TALLINN UNIVERSITY OF TECHNOLOGY

School of Information Technology
Department of Software Science

Kayla Marie Cannon 184563IVCM

AMERICA'S PANOPTICON: PRIVACY IMPLICATIONS OF FACIAL RECOGNITION BY LAW ENFORCEMENT

Master's Thesis

Supervisor:	Mika Kerttunen
	D.Soc.Sc.
Co-Supervisor:	Eneken Tikk
	D.Jur.

Tallinn 2019

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Kayla Marie Cannon 184563IVCM

AMEERIKA PANOPTIKON: ÕIGUSKAITSEORGANITE POOLT NÄOTUVASTUSE KASUTAMISE MÕJU PRIVAATSUSELE

Magistritöö

Juhendaja: Mika Kerttunen
D.Soc.Sc.
Juhendaja: Eneken Tikk
D.Jur.

Tallinn 2019

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Kayla Marie Cannon

13.05.2019

Abstract

Why are lawmakers in the United States apprehensive to regulate law enforcement's use of facial recognition technology, and how does this impact American citizens? These questions are pertinent in the study of law enforcement practices because new and improved investigative tools are being developed every day. Literature suggests that surveillance and facial recognition invade privacy, but few recognize that a panopticon is emerging in present-day society. The thesis seeks to uncover the mysteries behind American law enforcement's application of surveillance and facial recognition. Firstly, the growth of surveillance in the United States is addressed and the discussion of American surveillance becoming a panopticon is introduced. Technologies behind facial recognition and surveillance systems are then examined, explaining how the two work together. This discussion continues through the expression of privacy concerns surrounding the implementation of surveillance and facial recognition technologies. An analysis is later conducted on the law enforcement implementation of these technologies in the United States, the United Kingdom and China to consider other approaches. Finally, future research ideas are proposed regarding the impact that facial recognition has on minority populations. Altogether, this thesis demonstrates that the current application of surveillance and facial recognition in the United States should be improved so that citizens can enjoy both security and privacy.

This thesis is written in English and is 42 pages long, including five chapters, zero figures and zero tables.

Annotatsioon

Miks kardavad seadusandjad Ameerika Ühendriikides reguleerida õiguskaitseorganite näotuvastustehnoloogiate kasutust ja kuidas mõjutab see Ameerika kodanikke? Kuivõrd iga päev arendatakse uusi uurimisvahendeid, on need küsimused õiguskaitseorganite tegevuse uuringutes asjakohased. Kirjutatakse küll sellest, et jälgimistegevus ning näotuvastuse kasutamine tungivad inimeste privaatsusesse, kuid vähesed räägivad sellest, et juba täna on tekkimas panoptikon. Antud uurimuse eesmärk on uurida lähemalt, mis saladusi peitub Ameerika õiguskaitses kui asi puudutab järelvalvet ja näotuvastust. Esiteks võetakse luubi alla jälgimistegevuse kasv ja areng Ameerika Ühendriikides ning tutvustatakse ideed, mille kohaselt Ameerika järelvalve on muutumas panoptikoniks. Seejärel uuritakse näotuvastuse ja jälgimissüsteemide tehnoloogiaid ning kuidas need omavahel toimivad. Arutletakse probleeme, mis võivad tekkida jälgimise ning näotuvastuse tehnoloogiate rakendamisel ning milline on nende mõju inimeste privaatsusele. Võrdluseks tuuakse analüüs sellest, kuidas rakendatakse antud tehnoloogiaid nii Ameerika Ühendriikides, Ühendkuningriigis kui ka Hiinas. Lõpetuseks pakub autor välja ideid, kuidas edasi uurida, milline on näotuvastuse kasutuse mõju elanikkonna vähemuste esindajatele. Magistritöö tõestab, et praegust jälgimistegevuse ja näotuvastuse elluviimist ning kasutust Ameerika Ühendriikides tuleb parandada, et üheaegselt oleksid kaitstud nii kodanike privaatsus kui ka julgeolek.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 42 leheküljel, viis peatükki, null joonist, null tabelit.

List of abbreviations and terms

U.S.	United States
LEA	Law Enforcement Agency
MIRS	Maryland Image Repository System
ACLU	American Civil Liberties Union
U.K.	United Kingdom
UAV	Unmanned Aerial Vehicle
ARGUS-IS	Autonomous Real-Time Ground Ubiquitous Surveillance-Imaging System
9/11	September 11th, 2001
MPS	Metropolitan Police Service
DMV	Department of Motor Vehicles
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
FACES	Face Analysis Comparison and Examination System
APD	Albuquerque Police Department
FBI	Federal Bureau of Investigation
NGI	Next Generation Identification
IPS	Interstate Photo System
NYPD	New York Police Department
FOIA	Freedom of Information Act
GAO	Government Accountability Office
SCS	Social Credit System
SCC	Surveillance Camera Commissioner
ICO	Information Commissioner’s Office

Table of contents

1 Introduction

As of 2016, United States (U.S.) law enforcement agencies (LEAs) in nineteen states employed the use of facial recognition technology [1]. This technology has come to light as a result of media coverage of criminal investigations. One of the most recent cases involves a murder investigation was conducted after a man shot and killed five employees of the *Capital Gazette* newspaper in June 2018 [2]. The suspect, Jarrod Ramos, had no forms of identification and was noncooperative with police [2]. As a result, law enforcement officers identified Ramos after submitting his photo to Maryland's facial recognition database, the Maryland Image Repository System (MIRS) [2].

Facial recognition technology successfully helped law enforcement identify their suspect, but the deployment of such technology has been the centre of controversy surrounding the fact that it invades the privacy of citizens. In an attempt to preserve the privacy of Americans, the American Civil Liberties Union (ACLU) has urged the Justice Department to investigate law enforcement's use of facial recognition technology [3].

This thesis will discuss facial recognition technology and how, when paired with surveillance technologies, it can impact the data subject's privacy. Both facial recognition and surveillance technologies will be touched on, before analysing how they are employed by police in the United States. As a result, this thesis will guide the country's LEAs on how to better implement these technologies, so that citizens can enjoy both security and privacy. The goal is to bring attention to the potential threat that the country's current application of surveillance and facial recognition poses against American citizens. We will give suggestions to federal, state and local LEAs on how to make better use of their investigative tools.

This research will also draw a comparison between law enforcement's use of facial recognition within the United States, the United Kingdom (U.K.) and China. The result of this comparison is meant to serve as proof that regulating law enforcement in this context can be beneficial, while also serving as a warning of how facial recognition, when left unregulated, can be used to unnecessarily invade the privacy of citizens. The United

Kingdom and China serve as examples to highlight different practices around the world, which will either validate the practices of the U.S. or will bring about different methods to discuss. In doing so, we can determine how law enforcement agencies' use of this technology can be regulated and how they can be held accountable for their actions.

This report focuses on the employment of facial recognition systems that analyse facial features captured from still photos or security camera footage. This paper will not discuss the details of the categories of facial recognition, nor will it mention how facial recognition algorithms under these classifications function from a technical perspective. We will, however, evaluate how such algorithms are employed in a real-life setting. Facial recognition algorithms will not be investigated, but rather how they are applied in the setting of law enforcement.

2 Surveillance

The concept of surveillance can differ depending on the application in question. Surveillance can be conducted by a variety of actors, each having their own aims and motivation [4]. As Staples mentions, regardless of the actor involved or their motivation, the general intent of surveillance is to "mould, shape, and modify actions and behaviours" [5].

In the context of this thesis, surveillance is the continuous observation of citizens' activity to collect information about their behaviour [6] and the collection of their biometric data [7]. The intent of such surveillance is to modify behaviour and promote public safety [8]. Data collection is performed through technology, as behaviour is recorded through surveillance technologies and biometric data is collected and stored in facial recognition databases.

We will discuss the surveillance practices in the U.S., how surveillance technologies are employed by LEAs and problems associated with the use of said devices.

2.1 Video Surveillance Technologies

Video surveillance is a decades old technology. First introduced in the 1940s, its first applications ranged from education to rocket launch viewing [9]. In the decades since, grey-scale cameras supported colour, cameras communicated over an Ethernet network and also had significantly improved video resolution [9]. The video surveillance market has boomed because automated surveillance comes at a low cost and promises to improve operations [10]. Developments in video surveillance technologies eliminate the limitations that previously reduced the effectiveness of surveillance [4].

The increased level of surveillance over recent years, and thus the tremendous amounts of footage from said video surveillance, has encouraged the development of automated surveillance technologies. It has become almost impossible for all surveillance camera footage to be manually monitored, especially in areas monitored by hundreds or even thousands of cameras [10].

Today, LEAs have a variety of surveillance technologies at their disposal, and when equipped with facial recognition functionalities, these devices become very powerful investigative tools in the hands of officers.

2.1.1 Police Drones

Unmanned Aerial Vehicles (UAVs), or drones are used for aerial surveillance and allow for individuals to be tracked over considerable distances. Originally designed for military purposes, these drones have been increasingly employed in law enforcement applications [7]. Police forces have employed drones for surveillance and other use cases. For surveillance purposes, drones have been used to read license plates and track individuals [11]. Other use cases of drones include the location of stolen goods and runaways, reconstructing accident scenes, and assisting firefighters at fires [12].

Cameras give drones the power effectively perform in high-stakes applications. One such drone camera in particular has a 30x optical zoom and a 6x digital zoom for up to a total magnification of 180x [11] and is capable of seeing activity up to 6 kilometres away [13]. Military developments under the Defense Advanced Research Projects Agency have introduced the Autonomous Real-Time Ground Ubiquitous Surveillance-Imaging System (ARGUS-IS) [14]. This video surveillance technology has such a high resolution that it can "resolve details as small as six inches from an altitude of 20,000 feet" [15]. In terms of meters, this system can recognize a detail 15 centimetres in size from six kilometres away. When attached to a drone at this elevation, the ARGUS-IS is capable of seeing an area of 25 square kilometres at any one time [15].

Police drones flying in American skies contribute to the transparent society in the U.S. Their functionalities clearly break the "boundaries of … distance … and physical barriers that traditionally protected information" that Marx mentions [16]. Drones break the barrier of distance by being equipped with powerful cameras, while reducing the impact of physical barriers. Drones have the ability to fly freely around physical obstacles, however they will face a physical barrier when the surveillance target enters a building or another similar enclosure.

2.1.2 Surveillance Cameras

There are three main classifications of cameras used for public surveillance: overt, semi-covert and covert cameras [17]. Each of these classifications have their own specific design and purpose of surveillance, ranging from noticeable to secret. Overt cameras are designed to be clearly visible and their field of vision determined by the camera's direction [17]. Semi-covert cameras, just as the name describes, are more secretive than overt cameras, but are more apparent than covert cameras. These cameras have a dome-shaped housing which prevents an individual from recognizing the direction in which the camera is aimed [17]. Covert cameras are used for homeland security purposes, and are thus hidden from the wandering eye [17]. A significant characteristic of today's surveillance cameras is that they can be used to pan, tilt, and zoom. Such functionality allows the camera to have horizontal and vertical movement along with an adjustable focal length, thus drastically increasing the camera's area of coverage [18]. These functions can either be controlled by a remote operator or can be programmed using specialized software [18].

A recent expansion in police use of surveillance cameras is the introduction of so called 'blue light' cameras. Blue light cameras are highly visible devices installed for and operated by police departments, getting their namesake from the blue light they emit [19]. These cameras have been installed in cities around the country, most notably in Atlanta [19], Chicago, and Baltimore [20].

The spread of video surveillance, and the ever-increasing number of surveillance cameras installed in the U.S. contribute to the country's self-monitored society. This contribution is the most obvious, as Marx claims a self-monitored society to be one where "auto-surveillance plays a prominent role" [16]. We have already reached the point where surveillance cannot either be conducted or analysed solely by humans. Too much video footage exists to be analysed by a human reviewer, and the effective use of auto-surveillance can reduce the number of patrol officers needed [17].

2.1.3 Body-worn Cameras

A body-worn camera is a wearable audio, video and/or photographic recording system used to record events in which law enforcement officers are involved [21]. These cameras attach to an officer's uniform and document moments of police-public contact, and locations such as crime and accident scenes [22].

2.2 Problems with Surveillance Technologies

Surveillance technologies have been questioned by many. The problems found are not about the existence of these devices but rather their characteristics and implementation in society. We will mention these issues in two parts – the first being an analysis of the shortcomings of surveillance implementation and the second being a discussion about the limitations of the design of surveillance systems.

To discuss the implementation of technologies, issues lie in the decision-making and application by LEAs. Decision-making has been found problematic because agencies select and implement tools disregarding how the technology would affect their policing strategies or crime rates [23]. Research has also shown that a technology's effectiveness often plays a limited role in the decisions to either initially adopt or continue using it [23]. If law enforcement were to consider human rights when making decisions about surveillance technologies, security threats could be handled more effectively [24].

The major argument behind law enforcement's application of surveillance is that it is biased. Graham and Wood express how the implementation of digital surveillance are subject to social biases and, in turn, effects individuals in a variety of ways [25]. Digital surveillance can only perform as well as it is programmed to, or only as well as the human operating the surveillance. If bias is introduced in either the development or implementation stages of surveillance technologies, the implications of "social sorting" [26] done by said surveillance can worsen. The most significant bias in surveillance is racial bias, which is discussed below.

Surveillance conducted by U.S. law enforcement has come under fire because police departments face racial asymmetry. Racial asymmetry occurs when police departments underrepresent the community's racial minorities and are thus more likely to use surveillance technologies to monitor the 'problem' population [23]. Racial bias is the most prominent in communities where the African American population is underrepresented in police departments. Bias in communities perpetuates stereotypes linking race and crime, which encourages the idea that panoptic measures are necessary to racial minorities [23]. Stereotypes lead to a social sorting which likely labels African Americans as criminals, solely based on appearance. Increased surveillance on African

American populations contributes to the racial bias of facial recognition. We will discuss how facial recognition is racially biased in chapter 4.

