil liberties such as the right to protest and the right to privacy have also come under the microscope in terms of the NYPD's use of FRT. During the Black Lives Matter (BLM) protests in New York city in 2020, an activist was tracked down and identified by the NYPD using FRT on the basis that he assaulted a police officer (Vincent, 2020). It was later reported that the NYPD used a picture from one of the activist's social media profiles in order to find him as he had no previous criminal history, as was stated in his filed lawsuit, and would therefore not be in their database (Joseph & Offenhartz, 2020). When questioned on how this photo constituted a surveillance video, image or an arrest as per their FRT policy, the NYPD failed to comment (Joseph & Offenhartz, 2020). However, this activist was one of many. Following the outcry and lawsuit filed by civil liberty organisations Amnesty International and the Surveillance Technology Oversight Project, it was subsequently revealed, on instruction of the supreme court of New York, that the NYPD had used FRT covertly to surveil numerous activists throughout the BLM protests (Amnesty International, 2022b).

Additionally, while the police agency has been documented to consistently deny any affiliation with the controversial FRT known as 'Clearview AI', it was revealed that the NYPD had not been very transparent about this (Mac, Haskins & McDonald, 2020a; 2020b). Known for the invasive and secretive form of surveillance it provides by scraping facial images of thousands of individuals from the internet and storing these in a database indefinitely, Clearview AI has found itself facing a multitude of legal battles on the grounds of privacy law infractions (Dul, 2022; Evans, 2022). However, notwithstanding the NYPD's claims and questionable reputation of Clearview AI, a freedom of information request submitted to the NYPD revealed that a relationship between the two existed as far back as 2018 (Haskins, 2021). In fact, it was reported that the NYPD had run the software to conduct approximately 5,100 searches in an effort to create "investigative leads" (Mac *et al*, 2021). This is especially troubling because stated policies prohibit the NYPD from building an unsupervised database of images that facial recognition software can utilise and limit the use of the technology to a single team (Ryan-Mosley, 2021). Further violations of the NYPD's FRT policy were also discovered via the freedom of information request, which revealed that officers had downloaded the Clearview AI application onto their personal devices also (Ryan-Mosley, 2021). Thus, stated policy seems to have been circumvented in this instance.

Inaccuracy and Discrimination

Since its inception, the NYPD have not been particularly forthcoming with information in relation to their use of FRT or its effectiveness in terms of accuracy, which has given rise to criticism. As addressed in the literature review of this research paper, while it has been well-established and extensively documented within the academic space that FRT is not entirely accurate, particularly when it comes to the age, gender or ethnicity of individuals, there exists no published accuracy testing of FRT by the NYPD. However, what we do know is that 'Dataworks Plus', the FRT software primarily used by the NYPD that does not publish accuracy rates of their own, has been responsible for the wrongful arrest of at least two black men in the city of Detroit in Michigan (Brown, 2020; Stokes, 2020; Harwell, 2021). Notably, commenting on the technology, the Detroit police chief asserted that the technology misidentified individuals 96% of the time in his police agency's experience (Koebler, 2020).

Finally, the ability for the NYPD's use of facial recognition to promote and perpetuate the over-policing of minority ethnic groups has also been a concept of major concern for civil liberty advocates. In research conducted by Amnesty International (2021; 2022a) as part of their 'ban the scan' campaign, they discovered that in areas in New York city where there was a high 'stop and frisk' rate and the residents were predominantly of non-white in ethnicity, there was a huge discrepancy in the concentration of CCTV cameras. Thus, Amnesty International (2021; 2022a) argue that the NYPD's access to more than 15,000 CCTV cameras in these areas of the city, whereby they can gather still images to run through the FRT, reinforces the disparities that we have historically been observed seen in New York, leading to the "supercharging" of racially driven policing in a city where it is already apparent. For example, as outlined by the NYCLU (2018) in their analysis of the NYPD 'stop and frisk' reports, since the year 2003, ethnic minority groups such as individuals of black and latinx descent have been significantly overrepresented in the statistics when compared to their white counterparts

The Metropolitan Police Service of London

Background

Similarly to the NYPD in New York city, the Metropolitan police service (MPS) of London in the United Kingdom (UK) have had a long-standing interest in advanced surveillance technologies and their deployment in the policing context. This lengthy historical trajectory of the MPS's flirtation with surveillance-focused devices can be easily observed if we firstly look to the mid to late nineteenth wherein the 'Habitual Criminals Registry', a system allowing for the constant police surveillance of released prisoners, was moved from the Home Office to the hands of the MPS (Williams, 2003). Whilst not nearly as advanced as the NYPD's history with surveillance-focused technology such as Compstat Crime Statistics system, this device operated by distributing information about freed prisoners, who had been deemed likely to commit further offences in the future, to all police forces in the whole of the United Kingdom (The Digital Panopticon, n.d.).

This was followed by the police agency's uptake of fingerprinting, which was brought to the attention of the police agency in 1901 when pioneer of the technology, Edward Henry, joined the force (Williams, 2003). Once the technology had been made known to the MPS, the use of fingerprinting by the police agency and the reliance they placed on the technology was significant, as by the year 1950, there was excess of one million fingerprints from individuals who had come into contact with the police agency on file (Scott, 1954). Thus, at this stage, the extent of the MPS's use of surveillance in their respective policing approach was simply that offenders fingerprints were taken, habitual reoffenders were registered and tracked via the use of the Habitual Criminals Register, while the remainder of the populace was monitored and patrolled by the mundane watchful eye of the beat cop (Miller, 2017).

If we fast forward to the twentieth century, this growing interest in surveillance technologies exhibited by the MPS continued. Throughout the early and late 1950's, london-based police agencies were beginning to look into more advanced surveillance technologies such as closed-circuit television (CCTV). Initially, police agencies installed CCTV cameras around London city in 1953 during the queen's coronation, with CCTV later being used by law enforcement as a visual aid in conjunction with traffic light operations, that consisted of

only one man (Williams, 2003; Gentile, 2023). This spotlight placed on CCTV was met by comments made by well respected police officers and home office civil servants, who wanted to manage police manpower more efficiently through the use of technology and therefore encouraged UK police to arm themselves with new and avant-garde technological instruments for the job (Critchely, 1967; Rawlings, 2002).

This encouragement to adopt new and upcoming technologies to improve investigation efficiency was evidently taken into consideration by the MPS, as they began experimenting with CCTV as an investigative tool in the 1960's following the London underground bombing by the Irish Republican Army (Gentile, 2021; Professional Security, 2022). This would later evolve into the use of smart CCTV cameras by the MPS in 1998, which had the capacity to transform the low-resolution, black and white footage obtained by the earlier CCTV cameras to in-colour and better quality footage, with the capability of functions such as time-lapse and motion-only recording which saved time, money and resources (Fisher, 2021; Gentile, 2023).

From then on, the MPS proceeded to acquire more advanced and sophisticated surveillance technologies into their investigative apparatus. For instance, as asserted by Fussey (2007), the mid 1990's witnessed the deployment of automatic licence plate recognition (ANPR) systems across the city of London, which continue to be used by the MET police today (The Metropolitan police, n.d.). More recently, following a trial of the surveillance-focused technology in 2014, the MPS acquired the use of body-worn cameras, with a freedom of information request sought in 2021 revealing that since their official adoption in 2016, the police force have a total of 26,500 of these cameras now in operation (Press Association, 2016; Grimond, 2022).

However, as could be observed in New York City with the NYPD and most notably for the aim of this research paper, among the selection of surveillance technologies that the MPS have contemplated as a potential tool for law enforcement purposes is FRT.

Adoption, successes and purported benefits

FRT was first experimented with in the city of London in the late 1990's, however, limits of the technology at the time prevented it from progressing any further, which resulted in the temporary abandonment of the technology's use (Fussey, 2012). It was not until 2016, more than a decade later, that the MET police began formally trialling FRT as a tool for investigative purposes (Dodd, 2017). Between the years of 2016 and 2019, the MPS carried out a total of ten trials of live FRT across London, with the term 'live' meaning that the technology used allowed the police agency to, as Bradford *et al* (2020) note, "carry out real-time automated identity checks in public spaces". These were largely conducted via the use of a live facial recognition (LFR) van equipped with a camera mounted on the roof producing a live feed of passers by, which would be monitored by a central control centre, who would communicate with officers on the ground if an individual from the watch list database came into focus of the FRT (Fussey & Murray, 2020).

The first FRT trial performed by the MPS was completed at the Notting Hill Carnival in 2016, with the aim of identifying known or wanted offenders, however, they failed to successfully identify any (Purshouse & Campbell, 2019). The following year, during the trial at the 2017 Notting Hill Carnival, the MPS managed to successfully identify one person, whilst five others were wrongly flagged by the technology (Purshouse & Campbell, 2019). On Remembrance Sunday of the same year, a day in Britain dedicated to remembering those who have died in conflict, the MPS successfully identified an individual from their watch list (Goodey, 2015; Purshouse & Campbell, 2019). However, whilst this certainly seemed rather encouraging on the part of the MPS, the police agencies's identification process in this scenario was marred with controversy as the police agency were said to have utlised a watch list of people who were thought to obsessively follow certain public figures, with no viable evidence available that these people had previously committed any offences (Purshouse & Campbell, 2019). Further, in conjunction with British transport police, the MPS deployed FRT in 2018 at Stratford shopping centre located in London, that would, like the other trials, alert police officers if a person of interest came into the field of vision of the FRT (Dearden, 2018). This trial echoed the majorly unsatisfactory results of the prior FRT tests, leading to no positive identifications or arrests (Purshouse & Campbell, 2019).

Nevertheless, despite the evidently discouraging results that came from their trials of the technology, the MPS have expanded their use of FRT and have continued to credit the technology and its capabilities for investigative purposes. In fact, not only did the police force shift to official operational deployments of LFR in the earlier half of 2020, but they have also since implemented what they term "retrospective facial recognition" (RFR), which similar to the technology utilised by the NYPD, acts as an "after-the-event" option of identifying an individual suspected of a crime as it takes a still image from a photo or video and runs that image against a database of others (Fussey & Murray, 2020; Metropolitan Police, n.d.). Thus, it allows for the MPS to compare images against a far broader set of potential matches, rather than a limited watchlist as seen with the previously used LFR (Woollacott, 2021).

This development in the MPS's approach to policing has been accompanied by the same underpinning rationale that we saw in the context of the NYPD. This is that the deployment of FRT has the capacity to aid in the police's prevention and fight against crime by making it easier to catch wanted criminals, assist in the protection of vulnerable people (i.e missing persons) in society, resulting in the ultimate improvement of public safety and security (Gentile, 2021, Metropolitan Police. n.d.). The police agency has also further asserted that between February of 2020 and July 2022, it helped them arrest nine people who were 1) suspects for reported crimes and 2) individuals who had pending warrants out for their arrest (Gikay, 2023). Additional points made by the MPS in relation to the benefit of the use of FRT also include the comments made by Detective Inspector Bernie Galopin of the MPS on how the technology can build trust in the police force by displaying to the public what exactly they are doing (Deardean, 2018).

Regulation and policy

In contrast to the evidently problematic regulatory landscape, or lack thereof rather, shaping the NYPD's use of FRT in New York city, the MPS and their deployment of FRT is subject to various ethical and legal frameworks. Whilst similar to the situation in New York city insofar as there exists no specific piece of legislation that directly addresses the rollout and management of FRT by UK law enforcement agencies or otherwise, the MPS, and other

UK-based police agencies for that matter, are restricted by a number of regulations and policies that place limits on their use of the technology (Almeida *et al,* 2022).

General Data Protection regulation and The Data protection Act 2018

First and foremost, one of the fundamental principles guiding the deployment of FRT by the MPS is the European Union's (EU) General Data Protection regulation (GDPR), which was implemented into UK law via the enactment of the Data protection Act 2018, when the UK was still a member state (Government of UK, 2018; Richardson, 2021; Local Government Association, n.d.). Despite having since left the EU, the GDPR and its frequently referred to "gold standard" approach to protecting the rights and freedoms of EU residents, namely the right to privacy due its emphasis on consent, persists to apply within the context of the UK today (Popova, 2020; Almeida *et al,* 2022).

The GDPR established a stringent set of rules for the collection, processing and use of personal and sensitive data of individuals by both public and private entities (including law enforcement), which by virtue of article 9, encompasses the collection and analysis of biometric data obtained through the technological medium of FRT. As Almeida *et al* (2022) point out, there are multiple activities involving personal data that fall under the heading of 'processing' in this regard, ranging from the receiving and creation of data, to the deletion and destruction of said data. According to the Data Protection Commission (2019), there are a total of seven key principles at the heart of the GDPR that are central to its impact, which entities who are collecting and processing personal data need to adhere to and comply with, these are: 1) Lawfulness, fairness and transparency 2) Purpose Limitation 3) Data minimisation 4) Accuracy 5) Storage limitation 6) Integrity and Confidentiality and 7) Accountability.

To further explain these principles, they stipulate that: 1) data must be handled in a legal, just and open manner 2) Personal data can only be gathered for well-defined, clear, and lawful reasons and should not be used in ways that are inconsistent with those purposes 3) Data may only be processed if its appropriate, pertinent, and kept to the minimum necessary for the intended purpose 4) Only accurate and current data should be processed to the extent possible 5) Personal data should only be processed for the duration necessary for the specific purpose, and

controllers should establish retention criteria 6) Controllers must implement technical and organisational safeguards to protect personal data from unauthorised access, illegal handling, and accidental loss or damage and 7) Data controllers are responsible for complying with regulations and ust be able to demonstrate their compliance, which involves maintaining written records of their compliance efforts (Kotsios, 2019).

However, most importantly for the purposes of this research, article 9 of the GDPR stipulates that subject to exemptions, biometric data such as that recovered by the deployment of FRT used to identify a person, can not be utilised unless the person in question has given their explicit consent to do so. Among these areas of exemption both in the UK and across the entirety of the EU is law enforcement, with article 23 of the GDPR providing that the management of personal data for law enforcement reasons is determined by each member state individually (Almeida *et al*, 2022). GDPR also requires that for the purposes of high-risk applications of data collection and processing, such as FRT use by police agencies, a Data Protection Impact Assessment analysing and identifying the risks of such a process must be completed to ensure its justification and its appropriate implementation and management overtime (OECD, 2020).