The implementation of automated surveillance is questionable because it cannot perform alone in all scenarios, as they still require human operators [26]. Automating video surveillance can reduce the number of people required to monitor footage, but automation cannot replace those responders who react to what the footage shows [10]. Video surveillance technology does not yet have the reasoning capabilities of their human operator counterparts [10], so humans play a significant role in video surveillance. As long as these technologies are implemented without human supervision, surveillance is not effective.

Surveillance technologies, as mentioned before, only perform as well as they are designed. The idiom "a chain is only as strong as its weakest link" certainly applies here. A surveillance technology is only as effective or accurate as its weakest portion of code, or is "only as good as the way in which [it's] used and how well [it's] integrated" [27].

To discuss the design limitations of surveillance systems, we mention the success rate of surveillance algorithms. It is argued that the algorithms behind automated surveillance systems are not designed to work in a real-life setting [10]. Developers do not usually modify their algorithms to work in less than ideal situations in order to maintain an accuracy level worthy of publication [10]. When such surveillance algorithms are in used practice, they put many people at risk. Inefficient surveillance fails to protect the organization around which the surveillance is performed. How can we expect to identify and apprehend a suspect using low-quality surveillance footage?

2.3 Surveillance After 9/11

In a world living in the aftermath of September 11, 2001 (9/11 hereafter), the U.S. and many other countries around the world depend on surveillance for security [28]. Terrorism has plagued the planet and has met a front of surveillance and other security screenings in many facets of life. Many other attacks, deemed terroristic in nature, have occurred across the U.S. since 9/11 – most notably the Boston Marathon bombing [29]. These occurrences only strengthen the argument for increased surveillance and other security measures. With the growing emphasis on increasing security, technologies have been implemented before careful analysis has determined their implications of privacy and other fundamental rights [30].

As Lyon states, the underlying motive behind the growth of surveillance and surveillance technologies is suspicion [28]. Law enforcement is more suspicious of citizens and their actions, thus “massive systems [have been] designed to trace and track people, to monitor their behaviours, and to profile them” [28]. Undermining the citizens’ trust of “being considered innocent until proven guilty and in enjoying personal privacy and anonymity” has a significant impact on society [31]. While some are under more surveillance (i.e. persons believed to be linked with terrorist groups), everyone in the U.S. is under surveillance to prevent crimes, especially other massacres.

The phenomenon behind this shift in surveillance is known as function creep, where a technology’s use expands beyond its originally intended purpose [32]. In the context of this study, function creep occurs when security measures originally implemented to combat terrorism are used in broader applications, including criminal justice purposes [33]. Function creep of surveillance technologies is a consequence of the perpetuated fear of terroristic acts [34]. As a result, it is perceived negatively, especially in terms of its potential invasion of privacy [32]. Since the occurrences of 9/11, we have seen the use cases for counter-terrorism measures expand to catch criminals [35] which have negatively impacted Americans’ privacy.

What makes function creep significant is the belief that counter-terrorism measures only apply to the specific targets [36]. After 9/11, the response from U.S. authorities focused on noncitizens [37] which only strengthened this belief. Such a response is justified because the civil liberties of citizens are not threatened, as those of noncitizens are sacrificed [38]. We, as citizens, cannot assume that surveillance is only performed on certain demographics. In order for the few targets to be surveilled, “it is necessary for everyone to be supervised” [39].

The following subchapters describe the current state of surveillance in the U.S., the U.K. and China. They begin the conversation of what surveillance technologies are used and how their implementation with facial recognition is problematic.

2.3.1 Surveillance in the United States

Over 550 law enforcement agencies in 49 states use drones [40].[1] More than 190 of these agencies have acquired multiple drones, with the average count being 3 drones per agency [40]. Of the 49 states whose LEAs own and operate UAVs, 33 have at least ten in their arsenal of investigative tools [40]. The three states who have the most drones in use are Texas, California and Wisconsin, who own 67, 58 and 56 drones respectively [40].

Drone size is one factor of why they are a popular tool with police departments [41]. Microdrones[2] are being developed, some as small as flying insects [42]. Smaller drones are more manoeuvrable while also being less detectable [43].

As of 2017, there were 50 million surveillance cameras in operation across the country [44]. The installation of surveillance cameras are motivated by the growing number of uses in which video surveillance can be applied [45]. Cameras are now installed in police cars, jails, and even on individual law enforcement officers [45]. About half of the nation's law enforcement agencies have a body-worn camera program [46].

2.3.2 Surveillance in the United Kingdom

Richard Thomas, former Information Commissioner of the U.K., warned that the country may sleepwalk into a surveillance society back in 2004 [47]. He feared that more information would be collected and more accessible than British society would be comfortable with [47].

Police forces in the U.K. employ drones for investigative purposes, capable of real-time surveillance [48]. They are usually deployed in situations where the use of a helicopter would not be feasible [49]. The number of drones owned by police forces are considerably low compared to agencies in the U.S. For example, the Sussex and Surrey Police have one of the largest units with five drones [49]. Drones are said to be used to target criminals in public places, similar to traditional surveillance cameras [50].

As of 2013, there were approximately between 4.1 and 5.9 million surveillance cameras in the U.K. [51]. It is estimated that close to 500,000 of these cameras are in London

[1] Rhode Island is the only state whose LEAs do not use drones.

[2] The term 'microdrone' refers to a miniature UAV.

alone, who capture the average person 300 times per day [52]. The city with the second highest number of cameras is Bristol, with 658 cameras [53].

In contrast to American practice, British police wear body-worn cameras in order reduce the use force by and against police officers, as well as the complaints against officers [54]. One report found that 71 percent of surveyed police departments use body worn cameras and that British police forces own a total of nearly 48,000 cameras [55]. Owning at least 22,000 body-worn cameras, the Metropolitan Police Service (MPS) owns a significantly higher number of cameras than all other surveyed forces [55]. This is said to be the largest-scale use of police body cameras in the world [56]. Several trials were performed to determine how much these cameras effected the use of force and crime rates. The findings conclude that the use cameras had little to no effect on either, suggesting that the technology should be further tested more before being adopted [55].

There are regulations which mandate the use of police body-worn cameras in the United Kingdom. According to the College of Policing, "continuous, non-specific recording is not permitted" and that citizens must be told when they are being recorded [57].

2.3.3 Surveillance in China

China has become a surveillance state. The country has the largest video surveillance network in the world to monitor its citizens [58]. China's surveillance system performs near total surveillance, massive collection of personal data and data analysis with artificial intelligence [59]. Because Chinese law enforcement is able to freely surveil citizens, surveillance technologies will become more pervasive [60].

China has deployed over 176 million surveillance cameras around the country, and is expected to have over 600 million in use by 2020 [58]. These cameras are equipped with facial recognition technologies [58], with many capable of real-time facial recognition [61]. These cameras work to monitor citizens to "achieve both ethnic unity and social stability" [62]. Muslim ethnic minorities are targeted by surveillance, while behaviour profiles are created based on camera findings.

Aside from the millions of surveillance cameras watching the Chinese public, law enforcement in China also employs drones. Some police drones are used to monitor for traffic violations, capable of recording drivers without seatbelts or ones using their phone behind the wheel [63]. Others are meant for general surveillance purposes, such as those in the Dove programme [64]. These drones are designed to mimic the appearance and movements of real doves in the air, for the purpose of "[evading] human detection and even radar" [64]. Equipped with high-definition cameras, these drones become camouflaged "spy birds" watching the citizens below.

To address police body cameras, Chinese law enforcement are testing sunglasses with facial recognition capabilities [65]. The glasses give officers instant and more accurate feedback compared to the capabilities of surveillance cameras [65]. Officers wearing the "augmented reality" glasses are able to compare faces against the national database, in order to find suspects [66]. The use of these devices is warranted by the fact that they have helped capture suspects in major cases and many others traveling under false identities [60].

2.4 Support for Surveillance

Out of all reasons to support the growth of mass surveillance, the idea that security comes at a price and the notion of 'nothing to hide, nothing to fear' are most prominent. Both of these arguments pose security and privacy against one another, rather than suggesting the forces can work together.

According to government actors, "anyone who insists on opposing mass surveillance must be doing so not because they care about their privacy, but because they are hiding illegal behaviour" [24]. Privacy here is considered to only be useful for protecting secrets, while public safety is considered to be more valuable than any secret [24]. Authorities claim that security measures are not used to collect personal secrets, and in the case of secrets deemed illegal, they "do not deserve secrecy" [24].

This argument maintains that surveillance does not threaten privacy: although law enforcement surveillance collects data from everyone, it will only be used for crime prevention purposes [24]. Even if surveillance was to invade privacy, the government claims it is just the price needed to pay to ensure safety [24].

2.5 Panopticon Theory

In regards to the evolution of surveillance since 9/11, several scholars argue that Bentham's theories of surveillance, more specifically those surrounding his design of the Panopticon, are still relevant in society [67], [68]. Bentham himself even argued that the Panopticon could effectively extend beyond prisons and control society by other means [69].

The Panopticon is theorized to reform behaviour through the power of deterrence [70]. If surveillance is evident, in the case of the Panoptic tower or visible surveillance cameras, individuals are less likely to become involved in criminal behaviour [70]. By this theory, an individual who enters an area in range of surveillance cameras would most likely modify their actions as they are unsure if they are truly being watched [70]. Lyon states that surveillance cameras, like the panopticon, make it impossible for one to know if they are being watched [26] and lead to "the automatic functioning of power" [71]. Surveillance in public spaces aims to deter "delinquency or deviance" [67] similar to what Foucault referred to as curing the delinquent [71].

The United States is slowly moving towards the ideals of panopticism from the country's response to 9/11.[1] Instead of housing convicted criminals in circular prisons, we create prisoners in public by creating an environment where Americans are either constantly under inspection by "the eyes of the persons who should inspect them" or "conceive [themselves] to be so" [69]. Using Foucault's words, an American "is seen, but he does not see; he is the object of information" [71] as he is observed and most likely has his data stored in at least one law enforcement facial recognition database as a result.

LEAs in the U.S. have successfully created a panopticon-like environment through their employment of surveillance technologies. The number of surveillance cameras employed is enough to claim that our cities are becoming panopticons [67]. Once an individual leaves the privacy of his home, his is under near constant surveillance of cameras [72]. Just like in a panopticon, when he is under video surveillance, he is seen but he will never know when or by whom he is watched [67].

[1] The theory of panopticism was developed by Foucalt in 1977

Agencies across the country use a variety of surveillance technologies in their work to reduce crime. The devices most widely used, drones, surveillance cameras and body-worn cameras are discussed in the next chapter.

3 Facial Recognition

Surveillance has expanded to include "pervasive systems employing a wide range of technologies for manipulating social behaviour and, as a consequence, impacting social values, including especially privacy" [73]. The technologies mentioned here observe areas while an operator watches the footage seeking people who stand out or activity seeming out of place [45]. We will consider surveillance technologies to be the devices used to observe the behaviour of citizens [74].

Americans today live in a maximum security society as Marx describes [16]. He considers a maximum security society as one where the behaviour of citizens is known, thus leaving them susceptible to government control [16]. Marx defines such a society to have six features: dossier focused, actuarial, suspicious, engineered, transparent and self-monitored [16]. In the scope of facial recognition and surveillance, five of his six features, all except engineered, are prevalent in American society [16]. The deployment of surveillance and facial recognition technologies do not contribute to American society becoming engineered. They pressure people to make conscious decisions about their behaviours, but the possible choices are not limited by the environment [16].

American society is a dossier society because citizens have their data in "computerized records" [16]. In this case, records are in the form of facial data stored in facial recognition databases. An actuarial society is also prevalent, as individuals are affected by facial recognition and surveillance differently depending on their race, gender and age. This will be further discussed in the chapter 3.1.4. Suspicion exists in American society because all Americans find themselves under surveillance, as addressed in chapter 2.3. The extent to which a transparent and self-monitored society exists in the U.S. will be discussed in our analysis of video surveillance technologies.

3.1 Facial Recognition Technology

3.1.1 How Facial Recognition Works

By literal definition, face recognition is "the ability for a computer to scan, store, and recognize human faces for use in identifying people" [75]. By a technical definition, facial recognition technology records the geometry of prominent facial features [76] including, but not limited to, the ears, eyes, eyebrows, nose and mouth. In practise, this technology scans a data subject's face and uses an algorithm to determine the shape, size and relative position of their facial features. A facial signature of the data subject's face is then created from the facial geometry recorded [77]. The Association for Biometrics and International Computer Security Association define a biometric system as one with the following capabilities:

- capturing a biometric sample from an end user;
- extracting biometric data from said sample;
- comparing the biometric data sample with data in one or more reference templates;
- deciding how well the two data samples match; and
- indicating whether or not an identification has been made or an identity has been verified [78].

In this chapter, we will explain how facial recognition systems are used by LEAs. We will also discuss the standards and best practices of using facial recognition in law enforcement applications. To end the chapter, we will mention current developments in this technology, and how law enforcement will use these devices in future investigations.

3.1.2 Facial Recognition used with Surveillance

Law enforcement officers can use surveillance technologies to identify faces in video footage and compare identified faces to a facial recognition database. As Lyon states, "[a] key trend of today's surveillance is the use of searchable databases to process personal data" [26]. Facial recognition databases clearly fit the description of searchable databases capable of processing personal data. Nunn argues that the most significant element of a biometric system is the underlying database [45]. Using Lyons terminology, searchable databases give law enforcement the power to perform near real-time identity verification. As this technology improves, facial recognition systems will begin to watch over every inch of our world.

Facial recognition systems are already in use in a variety of locations, including, but not limited to, ports of entry, embassies and other large venues where crowds gather [45]. These locations are hotspots of activity and provide law enforcement large datasets to compare against facial recognition databases [45].

Facial recognition has already been used in conjunction with the deployment of the surveillance technologies discussed. Officers have used facial recognition with drones, other aircraft, and surveillance cameras on many occasions. Soon this functionality will work with body-worn cameras [79].

3.1.3 Identification Process

In the context of law enforcement use, an officer can use facial recognition to either verify a claimed identity or to identify an unknown subject [1]. While attempting to confirm a subject's identity, an officer will input a probe photo into the agency's facial recognition system. Here, the term probe refers to a data sample that is used as input for a facial recognition system and compared against its gallery, or database [80]. The probe photo can be captured by a law enforcement officer by using a camera or smartphone [81] or can be taken from high-quality video surveillance footage.

After the probe photo is submitted and comparisons are completed, the system responds with a list of photos in the database most similar to the probe photo. The people who are in the list matching results become candidates in their investigation [1]. In other words, because these faces were similar to that of the probe photo, the people will be subject to further investigation by police. This is significant because the resulting list of potential matches may, in fact, not be similar to the probe, depending on the accuracy of the facial recognition system itself. We will discuss how the accuracy of these systems affect the privacy of Americans later in this report.

3.1.4 Inaccuracy of Facial Recognition

Facial recognition algorithms have been tested for accuracy in a variety of scenarios. The results of these tests give rise to concerns regarding the privacy of the individuals whose faces are processed by these algorithms. We will discuss how algorithms have been found to be inaccurate, thus highlighting how they can negatively impact privacy.

Facial recognition technologies are inaccuracies lie in the photos in which they analyse. A facial recognition system's performance depends on the subject's appearance and other acquisition conditions [82]. Photos may be either poor quality or the subject's facial features not clearly visible, which can lead to inaccurate facial recognition search results.

Photos taken from surveillance footage are not guaranteed to have high quality necessary to effectively be run against facial recognition databases. Some images may be distorted, such as images taken from an Automated Teller Machine [81]. For other problematic photos, facial recognition software cannot always recognize the subject's facial features. In some cases, the subject's nostrils can be mistaken for their eyes, thus compromising the search [81]. In both of these scenarios, the analyst behind the search is capable of manipulating the probe photo using image enhancement tools [81]. Distorted photos can be corrected so that the subject has a normal appearance, whereas eyes can be manually added on photos to maintain the search's integrity [81]. In summation, unless the probe photo is taken under very similar conditions as that of the database's photos, the chances of an accurate identification are decreased [26].

Facial recognition systems are also inaccurate based on the age, race and gender of subjects. One study conducted on facial recognition algorithms participating the Face Recognition Vendor Test 2006 highlights that algorithms do not treat all races equally. The study analysed how well algorithms developed in East Asian and Western countries were able to identify East Asian and Caucasian faces [83]. More specifically, tests were conducted to determine whether the geographic origin of the algorithm, or the geographic location of where the algorithm was developed, affects the algorithm's accuracy [83]. The results of this study do, in fact, prove that the geographic origin of an algorithm affects its accuracy rate when identifying faces. The algorithms developed in East Asian countries were found to be more accurate in identifying East Asian faces, while the algorithms originating from Western countries more accurately identified Caucasian faces [83]. Such a phenomenon is known as the 'other-race effect', when an individual is more likely to misidentify a person of another race rather than a person of their own race [84].

Other commercial algorithms have been tested for accuracy, such as Amazon's Rekognition, after claims that it is capable of "real-time face recognition across tens of millions of faces; and detection of up to 100 faces in challenging crowded photos" [85]. Tests have found that Rekognition has both gender and racial bias, both in terms of racial and gender classification and facial recognition. Rekognition was shown to perform with the lowest accuracy when classifying photos of darker and female faces [86]. In terms of identifying faces, Rekognition incorrectly identified 28 members of Congress as individuals in a set of 25,000 mug shots [87].

Another study, which used commercial, non-trainable and trainable algorithms, tested the algorithms' accuracy based on the race, gender and age group of the faces identified [88]. Every algorithm used in this study had the lowest accuracy when identifying African American faces, females and in young people between the ages of 18 and 30 [88].

Arrest rates and other Department of Transportation statistics in the U.S. show how many Americans in these underserved demographics are likely enrolled in facial recognition databases. Between 2004 and 2014, individuals between 18 and 29 years olds were arrested most frequently (62.7 million total arrested) among all age groups with an average of over 5.7 million people per year [89].[1] During this same time period, 30.4 million women were arrested, an average of over 2.7 million per year [89]. Lastly, over 34 million African Americans were arrested over this time span, coming to over 3.1 million per year [89]. In 2017, there were close to 23.5 million licensed young male drivers (ages 29 and younger), while there were approximately 23 million licensed young female drivers [90]. Including the total of 114 million female drivers across the country [90], we can conclude that there are tens of millions of individuals in critical demographics enrolled in facial recognition databases, whether they were enrolled from a mug shot or a Department of Motor Vehicles (DMV) photograph.

Just as humans are needed to ensure the accuracy and performance of surveillance technologies, an analyst is also needed to work in tandem with facial recognition systems [81]. Rodriguez claims that analysts must "manually analyse images", which is critical to the identification process [81]. The identification process should never be fully automated, especially because the impact of a false identification can be life-changing.

Having a human reviewer is important for this process because a person is able to see similarities or differences between the probe and gallery that go unnoticed by the system. For example, a human reviewer could outperform a facial recognition system when comparing images that have a large age discrepancy. Automated systems are less accurate in this scenario [91], whereas a human reviewer could accurately identify the subject. To ensure that human reviewers help solve a system's accuracy problems, they must be

[1] All numbers calculated for age group statistics were based on data on individuals aged 18-29, as the range 18-30 years old could not be calculated without including erroneous data

properly trained. Without training, a human could actually perform worse than an algorithm [91].

3.2 Standardizing Facial Recognition Technology

The accuracy of facial recognition systems greatly depends on the quality of the images they use [81]. Standards and best practices for these systems are created to ensure a high level of accuracy during deployment. A best practice is a procedure that have been proven to produce optimal results [92]. In this context, a best practice would be an optimized procedure in the process of identity verification. We discuss standards set for facial recognition systems in part one and best practices for using these systems in part two.

3.2.1 Standards for Facial Recognition Systems

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) have published standards for all biometric systems, ranging from fingerprint to vascular image data in the ISO/IEC 19794 series [93]. We will briefly discuss ISO/IEC 19794-5 which specifies constraints for images used in face recognition applications [94].

ISO/IEC 19794-5 categorizes requirements based on scene, photographic, digital and format specifications [95]. Scene requirements state that the subject should have a neutral facial expression while their head must not be rotated more than five degrees in any direction, all while being in front of a plain background [95]. Stretched photos are not allowed under ISO/IEC 19794-5 as images must have a pixel ratio of 1:1 [95]. Regarding image resolution, facial photos are required to have a minimum width of 240 pixels, whereas a width of 480 pixels is recommended [95].

3.3 Future Developments

New facial recognition technologies are under development to meet the ever-growing need of in-the-go facial identification. Some of the developments expected to hit the market within the next few years include real-time facial recognition, behaviour tracking and crowd control.

Real-time facial recognition is a significant future development because of how many companies wish to implement it. Algorithms capable of real-time facial recognition accept a continuous video stream, and can detect or track faces before identifying the face [96]. Law enforcement agencies in the U.S., including Los Angeles, Chicago and Dallas have either claimed to currently use real-time facial recognition or expressed interest in purchasing tools to implement it [1]. Axon, the largest supplier of police body cameras in the U.S., is developing cameras capable of recognizing faces in captured video [97]. The company's Artificial Intelligence Ethics Board has already faced concerns from dozens of organizations regarding the ethics behind live video captured by body cameras [97].

Behaviour tracking, or behavioural biometrics, measure the characteristics or behaviour patterns of an individual rather than physical traits [45]. Examples of behavioural traits measured include voice patterns [45] and gait [98]. Some behavioural biometric systems use network software to monitor public spaces and find criminal behaviour [45]. These systems record normal behaviour and use them to predict the movements of subjects within view of the camera [45]. When any abnormal behaviour is detected, authorities are automatically notified [45].

3.4 Facial Recognition Implementation

3.4.1 Facial Recognition in the United States

Over 117 million Americans in 26 states, or close to 1 in 2 American adults nationwide, [1] have their data in facial recognition databases [99]. These databases include photos such as mug shots, driver's license and identification card photos [1]. A mug shot, a term coined from 18th century slang [100], is a photograph taken by police of a person's face and profile for police records [101]. Driver's license and identification card photos are the photographs taken for creating the identification documents in the DMV office. In other words, facial recognition databases hold photos taken for both criminal justice and other identification purposes. This, in turn, means that the data subjects in facial recognition databases include law-abiding individuals [1].[1]

[1] *Law-abiding Americans:* Term coined by the authors of this study, implicitly defined as Americans with no criminal record

A records request was sent to 135 municipal and state level law enforcement agencies across the country, and more than 43 of those agencies responded claiming to either currently use or have previously acquired facial recognition technology [1]. Of the states whose agencies use facial recognition, many have their own systems. These include the previously mentioned MIRS used in Maryland, as well as Justice Network Facial Recognition System in Pennsylvania, and the Face Analysis Comparison and Examination System (FACES) in Florida [1].

There are a few municipal agencies across the U.S. that have prominent facial recognition systems, including the San Francisco Police Department, Maricopa County Sheriff's Office in Arizona, and the Albuquerque Police Department (APD) [1]. Between these three systems alone, over 18 million photos can be accessed [1].

Facial recognition is employed by United States federal agencies as well. The Federal Bureau of Investigation (FBI) has its own facial recognition system, called the Next Generation Identification system (NGI), having a photo repository called the Interstate Photo System (IPS) [102]. This system allows law enforcement officers to conduct facial recognition searches against over 30 million mug shots [102]. The FBI can run face recognition searches against driver's license photos from at least 16 states [1].

3.4.2 Facial Recognition in the United Kingdom

We chose to compare the United Kingdom's law enforcement agencies' use of facial recognition technology to that of the United States to understand the European ideals of security and privacy. Although the U.K. is not the ideal role model considering surveillance and facial recognition, the country provides suitable regulations that should serve as a model to frame American regulations.

Facial recognition has become a very popular tool for British police forces. It is even said that police in the U.K. "have rolled out automatic facial recognition at a pace unlike any other democratic nation in the world" [103]. One study surveyed 50 polices forces in the U.K. to find more information about how their implementation of facial recognition systems impacts citizens' privacy.

The Police National Database holds at least 23 million mug shot photos, where at least 10 million can be used in facial recognition searches [104]. Facial recognition systems used by British police forces are capable of real-time recognition from video feed and identifying faces in large crowds.

3.4.3 Facial Recognition in China

We chose to compare the Chinese law enforcement agencies' use of facial recognition technology to that of the United States because China has become infamous for their surveillance. It has been said that China is a surveillance state and has become a digital panopticon [105]. China serves as an example of how intrusive surveillance and facial recognition can be when left unregulated.

Facial recognition is used to identify citizens in surveillance footage, who then have data collected about their whereabouts, behaviour, and other financial and commercial transactions [106]. In other words, Chinese authorities collect "store massive amounts of data on everyone they can identify regardless of their target's criminal status" [58].

Because Chinese streets are dotted with surveillance cameras having facial recognition technology, a suspect can be located within seven minutes [58]. China reportedly wants to be able to identify any citizen within seconds and is currently compiling a database to reach that goal [58].

4 Privacy

It is imperative to define what it means to have privacy to understand how it is threatened by facial recognition technology. As Kasper expresses, the concept of privacy is difficult to define in American society [107]. The legal definition of privacy, or what it means to have the right to privacy has evolved throughout history.

In 1890, Warren and Brandeis defined the right to privacy as the right to "be let alone" and stressed that this was essential because invading a man's privacy "subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury" [108]. While the ACLU of Florida suggests that this right to be let alone is widely accepted today [109], the meaning of privacy has evolved from Warren and Brandeis' time. The need for privacy has expanded beyond the physical body and applies to theoretical aspects of a person, such as the right to informational privacy [107]. Some suggest that the right to be let alone cannot be related to data protection, as keeping information private does not connect to "the right to be without company" [110]. The outdated values of privacy struggle to compare to current methods of security [111].

The literal definition of privacy is effective in explaining what exactly privacy advocates wish to be granted, which is the "freedom from damaging publicity . . . secret surveillance, or unauthorized disclosure of one's personal data or information, as by a government" [112]. We can presume that the ACLU would agree with this definition and argue for the government to better protect this freedom. People wish to have more privacy, specifically to keep their facial data from being stored in databases that are accessible by law enforcement officers.

4.1 Privacy in Surveillance

Although surveillance technologies can be beneficial in assisting law enforcement officers solve crimes, the act of surveillance itself impacts the privacy of the citizens being surveilled [113],[114]. Surveillance poses a threat to society because of its ubiquity, intensity and use of personally identifiable information [114]. As Lyon states, "[it] is no accident that interest in privacy has grown by leaps and bounds in the past decade" suggesting that this shift is caused by increased surveillance [26]. In this section, we will illustrate how police surveillance has impacted the privacy of Americans.

Kasper creates a typology of privacy invasions, defining types of invasion and their specific characteristics [107]. She claims that observation, or surveillance in general, invades privacy because individuals are unaware that they are being watched [107]. Kasper is also against surveillance technologies, as she states that the mere "presence of surveillance cameras" invades privacy [107].

In his discussion about privacy, Alan Westin mentioned several states of privacy [115]. We will only consider the states relevant to our argument, which are solitude and anonymity. When in the state of solitude, Westin claims an individual is free from the observation of other persons, although he may believe or fear that he is secretly being watched by some authority [115]. The state of anonymity is more specific to the individual's whereabouts, as he can be in a public place but is free from identification and surveillance [115].