Further requirements of the GDPR also include, but are not limited to, the establishment of an overseeing data protection ombudsman responsible for investigating complaints of GDPR breaches, to the appointment of data protection officers within any private entity or public authority that processes personal information such as biometric data, who are expected to take the stance of a 'whistleblower' when such parties fail to comply with the GDPR (Almeida *et al,* 2022).

Whilst the Data protection Act 2018 certainly placed the clearly set out requirements of the GDPR on a legislative footing in the UK, it makes notable provision for the use of FRT for identification purposes. For instance, as affirmed by Richardson (2021), one provision of the act states that the processing of all facial images is to be regarded as sensitive in nature, regardless of whether or not an image used matches individuals on the considered watchlist or if images are deleted later on. As such, any processing of data collected by FRT should be treated with the appropriate sensitive processing measures taken, adhering to the GDPR's regulations. Likewise, another provision of the Act is that data protection regulations apply to the whole process of

facial recognition identification (Richardson, 2021). In other words, rather than simply applying to the technology's general deployment alone, the regulations must also be contemplated when compiling comparison databases such as watchlists, as well as when deciding on the steps to be taken in terms of the deletion and processing of the data (Richardson, 2021).

Human Rights Act, the Surveillance Camera Code of Practice and AI-specific guidelines

In conjunction with the GDPR and Data protection Act 2018, the MPS and their deployment of FRT is also guided by the Human Rights Act, the surveillance camera code of practice and AI-specific guidelines that have been published by the UK Information Commissioner's Office (ICO).

If we firstly consider the Human Rights Act, this law has played a critical role in shaping the regulations around FRT in the UK. Passed in 1998, the act incorporated the European Convention on Human Rights into UK law, thereby emphasising individual fundamental rights such as the right to privacy and the right to respect for private and family life and compels public organisations including local councils, the police and the government to treat every person with fairness, equality, respect and dignity (Equality and Human Rights Commission, 2018; Liberty, 2020). Thus, the MPS and their use of FRT must be in line with these human rights principles, balancing the need for public safety and law enforcement with the protection of these fundamental individual rights.

Secondly, the Surveillance Camera Commissioner issued a code of practice in 2013, that offered specific guidance on the use of surveillance cameras, including FRT, by public authorities in England and Wales (Brown, 2022). This code, which has since been updated in accordance with the growing use of surveillance technologies in today's society, underscores the importance of transparency, necessity, and proportionality when deploying surveillance technologies such as FRT in public spaces (Brown, 2022). A core purpose for the initial publishing of the code, as highlighted by the Home Office (2013, p.5), was to instil confidence in the public that surveillance cameras are not being deployed to "spy" on them, but rather to support and protect them. As such, the code calls for law enforcement agencies to clearly define the purpose and objectives of their FRT deployments, ensuring that they are essential for

addressing specific security concerns (Home Office, 2013). Additionally, the code also calls for law enforcement agencies to provide information on other aspects of surveillance camera use such as details on who has access to the information gathered by surveillance cameras and the criteria that must be met for access to be granted (Home Office, 2021).

Thirdly, in response to the increasingly popular use of surveillance technologies that rely on AI such as FRT, the UK Information Commissioner's Office (2020) developed guidelines for auditing such technologies through impact assessments. Highlighting the potential pitfalls of AI-centred technology such as the effect of skewed ethnicity training data used to build a comparison database in the case of FRT, resulting in a higher possibility of inaccurate identifications, these guidelines are expected to further guide the MPS in terms of how to handle facial recognition data.

MPS's own policies and Published documents

Alongside the regulations, laws and guidelines discussed above, the MPS have also formulated an array of their own documents and policies that set out and advise how FRT is used within the police agency and deployed by police officers. These include published documents such as the Standard Operating Procedure for the use of LFR by the MPS (n.d.) and the Data Protection Impact Assessments (DPIA's) as required under the GDPR, for all FRT used by the MPS, including LFR and the more recently acquired RFR (2021; 2023). Additionally, as a further measure in conjunction with the DPIA's, the MPS also has an Equality Impact Assessment (EIA) framework that provides recommendations for addressing accuracy discrepancies based on individually unique characteristics such as age, race, gender and disability, which also guide the use of FRT by the MPS (Gikay, 2022). As such, the police agency has published EIA's on both LFR and RFR (n.d.; n.d.).

The MPS (n.d; n.d) have also published policies specifically dealing with the deployment of both LFR and RFR, that address various aspects of the technology's use by the police agency. For instance, key points set out in the MPS LFR policy (n.d, p.19) note that nobody is personally "targeted" by the LFR, rather, the LFR analyses the biometric data of any person that enters what they term the "zone of recognition", unless they are flagged to the MPS as being on the

watchlist. The policy (n.d, p. 19) also states that if an individual is included on the watchlist, this must be justified based on the principles of proportionality and necessity. Further, another key point mentioned in the LFR (n.d., p.19) policy is that any biometric data that is obtained by the LFR is both automatically and permanently deleted if it does not generate an alert to the police.

Similarly, the RFR policy (n.d.) sets out what images are used with the RFR technology, how those images are used, in addition to the governance and oversight that is necessary when adopting such technology. For example, under the 'what' section, the policy (p.11) outlines details of the database against which a 'probe image', or otherwise known as a 'still image' is compared. Similar to the NYPD's "photo repository", the policy refers to what the MPS term "Image reference libraries", that once approved by the MPS station reception officer, are used by the police agency for comparison purposes. Likewise, under the 'how' section of the policy (p.21), it states how RFR should only be used once all other avenues of investigative enquiry have been exhausted and cannot be deployed unless a police officer has received prior approval by a more senior officer. * note about unlike the NYPD's photo repository*

To ensure transparency and inform the public when it is happening, it is also mandatory for the MPS to provide information on where they intend to use FRT before the actual activity takes place. As noted by Richardson (2021), this includes informing the public via posts online, using signs in and around the areas subject to FRT analysis to make the public aware of its operation and having police officers speak to members of the public about FRT.

Criticism and Concerns

Adjacent to what we observed in the case of the NYPD, the use of FRT by the MET police has given rise to a considerable amount of legal challenges, debate and scrutiny, which has been voiced by a multitude of concerned parties including the non-profit and interest groups, academics, the public and other relevant stakeholders.

Insufficient legal framework

Despite having what would seem as a fortress of regulations, governance and oversight when compared to their New York counterparts, critics have argued that aspects of the current legal framework governing the MPS's use of FRT are insufficient. For instance, in the case of the

GDPR, whilst it has certainly allowed for a somewhat harmonised approach to protection of individual personal data across the EU, academics such as Peloquin *et al* (2020) have argued that oftentimes GDPR has proven hard and intricate to enforce in real-life, with many of its clauses being vague or ambiguous in nature which are in turn, difficult to interpret. Thus, this coincides with the point made by Molnár-Gábor (2022), which is that such clauses allow for member state autonomy in regards to interpretation and makes the ideal of a unified approach to data protection in the EU hard to obtain. An example of such, as Almeida *et al* (2022) point out, is the first principle of the GDPR which is that personal data must be processed in a lawful, transparent and fair manner, however, what exactly constitutes 'fair and lawful' is potentially open to legal contest and debate amongst member states and thus, allows for an inconsistency in interpretation, which can create divergence in approach. Thus, this very much mirrors the comments made by the State Comptroller in New York regarding the current legal framework governing FRT there.

Peloquin *et al* (2020) have also argued that the GDPR is not sufficient in its protections of individual and personal data also due to its facilitation of what they term 'derogations' that allow the side-stepping of consent for research purposes, for example, which as a result, limits the ability of people to exert rights over their rightfully owned data in such cases.

Further insufficiencies with the current legal framework governing the use of FRT by law enforcement in the UK have also been commented on. In correlation with the divergent nature of the GDPR mentioned above and the resultant vague regulations, the Ada Lovelace Institute recommended in 2022 report that the use of facial recognition technology be put on hold until there was a legally binding code of practice in place as the currently relied on surveillance code of practice 2013, for example, requires that the majority of UK police officers merely need to consider it (Home Office & Green, 2013; Gentile, 2021).

The institute (2022) recommended that the code of practice ought to identify the parties responsible for the oversight of the technology and include the courses of redress involved if the mishandling of the technology occurs, whilst also addressing the governing of the use of the technology in both public and private settings. Gikay (2022) also recommended that there should be a national policy guiding the use of facial recognition technologies, including the compiling

of watchlists to ensure that the protection of civil liberties is consistent. Gikay (2022) also recommended that FRT only be used in the case of serious crimes and solely when judicial approval has been provided. Gikay (2022) notes that these recommendations are in addition to his suggestion of limiting the use of technology in places with a lot of civil and political activities.

Violations of Privacy, Civil liberties and data misuse

Whilst not to the same level as exhibited in the context of the NYPD, which perhaps is attributed to the differences in regulation of FRT, concerning details have also surfaced regarding the MPS and their use of the technology. For instance, despite being mandatory that the MPS inform the public of when they are using FRT via the use of signs, online posts etc, it was reported that the MPS deployed FRT in one of the busiest districts in London known as 'King's Cross', in an experiment that lasted for months without informing the public (Moraes *et al*, 2021). Thus, notwithstanding the plethora of regulation and policy governing the use of FRT by the MPS that promote principles such as necessity and transparency, the police agency covertly surveilled passersby with FRT in this scenario and were not transparent by any accounts about their use of the technology.

Instances such as this and in the same way the use of the technology by law enforcement in general has in New York, the MPS and their use of FRT has also sparked criticisms and concerns regarding violations of privacy and civil liberties. One of the major concerns that has been voiced in the UK is that the use of FRT by law enforcement threatens civil liberties and violates basic human rights, such as the right to privacy. A fellow of the Alan Turing Institute in the UK, Leslie (2020), has highlighted that scholars in refute of the technology have argued that its use will lead to the eventual loss of democratic life as we know it and could also contribute to the deterioration of individual and social freedoms which are currently enjoyed.

In line with this, a multitude of human rights advocacy groups such as Big Brother Watch, liberty and Amnesty International have asserted that use of LFR in particular by UK police enables the mass and pervasive surveillance of individuals, essentially turning people into what they describe as "walking ID cards" (Sinmaz, 2023). In this way, they argue that the

technology is ‘Orwellian’ in nature, referring to the writings of George Orwell and his depiction of a dystopian and future totalitarian state in which the government control multiple aspects of individual’s lives (Raza & Awan, 2016; Sinmaz, 2023).

These concerns surrounding the right to privacy and individual civil liberties have also been illustrated in the form of court appearances in the UK. For instance, a protester once sued the MPS in the court of appeal for taking and storing his photo without his consent, an act he claimed violated his rights under the European Charter of Fundamental Rights (Purshouse & Campbell, 2021). Similarly, in a separate court ruling that took place in 2003 under the name of ‘*Peck vs the United Kingdom*’, it was found that mass video surveillance of public spaces, as seen to be carried out by the MPS using their LFR, violated the human rights granted under by article 8 of the European Charter of Human Rights (Bu, 2021).

Additionally, in tandem with their picking apart of the accuracy of the MPS’s deployed FRT, Fussey and Murray (2019) revealed that in the event that the exercise was tried in a court of law, it would be found to be unlawful due to the lack of publicly available material on how and under what circumstances the technology should be used. Thus, this depicts how important it is to have necessary legal outlines on how the technology should be used for it to be considered legally sound.

Finally, a further tension which has been voiced in relation to FRT use by law enforcement, especially those carrying out their policing duties in the UK, is that the use of the technology is done through public-private partnerships (Gentile, 2021). In the case of the MPS, the Japanese-based company known as ‘NEC’ supplies the police agency with FRT, with no transparent explanation publicly available as to why this specific partnership was commenced (Gentile, 2021). This, as a result, has raised concerns regarding the rules guiding public-private partnerships, especially when handling such sensitive data, as it increases the risk of data being mishandled (Gentile, 2021).

Inaccuracy & Discrimination

As detailed in the literature review of this paper, the extensively documented inability of FRT algorithms to accurately identify a person depending on individual characteristics such as age, gender, ethnicity and disability has also been a bone of contention in the UK, as observed in New York with the NYPD. However, unlike the NYPD and their apparent unwillingness to conduct experiments on the accuracy of the technology for law enforcement purposes, the MET police have taken steps to analyse the technology's effectiveness as an investigative tool.

Referred to in the literature review, this can be clearly observed in the pivotal study published by Fussey and Murray (2019). Based on the last six of the ten trial LFR deployments mentioned above that the MPS conducted between the years 2016 and 2019, the police agency invited academics Fussey and Murray to conduct an independent scholarly report on the technology's operational effectiveness. Echoing what has been reported in other studies on FRT accuracy, the report found that out of the total of the 46 watchlist potential matches generated by the MPS-used LFR, 8 of these were valid and correct matches. Worryingly, in light of the nature of the operation of the MPS LFR and the inclusion of the officer's decision on whether or not to approach an individual once they have been alerted to a potential match, officers deemed 26 out of the total 42 matches to be significant enough to apprehend the person. Further notes made in Fussey and Murray's (2019) report was that out of the 26 matches deemed credible enough to warrant the apprehension of the individual by the MPS police officers, 4 were subsequently lost in the crowds of people that surrounded the LFR van and 14 were completely invalid matches flagged by the technology.

However, what is even more concerning about the MPS and the accuracy of their FRT is that despite having asked academics both Fussey and Murray to complete an independent evaluation of the use of FRT by the MPS, which highlighted the problematic aspect of the accuracy of the technology in particular, the MPS later published their own report which contradicted the earlier results issued by the consulted scholars. Rather, in their report published in 2020, the MPS produced a significantly more positive view of the trials and concluded that with the comment that FRT will "stop dangerous people and make London safer" (Metropolitan Police, 2020, p.4). Thus, it would seem as though because the academic report did not have the

police agency's desired results, they issued their own one in an effort to promote a more positive stance, which was not entirely truthful.

Taking all of this into consideration and the fact that FRT has been continuously criticised for being unsound and prone to mistakes in terms of its accuracy, scholars note that it could lead to the inaccurate identifying of individuals that have characteristics that FRT finds hard to detect and could thus lead to the wrongful arrest of such individuals (Radiya-Dixit & Nef, 2023).

Hand in hand with this and as also seen in the context of the NYPD, scholars have also expressed concerns in relation to FRT's ability to promote racially-driven policing and facilitate discrimination in the UK. The over-policing of minority ethnic groups and individuals from disadvantaged communities has long been apparent in the UK and has been repeatedly highlighted by studies conducted by researchers such as Lewis *et al* (2011), Jefferson (2012) and Lammy (2017). In terms of the MPS more specifically, research carried out by the well-known non-governmental organisation and human rights advocate Amnesty International in 2018 revealed that this disproportionate treatment of such individuals was very much evident within this police agency in particular. Thus, academics such as Radiya-Dixit and Nef (2023) argue that due to these discrepancies in the world of UK policing still being witnessed presently, FRT has the capacity to continue and further this unequal and targeted policing of this cohort.

In the same vein and with emphasis placed on FRT algorithms inability to accurately identify people of non-white ethnicity, advocacy groups such as the Equality and Human Rights Commission (2020) have called for suspension of FRT in England and Wales due to its ability to promote discriminatory outcomes.

Detrimental impacts such as this that FRT could have on today's society in addition to the earlier mentioned ability of FRT to threaten our democratic rights and freedoms in various ways has led to countless calls to ban the use of FRT in public spaces by UK police. These have been articulated by various concerned bodies, such as the call put forward in a report constructed by the Minderoo Centre for Technology and Democracy (2022) due to the technology's blatant violation of fundamental rights. In addition to others such as the Big Brother Watch's (n.d.)

readily available online ‘stop facial recognition’ petition, there have also been suggestions made to improve its operation within UK law enforcement. However, there have also been recommendations for improvement made.

Conclusion

To conclude, despite each individual police agency and their respective use of FRT being subject to a variation of regulations, governance and oversight, similarities in the concerns and criticisms that have been voiced in each jurisdiction could be observed. In the following chapter, these similarities will be discussed in-depth in an effort to address my first research question ”Is the use of FRT by the police as an investigative tool justified?” . This will then be followed by a theoretical analysis in order to answer my second and final research question which is “To what extent can the lens of surveillance studies aid in explaining the drive to adopt FRT within law enforcement?”.

Chapter Five

Discussion

Introduction

The New York City Police Department (NYPD) in the United States and the Metropolitan Police Service (MPS) of London in the United Kingdom were selected for analysis as a part of this dissertation on the basis that each police agency and their respective use of Facial recognition technology (FRT) was separate and distinct. Although each police agency's use of FRT has been a source of controversy, each one is subject to different regulations, laws and policies in relation to their use of FRT due to being located in separate jurisdictions. In addition to this, each police agency has their own context surrounding FRT such as each of their individual histories with advanced surveillance technologies. Thus, by virtue of the research method of purposive sampling employed in this study and described in the earlier methodology chapter, the selection of these cases provides an interesting insight into whether or not the same points of concern were being raised in relation to both police agencies and if so, why that is. In the subsequent parts of this section, I will employ a critical synthesis of my findings from the literature review and my comparative case study analysis in an effort to answer 1) Is the use of FRT by the police as an investigative tool justified? And 2) To what extent can the lens of surveillance studies aid in explaining the drive to adopt FRT within law enforcement?

Emerging Themes

Through my comparative case study analysis of both police agencies, it quickly emerged that the same points of contention surrounding police use of FRT could be observed in the context of both police agencies, these were: 1) Ineffectiveness of current FRT regulatory frameworks 2) FRT's capacity to violate civil liberties and facilitate data misuse by police and 3) FRT's inherent inaccuracy and its ability to perpetuate discrimination.

Ineffectiveness of current FRT regulatory frameworks

As mentioned in the literature review, both Morrison (2018) and Pasztor and Wall (2016) state that regulations governing surveillance-focused technologies, such as FRT, very quickly become outdated. They also note that when, what they refer to as "thoughtful" regulation and governing policies are put in place, it is unlikely that such legal or regulatory barriers will

prevent FRT-enabled surveillance tools from creeping into unregulated spaces overtime via the avenue of Frischmann and Selinger's (2018) "technological mission creep", Koop's (2021) notion of "function creep", Da Costa et al's (2006) noted 'surveillance creep' or indeed Dauvergne's (2022) 'public to private creep'. From my research into both the NYPD and MPS, this observation can be made.

In the context of the NYPD, the "fragmented legislative landscape" in the U.S, as Almeida *et al* (2022, p. 383) put it, is a true depiction of this. Notwithstanding the establishment of the OIG-NYPD as an oversight mechanism for the NYPD's use of FRT and the enactment of the POST Act in 2020 which obligated the NYPD to publish 'use and impact' policies for their use of current and future use of surveillance technologies such as FRT, both initiatives have been largely ineffective and have not shifted the ultimate operation and control of FRT out of the police agency's hands. This problematic aspect of New York's regulation of police use of FRT can be clearly observed when the NYPD failed to take on board any recommendations made to them by the OIG-NYPD in their report earlier this year, as noted by Claburn (2023).

If we look at the MPS, their current legal framework has also been scrutinised for its pitfalls. GDPR, for example, has been criticised by scholars such as Peloquin *et al* (2020) and Molnár-Gábor (2022) for not being sufficient enough to protect personal data, with terms mentioned in the regulation being largely vague and ambiguous, making them hard to interpret. Likewise, this vagueness facilitates member states autonomy in terms of how to implement it, resulting in the idea of a 'unified' approach across the EU to personal data, virtually impossible to obtain. Critics have also scrutinised the current legal framework governing the MPS's use of FRT, noting that a new legally binding code and national policy needs to be established, in conjunction with the limitation of the technology's use in certain places.

FRT's capacity to violate Privacy, civil liberties and facilitate data misuse by police

As noted in the literature review by scholars Introna and Wood (2004) and Hill *et al* (2022), FRT is often referred to as a "silent technology" and thus, can be operated unbeknownst to the subject of the technology. This, as other concerned bodies such as Beodya and Frankle (2018) and Lively (2021) and Devich-Cyril (2020) argue, can facilitate the misuse of the

technology to conduct non consensual mass surveillance of the public, resulting in the invasion of civil liberties, such as the right to privacy and the right to protest. As noted in the literature review also by both Carter (2018) and Ringrose (2019), the lack of transparency around police use of FRT makes it very unclear how police use the technology and what happens to the data. These observations can be clearly witnessed across both police agencies.

In terms of the NYPD, numerous civil liberty advocates and other interest groups in New York City have raised concerns regarding civil liberty violations, such as the right to privacy and the right to protest in addition to the misuse of FRT data by the police. As observed in the case study, the NYPD appears to have consistently gone against their own policies. Not only were the NYPD reported by Mac, Haskins & McDonald (2020a; 2020b) to have used FRT to track down protester and revealed to have been using controversial FRT software 'Clearview AI' without the public's knowledge and despite consistently denying any affiliation, but they were also reported by Brandom (2019) to have been tampering with images of various individuals and then running these images through their FRT database, creating an avenue for false identification.

Similar happenings have occurred in the context of the MPS. Spurred on by instances such as the use of FRT at Kings Cross by the MPS without informing the public, as reported by Moraes *et al* (2021), despite the array of regulation and policies that place emphasis on consent and require that the MPS make it known when using such technology, scholars and civil liberty advocates have raised concerns and criticisms of the use of FRT by the police agencies in the UK. For instance, as noted by Sinmaz (2023), civil liberty advocates have asserted that FRT turns individuals into what they term "walking ID cards" and enables the mass and pervasive surveillance of people. Thus, creating what they believe to be a future totalitarian state awash with dystopian values. Likewise, as Leslie (2020) asserts, critics of the technology have warned that FRT has the potential to deteriorate the social freedoms we currently enjoy at present and eventually lead to the erosion of democracy.

Civil liberty concerns surrounding the MPS and their use of FRT have also been clearly displayed in multiple court proceedings that have been brought against the MPS. For example, I note in the case study that the MPS have been sued in the past for the taking and storing of a

protestors photo by the MPS without their informed consent, on the basis that it violated his rights granted by the European Charter of Human Rights of Fundamental Rights, as reported by Purshouse and Campbell (2021).

Further concerns in relation to civil liberties and misuse of FRT have also been highlighted by scholars such as Gentile (2021) as displayed in the case study. As Gentile (2021) states, the aspect of public-private partnerships existent between FRT corporations and police agencies and the ability for such collusion to increase the likelihood of personal data being misused and handled incorrectly has produced a plethora of concern, due to the often non-transparency aspect of such partnerships.

FRT's inherent inaccuracy and its ability to perpetuate discrimination

Lastly, as noted in the literature review, scholars such as Buolamwini and Gebru (2018) and Abdurrhaim (2018) have found that FRT is extremely inaccurate when it comes to the identification of certain unique characteristics of individuals such as their sex, ethnicity and age. Thus, as stated in the literature review, it has been voiced by scholars such as Reinbold (2020) that this problematic aspect of FRT can perpetuate the discrimination of people with black ethnicity, for instance, as they can be falsely identified by the technology as suspected criminals. In the same vein, Najibi (2020) argues that even if the technology was accurate in its identification, it still has the potential to be used in a discriminatory manner as it has the ability to be used to further the already existing discrimination of people of colour within the criminal justice system, as has long been recorded in studies across the field of criminological research. These observations have been clearly displayed in the context of both the NYPD and the MPS.

In terms of the NYPD, as noted by Brown, 2020; Stokes, 2020; Harwell, 2021, despite the FRT 'Dataworks Plus' employed by the NYPD having previously been responsible for the wrongful arrest of two men in Detroit in the state of Michigan in the U.S and existing research demonstrating FRT's inherent inaccuracy, the software company providing the technology do not publish accuracy testing of the FRT, nor have the NYPD ever conducted such tests on the technology used. While this is concerning in its own right, Amnesty International (2021; 2022a) have argued that by virtue of the volume of CCTV cameras that can be accessed for still images

to run through the NYPD's FRT system located in areas where the ethnicity of residents is largely non-white, the use of FRT by the NYPD has the ability to "supercharge" racist policing in New York. Thus, they argue that it can perpetuate the already existing over-policing of such cohorts that is already evident in the 'stop and frisk' statistics, as illustrated by the NYCLU (2018).

In the context of the MPS, the independent report on the trial roll-out of LFR conducted by Fussey and Murray (2019) highlighted the blatant inaccuracy of the deployed FRT used by the MPS. However, concerningly, this was reframed in a more positive and frankly dishonest light in a later report issued by the MPS themselves which completely contradicted the earlier report.

Further to this, as detailed in the case study, scholars such as Radiya-Dixit and Nef (2023) have argued that the over-policing of minority ethnic groups that has long been documented in the UK, specifically in the context of the MPS as illustrated by Amnesty International (2018), could exacerbate this already prevalent issue.

Surveillance lens applied

Taking all of the emerging themes into consideration and to answer my first research question which is "Is the use of FRT by the police as an investigative tool justified?", it has been clearly demonstrated in this study that there is too much at stake when it comes to the adoption of FRT into police agencies and indeed, into the criminal justice system as a whole. Considering Lyons (2001) idea of surveillance technology such as FRT being what he describes as a "double-edged sword" and thus, janus-faced in nature, it is my belief that whilst the technology certainly has the potential to be a significant crime-fighting tool, the evident potential risks of the technology ranging from its ability to perpetuate systemic racism, the inability of overarching regulations, policies and laws to sufficiently safeguard and constrain its use by police in addition to its capacity to erode democratic life as we know it are far too great to be complacent with its introduction into the law enforcement arena at present. On this point, I further submit that even if these problematic aspects of FRT were addressed, such as the improvement of governing regulations, laws and policies, will they be sufficient enough? As observed in the context of MPS with the introduction of regulations such as the GDPR and Data Protection Act 2018 along with

the array of other policies, guidelines and codes of practice, the MPS still covertly deployed LFR in Kings Cross as noted by Moreas *et al* (2021).

Additionally, despite numerous faults and problems being raised in relation to the use of FRT, it is still continuing to be rapidly adopted by a multitude of police agencies around the world. Thus, to answer my second research question which is "To what extent can the lens of surveillance studies aid in explaining the drive to adopt FRT within law enforcement?", I attempt to explore why this is.

A plethora of the existing literature analyses police use of FRT and its increasing prevalence through the lens of George Orwells 'Big brother' (1949). Foucault's panopticon (1979) Ericson and Haggerty's 'Surveillant Assemblage' (2000), for example, thus viewing the technology's expansion within law enforcement in tandem with underlying social control motivations. However, whilst all of these viewpoints certainly highlight important attributes to the discussion on police use of FRT, and the drive being witnessed to adopt the technology within law enforcement, I submit an analysis through an alternative lens.

As outlined in the literature review, it is my view that the theoretical concepts of technological solutionism, the surveillance-industrial complex, and surveillance capitalism are tightly interwoven in the context of police use of FRT. These concepts shed light on the motivations, dynamics, and consequences surrounding the adoption of FRT by law enforcement agencies.

The concept of technological solutionism coined by Morozov's (2013) is evident in how police view FRT as a quick fix for complex law enforcement challenges. They believe it can efficiently identify suspects, locate missing persons, and prevent crimes. However, this perspective often downplays the technology's inherent flaws, including biases and privacy concerns, as clearly observed in this study. The rush to deploy FRT can thus lead to insufficient consideration of the ethical and societal implications, as the allure of a technological solution overshadows potential drawbacks.

Ball and Snider's (2013) concept of the 'surveillance-industrial complex' plays a pivotal role in FRT adoption also. Private companies specialising in surveillance technologies collaborate with government agencies, such as police, to develop and deploy FRT systems. This mutually beneficial relationship results in the rapid expansion of FRT usage. Companies see profitable opportunities in providing these solutions, while law enforcement gains enhanced surveillance capabilities. The complex therefore reinforces FRT by creating a climate where surveillance technologies are seen as essential tools for maintaining order and security.

Finally, as Zuboff (2015) explains, surveillance capitalism thrives on the data collected through FRT. Law enforcement's use of FRT thus contributes to the continuous accumulation of biometric data without explicit consent. This data fuels the business models of tech giants and data brokers, who monetise it by targeting individuals with personalised ads and services. As FRT data grows, surveillance capitalism strengthens its grip on law enforcement policies and practices, further entrenching the adoption of this technology.

Conclusion

I argue that the adoption of FRT is intricately linked to these surveillance studies concepts. Technological solutionism drives the hastily implementation of FRT, often overlooking ethical and privacy concerns. The surveillance-industrial complex fosters a symbiotic relationship between law enforcement and technology vendors, bolstering FRT usage. Meanwhile, surveillance capitalism profits from the data collected by FRT, perpetuating the cycle of data extraction and commercialization. These concepts collectively illuminate the complex web of interests and motivations that underlie the widespread adoption of FRT in the law enforcement arena.