Applying these definitions to the context of facial recognition, an individual cannot guarantee that he can maintain either of these states of privacy once his photo is entered into a facial recognition database. His photo can and will be compared against probe photos in the system without his knowledge or consent. Otherwise, he must work to maintain his privacy from any surveillance cameras he might walk past in his daily life, an impossible task for one living in a contemporary city [67]. He can only have solitude when he is freed from the observation of these cameras, since his face could be extracted from this footage. To guarantee this state of privacy, the individual would not allow himself outside of his home, as it is impossible for him know the exact location and range of the cameras in his area. To ensure his anonymity in public places, he could turn to radical actions and disguise himself or otherwise cover his face enough to be unrecognizable by the surveillance cameras recording his actions [114]. In short, an individual would have to drastically change his lifestyle and habits to ensure his face cannot be extracted from surveillance camera footage and compared against facial recognition databases.

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, is a legislative example of privacy reduction in the United States. The Act provided law enforcement with more access to investigative tools to fight terrorism [116]. Considering function creep, this Act also gave law enforcement access to tools for the purpose of fighting domestic crime. Challenging the government's use of surveillance technologies for either of these purposes will be a difficult task [117].

4.1.1 Privacy and Aerial Surveillance

The impact that aerial surveillance, and thus police drones, have on privacy is rather serious. Police departments can deploy these drones to watch activity occurring miles away. We will briefly discuss the implications that the general use of aerial surveillance has on the privacy of citizens. Real-life examples of U.S. law enforcement aerial surveillance systems invading privacy will be brought forward.

A major implication of using cameras is that an individual or group of people can be unknowingly watched by a police-operated UAV. Laperruque suggests that these devices could watch an individual from their own yard, or even through a window without being noticed [14]. Microdrones can go unnoticed while conducting surveillance near ground-level, while systems performing at high elevations (such as the ARGUS-IS) is most likely near invisible from the ground.

Drones are more inconspicuous compared to police helicopters and allow for automatic tracking of individuals [11]. With said tracking functionality, drones can lock onto and follow a target at speeds of up to 32 kilometres per hour – all without the need of human intervention [11]. Aerial surveillance can identify an individual target, where either their past, current or future actions can be tracked [118].

To name a few, police departments in New York, California and Maryland have faced controversy because of their implementation of drones and other aerial surveillance programs.

In New York state, the New York Police Department (NYPD) recently acquired 14 drones [119]. The New York Civil Liberties Union fears that these drones may be used to spy on protestors [41], while police officials claim the drones will be used for crowd control and other investigative means [120]. The NYPD has expressed that the drones will not be used for surveillance purposes, but the department's drone policy ambiguities may allow for officers to misuse their drones [120]. Fear of the NYPD's possible drone misuse is amplified by the fact that the department has been found guilty of running an unlawful surveillance program in the past.[1] The NYPD's policy does forbid their drones from being equipped with facial recognition technology, but facial recognition can later be used on footage captured by drone cameras [41].

Los Angeles County Sheriff's Department allowed Ross McNutt's company, Persistent Surveillance Systems, to test aerial surveillance technologies in 2012 [118]. Citizens, nor the mayor knew that the tests were occurring [118].

During city-wide protests in Baltimore, Maryland, the Baltimore Police Department conducted aerial surveillance over the entire city and scanned protestors' faces with facial recognition technology [121]. Surveillance was conducted by the FBI and Persistent Surveillance [118]. The FBI's surveillance was focusing on specific targets while Persistent Surveillance Systems used wide-area motion imaging techniques [118].

Referring to his own technology, McNutt believes aerial surveillance is most effective when "used in a transparent, publicly acknowledged manner" [118]. This suggests that surveillance can be employed in a way that increases its efficacy and minimizes its impact on privacy.

Aerial surveillance is leading to an "air panopticon"[2] [14] as citizens can be unknowingly observed at any time [118]. Soon LEAs will have access to powerful equipment similar to the ARGUS-IS, leading to surveillance with both a wide field of view and great precision [14]. In order to keep our skies clear, restrictions should be placed on law enforcement and their use of drones.

Aerial surveillance technology has already developed beyond legislation and privacy is harmed as a result [14]. Laperruque and Janovsky say that limits placed on law enforcement's drone use, and on aerial surveillance in general, is a necessary first step in addressing privacy concerns [11].

[1] The NYPD's religious profiling program against Muslims was found unconstitutional inn Raza v. City of N.Y. 998 F. Supp. 2d 70 (E.D.N.Y. 2013).

[2] The term "air panopticon" was coined by Jake Laperruque.

4.1.2 Privacy and Surveillance Cameras

The ACLU's stance on surveillance cameras in that it is "particularly troubling in a democratic society" [122]. The organization believes that having cameras at locations deemed to be potential terrorist targets is reasonable, while "blanketing" our public spaces with surveillance is unacceptable, specifically giving four reasons why [122]. The ACLU argues against video surveillance because it is not effective, is susceptible to abuse, lacks restrictions and has a chilling effect on public life [122].

The most significant of these points is the susceptibility to abuse and the lack of restrictions on camera use. Police databases have been abused by officers since as early as 1997 [123]. Many officers use police databases to search for specific targets, like Leonel Marines did under the Bradenton Police Department in Florida [124]. Marines used the Driver and Vehicle Information Database to target at least 150 women, to then use social media, phone call or personal visits to get the women to date him [124]. Between 2013 and 2015, over 300 officers and law enforcement employees were either fired, suspended or resigned for misusing databases [125]. In over 250 other cases, the culprit faced lesser disciplinary actions [125]. To discuss camera restrictions, the ACLU claims that the U.S. needs laws "to limit privacy invasions and protect against abuse of [camera] systems" [122]. The organization believes these surveillance systems must be subject to checks and balances, but because technology progresses rapidly, said checks and balances do not exist [122].

Norris warns that coupling surveillance cameras with databases increases the surveillance system's panoptic power [126]. By extracting images from camera footage, and associating the subjects to a database of identified individuals, no one is anonymous [126]. Furthermore, any person captured in footage can be classified based on whether they are law-abiding, suspicious or wanted based in information in the database [126].

4.1.3 Privacy and Body Cameras

The impact that police body cameras is less than that of drones or surveillance cameras, but is significant, nonetheless. Police departments equip officers with these cameras to record their first-hand experience with citizens. The implications that these devices have on citizens is discussed alongside situations where these cameras impeded privacy.

Police body cameras are intended to increase the level of transparency of officers' behaviour by serving as reliable evidence of interactions between officers and citizens [127]. After identifying bad behaviour, body-worn cameras are hoped to deter officers from misusing forceful, violent, and discriminatory behaviour [127]. In the U.S., police departments deploy body cameras for reasons such as strengthening officer accountability, investigating officer-involved incidents and reducing officers' racial profiling [128].

Privacy implications surrounding the use of body cameras involve the departments' use policies, whether citizens must be informed of video recording, and who has access to camera footage [127]. Some police departments have published their body camera use policies while others either refuse to publish their policies or have not created one [129]. Depending on the department in question, officers also may not be required to inform individuals that their camera is recording, or otherwise ask for permission to record others [127]. Under the Freedom of Information Act (FOIA), police body camera footage can be considered public record [127]. Each state has its own FOIA determining whether body camera footage captured in their jurisdiction is accessible to the public – these laws greatly vary from state to state [130]. For example, South Carolina has exempted police body camera footage from public disclosure [130] while New Hampshire considers footage exempt unless it contains police use of force or the discharge of a firearm [131]. The ACLU suggests that police departments should allow video involving use of force or other misconduct to be publicly disclosed [127].

In an interview, Jay Stanley, the Senior Policy Analyst of the ACLU gives other aspects of the organization's stance on police body cameras. He states that the ACLU supports the use of body-worn cameras as long as they operate under an effective policy that has privacy protections in place. Regarding facial recognition, the ACLU does not want body cameras to use it while watching and collecting information on the public. Stanley says that the biggest issue surrounding cameras is whether they will be used in a manner that increases public trust in officers. He specifically states that public trust, the need for privacy and law enforcement interests can be balanced through proper policies.

Apart from the previously mentioned ways that body cameras can intrude privacy, the possibility of officers manipulating video footage also poses a threat. If not monitored, officers could decide when to begin, pause or stop recording [132]. When officers manipulate their body camera footage, it undermines the camera's purpose of detecting police misconduct [133].

Officers in several departments across the country have been found manipulating their body camera footage. In 2012, officers of the Oakland Police Department in California were accused of misconduct after their body cameras were purposely turned off during protests [134]. Officers had turned off their cameras while arresting protestors, while the Oakland Police Department's policy states that officer's must have their cameras on while making arrests [134]. In 2018, an officer of the Baltimore Police Department, Richard Pinheiro, was found guilty of misconduct because he used his body camera to re-create evidence [135]. The footage included the discovery of pills that belonged to a suspect, who was then arrested [135]. This person was released from jail and had their charges dropped, along with the charges in over one hundred other cases involving Pinheiro and other officers [135].

Officer manipulation of body camera footage can lead to unseen occurrences of police violence and wrongful arrests of citizens. To lessen the probability of either happening, proper oversight must be done within police departments. Officers need to follow protocol and should be held accountable for their actions.

4.2 Constitutional Implications of Facial Recognition and Surveillance

The United States Constitution has come into question on numerous occasions to determine the legality of video surveillance. The main argument lies on whether surveillance intrudes upon the rights given in the first and fourth amendments.

4.2.1 Supporting Surveillance

While there are many arguments to limit the use of video surveillance, supporters of surveillance claim that cameras do not invade privacy. Specifically, Nieto points out that cameras are essentially "mechanical police [officers]" that "[record] events occurring in public space for which individuals do not have reasonable expectations of privacy" [136]. An example is brought, that an individual walking in public cannot reasonably expect that their activity is hidden from the public eye or police observation [136]. To bring a relevant court case, Laird v. Tatum was dismissed in 1972 because of a lack of evidence proving that surveillance systems chilled First Amendment rights [137].

A continuation of this argument mentions the Fourth Amendment implications of video surveillance. The U.S. Supreme Court case United States vs. Knotts held that a person travelling in public has no reasonable expectation of privacy, as they voluntarily convey their actions to anyone willing to look [138]. United States vs. Taketa asserted that videotaping in public places does not violate a reasonable expectation of privacy nor the fourth amendment [139]. For these reasons, it has been said that the Fourth Amendment will not provide protection against video surveillance [140].

To sum these arguments together, Americans have the right to be free from illegal searches, but the government has no constitutional duty to preserve an individual's private space [141]. For these reasons, it is very unlikely that an individual will successfully bring an argument about video surveillance intruding privacy to the United States Supreme Court [140].

4.2.2 Surveillance Impeding Constitutional Rights

The most widely discussed topic regarding facial recognition surveillance and the constitution is the impact on First Amendment-protected activities [142]. Surveillance without judicial authorization could be used to catalogue citizens based on their activities [142]. We have already seen facial recognition used during protests, but cameras could be used to identify people who enter places of worship [142]. Another fear is that the government could build profiles on citizens based on their activities, which could be used to take selective action against minorities [142]. Such an abuse is warranted given the history of U.S. government surveillance targeting minority populations [142].

The chilling effect of video surveillance threatens first amendment rights [136] by making citizens afraid to exercise their rights [142]. Since facial recognition does not require the subject to either give consent or be notified, the technology's ability to chill first amendment-protected activities is significantly increased [142]. Former House Oversight Committee Chair Jason Chaffetz recognizes that facial recognition "can be used in a way that chills free speech and free association by targeting people attending certain political meetings, protests, churches" or other public places [143].

4.3 Privacy Concerns with Facial Recognition

Privacy is affected when surveillance technologies are combined with "people-finding tools" such as facial recognition systems [67]. Much like fingerprint biometrics, facial recognition is a form of biometric identification using information that is difficult to change without drastic measures [144]. Because it is a daunting task to opt out of facial recognition [144], it should be used in a manner that "maximizes the advantages that such technology [brings] us" while also applying basic privacy principles during their use [145].

One privacy implication of facial recognition systems is that they are usually not used in a manner that allow incorrect identifications to be challenged or otherwise mitigated [144]. Without oversight or other accountability measures in place, problematic automated decisions cannot be discovered [144]. Issues are only realized through a pattern of discrimination, after all harm has been done [144]

The use of facial recognition technology, regardless of its intended purpose, has faced public scrutiny over the fact that it is inaccurate and racially biased. Specific facial recognition systems currently in use by U.S. law enforcement agencies have also been criticized because of their accuracy and other privacy implications.

4.3.1 Concerns Regarding the FBI

The FBI's facial recognition capabilities have been studied by the United States Government Accountability Office (GAO), and the results were that the system does not follow all recommended guidelines to protect the privacy of American citizens. Not only does the FBI have access to tens of millions of non-criminal photos, it's use of facial recognition is not transparent and its system has not been properly tested for accuracy.

The FBI has access to millions of non-criminal photographs, such as the United States Department of State's Visa and Passport databases, aside from the DMV photos [91]. The organization has expressed interest in expanding its use of non-criminal photographs, including to track people's movements to and from "critical events" and identify subjects in public datasets [146]. It's interest suggests that the FBI could identify faces in crowds and in pictures posted on social media platforms, even if the persons identified are not suspects [91].

The GAO was asked to review the FBI's use of facial recognition and found that the NGI-IPS system underwent limited tests to evaluate the system's accuracy [147]. The GAO audited this system in order to "ensure better privacy and accuracy, especially given how sensitive [it] is" [148].

The detection rate, when the NGI-IPS returns a person's match within a candidate list of 50 potential matches, is at least 85 percent [147], meaning an innocent person may become a suspect of a crime about 15 percent of the time. However, there have been no tests conducted evaluating the system's accuracy when given requests of candidate lists fewer than 50 photos [147]. The false positive rate, or how frequently the system erroneously matches a person to the database, of the system has also not been assessed, because "the results are not intended to serve as positive identifications" [147]. These metrics have a significant impact on privacy, as such a low detection rate suggests that an individual may not be matched up to 15 percent of the time. The number of false matches not only mark innocent people as suspects, but it also takes up the time and resources of law enforcement agencies who use this tool. If the FBI further tests the NGI-IPS in the future, it will protect the privacy of U.S. citizens enrolled in the database [147].

Apart from the FBI's NGI-IPS, external systems used by the agency's Facial Analysis, Comparison, and Evaluation Services Unit are also not tested for accuracy [147]. Such external systems include the several states who have facial recognition systems and have entered a memorandum of understanding and share system access with the FBI. The main arguments for this are because "their external partners are responsible for ensuring the accuracy of their own face recognition systems" and "accuracy requirements for criminal investigative purposes may be different" [147]. The FBI should test the accuracy for not only its own facial recognition system, but the external systems it uses. It has been seen that some states have not properly tested or audited their own systems, so the FBI essentially uses facial recognition systems that are not proven to work effectively.

The NGI-IPS also faces an accuracy problem based on its size. A facial recognition system performs with lower accuracy as the number of images in its database increases [91]. Holding at least 50 million searchable facial images [149], it is evident that the NGI-IPS faces such an obstacle.

The FBI has passed a final rule to have the NGI system exempt from certain provisions of the Privacy Act of 1974 [150], a process which is allowed by the Act [147]. The Privacy Act provides citizens or lawful permanent residents the right of access to federal agency records in which they are subject, unless said records are protected by an exemption [151]. The NGI system is exempt from making records available to a data subject on the grounds that the disclosure would "reveal investigative interest by the FBI" and "provide the record subject with the opportunity to evade or impede the investigation" [150]. This exemption reduces the level of transparency the FBI has with the American public, not to mention that it limits the privacy of Americans.

4.3.2 Concerns Regarding State and Municipal Law Enforcement Agencies

Of the state and municipal level LEAs with their own facial recognition systems, many impact citizens' privacy. The variety of ways that these systems impact privacy, such as the lack of transparency and oversight, access restrictions and database updates, will be examined in this subchapter. We will discuss privacy implications in two parts: the first being how the database photos impact privacy, whereas the second part discusses how the LEAs' use of their respective systems impacts the privacy of its subjects.

The photos stored within state and municipal databases misrepresent minority populations, are not compliant with international standards and are not properly updated. As mentioned before, facial recognition algorithms perform with lower accuracy when identifying faces with darker complexions. Several databases do nothing to help solve this problem, as many include a disproportionate number of photos portraying African Americans. To mention a few, this occurs in agencies' systems in Minnesota, Maryland, Virginia and San Diego [1]. African Americans are overrepresented the most in the Minnesota Repository of Arrest Photos, because they arrested at a staggering 354 percent higher rate than other demographics in the state [1]. Another significant way that these facial recognition databases impact Americans' privacy is that photos are not removed from mug shot databases when necessary. Mug shots should be removed from databases when the subject is found to be innocent, or when their charges are dropped [1]. Responding to a records request, Virginia State Police claims that the state's mug shots are retained indefinitely, while it is unclear if other states, remove photos of the innocent [1].

Not all photos in law enforcement databases are ISO/IEC 19794-5 compliant. Law enforcement agencies are not required to follow these standards since they are not legally binding [152]. However, these standards are referred to as an example of good practice [152]. Under the Code of Federal Regulations Title 6 (6 CFR § 37.17), states are required to follow ISO/IEC 19794-5 for Real ID driver's license photos[1] [153]. Currently, eight states are listed as Real ID non-compliant or are currently under review for compliance [154], which means that a majority of DMV photos are ISO/IEC 19794-5 compliant. Mug shot photos are not compliant to this regulation, however, so citizens could be misidentified by state or municipal facial recognition systems because of these photos.

Agencies' use of their facial recognition systems impact citizens' privacy because of poor oversight and restrictions. Poor oversight involves the lack of policy creation and system auditing. Maryland's MIRS is a prime example of poor system auditing, as it has not been audited during its years of operation [1]. Other systems that have not been audited for misuse are the Pinellas County Sheriff's Office's FACES system in Florida and the Nebraska DMV system [1]. Many states either do not have facial recognition system use policies or have not made their policies public, which brings about transparency problems. For example, Nebraska State Police has claimed that they do not have use policies for their access to the Nebraska DMV system while the APD procedural order has not been made public [1].

The lack of proper department policies for these systems has led to unnecessary access rights and possible misuse. Several states have systems susceptible to this threat, including but not limited to, Ohio, Florida, Pennsylvania and Maryland [1]. Over 9000 people have access to these facial recognition systems alone [1]. Because law enforcement agencies have not yet placed limits on which crimes facial recognition can be used to investigate, police officers can use this technology to arrest-at-will [142]. Having an arrest-at-will authority means an officer could conduct a facial recognition scan and arrest any individual found to have an open warrant [142]. If used to scan large crowds, police could engage in mass arrests [142].

[1] Real ID driver's licenses are issued under compliance of the Real ID Act of 2005.

Aside from departmental policies, little legislation exists that provides restrictions or standards regarding law enforcement's use of facial recognition [144]. Out of the few states that have considered regulating biometrics, the most notable law is Illinois's Biometric Information Privacy Act, which creates guidelines surrounding the process of collecting biometric data [155]. Although the Act does not explicitly state regulations for facial recognition systems [155], its mandates are being applied to the collection of facial data from surveillance technologies [144].

To continue the discussion about LEAs implementation of facial recognition, two agencies have become well known for their use Rekognition: the Washington County Sheriff's Office in Oregon and the Orlando Police Department in Florida.

The Washington County Sheriff's Office became the first LEA in the U.S. to use Rekognition in 2017 [156]. The system has been used to compare probe photos with a database of over 300,000 mug shots dating back to 2001 and is growing by approximately 19,000 photos per year [156]. However, it was discovered that officers were using Rekognition in troubling situations, such as identifying police sketches [157]. Using police sketches as a probe photo can lead to more false identifications [157], likely marking innocent people as suspects. The Sheriff's Office uses Rekognition to solve a variety of crimes, but a majority of these cases are misdemeanours, and involve situations where the system was not needed to perform an identification [158]. The Washington County police believe that facial recognition should be utilized in a responsible manner [158], so they have created and published a facial recognition use policy [159]. The policy is thorough, outlining acceptable use cases, periodic system audits and penalties for system misuse [159].

The Orlando Police Department is currently testing its second pilot of Amazon's Rekognition [160]. The original trial occurred between December 2017 and June 2018, ending after public criticism and feedback from the ACLU of Florida [161]. The second pilot began in October 2018 and is expected to last nine months [160]. Orlando police uses Rekognition to compare crime scene photos with mug shots, as well as performing real-time recognition in surveillance camera feed [162]. The few cameras using this technology can notify police if a "person of interest" is found, and are capable of recreating the suspect's earlier movements [162]. The current pilot is not being used for investigative purposes and will only track Orlando officers who have volunteering to take part [160].

Law enforcement's use of Rekognition has sparked public criticism, stemming from the ACLU and Amazon itself. Last year, the ACLU has demanded that Amazon stop allowing the government to use Rekognition [163]. The organization also raised concerns with Amazon's push to have LEAs use Rekognition with body-worn cameras, which prompted Amazon to stop promoting this use [163]. Inside of Amazon, over 450 employees signed a letter to Jeff Bezos and other executives, stating their demand to stop selling Rekognition to "police departments around the country" [164]. Another significant demand was to create a system of employee oversight for considering ethical decisions [164]. Amazon responded to employees stating that the company will continue to sell Rekognition to LEAs because they feel "really strongly about the value that [Rekognition] is providing [their] customers" [165]. Continuing to push the widescale use of an inaccurate facial recognition system, and refusing further algorithm testing [165], Amazon's privacy battle is not likely to end in the near future.

4.3.3 Concerns in the United Kingdom

Privacy concerns on facial recognition in the U.K. stem from poor accuracy, social biases and the unnecessary retention of mug shot photos. Each of these concerns are discussed in this subchapter.

Regarding system accuracy, the study found that, on average, 95 percent of face matches were incorrect [103]. The Metropolitan Police's system was said to have a 98 percent false positive rate [166]. Apart from having such a high false positive rate, the system has only correctly identified two individuals, and neither were criminals [166]. In South Wales, deployed facial recognition on the crowds at the Union of European Football Associations Champions League final in 2017, which produced over 2,400 potential matches [167]. It turns out that about 92 percent of these matches were false positives [167]. The South Wales Police claims that the rate of false positives was due to the low quality image provided, adding that no one has been arrested after being incorrectly matched [167]. Addressing concerns, the police force also stated that it does not take the use of facial recognition technology lightly and that it is working to make sure their system is accurate [167].

British facial recognition systems are also susceptible to racial and other demographic biases. In the case of real-time recognition, faces are compared to ‘watch list’, however many people on the list have mental health issues [166]. The fact that the police had not consulted with mental health professionals about the individuals in the list threatens the rights of this demographic [166]. British systems are also subject to having racial bias, where any disproportionate numbers of identifications will not be recorded based on race, therefore leaving the systems unaccountable [166]. Some systems in use by British police have not been tested for racial biases [103].

Much like in the U.S., the risks of facial recognition posed by British police databases exist. People who have old or minor convictions, or have been arrested but not convicted find themselves at risk of being profiled by facial recognition and surveillance [168]. The Police National Database holds–hundreds of thousands are images of innocent people [169]. It could be at least years before images of the convicted can be separated from those who were not convicted [104] because there is no simple process of finding and removing the images of innocent persons from databases [103]. During the six-year period of photo retention, all people in the database – convicted or not – can apply to have their images removed [104].

4.3.4 Concerns in China

Surveillance technologies and facial recognition impede the privacy and freedoms of Chinese citizens in several ways. Not only is their national surveillance racially biased, it is used to control citizens’ behaviours and makes China a true panopticon.

Surveillance is being used to monitor and intimidate ethnic minorities, such as the Muslim Uighur population in western China [58]. The Chinese government claims such security measures are necessary to neutralize the threat of violence posed by Uighur militants [62]. Surveillance cameras are said to seek out Uighurs based on their appearance, and then track their travels [170]. Hundreds of thousands of Uighurs have also been placed into re-education camps [170] for offences as minor as using Western social media applications [62].

The Chinese government has successfully created an infrastructure for social control with the deployment of its Social Credit System (SCS). The SCS is meant to monitor an individual’s activities and assign them a computational score, which is then used to determine whether that individual deserves benefits or punishments [106]. The purpose of this system is to bring about a more trustworthy country [171]. Those deemed ‘untrustworthy’ are placed in the List of Dishonest Persons Subject to Enforcement, including the reasoning for their demerit [171]. This list contains the names of over 7 million citizens [171].

An example punishment passed down from having a low credit system score is the revocation of travel rights [172]. Citizens could lose the privilege to travel on planes or trains up to one year if found to have “committed misdeeds” [173]. Aside from being used to pass down punishment, the SCS is used for public humiliation. For example, surveillance cameras in Jinan identify jaywalkers and humiliate offenders by showing their photo, home address and personal identification number on a nearby screen [58].

5 Conclusion

The analysis of American law enforcement's implementation of facial recognition and the comparison of British methods call attention to where American methods need to be improved. The most critical improvements address the accountability, transparency and accuracy of agencies' facial recognition systems. Such improvements must be made before it becomes impossible to alleviate the impact that surveillance and facial recognition technology has had on American privacy [140].

5.1 Addressing Accountability

The United Kingdom provides a great example of how police technologies are accountable, as there are governing bodies in place to oversee British police forces. The Surveillance Camera Commissioner (SCC) oversees the police's use of body-worn cameras and encourages compliance with the Surveillance Camera Code of Practice, while the Information Commissioner's Office (ICO) regulates processing of personal data obtained by surveillance systems [55]. This code of conduct also makes police accountable for their actions, as they need to justify the need to use surveillance cameras [127]. Taking privacy into account, the Code of Practice mandates that the use of cameras be evaluated to review how the cameras affect individuals and whether transparency or accountability mechanisms should be implemented [127]. These Codes of Practice ensure that surveillance technologies are "used only when necessary and in a proportionate and transparent way" [55].

To improve the accountability of American law enforcement's facial recognition, agencies must develop strict use policies and audit their systems. Use policies should guarantee security and implement human rights standards [24]. Departmental use policies should state the following: which photo database is accessible, the scenarios in which surveillance technologies and facial recognition may be used, who has access to the system, and punishments for officers found to be misusing their system privileges [1]. Before enforcing their use policies, police should seek approval from city councils and other legislative bodies [1].

System audits and other measures of departmental oversight should be provided to sanction excessive surveillance and influence future implementations of surveillance technologies [114]. Oversight of facial recognition systems must occur at the state and Federal level. States need to ensure that their systems are not being misused or accessible to more officers than necessary. The FBI should oversee and enforce standards on the state databases to which it has access. It is irresponsible for the FBI to rely on states to perform oversight on their respective systems, since some states have not yet done so. State and federal facial recognition systems must be subject to oversight from the GAO to eliminate bias. The GAO must also develop a schedule to audit these systems in a time frame they deem necessary.

Moving forward, law enforcement agencies should keep accountability in mind when implementing facial recognition systems. In doing so, officers' action can be challenged if they are deemed to invade privacy [174]. American law enforcement already has more oversight over approaches to surveillance and facial recognition than their Chinese counterparts [60]. Officers and their respective police departments must be held accountable for their practices to make sure surveillance does not become as pervasive in the U.S. as it has in China.

5.2 Becoming More Transparent

Police departments in the U.K. have been more transparent with their use of surveillance technologies in public than their American counterparts. For example, the Bedfordshire and Hampshire Regional Police Forces have released specifications of their body-worn camera policies [175]. Publications are thorough, demonstrated by the West Midlands Police Force drone usage, ranging from how and when the drones are used to how long recorded footage is kept [50].