Thus, it is my recommendation that more attention needs to be paid to this aspect of FRT implementation which is the relationship existing between the corporations that invent and sell this technology and policing agencies that adopt it, placing particular emphasis on the intentions and morals that underpin this partnership.

Chapter Six
Conclusion

In conclusion, this dissertation delved into the contentious realm of police use of Facial Recognition Technology (FRT) through a comparative case study analysis of the Metropolitan Police of London in the United Kingdom and the New York City Police Department in the United States. The primary aim of this research was to provide insights into the adoption of this technology by law enforcement in light of the willingness to embrace the technology into the Irish policing space, which has been recently articulated by Irish government officials. Two central research questions guided this exploration: firstly, whether the employment of FRT as an investigative tool by law enforcement is justified, and secondly, what surveillance studies concepts can reveal about the motivations driving its adoption.

Through the comparative case study analysis, three recurring themes emerged across both jurisdictions. These themes pertained to the ineffectiveness of current FRT regulatory frameworks, the potential for FRT to violate civil liberties and facilitate data misuse by police, and the inherent inaccuracies of FRT that perpetuate discrimination. These findings collectively suggest that the use of FRT by law enforcement agencies cannot be considered justified, given the substantial risks and implications it poses.

Drawing upon the insightful observations of Lyons (2001), who characterises surveillance technologies as being "double-edged swords" capable of benefiting society while also exacerbating social inequalities, this study underscores the complex nature of FRT deployment. Despite the evident problems associated with FRT, there remains a growing interest in its adoption by police agencies.

To address the second research question, this dissertation highlighted three pivotal surveillance theoretical concepts: Morozovs (2013) technological solutionism, Ball and Snider's (2013) surveillance-industrial complex, and Zuboff's (2015) idea of surveillance capitalism. These concepts shed light on the intricate interplay between corporations and law enforcement, emphasising their symbiotic relationship in the drive to embrace FRT.

In light of these findings, it is recommended that greater attention be devoted to examining and regulating the multifaceted relationships between private corporations and law enforcement agencies. Policymakers, scholars, and the broader public must critically assess the implications of FRT adoption, recognizing the need for robust regulatory frameworks that prioritise civil liberties, accuracy, and accountability. Furthermore, public discourse and awareness regarding the potential societal consequences of FRT use should be fostered to ensure that decisions concerning surveillance technologies are made with a clear understanding of the complex dynamics at play.

In an era where the boundaries between security, privacy, and technological advancement are continually shifting, this research calls for a balanced and informed approach to the deployment of FRT within law enforcement, one that reconciles the objectives of public safety with the safeguarding of individual rights and societal well-being.

Bibliography

Abdurrhaim, S.H., Samad, S.A. and Huddin, A.B. (2018). Review on the effects of age, gender, and race demographics on automatic face recognition. *The Visual Computer*, 34, pp.1617–1630.

Ada Lovelace Institute (2022). *Countermeasures: the need for new legislation to govern biometric technologies in the UK*. [online] Ada Lovelace Institute . Available at: https://www.adalovelaceinstitute.org/wp-content/uploads/2022/06/Countermeasures-the-need-for-new-legislation-to-govern-biometric-technologies-in-the-UK-Ada-Lovelace-Institute-June-2022.pdf [Accessed 7 Sep. 2023].

AL-Aadamy, M.M.J. and AL-Dulaim, M.K.H. (2023). Enhancing The Security Of Iraqi Banks Through The Use Of Electronic Authentication And Facial Recognition Technology. *resmilitaris* , 13(2), pp.5189–5200.

Almeida, D., Shmarko, K. and Lomas, E. (2022). The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks. *AI and Ethics*, 2(3), pp.377–387.

American Civil Liberties Union (n.d.). *The Fight to Stop Face Recognition Technology*. [online] American Civil Liberties Union. Available at: https://www.aclu.org/news/topic/stopping-face-recognition-surveillance [Accessed 2 May 2023].

Amnesty International (2018). *Trapped IN THE MATRIX: Secrecy, stigma, and bias in the Met's Gangs Database*. [online] Available at: https://www.amnesty.org.uk/files/reports/Trapped%20in%20the%20Matrix%20Amnesty%20report.pdf [Accessed 7 Sep. 2023].

Amnesty International (2021). *New York is in danger of becoming a total surveillance city*. [online] Amnesty International. Available at: https://www.amnesty.org/en/latest/news/2021/06/scale-new-york-police-facial-recognition-revealed/ [Accessed 27 Feb. 2023].

Amnesty International (2022a). *USA: Facial recognition technology reinforcing racist stop-and-frisk policing in New York – new research*. [online] Amnesty International. Available at: https://www.amnesty.org/en/latest/news/2022/02/usa-facial-recognition-technology-reinforcing-racist-stop-and-frisk-policing-in-new-york-new-research/ [Accessed 27 Feb. 2023].

Amnesty International (2022b). *USA: NYPD ordered to hand over documents detailing surveillance of Black Lives Matter protests following lawsuit*. [online] Amnesty International. Available at: https://www.amnesty.org/en/latest/news/2022/08/usa-nypd-black-lives-matter-protests-surveilliance/#:~:text=The%20New%20York%20Police%20Department [Accessed 5 Aug. 2023].

Anderson, G. (1993). *Fundamentals of Educational Research*. London: Falmer Press, pp.152–160.

Andreichenko, K. and Kolisnyk, M. (2022). Using facial recognition technologies in the modern world. In: *Science of XXI century: development, main theories and achievements: collection of scientific papers 'SCIENTIA' with Proceedings of the III International Scientific and Theoretical Conference, December 2, 2022. Helsinki, Republic of Finland*. [online] European Scientific Platform. Available at: https://ela.kpi.ua/bitstream/123456789/57477/1/Andreichenko_Kolisnyk_Using_facial_recognition.pdf [Accessed 5 Aug. 2023].

Andrejevic , M. and Selwyn, N. (2019). Facial recognition technology in schools: critical questions and concerns. *Learning, Media and Technology*, 45(2), pp.115–128.

Apampa, K., Wills, G. and Argles, D. (2010). An Approach to Presence Verification in Summative e-Assessment Security.". In: *2010 International Conference on Information Society*. IEEE, pp.647–651.

Apuzzo, M. and Goldman, A. (2013). *Enemies within: Inside the NYPD's secret spying unit and bin laden's final plot against America*. New York: Atria Books.

Baker, S. and Greenbaum, D. (2017). Now you see me: Now you still do: Facial recognition technology and the growing lack of privacy. *BUJ Sci. & Tech. L.,* 23, p.88.

Bakshi, P. (2023). *Countries With Airports Using Facial Recognition Instead Of Boarding Pass*. [online] Travel and Leisure Asia | Global. Available at: https://www.travelandleisureasia.com/global/news/airports-that-use-facial-recognition-instead-of-boarding-pass/#:~:text=The%20facial%20recognition%20system%20is [Accessed 25 Aug. 2023].

Ball, K. and Snider, L. (2013). *The Surveillance-Industrial Complex: A Political Economy of Surveillance*. Routledge .

Bareis, J. and Katzenbach, C. (2022). Talking AI into Being: The Narratives and Imaginaries of National AI Strategies and Their Performative Politics. *Science, Technology, & Human Values*, 47(5), pp.855–881.

Benedict, T.J. (2022). The Computer Got It Wrong: Facial Recognition Technology and Establishing Probable Cause to Arrest . *Washington and Lee Law Review*, 79(2), p.849.

Benson, D. (2017). *The Impact of Facial Recognition Technology on Society*. [online] Available at: https://www.cs.tufts.edu/comp/116/archive/fall2017/dbenson.pdf [Accessed 5 Aug. 2023].

Big Brother Watch (n.d.). *Stop Facial Recognition — Big Brother Watch*. [online] Stop Facial Recognition — Big Brother Watch. Available at: https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/ [Accessed 7 Sep. 2023].

Bischoff, P. (2021). *Facial recognition technology (FRT): 100 countries analyzed*. [online] Comparitech. Available at: https://www.comparitech.com/blog/vpn-privacy/facial-recognition-statistics/ [Accessed 2 May 2023].

Boden, M.A. (1996). *Artificial Intelligence* . Elsevier.

Bracken-Roche, C., Farries, E. and Cronin, O. (2023). *Facial-recognition technology will turn gardaí into roaming surveillance units*. [online] The Irish Times. Available at: https://www.irishtimes.com/opinion/2023/04/18/facial-recognition-technology-will-turn-gardai-into-roaming-surveillance-units/#:~:text=The%20use%20of%20body%2Dworn [Accessed 2 May 2023].

Bradford, B., Yesberg, J.A., Jackson, J. and Dawson, P. (2020). Live Facial Recognition: Trust and Legitimacy as Predictors of Public Support for Police Use of New Technology. *The British Journal of Criminology* , 60(6), pp.1502–1522.

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

Brandom, R. (2019). *The NYPD uses altered images in its facial recognition system, new documents show*. [online] The Verge. Available at: https://www.theverge.com/2019/5/16/18627548/nypd-facial-recognition-altered-faces-privacy [Accessed 5 Aug. 2023].

Brennan Center for Justice (2021). *The Public Oversight of Surveillance Technology (POST) Act: A Resource Page | Brennan Center for Justice*. [online] www.brennancenter.org. Available at: https://www.brennancenter.org/our-work/research-reports/public-oversight-surveillance-technology-post-act-resource-page [Accessed 29 Jul. 2023].

Brogan, J. (2016). *Defining Algorithms—a Conversational Explainer*. [online] Slate Magazine. Available at: https://slate.com/technology/2016/02/whats-the-deal-with-algorithms.html [Accessed 28 May 2023].

Brown, S. (2020). *Brown Blasts DataWorks Plus' Unreliable Facial Recognition Technology | U.S. Senator Sherrod Brown of Ohio*. [online] www.brown.senate.gov. Available at: https://www.brown.senate.gov/newsroom/press/release/brown-blasts-dataworks-unreliable-facial-recognition-technology [Accessed 7 Sep. 2023].

Bu, Q. (2021). "The global governance on automated facial recognition (AFR): ethical and legal opportunities and privacy challenges. *International Cybersecurity Law Review*, 2, pp.113–145.

Buolamwini, J. and Gebru, T. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Proceedings of Machine Learning Research*, 81, pp.1–15.

Camplin, O. (2022). Ethics of Facial Recognition Technology in Law Enforcement: A Case Study. In: *Proceedings of the Wellington Faculty of Engineering Ethics and Sustainability Symposium*.

Carter, A.M. (2018). *FACING REALITY: THE BENEFITS AND CHALLENGES OF FACIAL RECOGNITION FOR THE NYPD*. [online] Available at: https://apps.dtic.mil/sti/pdfs/AD1065272.pdf [Accessed 16 Apr. 2023].

CBS New York (2019). *NYPD Under Fire Over Use Of Celebrity Lookalike Photos In Facial Recognition Investigations - CBS New York*. [online] www.cbsnews.com. Available at: https://www.cbsnews.com/newyork/news/nypd-celebrity-facial-recognition-controversy/ [Accessed 5 Aug. 2023].

Chabinsky, S. and Pittman, P.F. (2020). USA. In: *Data Protection Laws and Regulations 2020: Global legal Group*.

Charter of Fundamental Rights of the European Union. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT [Accessed 7 Sep. 2023].

Cheshire, T. (2017). *Piccadilly Circus lights facial detection system 'incredibly intrusive'*. [online] Sky News. Available at: https://news.sky.com/story/piccadilly-circus-lights-facial-detection-system-incredibly-intrusive-11087020 [Accessed 5 Aug. 2023].

Chivers, T. (2019). *Facial recognition… coming to a supermarket near you*. [online] the Guardian. Available at:

https://www.theguardian.com/technology/2019/aug/04/facial-recognition-supermarket-facewatch-ai-artificial-intelligence-civil-liberties [Accessed 5 Aug. 2023].

Chopard, K. and Przbylski, R. (2021). *Methods Brief: Case Studies*. [online] Justice Research and Statistics Association. Available at: https://www.jrsa.org/pubs/factsheets/jrsa-research-methods-brief-case-studies.pdf [Accessed 6 Jun. 2023].

Claburn, T. (2023). *NYPD ignored 93 percent of surveillance law rules*. [online] www.theregister.com. Available at: https://www.theregister.com/2023/03/31/nypd_surveillance_rules/ [Accessed 5 Aug. 2023].

Cohen, A. (2023). *Facial recognition in sports: The biometrics technology shaping ticketing, payments, security, more*. [online] www.sportsbusinessjournal.com. Available at: https://www.sportsbusinessjournal.com/Journal/Issues/2023/01/09/Technology/facial-recognition-technology-sports-stadiums.aspx#Fan-experience [Accessed 23 Aug. 2023].

Cook, C.M., Howard, J.J., Sirotin, Y.B., Tipton, J.L. and Vemury, A. (2019). Demographic effects in facial recognition and their dependence on image acquisition: An evaluation of eleven commercial systems. *IEEE Transactions on Biometrics*, 1(1), pp.32–41.

Corbo, A. (2022). *What Is an Algorithm? (Definition, Examples, Analysis) | Built In*. [online] builtin.com. Available at: https://builtin.com/software-engineering-perspectives/algorithm [Accessed 28 May 2023].

Corum, C. (2019). *Facial recognition helps find hurricane victims*. [online] SecureIDNews. Available at: https://www.secureidnews.com/news-item/facial-recognition-helps-find-hurricane-victims/ [Accessed 5 Aug. 2023].

Crawford, K. (2019). Halt the use of facial-recognition technology until it is regulated. *Nature*, 572(7771), p.565.

Cresswell, J.W. and Plano clark, V.L. (2011). *Designing and conducting mixed method research*. Thousand Oaks, CA: Sage Publications.

Critchley, T.A. (1967). *A History of Police in England and Wales: 1900–1966.* London: Constable, pp.255–256.

Crowe, S., Cresswell, K., Robertson, A., Huby, G., Avery, A. and Sheikh, A. (2011). The case study approach. *BMC Medical Research Methodology*, 11(100).

Da Costa, B., Schulte, J. and Singer, B. (2006). Surveillance Creep! New Manifestations of Data Surveillance at the Beginning of the Twenty-First Century. *Radical History Review*, (95), pp.70–88.

Dahl, E.J. (2014). Local approaches to counterterrorism: The New York Police Department model. *Journal of Policing, Intelligence and Counterintelligence*, 9, pp.81–97.

Dammer, H.R. and Albanese, J.S. (2014). Introduction. In: *Comparative Criminal Justice Systems*. Wadsworth, CA: Cengage Learning.

Dang, V.T., Nguyen, N., Nguyen, H.V., Van Huy, L., Tran, V.T. and Nguyen, T.H. (2022). Consumer attitudes toward facial recognition payment: an examination of antecedents and outcomes. *International Journal of Bank Marketing*, 40(3), pp.511–535.

Data Protection Act 2018. Available at: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted [Accessed 7 Sep. 2023].

Data Protection Commission (2019). *Quick Guide to the Principles of Data Protection*. [online] Data Protection Commission . Available at: https://www.dataprotection.ie/sites/default/files/uploads/2019-11/Guidance%20on%20the%20Principles%20of%20Data%20Protection_Oct19.pdf [Accessed 7 Sep. 2023].

Dauvergne, P. (2022a). Chapter 4: The Politics of facial recognition bans in the United States. In: *Identified, tracked and profiled: The Politics of Resisting Facial recognition technology*. Edward Elgar Publishing Ltd, pp.32–42.

Dauvergne, P. (2022b). Facial Recognition Technology for policing and surveillance in the Global South: a call for bans. *Third World Quarterly*, 43(9), pp.2325–2335.

Dauvergne, P. (2022c). The globalisation of facial recognition technology. In: *Identified, Tracked and Profiled: The politics of Resisting Facial Recognition Technology*. Edward Elgar Publishing.

Davis, A.Y. (1944-1999). *The prison industrial complex and its impact on communities of color.* Madison, WI: University of Wisconsin--Madison.

Davis, N., Perry, L. and Santow, E. (2022). *Facial recognition technology: Towards a model law*. [online] Human Technology Institute. Available at: https://www.uts.edu.au/sites/default/files/2022-09/Facial%20recognition%20model%20law%20report.pdf [Accessed 5 Aug. 2023].

De Sario, G.D., Haider, C.R., Maita, K.C., Torres-Guzman, R.A., Emam, O.S., Avila, F.A., Garcia, J.P., Borna, S., McLeod, C.J., Bruce, C.J., Carter, R.E. and Forte, A.J. (2023). Using AI to Detect Pain through Facial Expressions: A Review. *Bioengineering*, 10(5), p.548.

Dearden, L. (2018). *Facial recognition trial in London 'results in zero arrests'*. [online] The Independent. Available at: https://www.independent.co.uk/news/uk/crime/facial-recognition-police-uk-london-trials-stratford-no-arrests-privacy-human-rights-false-positives-a8429466.html [Accessed 7 Sep. 2023].

Department of Justice (2023). *An Garda Síochána to immediately begin process of purchasing bodycams*. [online] www.gov.ie. Available at: https://www.gov.ie/en/press-release/36d59-an-garda-siochana-to-immediately-begin-process-of-purchasing-bodycams/# [Accessed 5 Aug. 2023].

Derrick Ingram vs CITY OF NEW YORK, DESIRAE LAFURNO, ROBERT TOWNSEND, PETER ELLISON, GUSTAVO PAUL, ANDREW SMITH, MICHAEL CAFERO; and NYPD Members of the Service JOHN and JANE DOES #1–60 [2021] Available at:

https://static1.squarespace.com/static/5dc4ddc1431b5833eece7a54/t/6182cbd13741a75a38067207/1635961847280/Derrick+Ingram+-+Filed+Complaint.pdf [Accessed 5 Aug. 2023].

Devich-Cyril, M. (2020). *Defund Facial Recognition*. [online] The Atlantic. Available at: https://www.theatlantic.com/technology/archive/2020/07/defund-facial-recognition/613771/ [Accessed 2 May 2023].

Dodd, V. (2017). *Met police to use facial recognition software at Notting Hill carnival*. [online] the Guardian. Available at: https://www.theguardian.com/uk-news/2017/aug/05/met-police-facial-recognition-software-notting-hill-carnival [Accessed 7 Sep. 2023].

DOI'S OFFICE OF THE INSPECTOR GENERAL FOR THE NEW YORK CITY POLICE DEPARTMENT ISSUES NINTH ANNUAL REPORT. (2023). [online] New York: The City of New York Department of Investigation. Available at: https://www.nyc.gov/assets/doi/reports/pdf/2023/13OIGNYPDRpt.Release.03.30.2023.pdf [Accessed 5 Aug. 2023].

Dul, C. (2022). Facial Recognition Technology vs Privacy: The Case of Clearview AI. *Queen Mary Law Journal*, 3(1), pp.1–24.

Eneman, M., Ljungberg, J., Ravioli, E. and Rolandsson, B. (2022). The Sensitive nature of facial recognition: Tensions between the Swedish police and regulatory bodies. *Information Polity* , 27, pp.219–232.

Equality and Human Rights Commission (2018). *The Human Rights Act*. [online] Equality and human rights commission. Available at: https://www.equalityhumanrights.com/en/human-rights/human-rights-act [Accessed 7 Sep. 2023].

Equality and Human Rights Commission (2020). *Facial recognition technology and predictive policing algorithms out-pacing the law*. [online] Equality and Human Rights Commission. Available at:

https://www.equalityhumanrights.com/en/our-work/news/facial-recognition-technology-and-predictive-policing-algorithms-out-pacing-law [Accessed 11 Mar. 2023].

Eterno, J.A. and Silverman, E.B. (2010). The NYPD's Compstat: Compare Statistics or Compose Statistics? *International Journal of Police Science & Management*, 12(3), pp.426–449.

Evans, L. (2022). Uncovered: Facial Recognition and a Systemic Effects Approach to First Amendment Coverage. *Georgetown Law Technology Review*, 6, p.248.

Fan, M.D. (2018). Body cameras, big data, and police accountability. *Law & Social Inquiry*, 43(4), pp.1236–1256.

Fisher, D. (2021). *The Evolution of Closed-Circuit Television (CCTV) Systems*. [online] Vector Security Networks. Available at: https://vectorsecuritynetworks.com/the-evolution-of-closed-circuit-television-cctv-systems/ [Accessed 7 Sep. 2023].

Forbes Technology Council (2023). *Council Post: 14 Intriguing New And Potential Uses For Facial Recognition Technology*. [online] Forbes. Available at: https://www.forbes.com/sites/forbestechcouncil/2023/08/18/14-intriguing-new-and-potential-uses-for-facial-recognition-technology/ [Accessed 23 Aug. 2023].

Foucault, M. (1979). Panopticism . In: *Discipline and Punish: The Birth of the Prison*. New York: Vintage Books, pp.195–230.

Freedom of information Act 2014. Available at: https://www.irishstatutebook.ie/eli/2014/act/30/enacted/en/html [Accessed 7 Sep. 2023].

Friedersdorf, C. (2015). The NYPD is using Mobile X-Ray Vans to Spy on Unknown Targets. *The Atlantic*. [online] Available at: https://www.theatlantic.com/politics/archive/2015/10/the-nypd-is-using-mobile-x-rays-to-spy-on-unknown-targets/411181/ [Accessed 3 Jul. 2023].

Frischmann, B. and Selinger, E. (2018). *Re-Engineering Humanity*. Cambridge, UK: Cambridge University Press.

Fussey, P. (2007). Observing Potentiality in the Global City: Surveillance and Counterterrorism in London. *International Criminal Justice Review*, 17(3), pp.171–192.

Fussey, P. (2012). Eastern promise? East London transformations and the state of surveillance. *Information Polity* , 17(1), pp.21–34.

Fussey, P., Davies, B. and Innes, M. (2021). 'ASSISTED' FACIAL RECOGNITION AND THE REINVENTION OF SUSPICION AND DISCRETION IN DIGITAL POLICING. *British journal of Criminology*, 61(2), pp.325–344.

Fussey, P. and Murray, D. (2019). *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*. [online] University of Essex Human Rights Centre. Available at: https://repository.essex.ac.uk/24946/1/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report-2.pdf [Accessed 11 Mar. 2023].

Fussey, P. and Murray, D. (2020). Policing uses of live facial recognition in the United Kingdom. *Regulating Biometrics: Global Approaches and Urgent Questions* , pp.78–85.

Galterio, M.G., Shavit , S.A. and Hayajneh, T. (2018). A Review of Facial Biometrics Security for Smart Devices. *Computers*, 7(37), pp.1–11.

Garvie, C. (2019). *Garbage In. Garbage Out. Face Recognition on Flawed Data*. [online] Garbage In. Garbage Out. Face Recognition on Flawed Data. Available at: https://www.flawedfacedata.com/ [Accessed 3 Aug. 2023].

Garvie, C., Bedoya, A. and Frankle, J. (2016a). *The Perpetual Line-Up: Unregulated Police Face Recognition in America*. [online] Perpetual Line Up. Available at: https://www.perpetuallineup.org/background#footnote8_zix7uxb [Accessed 1 Mar. 2023].

Garvie, C., Bedoya, A. and Frankle, J. (2016b). *The Perpetual Line-Up: Unregulated Police Face Recognition in America*. [online] Perpetual Line Up. Available at: https://www.perpetuallineup.org/background#footnote8_zix7uxb [Accessed 1 Mar. 2023].

GCFGlobal (n.d.). *Computer Science: Algorithms*. [online] GCFGlobal.org. Available at: https://edu.gcfglobal.org/en/computer-science/algorithms/1/ [Accessed 28 May 2023].

General Data Protection Regulation. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 [Accessed 7 Sep. 2023].

Gentile, G. (2023). Does Big Brother exist? Face Recognition Technology in the United Kingdom. *Forthcoming in The Cambridge Handbook on Facial Recognition in the Modern State*. [online] Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4331633 [Accessed 7 Sep. 2023].

Gentilo, R. and Santana, R. (2023). *TSA is testing facial recognition at more airports, raising privacy concerns*. [online] AP NEWS. Available at: https://apnews.com/article/facial-recognition-airport-screening-tsa-d8b6397c02afe16602c8d34409d1451f [Accessed 5 Aug. 2023].

George, A.L. and Bennet, A. (2005). *Case Studies and Theory Development in the Social Sciences*. Cambridge, MA: MIT Press.

Gikay, A.A. (2023). Incrementalism–Regulating Law Enforcement Use of Real-Time Facial Recognition Technology in Public Spaces in the UK. *Forthcoming (Cambridge Law Journal)*.

Gillis, A. (2022). *What is algorithm? - Definition from WhatIs.com*. [online] WhatIs.com. Available at: https://www.techtarget.com/whatis/definition/algorithm [Accessed 28 May 2023].

Goldenberg, S. and Anuta, J. (2022). *Adams eyes expansion of highly controversial police surveillance technology*. [online] POLITICO. Available at: https://www.politico.com/news/2022/02/08/adams-police-surveillance-technology-00006230 [Accessed 5 Aug. 2023].

Goodey, E. (2015). *Remembrance Day*. [online] The Royal Family. Available at: https://www.royal.uk/remembrance-day#:~:text=On%20the%20second%20Sunday%20of [Accessed 7 Sep. 2023].

Government of UK (2018). *Data protection*. [online] GOV.UK. Available at: https://www.gov.uk/data-protection#:~:text=The%20Data%20Protection%20Act%20201 8 [Accessed 7 Sep. 2023].

Grimond, W. (2022). *Body-worn cameras are quietly taking over London*. [online] Huck. Available at: https://www.huckmag.com/article/body-worn-cameras-are-quietly-taking-over-london [Accessed 7 Sep. 2023].

Grother, P., Ngan, M. and Hanaoka, K. (2019). *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*. [online] National Institute of Standards and Technology. Available at: https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf [Accessed 11 Mar. 2023].

Guillén-Gámez, F., García-Magariño, I. and Prieto-Preboste, S. (2014). Facial Authentication Within Moodle Lessons. *Contemporary Engineering Sciences*, 7(8), pp.391–395.

Gummesson , E. (1991). *Qualitative Methods in Management Research*. California: Sage Publication, pp.83–156.

Güven, K. (2019). *Facial Recognition Technology: Lawfulness of processing under the GDPR in Employment, Digital signage and Retail Context*. [online] Available at: http://arno.uvt.nl/show.cgi?fid=147258 [Accessed 5 Aug. 2023].

Haggerty, K.D. and Ericson, R.V. (2000). The surveillant assemblage. *The British journal of sociology*, 51(4).

Hamann, K. and Smith, R. (2019). Facial Recognition Technology. *Criminal Justice*, 34(1), pp.9–13.

Hammond, A. (2020). *The 20 Biggest Advances in Tech Over the Last 20 Years | Alexander Hammond*. [online] fee.org. Available at:

https://fee.org/articles/the-20-biggest-advances-in-tech-over-the-last-20-years/ [Accessed 5 Aug. 2023].

Harwell, D. (2019). Federal study confirms racial bias of many facial-recognition systems, casts doubt on their expanding use. *The Washington Post*. [online] 19 Dec. Available at: https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/ [Accessed 28 Feb. 2023].

Harwell, D. (2021). Wrongfully arrested man sues Detroit police over false facial recognition match. *Washington Post*. [online] 13 Apr. Available at: https://www.washingtonpost.com/technology/2021/04/13/facial-recognition-false-arrest-lawsuit/ [Accessed 7 Sep. 2023].

Haskins, C. (2021). The NYPD Has Misled The Public About Its Use Of Facial Recognition Tool Clearview AI. *BuzzFeed News*. [online] 6 Apr. Available at: https://www.buzzfeednews.com/article/carolinehaskins1/nypd-has-misled-public-about-clearview-ai-use [Accessed 5 Aug. 2023].

Hernández, J., Ortiz, A., Andaverde, J. and Burlak, G. (2008). *Biometrics in Online Assessments: A Study Case in High School Students." In 18th International Conference on Electronics, Communications and Computers (conielecomp 2008)*. IEEE, pp.111–116.

Hill, D., O'Connor, C.D. and Slane, A. (2022). Police use of facial recognition technology: The potential for engaging the public through co-constructed policy-making. *International Journal of Police Science & Management*, 24(3), pp.325–335.

Hill, K. (2023). Which Stores Are Scanning Your Face? No One Knows. *The New York Times*. [online] 10 Mar. Available at: https://www.nytimes.com/2023/03/10/technology/facial-recognition-stores.html#:~:text=Typically%2C%20a%20store%20using%20facial [Accessed 5 Aug. 2023].