After creating use policies, police departments in the U.S. need to publish them. To increase the transparency of policing, citizens must be told the purpose of data collection, how their data is being secured, if the is shared, along with contact information for those to contact about data retention [174]. It has been found that less than ten percent of surveyed LEAs have published facial recognition policies [1]. The American public deserves to know about how and when their data is collected, especially if said data is collected without their knowledge [91].

The FBI has weakened its transparency when declaring it's NGI system exempt from the Privacy Act. This does not set a good example for state and municipal agencies who may wish to do the same. The exemption takes away the right for citizens to view federal records containing their personal information. It has already been argued that the FBI should be transparent about its use of facial recognition [1]. Aside from reversing its decision about exempting its system from the Privacy Act, the FBI should release more information about the photo databases its system accesses and statistics on searches it completes [1].

While demanding for more transparency in American policing, it is important to remember that U.S. law enforcement is much more transparent than Chinese law enforcement. American society encourages LEAs to be transparent, while "China's authoritarian system has diminished the transparency and accountability" of surveillance and facial recognition technologies [176].

5.3 Improving Accuracy

The last significant improvement necessary is the improved level of accuracy at which law enforcement implemented facial recognition algorithms perform. Currently the algorithms used by American law enforcement are more accurate than those in the U.K. but less accurate than those implemented in China. The accuracy of British systems stands close to five percent [103] while China's facial recognition systems surpassed the accuracy rate of the human eye in 2014 [58].

British police offer a unique perspective on how to improve the accuracy of their systems. the MPS has a team of 'super-recognisers' to perform identifications [177]. The term super-recogniser refers to a person with exceptional face recognition abilities [178]. The recognisers' accuracy was tested against that of other police trainees, and they performed better on all given face matching tests [177]. Recruiting officers with such high levels of performance reduces the chances of a citizen being wrongly identified as a suspect. Using super-recognisers as human reviewers can decrease the number of incorrectly identified individuals.

Another technique of improving a facial recognition system's accuracy stems from the photo database it uses. Filling the database with more photos depicting a given demographic can improve the accuracy for that group [179]. More specifically, feeding a facial recognition software with a variety of photos of the same person in different positions, or even with glasses on, will improve the system's accuracy in identifying that person [179].

Other best practices have been suggested on how to record high quality images for the purpose of increasing a system's accuracy. While capturing images in the field, an officer should instruct the subject to look ahead and not tilt their head [81]. For mug shot images, the inner part of the face must not be obstructed by hair [81]. After the probe photo is captured, it is suggested to submit the original, uncropped version– no picture taken from another device should be used [81]. Although these are simple measures for law enforcement officers to take, best practices help to reinforce standards, such as ISO/IEC 19794-5.

5.4 Moving Forward

Many deeper research topics can be derived from the work presented in this thesis, however, only two significant research questions have arisen. Surveillance and facial recognition should be studied to determine how the technologies impact minority populations in the U.S. and their level of trust toward their local police department. To continue with the methodology of a country comparison, further research could compare American methods with those of other countries around the world.

Research could be done on how surveillance and facial recognition affects minority populations, especially the African American population in the U.S. In recent years, numerous riots have occurred across the country involving police brutality against African American citizens. Research could determine whether or not the improvement and development of surveillance technologies positively influences the relationship between police officers and minority groups. Another aspect of this research would involve the racial asymmetry faced by police departments across the country. Finding a way to resolve the racial tension between police and citizens in the U.S. will change American society for the better.

American surveillance methods could also be analysed in comparison with other countries, such as Germany and Singapore. This comparison would bring much more to the discussion of how LEAs can implement facial recognition in a more responsible manner, especially since these countries are currently surveillance technologies equipped with facial recognition. Germany would be relevant to discuss European ideals while Singapore offers an eastern perspective, without having an authoritarian rule like China. Such an analysis may offer a greater contribution to American law enforcement.

References

[1] C. Garvie, A. M. Bedoya, and J. Frankle, “The Perpetual Line-Up,” 2016.

[2] Derek Hawkins, “How Maryland police used facial recognition to catch Annapolis shooter Jarrod Ramos,” *The Independent*, 2018. [Online]. Available: https://www.independent.co.uk/news/world/americas/annapolis-shooting-maryland-police-facial-recognition-catch-jarrod-ramos-a8427181.html. [Accessed: 30-Nov-2018].

[3] “ACLU Urges Justice Department to Investigate Police Use of Face Recognition,” *ACLU*, 2016. [Online]. Available: https://www.aclu.org/news/aclu-urges-justice-department-investigate-police-use-face-recognition. [Accessed: 30-Nov-2018].

[4] N. Steinfeld, “Track me, track me not: Support and consent to state and private sector surveillance,” *Telemat. Informatics*, vol. 34, no. 8, pp. 1663–1672, 2017.

[5] W. G. Staples, *Everyday Surveillance: Vigilance and Visibility in Postmodern Life*, Second. Rowman & Littlefield, 2014.

[6] “Surveillance,” *Dictionary.com*. [Online]. Available: https://www.dictionary.com/browse/surveillance. [Accessed: 07-Mar-2019].

[7] W. Bloss, “Escalating U.S. police surveillance after 9/11: An examination of causes and effects,” *Surveill. Soc.*, vol. 4, no. 3, pp. 208–228, 2007.

[8] D. Lyon, *Surveillance society: monitoring everyday life*. Open University Press, 2001.

[9] B. Mesnik, “The History of Video Surveillance,” *Kintronics*, 2016. [Online]. Available: https://kintronics.com/the-history-of-video-surveillance/. [Accessed: 23-Mar-2019].

[10] F. Porikli *et al.*, “Video surveillance: Past, present, and now the future,” *IEEE Signal Process. Mag.*, vol. 30, no. 3, pp. 190–198, 2013.

[11] J. Laperruque and D. Janovsky, “These Police Drones are Watching You,” *pogo.org*, 2018. [Online]. Available: https://www.pogo.org/analysis/2018/09/these-police-drones-are-watching-you/. [Accessed: 10-Mar-2019].

[12] D. Gettinger, “Public Safety Drones,” 2017.

[13] “DJI Zenmuse Z30 テスト 1,” 2017. [Online]. Available: https://www.youtube.com/watch?v=y5w73Q5GnhU.

[14] J. Laperruque, “Preventing an Air Panopticon: a Proposal for Reasonable Legal Restrictions on Aerial Surveillance,” *Univeristy Richmond Law Rev.*, vol. 51, pp. 705–726, 2013.

[15] S. Anthony, “DARPA shows off 1.8-gigapixel surveillance drone, can spot a terrorist from 20,000 feet - ExtremeTech,” *extremetech.com*, 2013. [Online]. Available: http://www.extremetech.com/extreme/146909-darpa-shows-off-1-8-gigapixel-surveillance-drone-can-spot-a-terrorist-from-20000-feet. [Accessed: 10-Apr-2019].

[16] G. T. Marx, “Surveillance and Society,” in *Encyclopedia of Social Theory*, G. Ritzer, Ed. Sage Publications, Inc., 2005, pp. 816–821.

[17] N. G. La Vigne, S. S. Lowry, A. M. Dwyer, and J. A. Markman, “Using Public Surveillance Systems for Crime Control and Prevention: A Practical Guide for Law Enforcement and Their Municipal Partners,” 2011.

[18] “What is a PTZ Camera?,” *VideoSurveillance.com LLC*. [Online]. Available: https://www.videosurveillance.com/tech/ptz-technology.asp. [Accessed: 11-Mar-

2019].
[19] K. Arora, “Buckhead Blue-Light Police Cameras: Do They Really Work? - Buckhead,” *Buckhead*, 2017. [Online]. Available: https://www.buckhead.com/buckhead-blue-light-police-cameras-do-they-really-work/. [Accessed: 06-Apr-2019].
[20] S. Beyer, “Do Cities Need Flashing Police Cameras? - The Market Urbanism Report,” *The Market Urbanism Report*, 2018. [Online]. Available: https://marketurbanismreport.com/cities-need-flashing-police-cameras/. [Accessed: 06-Apr-2019].
[21] “Body worn video (police equipment),” *Wikipedia*. [Online]. Available: https://en.wikipedia.org/wiki/Body_worn_video_(police_equipment). [Accessed: 03-Dec-2019].
[22] “Body-Worn Cameras Policy.” Labor Relations Information System, 2014.
[23] J. A. Hendrix, T. A. Taniguchi, K. J. Strom, K. Barrick, and N. J. Johnson, “The eyes of law enforcement in the new panopticon: Police-community racial asymmetry and the use of surveillance technology,” *Surveill. Soc.*, vol. 16, no. 1, pp. 53–68, 2018.
[24] I. Butler, “Security Through Human Rights,” 2017.
[25] S. Graham and D. Wood, “Digitizing surveillance : categorization , space ,” *Crit. Soc. Policy Ltd*, vol. 23, no. 2, pp. 227–248, 2003.
[26] D. Lyon, “Surveillance as social sorting: Computer codes and mobile bodies,” in *Surveillance as Social Sorting: Privacy, risk, and digital discrimination*, D. Lyon, Ed. Routledge, 2003, pp. 13–30.
[27] N. G. La Vigne, S. S. Lowry, J. A. Markman, and A. M. Dwyer, “Evaluating the Use of Public Surveillance Cameras for Crime Control and Prevention - A Summary,” 2011.
[28] D. Lyon, *Surveillance after September 11*. Polity Press, 2003.
[29] “Boston Marathon Bombing,” *A&E Television Networks*, 2014. [Online]. Available: https://www.history.com/topics/21st-century/boston-marathon-bombings. [Accessed: 24-Mar-2019].
[30] F. Coudert, “When video cameras watch and screen: Privacy implications of pattern recognition technologies,” *Comput. Law Secur. Rev.*, vol. 26, no. 4, pp. 377–384, 2010.
[31] I. Maghiros *et al.*, “Security and Privacy for the Citizen in the Post-September 11 Digital Age : A Prospective Overview,” 2003.
[32] “Function creep,” *www.dictionary.com*. [Online]. Available: https://www.dictionary.com/browse/function-creep. [Accessed: 12-May-2019].
[33] D. Cole and J. X. Dempsey, *Terrorism and the Constitution: Sacrificing Civil Liberties in the Name of National Security*. The New Press, 2006.
[34] M. Jacobs, “Function Creep in Surveillance Situations Identifying control paradoxes through agency and power relations using ANT,” Utrecht Univeristy, 2016.
[35] M. Ignatieff, *The Lesser Evil: Political Ethics in an Age of Terror*. Princeton, New Jersey: Princeton Univeristy Press, 2004.
[36] M. H. Maras, “The social consequences of a mass surveillance measure: What happens when we become the ‘others’?,” *Int. J. Law, Crime Justice*, vol. 40, no. 2, pp. 65–81, 2012.
[37] C. R. Sunstein, *Laws of Fear: Beyond the Precautionary Principle*. Cambridge University Press, 2005.
[38] D. Cole, “Enemy Aliens,” *Stanford Law Rev.*, vol. 54, no. 5, pp. 953–1004, 2002.

[39] J. Ellul, *The Technological Society*. Knopf, 1964.

[40] D. Gettinger, “Public Safety Drones: an Update,” 2018.

[41] M. Sisitzky and S. McCormack, “New NYPD Drone Policy Represents a Serious Threat to Privacy,” *nyclu.org*, 2018. [Online]. Available: https://www.nyclu.org/en/news/new-nypd-drone-policy-represents-serious-threat-privacy. [Accessed: 11-Apr-2019].

[42] M. Zhang, “The $40,000 ‘Bug’ Camera Drone Being Tested by the US Military,” *PetaPixel*, 2015. [Online]. Available: https://petapixel.com/2015/12/07/the-40000-bug-camera-drone-being-tested-by-the-us-military/. [Accessed: 09-Apr-2019].

[43] K. Osborn, “Air Force chief scientist: future drones stealthier -more autonomous -- Defense Systems,” *1105 Media, Inc.*, 2016. [Online]. Available: https://defensesystems.com/articles/2016/10/10/future-drones.aspx. [Accessed: 09-Apr-2019].

[44] F. Hersey, “China to have 626 million surveillance cameras within 3 years · TechNode,” *TechNode*, 2017. [Online]. Available: https://technode.com/2017/11/22/china-to-have-626-million-surveillance-cameras-within-3-years/. [Accessed: 12-Mar-2019].

[45] S. Nunn, “Police technology in cities: Changes and challenges,” *Technol. Soc.*, vol. 23, no. 1, pp. 11–27, 2001.

[46] K. Kindy, “Some U.S. police departments dump body-camera programs amid high costs - The Washington Post,” *The Washington Post*, 2019. [Online]. Available: https://www.washingtonpost.com/national/some-us-police-departments-dump-body-camera-programs-amid-high-costs/2019/01/21/991f0e66-03ad-11e9-b6a9-0aa5c2fcc9e4_story.html?utm_term=.e1657db33680. [Accessed: 12-Mar-2019].

[47] “Watchdog’s Big Brother UK warning,” *BBC News*, 2004. [Online]. Available: http://news.bbc.co.uk/2/hi/uk_news/politics/3568468.stm. [Accessed: 18-Apr-2019].

[48] S. J. Fox, “Policing - The technological revolution: Opportunities & challenges!,” *Technol. Soc.*, vol. 56, no. August 2018, pp. 69–78, 2019.

[49] “How UK Police are using drones to catch criminals and locate missing persons,” *www.upliftdronetraining.com*, 2019. [Online]. Available: https://www.upliftdronetraining.com/how-uk-police-are-using-drones-to-catch-criminals-and-locate-missing-persons/. [Accessed: 11-May-2019].

[50] “Police Drones,” *www.west-midlands.police.uk*. [Online]. Available: https://www.west-midlands.police.uk/frequently-asked-questions/police-drones. [Accessed: 22-Apr-2019].

[51] “British Security Industry Association - Overview.”