Home Office (2013). *Surveillance Camera Code of Practice*. [online] London: The Stationery Office. Available at:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/204775/Surveillance_Camera_Code_of_Practice_WEB.pdf [Accessed 7 Sep. 2023].

Home Office (2021). *Surveillance Camera Code of Practice: First Published June 2013 Amended November 2021*. [online] Home Office. Available at: Surveillance Camera Code of Practice First Published June 2013 Amended November 2021 [Accessed 7 Sep. 2023].

Home Office and Green, R.H.D. (2013). *Circular 011/2013: surveillance camera code of practice*. [online] GOV.UK. Available at: https://www.gov.uk/government/publications/circular-0112013 [Accessed 7 Sep. 2023].

Hooks, G. (2008). Military-Industrial Complex, Organization and History. *Encyclopaedia of Violence, Peace & Conflict*, 3, pp.207–214.

Horowitz, M.C., Kahn, L., Macdonald, J. and Schneider, J. (2023). Adopting AI: how familiarity breeds both trust and contempt. *AI & Society*, pp.1–15.

Hou, R. (2017). Neoliberal governance or digitalized autocracy? The rising market for online opinion surveillance in China. *Surveillance & Society*, 15(3/4), pp.418–424.

Huang, J. and Tsai, K.S. (2022). Securing authoritarian capitalism in the digital age: The political economy of surveillance in China. *The China Journal*, 88(1), pp.2–28.

Introna, L. and Wood, D. (2004). Picturing algorithmic surveillance: The politics of facial recognition systems. *Surveillance & Society*, 2(2/3), pp.177–198.

Irish Council for Civil Liberties (2022). *Garda use of Facial Recognition Technology poses extreme risk to human rights*. [online] Irish Council for Civil Liberties. Available at: https://www.iccl.ie/police-justice-reform/garda-use-of-facial-recognition-technology-poses-extreme-risk-to-human-rights/ [Accessed 2 May 2023].

Irish Legal News (2023). *Government to introduce standalone bill on facial recognition technology*. [online] Irish Legal News. Available at:

https://www.irishlegal.com/articles/government-to-introduce-standalone-bill-on-facial-recognition-technology [Accessed 7 Sep. 2023].

Israel, T. (2020). *Facial recognition is transforming our borders, and we are not prepared*. [online] Policy Options. Available at: https://policyoptions.irpp.org/magazines/november-2020/facial-recognition-is-transforming-our-borders-and-we-are-not-prepared/ [Accessed 5 Aug. 2023].

Jefferson, T. (2012). Policing the riots: from Bristol and Brixton to Tottenham, via Toxteth, Handsworth, etc: Tony Jefferson tells the angry, ongoing story of rioting over the past 30 years. *Criminal justice matters*, 87(1), pp.8–9.

Johnson, D. (1994). *Research Methods in Educational Management*. Essex: Longman Group.

Johnson, T.L., Johnson, N.N., McCurdy, D. and Olajide, M.S. (2022). Facial recognition systems in policing and racial disparities in arrests. *Government Information Quarterly* , 39(4), p.101753.

Joseph, G. and Offenhartz, J. (2020). *NYPD Used Facial Recognition Technology In Siege Of Black Lives Matter Activist's Apartment*. [online] Gothamist. Available at: https://gothamist.com/news/nypd-used-facial-recognition-unit-in-siege-of-black-lives-matter-activists-apartment [Accessed 5 Aug. 2023].

Kamali, S. (2017). Informants, Provocateurs, and Entrapment: Examining the Histories of the FBI's PATCON and the NYPD's Muslim Surveillance Program. *Surveillance & Society*, 15(1), pp.68–78.

Katsanis, S.H., Claes, P., Doerr, M., Cook-Deegan, R., Tenenbaum, J.D., Evans, B.J., Lee, M.K., Anderson, J., Weinberg, S.M. and Wagner, J.K. (2021). A survey of US public perspectives on facial recognition technology and facial imaging data practices in health and research contexts. *PloS one* , 16(10), p.e0257923.

Kempf, R.J. (2020). *The power of accountability: Offices of inspector general at the state and local levels* . Lawrence, KS: University of Kansas Press.

Khan, N. and Efthymiou, M. (2021). The use of biometric technology at airports: The case of customs and border protection (CBP). *International Journal of Information Management Data Insights*, 1, p.100049.

Klare, B.F., Burge, M.J., Klontz, J.C., Vorder Bruegge, R.W. and Jain, A.K. (2012). Face Recognition Performance: Role of Demographic Information. *IEEE Transactions on Information Forensics and Security*. [online] Available at: https://www.mitre.org/sites/default/files/pdf/11_4962.pdf [Accessed 25 Apr. 2023].

Klum, S.J., Han, H., Klare, B.F. and Jain, A.K. (2014). The FaceSketchID System: Matching Facial Composites to Mugshots. *Transactions on Information Forensics and Security*, 9(12), pp.2248–2263.

Knight, C.G. (2001). Human-Environment Relationship: Comparative Case Studies. In: *International Encyclopaedia of the Social & Behavioural Sciences*. pp.7039–7045.

Koebler, J. (2020). *Detroit Police Chief: Facial Recognition Software Misidentifies 96% of the Time*. [online] www.vice.com. Available at: https://www.vice.com/en/article/dyzykz/detroit-police-chief-facial-recognition-software-misidentifies-96-of-the-time [Accessed 5 Aug. 2023].

Kofman, A. (2017). *NYPD Refuses to Disclose Information About Its Face Recognition Program, So Privacy Researchers Are Suing*. [online] The Intercept. Available at: https://theintercept.com/2017/05/02/nypd-refuses-to-disclose-information-about-its-face-recognition-program-so-privacy-researchers-are-suing/ [Accessed 29 Jul. 2023].

Koops, B.J. (2021). The concept of function creep. *Law, Innovation and Technology*, 13(1), pp.29–56.

Kostka, G., Steinacker, L. and Meckel, M. (2023). Under big brother's watchful eye: Cross-country attitudes toward facial recognition technology. *Government information Quarterly*, 40(1), p.101761.

Kotsios, A., Magnani, M., Vega, D., Rossi, L. and Shklovski, I. (2019). An analysis of the consequences of the general data protection regulation on social network research. *ACM Transactions on Social Computing*, 2(3), pp.1–22.

Lammy, D. (2017). *The Lammy Review: An independent review into the treatment of, and outcomes for, Black, Asian and Minority Ethnic individuals in the Criminal Justice System*. [online] Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/643001/lammy-review-final-report.pdf [Accessed 7 Sep. 2023].

Landon-Murray, M. and Milliman, J. (2023). From 9/11 to the POST Act: democratic oversight of police surveillance technologies in New York City. *Journal of Policing, intelligence and Counter Terrorism*, pp.1–16.

Leslie, D. (2020). Understanding bias in facial recognition technologies: an explainer. *The Alan Turing Institute.* doi:https://doi.org/10.5281/zenodo.4050457.

Levine, E.S., Tisch, J., Tasso, A. and Joy, M. (2017). The New York City police department's domain awareness system. *Interfaces*, 47(1), pp.70–84.

Lewis, J.A. and Crumpler, W. (2021). *How Does Facial Recognition Work?* [online] www.csis.org. Available at: https://www.csis.org/analysis/how-does-facial-recognition-work [Accessed 28 May 2023].

Lewis, P., Newburn, T., Taylor, M., Mcgillivray, C., Greenhill, A., Frayman, H. and Proctor, R. (2011). *Reading the Riots: Investigating England's summer of disorder*. [online] Available at: http://eprints.lse.ac.uk/46297/1/Reading%20the%20riots%28published%29.pdf [Accessed 7 Sep. 2023].

Li, Z., Guo, Y., Yarime, M. and Wu, X. (2023). Policy designs for adaptive governance of disruptive technologies: the case of facial recognition technology (FRT) in China. *Policy Design and Practice*, 6(1), pp.27–40.

Liberty (2020). *The human rights act*. [online] Liberty. Available at: https://www.libertyhumanrights.org.uk/your-rights/the-human-rights-act/#:~:text=are%20under%20threat- [Accessed 7 Sep. 2023].

Lively, T.K. (2021). *Facial Recognition in the US: Privacy Concerns and Legal Developments*. [online] www.asisonline.org. Available at: https://www.asisonline.org/security-management-magazine/monthly-issues/security-technology/archive/2021/december/facial-recognition-in-the-us-privacy-concerns-and-legal-developments/ [Accessed 2 May 2023].

Local Government Association (n.d.). *General Data Protection Regulation (GDPR) | Local Government Association*. [online] www.local.gov.uk. Available at: https://www.local.gov.uk/our-support/research-and-data/data-and-transparency/general-data-protection-regulation-gdpr#:~:text=New%20rules%20relating%20to%20how [Accessed 7 Sep. 2023].

Long, C. (2016). *NYPD has used cell tracking technology 1,000 times since '08*. [online] The Seattle Times. Available at: https://www.seattletimes.com/nation-world/nypd-has-used-cell-tracking-technology-1000-times-since-08/ [Accessed 3 Jul. 2023].

Lunter, J. (2020). Beating the bias in facial recognition technology. *Biometric Technology Today*, 9, pp.5–7.

Luo, Y. and Guo, R. (2021). Facial Recognition in China: Current Status, Comparative Approach and the Road Ahead. *U. Pa. JL & Soc. Change*, 25, p.153.

Lyons, D. (2001). *Surveillance Society: Monitoring Everyday Life*. Buckingham: Open University.

Lyons, K. (2021). *Use of Clearview AI facial recognition tech spiked as law enforcement seeks to identify Capitol mob*. [online] The Verge. Available at: https://www.theverge.com/2021/1/10/22223349/clearview-ai-facial-recognition-law-enforcement-capitol-rioters [Accessed 5 Aug. 2023].

Mac, R., Haskins, C. and McDonald, L. (2020). *Clearview AI Says Its Facial Recognition Software Identified A Terrorism Suspect. The Cops Say That's Not True.* [online] BuzzFeed News. Available at: https://www.buzzfeednews.com/article/ryanmac/clearview-ai-nypd-facial-recognition [Accessed 5 Aug. 2023].

Mac, R., Haskins, C., Sacks, B. and McDonald, L. (2021). How A Facial Recognition Tool Found Its Way Into Hundreds Of US Police Departments, Schools, And Taxpayer-Funded Organizations. *BuzzFeed News*. [online] Available at: https://www.buzzfeednews.com/article/ryanmac/clearview-ai-local-police-facial-recognition [Accessed 5 Aug. 2023].

Mann, M. and Smith, M. (2017). Automated facial recognition technology: Recent Developments and approaches to oversight. *University of New South Wales Law Journal*, 40(1), pp.121–145.

Mantello, P. (2016). The machine that ate bad people: The ontopolitics of the precrime assemblage. *Big Data & Society*, 3(2).

Mason, J. (2002). *Qualitative researching*. London: Sage Publications.

McCarthy, C. (2019a). *Facial recognition leads cops to alleged rapist in under 24 hours*. [online] New York Post. Available at: https://nypost.com/2019/08/05/facial-recognition-leads-cops-to-alleged-rapist-in-under-24-hours/ [Accessed 8 Jul. 2023].

McCarthy, C. (2019b). *How NYPD's facial recognition software ID'ed subway rice cooker kook*. [online] New York Post. Available at: https://nypost.com/2019/08/25/how-nypds-facial-recognition-software-ided-subway-rice-cooker-kook/ [Accessed 8 Jul. 2023].

McSorley, T. (2021). The Case for a Ban on Facial Recognition Surveillance in Canada. *Surveillance & Society* , 19(2).

Mejía, P. (2019). *Report: NYPD Used Celebrity Images, Including Woody Harrelson, In Facial Recognition Dragnets*. [online] Gothamist. Available at: https://gothamist.com/news/report-nypd-used-celebrity-images-including-woody-harrelson-in-facial-recognition-dragnets [Accessed 5 Aug. 2023].

Metropolitan Police (n.d.). *Automatic Number Plate Recognition (ANPR)*. [online] Metropolitan Police. Available at: https://www.met.police.uk/advice/advice-and-information/rs/road-safety/automatic-number-plate-recognition-anpr/ [Accessed 7 Sep. 2023].

Metropolitan Police (n.d.). *EQUALITY IMPACT ASSESSMENT STEPS 1 TO 7*. [online] Metropolitan Police Service. Available at: https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/impact-assessments/lfr-eia2.pdf [Accessed 7 Sep. 2023].

Metropolitan Police (n.d.). *EQUALITY IMPACT ASSESSMENT STEPS 1 TO 7*. [online] Metropolitan Police Service. Available at: https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/new/rfr-eia-2023-v1-web.pdf [Accessed 7 Sep. 2023].

Metropolitan Police (n.d.). *Facial Recognition Technology*. [online] Metropolitan Police. Available at: https://www.met.police.uk/advice/advice-and-information/fr/facial-recognition-technology/ [Accessed 7 Sep. 2023].

Metropolitan Police (n.d.). *MPS LFR POLICY DOCUMENT: Direction for the MPS Deployment of overt Live Facial Recognition Technology to locate person(s) on a Watchlist*. [online] Metropolitan Police Service. Available at: https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/policy-documents/lfr-policy-document2.pdf [Accessed 7 Sep. 2023].

Metropolitan Police (n.d.). *MPS POLICY - RETROSPECTIVE FACIAL RECOGNITION SYSTEM*. [online] Metropolitan Police Service. Available at:

https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/new/rfr-policy-v1-final.pdf [Accessed 7 Sep. 2023].

Metropolitan Police (n.d.). *STANDARD OPERATING PROCEDURE (SOP) FOR THE OVERT DEPLOYMENT OF LIVE FACIAL RECOGNITION (LFR) TECHNOLOGY*. [online] Metropolitan Police Service. Available at: https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/policy-documents/lfr-sop.pdf [Accessed 7 Sep. 2023].

Metropolitan Police Service (2021). *DATA PROTECTION IMPACT ASSESSMENT (DPIA)*. [online] Metropolitan Police Service. Available at: https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/impact-assessments/lfr-dpia.pdf [Accessed 7 Sep. 2023].

Metropolitan Police Service (2023). *DATA PROTECTION IMPACT ASSESSMENT (DPIA)*. [online] Metropolitan Police Service. Available at: https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/new/mps-rfr-dpia-v1-web.pdf [Accessed 7 Sep. 2023].

Miller, W.R. (2017). Police authority in London and New York City 1830–1870. In: *The New Police in the Nineteenth Century,*. Routledge, pp.493–512.

Minderoo Centre for Technology and Democracy (2022). *A Sociotechnical Audit: Assessing Police use of Facial Recognition*. [online] Available at: https://www.mctd.ac.uk/a-sociotechnical-audit-assessing-police-use-of-facial-recognition/ [Accessed 7 Sep. 2023].

Mishra, A., Dash, S.S. and Tiwari, S. (2023). UNLOCKING THE MAGIC OF FACIAL RECOGNITION: EMPOWERING SECURITY AND EMOTIONS WITH SVM. *Journal of Data Acquisition and Processing*, 38(2), p.2402.

Mohammad, S.M. (2020). Facial recognition technology. *International Journal of Innovations in Engineering Research and Technology*, 7(6), pp.2394–3696.

Mohsin, K. (2020). *Facial Recognition - Boon or Bane*. [online] Available at: https://www.researchgate.net/profile/Kamshad-Mohsin/publication/343515450_Facial_Recognition_-_Boon_or_Bane/links/5f33cde6a6fdcccc43c24af9/Facial-Recognition-Boon-or-Bane.pdf [Accessed 2 May 2023].

Molnár-Gabor, F., Sellner, J., Pagil, S., Slokenberga, S., Tzortzatou-Nanopoulou, O. and Nyström, K. (2022). Harmonization after the GDPR? Divergences in the rules for genetic and health data sharing in four member states and ways to overcome them by EU measures: Insights from Germany, Greece, Latvia and Sweden . In: *Seminars in Cancer Biology*. Academic Press , pp.271–283.

Montgomery, J. and Marais., A. (2014). *Educational Content Access Control System*. U.S. Patent Application 14/ 212,069.

Moraes, T.G., Almeida, E.C. and De Pereira, J.R.L. (2021). Smile, you are being identified! Risks and measures for the use of facial recognition in (semi-) public spaces. *AI and Ethics*, 1, pp.159–172.

Morozov, E. (2013). *To Save Everything, Click Here: The Folly of Technological Solutionism*. New York: PublicAffairs.

Morrison, D. (2018). *IoT Regulation Still Catching Up to Industry*. [online] www.loopsec.com.au. Available at: https://www.loopsec.com.au/blog-events/blog/iot-regulation-still-catching-up [Accessed 2 May 2023].

Nagaraj, A. (2020). Indian police use facial recognition app to reunite families with lost children. *Reuters*. [online] 14 Feb. Available at: https://www.reuters.com/article/us-india-crime-children-idUSKBN2081CU [Accessed 5 Aug. 2023].

Najibi, A. (2020). *Racial Discrimination in Face Recognition Technology*. [online] Harvard University: The Graduate School of Arts and Sciences. Available at: https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technol

ogy/#:~:text=Even%20if%20accurate%2C%20face%20recognition [Accessed 7 Sep. 2023].

Naker, S. and Greenbaum, D. (2017). Now you see me: Now you still do: Facial recognition technology and the growing lack of privacy. *BUJ Sci. & Tech. L.*, 23, p.88.

National Physical Laboratory and Metropolitan Police Service (2020). *Metropolitan Police Service Live Facial Recognition Trials*. [online] National Physical Laboratory and Metropolitan Police Service. Available at: https://www.met.police.uk/SysSiteAssets/media/downloads/central/services/accessing-information/facial-recognition/met-evaluation-report.pdf [Accessed 12 Mar. 2023].

NEC (2019). *7 Ways Facial Recognition Can Unlock A Secure, Frictionless and Personalised Travel Experience courtesy of a single, unified biometric digital ID*. [online] Available at: https://www.necam.com/docs/?id=ca64497c-5a3e-496d-a7d8-0fae73340c7e#:~:text=With%20facial%20recognition%2C%20airport%20security,addressing%20potential%20and%20actual%20threats. [Accessed 5 Aug. 2023].

Nestrova, I. (2020). Mass data gathering and surveillance: the fight against facial recognition technology in the globalized world. *SHS Web of Conferences*, 74, p.03006.

NIST (2019). *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*. [online] Available at: https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf [Accessed 5 Aug. 2023].

Noor, K.B. (2008). Case Study: A Strategic Research Methodology. *American Journal of Applied Sciences* , 5(11), pp.1602–1604.

Nussbaum, B. (2012). From Brescia to Bin Laden: The NYPD, international policing, and 'national' security. *Journal of Applied Security Research*, 7, pp.178–202.

NYCLU (2018). *Stop-and-Frisk Data*. [online] New York Civil Liberties Union. Available at: https://www.nyclu.org/en/stop-and-frisk-data [Accessed 5 Aug. 2023].

NYCLU (2021). *Re: Comments on Draft Surveillance Impact and Use Policies*. [online] Available at: https://www.nyclu.org/sites/default/files/field_documents/nyclu_letter_on_post_act_draft_policies_0.pdf [Accessed 5 Aug. 2023].

NYPD (n.d.). *Facial Recognition - NYPD*. [online] www.nyc.gov. Available at: https://www.nyc.gov/site/nypd/about/about-nypd/equipment-tech/facial-recognition.page#:~:text=Since%202011%2C%20the%20NYPD%20has [Accessed 29 Jul. 2023].

NYPD (2020). *Patrol Guide: Facial Recognition Technology*. [online] Available at: https://www.nyc.gov/assets/nypd/downloads/pdf/nypd-facial-recognition-patrol-guide.pdf [Accessed 29 Jul. 2023].

NYPD (2021). *FACIAL RECOGNITION: IMPACT AND USE POLICY*. [online] Available at: https://www.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/facial-recognition-nypd-impact-and-use-policy_4.9.21_final.pdf [Accessed 29 Jul. 2023].

Ó Conghaile, P. (2018). *Irish airports first in Europe with facial recognition for US Preclearance*. [online] Independent.ie. Available at: https://www.independent.ie/life/travel/travel-news/irish-airports-first-in-europe-with-facial-recognition-for-us-preclearance/37412082.html [Accessed 25 Aug. 2023].

O'Mallon, F. (2019). *Home Affairs suggests porn viewers be subject to face scans*. [online] The Sydney Morning Herald. Available at: https://www.smh.com.au/politics/federal/home-affairs-suggests-porn-viewers-be-subject-to-face-scans-20191028-p534yk.html [Accessed 5 Aug. 2023].

OECD (2020). *Ensuring data privacy as we battle COVID-19* . [online] OECD. Available at: https://read.oecd-ilibrary.org/view/?ref=128_128758-vfx2g82fn3&title=Ensuring-data-privacy-as-we-battle-COVID-19 [Accessed 7 Sep. 2023].

Office of the New York State Comptroller (2023). *New York City Office of Technology and Innovation: Artificial Intelligence Governance*. [online] Office of the New York State Comptroller. Available at:

https://www.osc.state.ny.us/files/state-agencies/audits/pdf/sga-2023-21n10.pdf [Accessed 5 Aug. 2023].

OIG-NYPD (2022). *DOI'S OFFICE OF THE INSPECTOR GENERAL FOR THE NYPD ISSUES REPORT ASSESSING NYPD'S RESPONSE TO THE PUBLIC OVERSIGHT OF SURVEILLANCE TECHNOLOGY ACT OF 2020* . [online] New York: The City of New York Department of Investigation . Available at: https://www.nyc.gov/assets/doi/reports/pdf/2022/20PostActRelease.Rpt.11.03.2022.pdf [Accessed 29 Jul. 2023].

Orwell, G. (1949). *Nineteen Eighty-four*. London: Secker & Warburg.

Palinkas, L.A., Horwitz, S.A., Green, C.A., Wisdom, J.P., Duan, N. and Hoagwood, K. (2015). Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. *Adm Policy Ment Health*, 42(5), pp.533–544.

Parker, J. (2020). *Facial Recognition Success Stories Showcase Positive Use Cases of the Technology*. [online] Security Industry Association. Available at: https://www.securityindustry.org/2020/07/16/facial-recognition-success-stories-showcase-positive-use-cases-of-the-technology/ [Accessed 8 Jul. 2023].

Pasztor, A. and Wall, R. (2016). *Drone Regulators Struggle to Keep Up With the Rapidly Growing Technology*. [online] WSJ. Available at: https://www.wsj.com/articles/drone-regulators-struggle-to-keep-up-with-the-rapidly-growing-technology-1468202371#:~:text=Air%2Dsafety%20authorities%20on%20both [Accessed 2 May 2023].

Patel, F. and Price, M. (2017). *Keeping Eyes on NYPD Surveillance | Brennan Center for Justice*. [online] www.brennancenter.org. Available at: https://www.brennancenter.org/our-work/analysis-opinion/keeping-eyes-nypd-surveillance [Accessed 29 Jul. 2023].

Patton, M.Q. (2002). *Qualitative Research and evaluation methods*. Thousand Oaks, CA: Sage Publications.

Peck vs the United Kingdom [2003] (European Court of Human Rights) Available at: https://www.zmogausteisiugidas.lt/en/case-law/peck-v-the-united-kingdom#:~:text=The%20Court%20ruled%20that%20the,the%20disclosure%20of%20the%20footage. [Accessed 7 Sep. 2023].

Peloquin, D., DiMaio, M., Bierer, B. and Barnes, M. (2020). Disruptive and avoidable: GDPR challenges to secondary research uses of data. *European Journal of Human Genetics*, 28, pp.697–705.

Perego, A. (2021). A New Age of Surveillance: Facial Recognition in Policing and Why It Should Be Abolished. *Journal of Equal Rights and Social Justice*, 28(1), p.79.

Petrescu, R.V. (2019). Face recognition as a biometric application. *Journal of Mechatronics and Robotics*, 3, pp.237–257.

Phillips, P., O'Toole, A., Narvekar, A., Jiang, F. and Ayadd, J. (2010). *An Other-Race Effect for Face Recognition Algorithms*. [online] National Institute of Standards and Technology. Available at: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=904972 [Accessed 25 Apr. 2023].

Pierce, J.D., Rosipko, B., Youngblood, L., Gilkeson, R.C., Gupta, A. and Bittencourt, L.K. (2021). Seamless Integration of Artificial Intelligence Into the Clinical Environment: Our Experience With a Novel Pneumothorax Detection Artificial Intelligence Algorithm. *Journal of the American College of Radiology*, 18(11), pp.1497–1505.

Pinnock, H., Huby, G., Powell, A., Kielmann, T., Price, D., Williams, S. and Sheikh , A. (2008). *The process of planning, development and implementation of a General Practitioner with a Special Interest service in Primary Care Organisations in England and Wales: a comparative prospective case study*. Report for the National Co-ordinating Centre for NHS Service Delivery and Organisation R&D (NCCSDO).

Popova, A. (2020). *Facing a Privacy Breach Under Growing GDPR-inspired Laws Can Pose Challenges for Companies*. [online] Security Intelligence. Available at:

https://securityintelligence.com/posts/companies-face-challenges-due-to-increasing-number-of-gdpr-inspired-regulations/ [Accessed 7 Sep. 2023].

Press Association (2016). *Thousands of Metropolitan police to be equipped with body-worn cameras*. [online] The Guardian. Available at: https://www.theguardian.com/uk-news/2016/oct/17/thousands-of-metropolitan-police-to-be-equipped-with-body-worn-cameras [Accessed 7 Sep. 2023].

Privacy International (n.d.). *Facial Recognition | Privacy International*. [online] privacyinternational.org. Available at: https://privacyinternational.org/learn/facial-recognition [Accessed 2 Mar. 2023].

Professional Security (2022). *Police's 1960s CCTV experiments: part 1*. [online] Professional Security Magazine Online. Available at: https://professionalsecurity.co.uk/news/case-studies/polices-1960s-cctv-experiments-part-1/ [Accessed 7 Sep. 2023].

Pujianto, S. (2023). *The Development of Face Recognition System in Computer Vision Using Deep Learning: Deep Siamese Networks Method*. [online] Available at: http://etd.repository.ugm.ac.id/penelitian/detail/219735 [Accessed 5 Aug. 2023].

Purshouse, J. and Campbell, L. (2019). Privacy, crime control and police use of automated facial recognition technology. *Criminal Law Review*, 3, pp.188–204.

Puthea, K., Hartanto, R. and Hidayat, R. (2017). *A Review Paper on Attendance Marking System Based on Face Recognition." In 2nd International Conferences on Information Technology, Information Systems and Electrical Engineering*. IEEE, pp.304–309.

Qiang, J., Wu, D., Du, H., Zhu, H., Chen, S. and Pan, H. (2022). Review on Facial-Recognition-Based Applications in Disease Diagnosis. *Bioengineering,* 9(7), p.273.

Quinn, J.F., Holman, J.E. and P.M Toblowsky (2006). A case study method for teaching theoretical criminology. *Journal of Criminal Justice Education*, 3(1), pp.53–70.

Radiya-Dixit, E. and Neff, G. (2023). A Sociotechnical Audit: Assessing Police Use of Facial Recognition. *Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency*, pp.1334–1346.

Rai, N. and Thapa, B. (2015). A study on purposive sampling method in research. *Kathmandu: Kathmandu School of Law*, 5.

Rainie, L., Funk, C., Anderson, M. and Tyson, A. (2022). *Public more likely to see facial recognition technology use by police as good for society*. [online] Pew Research Center: Internet, Science & Tech. Available at: https://www.pewresearch.org/internet/2022/03/17/public-more-likely-to-see-facial-recognition-use-by-police-as-good-rather-than-bad-for-society/ [Accessed 5 Aug. 2023].

Rajesh, C. (2017). Technology and its impact on Natural Environment. In: *Environmental Studies: Problems and Issues*. United States: Lulu Publication.

Rawlings, P. (2002). *Policing: A Short History.* Cullompton: Willan, pp.199–200.

Raza, S.A. and Awan, A.G. (2016). THE EFFECTS OF TOTALITARIANISM AND MARXISM TOWARDS DYSTOPIAN SOCIETY IN GEORGE ORWELL'S SELEECTED FICTIONS. *Global Journal of Management and Social Sciences*, 2(4), pp.21–37.

Rebelo, A.D., Verboom, D.E., Dos Santos, N.R. and De Graaf, J.W. (2023). The impact of artificial intelligence on the tasks of mental healthcare workers: A scoping review. *Computers in Human Behavior: Artificial Humans*, 1(2), p.100008.