[52] “How Many CCTV Cameras in London?,” *www.caughtoncamera.net*. [Online]. Available: https://www.caughtoncamera.net/news/how-many-cctv-cameras-in-london/. [Accessed: 11-May-2019].

[53] A. Bannister, “A UK map of CCTV cameras: Towns and cities by surveillance camera concentration,” *www.ifsecglobal.com*, 2018. [Online]. Available: https://www.ifsecglobal.com/video-surveillance/uk-map-cctv-cameras-towns-cities-by-surveillance-camera-concentration/. [Accessed: 11-May-2019].

[54] B. Ariel, W. A. Farrar, and A. Sutherland, “The Effect of Police Body-Worn Cameras on Use of Force and Citizens’ Complaints Against the Police: A Randomized Controlled Trial,” *J. Quant. Criminol.*, vol. 31, no. 3, pp. 509–535, Sep. 2015.

[55] "Smile you're on body worn camera Part II-Police The use of body worn cameras by UK police forces," 2017.

[56] "Metropolitan Police body-worn cameras rolled out," *www.bbc.com*, 2016. [Online]. Available: https://www.bbc.com/news/uk-england-london-37654326. [Accessed: 05-May-2019].

[57] "Body-Worn Video," 2014.

[58] R. Grenoble, "Welcome To The Surveillance State: China's AI Cameras See All," *huffpost.com*, 2017. [Online]. Available: https://www.huffpost.com/entry/china-surveillance-camera-big-brother_n_5a2ff4dfe4b01598ac484acc. [Accessed: 22-Apr-2019].

[59] P. Crespo, "China's High-Tech Surveillance State: a &quot;Digital Despotism&quot;," *bitterwinter.org*, 2019. [Online]. Available: https://bitterwinter.org/chinas-high-tech-surveillance-state-a-digital-despotism/. [Accessed: 12-May-2019].

[60] J. Vincent, "Chinese police are using facial recognition sunglasses to track citizens - The Verge," *www.theverge.com*, 2018. [Online]. Available: https://www.theverge.com/2018/2/8/16990030/china-facial-recognition-sunglasses-surveillance. [Accessed: 04-May-2019].

[61] M. Kaste, "Real-Time Facial Recognition Is Available, But Will U.S. Police Buy It?," *npr.org*, 2018. [Online]. Available: https://www.npr.org/2018/05/10/609422158/real-time-facial-recognition-is-available-but-will-u-s-police-buy-it. [Accessed: 22-Apr-2019].

[62] M. Rajagopalan, "This Is What A 21st-Century Police State Really Looks Like," *buzzfeednews.com*, 2017. [Online]. Available: https://www.buzzfeednews.com/article/meghara/the-police-state-of-the-future-is-already-here#.kej0OWw555. [Accessed: 22-Apr-2019].

[63] W. Keju, "Drones aid traffic police, but privacy, safety questioned," *global.chinadaily.com.cn*, 2019. [Online]. Available: http://global.chinadaily.com.cn/a/201904/09/WS5cabf6d8a3104842260b5195.html. [Accessed: 03-May-2019].

[64] S. Chen, "China takes surveillance to new heights with flock of robotic Doves, but do they come in peace?," *www.scmp.com*, 2018. [Online]. Available: https://www.scmp.com/news/china/society/article/2152027/china-takes-surveillance-new-heights-flock-robotic-doves-do-they. [Accessed: 03-May-2019].

[65] S. Liao, "Chinese police are expanding facial recognition sunglasses program," *www.theverge.com*, 2018. [Online]. Available: https://www.theverge.com/2018/3/12/17110636/china-police-facial-recognition-sunglasses-surveillance. [Accessed: 04-May-2019].

[66] M. Chan, "Chinese startup makes facial recognition glasses for police," *asia.nikkei.com*, 2018. [Online]. Available: https://asia.nikkei.com/Business/Companies/Chinese-startup-makes-facial-recognition-glasses-for-police. [Accessed: 04-May-2019].

[67] H. Koskela, "'Cam Era' – the contemporary urban panopticon," *Surveill. Soc.*, vol. 1, no. 3, pp. 292–313, 2003.

[68] T. McMullan, "What does the panopticon mean in the age of digital surveillance?," 2015. [Online]. Available: https://www.theguardian.com/technology/2015/jul/23/panopticon-digital-surveillance-jeremy-bentham. [Accessed: 23-Mar-2019].

[69] M. Božovič, *Jeremy Bentham: The Panopticon Writings*. Verso, 1995.

[70] E. Stoycheff, J. Liu, K. Xu, and K. Wibowo, “Privacy and the Panopticon: Online mass surveillance’s deterrence and chilling effects,” *New Media Soc.*, vol. 21, no. 3, pp. 602–619, 2019.

[71] M. Foucault, *Discipline & Punish: The Birth of the Prison*, 2nd ed. Vintage Books, 1977.

[72] C. Norris, J. Moran, and G. Armstrong, *Surveillance, Closed Circuit Television and Social Control*. Routledge, 2016.

[73] D. Wright *et al.*, “Sorting out smart surveillance,” *Comput. Law Secur. Rev.*, vol. 26, no. 4, pp. 343–354, 2010.

[74] D. Lyon, *Surveillance Studies: An Overview*. Polity Press, 2007.

[75] “Face recognition definition and meaning,” *Collins English Dictionary*. [Online]. Available: https://www.collinsdictionary.com/dictionary/english/face-recognition. [Accessed: 30-Nov-2018].

[76] J. D. Woodward, C. Horn, J. Gatune, and A. Thomas, “Documented Briefing,” 2003.

[77] S. Symanovich, “How does facial recognition technology work?,” *Symantec Corporation*. [Online]. Available: https://us.norton.com/internetsecurity-iot-how-facial-recognition-software-works.html. [Accessed: 20-Feb-2019].

[78] T. Mansfield and G. Roethenbaugh, “Glossary of Biometric Terms.” Association for Biometrics and International Computer Security Association, 1999.

[79] D. Harwell, “Facial recognition may be coming to a police body camera near you - The Washington Post,” *The Washington Post*, 2018. [Online]. Available: https://www.washingtonpost.com/news/the-switch/wp/2018/04/26/facial-recognition-may-be-coming-to-a-police-body-camera-near-you/?noredirect=on&utm_term=.decd64ce4291. [Accessed: 12-Mar-2019].

[80] “Biometric Definitions,” *Zvetco Biometrics LLC.* [Online]. Available: http://www.zvetcobiometrics.com/Support/definitions.php. [Accessed: 30-Nov-2018].

[81] R. Rodriguez, “Facial recognition: Art or Science?,” *LAW ORDER*, vol. 64, no. 9, pp. 36–39, 2016.

[82] “Information technology - Biometric sample quality - Part 5: Face image data,” ISO/IEC TR 29794-5:2010(E), 2010.

[83] A. Narvekar, A. J. O’Toole, F. Jiang, P. J. Phillips, and J. Ayyad, “An other-race effect for face recognition algorithms,” *ACM Trans. Appl. Percept.*, vol. 8, no. 2, pp. 1–11, 2011.

[84] L. Ge *et al.*, “Two faces of the other-race effect: Recognition and categorisation of Caucasian and Chinese faces,” *Perception*, vol. 38, no. 8, pp. 1199–1210, 2009.

[85] “Amazon Rekognition announces real-time face recognition, Text in Image recognition, and improved face detection,” *aws.amazon.com*, 2017. [Online]. Available: https://aws.amazon.com/about-aws/whats-new/2017/11/amazon-rekognition-announces-real-time-face-recognition-text-in-image-recognition-and-improved-face-detection/. [Accessed: 10-May-2019].

[86] I. D. Raji and J. Buolamwini, “Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products,” 2019.

[87] J. Snow, “Amazon’s Face Recognition Falsely Matched 28 Members of Congress With Mugshots,” *www.aclu.org*, 2018. [Online]. Available: https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28. [Accessed: 06-May-

2019].
[88] B. F. Klare, M. J. Burge, J. C. Klontz, R. W. Vorder Bruegge, and A. K. Jain, "Face recognition performance: Role of demographic information," *IEEE Trans. Inf. Forensics Secur.*, vol. 7, no. 6, pp. 1789–1801, 2012.
[89] "Bureau of Justice Statistics (BJS) - Data Analysis Tools - Arrest Data Analysis Tool," *Bureau of Justice Statistics*. [Online]. Available: https://www.bjs.gov/index.cfm?ty=datool&surl=/arrests/index.cfm#. [Accessed: 16-Mar-2019].
[90] "Table DL-22 - Highway Statistics 2017," *U.S. Department of Transportation Federal Highway Administration*. [Online]. Available: https://www.fhwa.dot.gov/policyinformation/statistics/2017/dl22.cfm. [Accessed: 20-Mar-2019].
[91] J. Lynch, "Face off: Law enforcement use of face recognition technology," 2018.
[92] "Best Practice," *Merriam-Webster, Incorporated*. [Online]. Available: https://www.merriam-webster.com/dictionary/best practice. [Accessed: 03-Apr-2019].
[93] "BS ISO/IEC 19794 Series - BSI Shop," *British Standards Institution*. [Online]. Available: https://shop.bsigroup.com/Browse-By-Subject/Biometrics/BS-ISOIEC-19794-SERIES/. [Accessed: 04-Apr-2019].
[94] "Information technology - Biometric data interchange formats - Part 5: Face image data," ISO/IEC 19794-5:2005/Amd.1:2007(E), 2007.
[95] P. Griffin, "Understanding The Face Image Format Standards." Identix, 2005.
[96] P. J. Grother, G. W. Quinn, and M. L. Ngan, "Face in video evaluation (FIVE) face recognition of non-cooperative subjects," 2017.
[97] C. Burt, "Police body camera maker Axon weighs implementation of real-time facial recognition," *biometricupdate.com*, 2018. [Online]. Available: https://www.biometricupdate.com/201805/police-body-camera-maker-axon-weighs-implementation-of-real-time-facial-recognition. [Accessed: 06-Apr-2019].
[98] E. Morphy, "What Are Behavioral Biometrics and How Do They Fit Into Marketing?," *cmswire.com*, 2018. [Online]. Available: https://www.cmswire.com/customer-experience/what-are-behavioral-biometrics-and-how-do-they-fit-into-marketing/. [Accessed: 07-Apr-2019].
[99] "Half of All American Adults are in a Police Face Recognition Database, New Report Finds," *Georgetown Law*, 2016. [Online]. Available: https://www.law.georgetown.edu/news/half-of-all-american-adults-are-in-a-police-face-recognition-database-new-report-finds/. [Accessed: 31-Jan-2019].
[100] Kara Kovalchik, "Who Originated The Mug Shot in America?," *Mental Floss*, 2015. [Online]. Available: http://mentalfloss.com/article/61358/who-originated-mug-shot-america. [Accessed: 06-Mar-2019].
[101] "Mug Shot," *Merriam-Webster, Incorporated*. [Online]. Available: https://www.merriam-webster.com/dictionary/mug shot. [Accessed: 06-Mar-2019].
[102] "Next Generation Identification (NGI) — FBI," *U.S. Department of Justice*. [Online]. Available: https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi. [Accessed: 24-Feb-2019].
[103] "Face Off: The lawless growth of facial recognition in UK policing," 2018.
[104] S. K. Skelton, "UK police should not deploy live facial recognition technology until issues are resolved, MPs told," *www.computerweekly.com*, 2019. [Online]. Available: https://www.computerweekly.com/news/252460016/UK-police-

should-not-deploy-live-facial-recogntion-technology-until-issues-are-resolved-MPs-told. [Accessed: 05-May-2019].

[105] L. Lucas and E. Feng, "Inside China's surveillance state," *www.ft.com*, 2018. [Online]. Available: https://www.ft.com/content/2182eebe-8a17-11e8-bf9e-8771d5404543. [Accessed: 04-May-2019].

[106] F. Liang, V. Das, N. Kostyuk, and M. M. Hussain, "Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure," *Policy and Internet*, vol. 10, no. 4, pp. 415–453, 2018.

[107] D. V. S. Kasper, "The Evolution (Or Devolution) of Privacy," *Sociol. Forum*, vol. 20, no. 1, pp. 69–92, 2005.

[108] S. D. Warren and L. D. Brandeis, "The Harvard Law Review Association," *Harv. Law Rev.*, vol. 4, no. 5, pp. 193–220, 1890.

[109] "Privacy," *ACLU of Florida*. [Online]. Available: https://www.aclufl.org/en/issues/privacy. [Accessed: 01-Dec-2018].

[110] G. A. Kaufman, "The right not to be let alone," *J. Priv. Int. Law*, vol. 4, no. 4, pp. 445–456, 2011.

[111] J. E. Cohen, "What Privacy Is For," *Harv. Law Rev.*, vol. 126, no. 7, pp. 1904–1933, 2013.

[112] "Privacy," *Dictionary.com*. [Online]. Available: https://www.dictionary.com/browse/privacy. [Accessed: 01-Dec-2018].

[113] "Mass Surveillance," *Privacy International*. [Online]. Available: https://www.privacyinternational.org/topics/mass-surveillance. [Accessed: 07-Mar-2019].

[114] D. Wright *et al.*, "Questioning surveillance," *Comput. Law Secur. Rev.*, vol. 31, no. 2, pp. 280–292, 2015.

[115] A. F. Westin, *Privacy and Freedom*. The Bodley Head Ltd., 1967.

[116] "The USA PATRIOT Act: Preserving Life and Liberty," *justice.gov*. [Online]. Available: https://www.justice.gov/archive/ll/highlights.htm. [Accessed: 18-Apr-2019].

[117] S. Boyne, "The Future of Liberal Democracies in a Time of Terror: A Comparison of the Impact of Civil Liberties in the Federal Republic of Germany and the United States," *Tulsa J. Comp. Const. Law*, vol. 11, no. 1, pp. 111–178, 2003.