Reinbold, P. (2020). Facing Discrimination : Choosing Equality over Technology. [online] Available at: https://www.zbw.eu/econis-archiv/bitstream/11159/460306/1/EBP078154626_0.pdf [Accessed 7 Sep. 2023].

Restrepo, M.A. (2023). *She was denied entry to a Rockettes show — then the facial recognition debate ignited*. [online] NPR. Available at: https://www.npr.org/2023/01/21/1150289272/facial-recognition-technology-madison-square-garden-law-new-york [Accessed 29 Jul. 2023].

Review on the effects of age, gender, and race demographics on automatic face recognition. (2018). *Vis Comput*, 34, pp.1617–1630.

Richardson, R. (2021). Facial recognition in the public sector: the policy landscape. *The German Marshall Fund of the United States.*.

Ring, J. (2023). *30 years ago, one decision altered the course of our connected world*. [online] NPR. Available at: https://www.npr.org/2023/04/30/1172276538/world-wide-web-internet-anniversary#:~:text=Hip%2DHop%2050- [Accessed 5 Aug. 2023].

Ringrose, K. (2019). Law Enforcement's pairing of facial recognition technology with body-worn cameras escalates privacy concerns. *Virginia Law Review Online*, 105, pp.57–66.

Ritchie, K.L., Cartledge, C., Growns, B., Yan, A., Wang, Y., Guo, K., Kramer, R.S., Edmond, G., Martire, K.A., San Roque, M. and White, D. (2021). Public attitudes towards the use of automatic facial recognition technology in criminal justice systems around the world. *PloS one*, 16(10), p.e0258241.

Roach, J. (2020). *Using AI, people who are blind are able to find familiar faces*. [online] Microsoft | Source. Available at: https://news.microsoft.com/source/features/diversity-inclusion/project-tokyo [Accessed 5 Aug. 2023].

Robinowicz, C. (2023). Approaches to Regulating Government Use of Facial Recognition Technology. *Harvard Journal of Law & Technology*. [online] Available at: https://jolt.law.harvard.edu/digest/approaches-to-regulating-government-use-of-facial-recognition-technology [Accessed 5 Aug. 2023].

Robson, D. (2011). *Facial recognition a system problem gamblers can't beat?* [online] Toronto Star. Available at: https://www.thestar.com/news/gta/facial-recognition-a-system-problem-gamblers-can-t-beat/article_b7a693a5-5357-5e74-bfd2-b3160e516240.html [Accessed 5 Aug. 2023].

Roeloffs, M.W. (2023). *DHS Says It Identified 311 New Child Sexual Exploitation Victims—After Forbes Reports AI Facial Recognition Push*. [online] Forbes. Available at: https://www.forbes.com/sites/maryroeloffs/2023/08/09/dhs-says-it-identified-311-new-child-sexual-exploitation-victims-after-forbes-reports-ai-facial-recognition-push/ [Accessed 5 Aug. 2023].

Russell, A. (2020). RCMP used Clearview AI facial recognition tool in 15 child exploitation cases, helped rescue 2 kids. *Global News*. [online] 27 Feb. Available at: https://globalnews.ca/news/6605675/rcmp-used-clearview-ai-child-exploitation/ [Accessed 16 Apr. 2023].

Ryan-Mosley, T. (2021). *The new lawsuit that shows facial recognition is officially a civil rights issue*. [online] MIT Technology Review. Available at: https://www.technologyreview.com/2021/04/14/1022676/robert-williams-facial-recognition-lawsuit-aclu-detroit-police/ [Accessed 5 Aug. 2023].

Schippers, B. (2019). *Facial recognition: ten reasons you should be worried about the technology*. [online] The Conversation. Available at: https://theconversation.com/facial-recognition-ten-reasons-you-should-be-worried-about-the-technology-122137 [Accessed 25 Apr. 2023].

Schuppe, J. (2019). NYPD used celebrity doppelgängers to fudge facial recognition results, researchers say. *NBC News*. [online] 19 May. Available at: https://www.nbcnews.com/news/us-news/nypd-used-celebrity-doppelg-ngers-fudge-facial-recognition-results-researchers-n1006411 [Accessed 5 Aug. 2023].

Scott, H. (1954). *Scotland Yard*. London: André Deutsch, pp.130–136.

Selinger, E. and Hartzog, W. (2020). The inconsentability of facial surveillance. *Loy. L. Rev.*, 66, p.33.

Selwyn, N., Andrejevic, M., O'Neil, C. and Gu, X. (n.d.). Facial recognition technology: key issues and emerging concerns. In: *Cambridge Handbook on Facial Recognition in the Modern State.* Cambridge University Press.

Seng, S., Al-Ameen, M.N. and Wright, M. (2021). A First Look into Users' Perceptions of Facial Recognition in the Physical World. *Computers & Security*, 105, p.102227.

Simerman, J. (2023). *What is facial recognition technology, and how do police use it? 5 things to know*. [online] NOLA.com. Available at: https://www.nola.com/news/crime_police/whats-facial-recognition-tech-and-how-do-police-use-it/article_352ce43a-888a-11ed-a486-db6b661d0829.html [Accessed 28 May 2023].

Sinmaz, E. (2023). Live facial recognition labelled 'Orwellian' as Met police push ahead with use. *The Guardian*. [online] 5 Apr. Available at: https://www.theguardian.com/technology/2023/apr/05/live-facial-recognition-criticised-metropolitan-police#:~:text=It%20was%20commissioned%20by%20the [Accessed 7 Sep. 2023].

Sisitzky, M. and Schaefer, B. (2021). *The NYPD Published Its Arsenal of Surveillance Tech. Here's What We Learned*. [online] New York Civil Liberties Union. Available at: https://www.nyclu.org/en/news/nypd-published-its-arsenal-surveillance-tech-heres-what-we-learned [Accessed Aug. 2023].

Slobogin, C. (2017). Policing, databases and surveillance. *Criminology, Criminal Justice, Law & Society*, 18(3), pp.70–84.

Smith, M. and Miller, S. (2022). The ethical application of biometric facial recognition technology. *AI and Society*, 37, pp.167–175.

Stake, R.E. (1995). *The art of case study research*. London: Sage Publications.

Steinacker, L., Meckel, M., Kostka, G. and Borth, D. (2020). Facial Recognition: A cross-national Survey on Public Acceptance, Privacy, and Discrimination. *arXiv preprint arXiv:2008.07275*.

Stokes, E. (2020). *Wrongful arrest exposes racial bias in facial recognition technology*. [online] www.cbsnews.com. Available at:

https://www.cbsnews.com/news/detroit-facial-recognition-surveillance-camera-racial-bias-crime/ [Accessed 7 Sep. 2023].

Surveillance Studies Network (2014). *An introduction to the surveillance society – The Surveillance Studies Network*. [online] Surveillance-studies.net. Available at: https://www.surveillance-studies.net/?page_id=119 [Accessed 7 Sep. 2023].

Surveillance Technology Oversight Project (2020). *S.T.O.P. Condemns NYPD Facial Recognition Surveillance Of BLM Protest Leader*. [online] S.T.O.P. - The Surveillance Technology Oversight Project. Available at: https://www.stopspying.org/latest-news/2020/8/14/stop-condemns-nypd-facial-recognition-surveillance-of-blm-protest-leader [Accessed 2 May 2023].

Surveillance Technology Oversight Project (2022). *S.T.O.P. Welcomes OIG Report On NYPD Violations of Surveillance Transparency Law*. [online] S.T.O.P. - The Surveillance Technology Oversight Project. Available at: https://www.stopspying.org/latest-news/2022/11/3/mdm1a76sdohz1um4azvjm1k6sbnnz5 [Accessed 30 Jul. 2023].

Tedeneke, A. (2021). *Law Enforcement Agencies Develop Best Practices for Using Facial Recognition*. [online] World Economic Forum. Available at: https://www.weforum.org/press/2021/10/law-enforcement-agencies-develop-best-practices-for-using-facial-recognition/#:~:text=%E2%80%9CAround%20the%20world%2C%20law%20enforcement [Accessed 5 Aug. 2023].

Teller, A., Bublies, T., Staudinger, T., Oswald, I., Meißner, S. and Allen, M. (2009). The Mobile Phone: Powerful Communicator and Potential Metal Dissiapator. In: *Ecological Perspectives for Science and Society*. [online] GAIA. Available at: https://www.wu.ac.at/fileadmin/wu/d/i/wgi/reller/reller4_mobilephone_powerful_communicator_and_potential_metal_dissipator.pdf [Accessed 5 Aug. 2023].

Tellis, W.M. (1997). Introduction to Case Study. *The Qualitative Report*, [online] 3(2). Available at: https://nsuworks.nova.edu/tqr/vol3/iss2/4/ [Accessed 20 Jun. 2023].

Tempey, N. (2016). The NYPD Is Tracking Drivers Across The Country Using License Plate Readers. *The Gothamist*. [online] Available at: https://gothamist.com/news/the-nypd-is-tracking-drivers-across-the-country-using-license-plate-readers [Accessed 29 Jul. 2023].

The British Museum (n.d.). *Our earliest technology? – Smarthistory*. [online] smarthistory.org. Available at: https://smarthistory.org/our-earliest-technology/#:~:text=Made%20nearly%20two%20million%20years [Accessed 5 Aug. 2023].

The Digital Panopticon (n.d.). *Metropolitan Police Register of Habitual Criminals 1881-1925 | The Digital Panopticon*. [online] www.digitalpanopticon.org. Available at: https://www.digitalpanopticon.org/Metropolitan_Police_Register_of_Habitual_Criminals_1881-1925 [Accessed 7 Sep. 2023].

Thrall, J.H., Li, X., Li, Q., Cruz, C., Do, S., Dreyer, K. and Brink, J. (2018). Artificial Intelligence and Machine Learning in Radiology: Opportunities, Challenges, Pitfalls, and Criteria for Success. *Journal of the American College of Radiology*, 15(3), pp.504–508.

Tucker, J. (2014). *How facial recognition technology came to be*. [online] Available at: https://www.wesleyan.edu/allbritton/cspl/scholarship/jennifertucker.pdf [Accessed 26 Jun. 2023].

Turley, J. (2020). Anonymity, obscurity, and technology: Reconsidering privacy in the age of biometrics. *BUL Rev.,* 100, p.2179.

U.S Customs and Border Protection (n.d.). *Biometrics | U.S. Customs and Border Protection*. [online] www.cbp.gov. Available at: https://www.cbp.gov/travel/biometrics#:~:text=CBP%20is%20leading%20the%20way [Accessed 25 Aug. 2023].

UK Information Commissioners Office (2020). *Guidance on the AI auditing framework: Draft guidance for consultation*. [online] Information Commissioners Office. Available at:

https://ico.org.uk/media/2617219/guidance-on-the-ai-auditing-framework-draft-for-consultation.pdf [Accessed 7 Sep. 2023].

United States Government Accountability Office (2022). *Facial Recognition Technology: CBP Traveler Identity Verification and Efforts to Address Privacy Issues*. [online] United States Government Accountability Office. Available at: https://www.gao.gov/assets/gao-22-106154.pdf [Accessed 25 May 2023].

University of York (2022). *How do algorithms work?* [online] University of York. Available at: https://online.york.ac.uk/how-do-algorithms-work/ [Accessed 28 May 2023].

Urquhart, L. and Miranda, D. (2022). Policing faces: the present and future of intelligent facial surveillance. *Information & Communications Technology Law*, 31(2), pp.194–219.

Van Cleave, K. (2023). *TSA expands controversial facial recognition program - CBS News*. [online] www.cbsnews.com. Available at: https://www.cbsnews.com/news/tsa-facial-recognition-program-airports-expands/ [Accessed 5 Aug. 2023].

Verganti, R. (2009). *Design-Driven Innovation: Changing the rules of Competition by radically Innovating What Things Mean*. [online] Harvard Business Press. Available at: https://books.google.ie/books?id=x30ovxn2eCcC&pg=PA75&redir_esc=y#v=onepage&q&f=false [Accessed 5 Aug. 2023].

Vincent, J. (2020). NYPD used facial recognition to track down Black Lives Matter activist. *The Verge*. [online] Available at: https://www.theverge.com/2020/8/18/21373316/nypd-facial-recognition-black-lives-matter-activist-derrick-ingram [Accessed 5 Aug. 2023].

Waltl, B. and Vogl, R. (2018). Explainable artificial intelligence the new frontier in legal informatics. *Jusletter IT,* 4, pp.1–10.

Watkins, A. (2021). Cameras, Drones and X-Ray Vans: How 9/11 Transformed the N.Y.P.D. Forever. *The New York Times*. [online] 8 Sep. Available at:

https://www.nytimes.com/2021/09/08/nyregion/nypd-9-11-police-surveillance.html [Accessed 3 Jul. 2023].

Williams, C.A. (2003). Police Surveillance and the Emergence of CCTV in the 1960s. *Crime Prevention and Community Safety*, 5, pp.27–37.

Williams, K. (2020). *Case Studies in the Social Sciences*. [online] www.epa.gov. Available at: https://www.epa.gov/research/case-studies-social-sciences#:~:text=Case%20studies%20are%20used%20to%3A [Accessed 19 Jun. 2023].

Wong, L. (2020). Smart glasses for dementia land students top tech prize. *The Straits Times*. [online] 28 Dec. Available at: https://www.straitstimes.com/tech/tech-news/smart-glasses-for-dementia-land-students-top-tech-prize [Accessed 5 Aug. 2023].

Woollacott, E. (2021). *London's Met Police Buying Retrospective Facial Recognition Technology*. [online] Forbes. Available at: https://www.forbes.com/sites/emmawoollacott/2021/09/28/londons-met-police-buying-retrospective-facial-recognition-technology/ [Accessed 7 Sep. 2023].

Yin, R. (1984). *Case Study Research: Design and Methods*. California: Sage Publication, pp.11–15.

Yin, R. (1993). *Application of Case Study Research*. California : Sage Publication, pp.33–35.

Yin, R.K. (1990). *Case Study Research, Design and Methods.* Revised ed. *Applied Social Research Methods Series*, Newbury Park, CA: Sage Publications.

Yin, R.K. (2009). *Case study research: Design and method*. London: Sage publications.

Zainal, Z. (2007). Case study as a research method. *Jurnal kemanusiaan*, 5(1).

Zuboff, S. (2015). Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, 30(1), pp.75–89.