[118] M. Reel, "Secret Cameras Record Baltimore's Every Move From Above," *Bloomberg Businessweek*, 2016. [Online]. Available: https://www.bloomberg.com/features/2016-baltimore-secret-surveillance/. [Accessed: 09-Apr-2019].

[119] E. Elizade and T. Tracy, "Send in the drones: NYPD launches its new 'unmanned aircraft' system," *nydailynews.com*, 2018. [Online]. Available: https://www.usa-proxy.org/browse.php?u=K2O0RVdOjkXriJXi67L1I8mp1e5XJY9qzHQt8yBw319HDuCXtMQ0T%2FEtihbtFRo0UWRfR70eK%2BltTYZyJ5xVQ8aPwwUUlTcfi1Pp9136w0YKOxJxbZoe7a%2FMMw4%3D&b=61&f=norefer. [Accessed: 11-Apr-2019].

[120] "Rise in US police use of drones triggers backlash over spying and other abuses, Technology - THE BUSINESS TIMES," *The Business Times*, 2018. [Online]. Available: https://www.businesstimes.com.sg/technology/rise-in-us-police-use-of-drones-triggers-backlash-over-spying-and-other-abuses. [Accessed: 12-Mar-2019].

[121] B. Powers, "How Baltimore Police Use Military Technology to Track You – Rolling Stone," *Rolling Stone*, 2017. [Online]. Available:

https://www.rollingstone.com/culture/culture-features/eyes-over-baltimore-how-police-use-military-technology-to-secretly-track-you-126885/. [Accessed: 12-Mar-2019].

[122] "What's Wrong With Public Video Surveillance?," *aclu.org*. [Online]. Available: https://www.aclu.org/other/whats-wrong-public-video-surveillance. [Accessed: 15-Apr-2019].

[123] A. Thomas-Lester and T. Locy, "Chief's Friend Accused of Extortion," *The Washington Post*, 1997. .

[124] M. Ehrenkranz, "Cop Used Police Database to Creep on Over 100 Women, Investigation Finds," *gizmodo.com*, 2019. [Online]. Available: https://gizmodo.com/cop-uses-police-database-to-creep-on-over-100-women-in-1833156806. [Accessed: 16-Apr-2019].

[125] "Police sometimes misuse confidential work databases for personal gain: AP," *cbsnews.com*, 2016. [Online]. Available: https://www.cbsnews.com/news/police-sometimes-misuse-confidential-work-databases-for-personal-gain-ap/. [Accessed: 16-Apr-2019].

[126] C. Norris, "From personal to digital: CCTV, the panopticon, and the technological mediation of suspicion and social control," in *Surveillance as Social Sorting: Privacy, risk, and digital discrimination*, D. Lyon, Ed. Routledge, 2003, pp. 249–281.

[127] F. Coudert, D. Butin, and D. Le Métayer, "Body-worn cameras for police accountability: Opportunities and risks," *Comput. Law Secur. Rev.*, vol. 31, no. 6, pp. 749–762, 2015.

[128] L. Miller and J. Toliver, "Implementing a Body-Worn Camera Program: Recommendations and Lessons Learned," Washington, D.C., 2014.

[129] J. Stanley, "I spy with my fly: When video surveillance goes mobile," *Computers, Privacy and Data Protection*. Brussels, 2015.

[130] J. Wenner, "Who Watches the Watchmen's Tape? FOIA's Categorical Exemptions and Police Body-Worn Cameras," *Univ. Chic. Leg. Forum*, vol. 2016, no. 23, pp. 873–906, 2016.

[131] *New Hampshire Right to Know Law*. 2017.

[132] "Police Body Cameras."

[133] J. Stanley, "Police Body-Mounted Cameras: With Right Policies in Place, a Win For All Introduction 1," 2013.

[134] A. Winston, "A New Way to Punish Oakland Cops?," *East Bay Express*, 2012. [Online]. Available: https://www.eastbayexpress.com/oakland/a-new-way-to-oakland-cops/Content?oid=3125656. [Accessed: 15-Apr-2019].

[135] S. Fussel, "The Always-On Police Camera," *The Atlantic*, 2018. [Online]. Available: https://www.theatlantic.com/technology/archive/2018/09/body-camera-police-future/571402/. [Accessed: 15-Apr-2019].

[136] M. Nieto, "Public Video Surveillance: Is It An Effective Crime Prevention Tool?," Sacramento, 1997.

[137] *Laird v. Tatum 408 U.S. 1*. 1972, p. 1.

[138] *United States v. Knotts 460 U.S. 276*. 1983, p. 276.

[139] *United States v. Taketa 923 F2d 665*. 1988, p. 665.

[140] Q. Burrows, "Scowl Because You're on Candid Camera: Privacy and Video Surveillance," *Valparaiso Univ. Law Rev.*, vol. 31, pp. 1079–1139, 1997.

[141] N. Jacoby, "Redefining the Right to Be Let Alone: Privacy Rights and the Constitutionality of Technical Surveillance Measures in Germany and the United States," *Georg. J. Int. Comp. Law*, vol. 35, no. 3, pp. 433–493, 2007.

[142] J. Laperruque, “Preserving the Right to Obscurity in the Age of Facial Recognition,” *tcf.org*, 2017. [Online]. Available: https://tcf.org/content/report/preserving-right-obscurity-age-facial-recognition/?agreed=0. [Accessed: 11-Apr-2019].

[143] “Committee to Review Law Enforcement’s Policies on Facial Recognition,” 2017.

[144] M. Whittaker *et al.*, “AI Now Report 2018,” 2018.

[145] “Surveillance Technologies,” *ACLU*. .

[146] R. W. V. Bruegge, “Facial Recognition and Identification Initiatives.” Federal Bureau of Investigation, 2010.

[147] J. Beddor, Jennifer; Copeland, Orlando; Currie, Chris; Fejfar, Michele; de Ferrari, John; Hauswirth, Eric; Hsu, Susan; Hung, Richard; Kelly, Monica; Kuebler, Susanna; Olson, Alexis; Plocher, David; Temko-Blinder, “FACE RECOGNITION TECHNOLOGY FBI Should Better Ensure Privacy and Accuracy,” 2016.

[148] T. Ring, “Privacy in peril: is facial recognition going too far too fast?,” *Biometric Technol. Today*, vol. 2016, no. 7–8, pp. 7–11, 2016.

[149] “CJIS Annual Report 2016,” Clarksburg, 2016.

[150] P. A. Winn, “Privacy Act of 1974; Implementation,” *Fed. Regist.*, vol. 82, no. 146, pp. 35651–35654, 2017.

[151] “FOIA/PA Overviews, Exemptions, and Terms — FBI,” *U.S. Department of Justice*. [Online]. Available: https://www.fbi.gov/services/information-management/foipa/foia-pa-overviews-exemptions-and-terms. [Accessed: 25-Feb-2019].

[152] C. Saez, “International Standards Key To Helping The World With Many Issues, ISO Says,” *ip-watch.org*, 2012. [Online]. Available: http://www.ip-watch.org/2012/05/18/international-standards-key-to-helping-the-world-with-many-issues-iso-says/. [Accessed: 21-Apr-2019].

[153] *Code of Federal Regulations Title 6*. United States of America, 2010, p. 222.

[154] “REAL ID,” *Department of Homeland Security*. [Online]. Available: https://www.dhs.gov/real-id. [Accessed: 21-Apr-2019].

[155] *Biometric Information Privacy Act*. 2008.

[156] D. Harwell, “Oregon became a testing ground for Amazon’s facial-recognition policing. But what if Rekognition gets it wrong?,” *www.washingtonpost.com*, 2019. [Online]. Available: https://www.washingtonpost.com/technology/2019/04/30/amazons-facial-recognition-technology-is-supercharging-local-police/?noredirect=on&utm_term=.85b162d17a9c. [Accessed: 10-May-2019].

[157] K. Houser, “Police Are Using Facial Recognition Tech on Unconscious Suspects,” *futurism.com*, 2019. [Online]. Available: https://futurism.com/police-facial-recognition-unconscious-suspects. [Accessed: 10-May-2019].

[158] C. Burt, “Facial recognition mostly used by Washington County police to investigate minor crimes,” *www.biometricupdate.com*, 2019. [Online]. Available: https://www.biometricupdate.com/201903/facial-recognition-mostly-used-by-washington-county-police-to-investigate-minor-crimes. [Accessed: 10-May-2019].

[159] “Using Facial Recognition Systems.” Washington County Sheriff’s Office, 2019.

[160] D. Harris, “Orlando police starting 2nd test phase of Amazon facial-recognition software,” *www.orlandosentinel.com*, 2018. [Online]. Available: https://www.orlandosentinel.com/news/breaking-news/os-ne-orlando-police-

amazon-facial-recognition-20181018-story.html. [Accessed: 10-May-2019].

[161] J. Creswell, “Orlando Pulls the Plug on Its Amazon Facial Recognition Program,” *www.nytimes.com*, 2018. [Online]. Available: https://www.nytimes.com/2018/06/25/business/orlando-amazon-facial-recognition.html. [Accessed: 10-May-2019].

[162] M. Kaste, “Orlando Police Testing Amazon’s Real-Time Facial Recognition,” *www.wlrn.org*, 2018. [Online]. Available: https://www.wlrn.org/post/orlando-police-testing-amazons-real-time-facial-recognition. [Accessed: 10-May-2019].

[163] M. Cagle and N. Ozer, “Amazon Teams Up With Government to Deploy Dangerous New Facial Recognition Technology,” *www.aclu.org*, 2018. [Online]. Available: https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazon-teams-government-deploy-dangerous-new. [Accessed: 10-May-2019].

[164] “I’m an Amazon Employee. My Company Shouldn’t Sell Facial Recognition Tech to Police.,” *medium.com*, 2018. [Online]. Available: https://medium.com/s/powertrip/im-an-amazon-employee-my-company-shouldn-t-sell-facial-recognition-tech-to-police-36b5fde934ac. [Accessed: 10-May-2019].

[165] N. Statt, “Amazon told employees it would continue to sell facial recognition software to law enforcement,” *www.theverge.com*, 2018. [Online]. Available: https://www.theverge.com/2018/11/8/18077292/amazon-rekognition-jeff-bezos-andrew-jassy-facial-recognition-ice-rights-violations. [Accessed: 10-May-2019].

[166] R. Hill, “Zero arrests, 2 correct matches, no criminals: London cops’ facial recog tech slammed,” *www.theregister.co.uk*, 2018. [Online]. Available: https://www.theregister.co.uk/2018/05/15/met_police_slammed_inaccurate_facial_recognition/. [Accessed: 04-May-2019].

[167] “Welsh police wrongly identify thousands as potential criminals,” *www.theguardian.com*, 2018. [Online]. Available: https://www.theguardian.com/uk-news/2018/may/05/welsh-police-wrongly-identify-thousands-as-potential-criminals. [Accessed: 04-May-2019].

[168] “Police use of facial recognition technology must be governed by stronger legislation,” *theconversation.com*, 2018. [Online]. Available: https://theconversation.com/police-use-of-facial-recognition-technology-must-be-governed-by-stronger-legislation-111325. [Accessed: 04-May-2019].

[169] “Facial recognition database ‘risks targeting innocent people,’” *www.bbc.com*, 2017. [Online]. Available: https://www.bbc.com/news/uk-41262064. [Accessed: 11-May-2019].

[170] P. Mozur, “China turn facial scans into racial profiling,” *The New York Times*, 2019. [Online]. Available: http://iht.newspaperdirect.com/epaper/viewer.aspx?issue=10032019041600000000001001&page=1&article=50412272-c438-4ba1-95e4-024cfb016037&key=o1nbRdCiozl58qCahrDOgA%3D%3D&feed=rss. [Accessed: 22-Apr-2019].

[171] N. Vanderklippe, “Chinese blacklist an early glimpse of sweeping new social-credit control,” *www.theglobeandmail.com*, 2018. [Online]. Available: https://www.theglobeandmail.com/news/world/chinese-blacklist-an-early-glimpse-of-sweeping-new-social-credit-control/article37493300/. [Accessed: 03-May-2019].

[172] D. Z. Morris, “China Will Block Travel for Those With Bad ‘Social Credit,’” *fortune.com*, 2018. [Online]. Available: http://fortune.com/2018/03/18/china-travel-ban-social-credit/. [Accessed: 03-May-2019].

[173] “China to bar people with bad ‘social credit’ from planes, trains,” *reuters.com*, 2018. [Online]. Available: https://www.reuters.com/article/us-china-credit/china-to-bar-people-with-bad-social-credit-from-planes-trains-idUSKCN1GS10S. [Accessed: 03-May-2019].

[174] K. Aquilina, “Public security versus privacy in technology law: A balancing act?,” *Comput. Law Secur. Rev.*, vol. 26, no. 2, pp. 130–143, 2010.

[175] “Body Worn Video Cameras,” London.

[176] Z. Doffman, “Beyond 5G: Huawei’s Links To Xinjiang And China’s Surveillance State,” *www.forbes.com*, 2019. [Online]. Available: https://www.forbes.com/sites/zakdoffman/2019/04/25/huawei-xinjiang-and-chinas-high-tech-surveillance-state-joining-the-dots/#265bb87ecd52. [Accessed: 13-May-2019].

[177] D. J. Robertson, E. Noyes, A. J. Dowsett, R. Jenkins, and A. M. Burton, “Face Recognition by Metropolitan Police Super-Recognisers,” *PLoS One*, vol. 11, no. 2, 2016.

[178] R. Russell, B. Duchaine, and K. Nakayama, “Super-recognizers: People with extraordinary face recognition ability,” *Psychon. Bull. Rev.*, vol. 16, no. 2, pp. 252–257, 2009.

[179] M. Yan, “Facial recognition is almost perfectly accurate — here’s why that could be a problem,” *www.business*, 2019. [Online]. Available: https://www.businessinsider.com/facial-recognition-technology-regulation-creepy-future-2019-4. [Accessed: 13-May-2019].