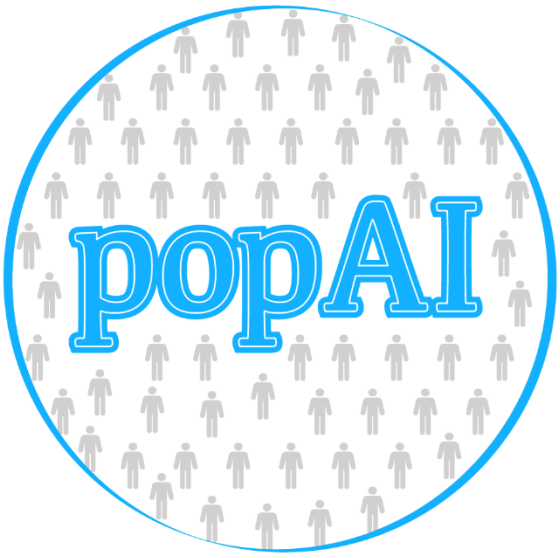

A European Positive Sum Approach towards AI tools in support of Law Enforcement and safeguarding privacy and fundamental rights

D2.3: The controversies and risks that have shaped innovation and will shape AI in the next 20 years.

Grant Agreement ID	101022001	**Acronym**	popAI
Project Title	A European Positive Sum Approach towards AI tools in support of Law Enforcement and safeguarding privacy and fundamental rights		
Start Date	01/10/2021	**Duration**	24 Months
Project URL	https://www.pop-ai.eu/		
Document date	30/11/2022		
Nature	R = Document, report	**Dissemination Level**	PU = Public
Authors	Francesca Trevisan (Eticas), Pinelopi Troullinou (TRI), Eliza Jordan (TRI)		
Contributors	Paola Fratantoni (Zanasi & Partners), Dimitra Papadaki (KEMEA), Gemma Galdon Clavell (Eticas), Carlos Zednik (TU/e), Vincent Muller (TU/e)		
Reviewers	Dimitris Kyriazanos (NCSRD), Andeas Ikonomopoulos (NCSRD)		

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 101022001.

Executive Summary

The development of Artificial Intelligence (AI) has made a big leap in the recent years. Its deployment has become ubiquitous in many public sectors such as education, health and security bringing great promises as well as new risks. Law Enforcement Agencies (LEAs) and Judicial Authorities around the world are among the actors that are increasingly using AI. AI applications (see D2.1) are playing an increasingly significant role in crime prevention and investigation, in migration asylum and border control management, in the administration of justice, cyber operations and LEAs' training (see D3.1). AI applications are used in the security domain for a variety of purposes, with the promise of increasing safety, efficiency, and human capabilities and currently, regulatory frameworks are emerging both from the private and public sectors in the form of soft and hard laws (see D2.2). Nonetheless, AI engenders challenges that prompt social debates questioning how these technologies are being employed and whether they respect human rights. Public trust has been undermined by a lack of transparency and accountability and by the power asymmetry that characterize those who employ AI technologies and those who are subjected to it. Democratic oversight of AI is sunrising, under mounting evidence of how AI in the security domain can be misused, infringe rights, while reinforcing discrimination and historical biases.

To foster trust in AI, and for a more efficient development and use of AI in law enforcement, it is important to identify how technology is socially constructed from its development to its deployment. To achieve this goal, this report documents the past and present social controversies that have characterized technology and innovation in the security domain and beyond. After an introduction outlining the topic discussed, this report debunks the myth of technology backlash and shows how social controversies are a tool of tech democracy that shape innovation from its development to its deployment and change. It shows how social controversies are essential to de-black-box technology as they allow to identify the meanings that people attribute to innovation, its risks and to create new strategies address them. These meanings urge creators, organizations, and consumers to produce and use more responsible and sustainable technologies that meet societal demands. The report also demonstrates how artefacts are socially and technically constructed and how examining social controversies allows for the development of new tech and governance models. This analysis is supported by a series of case studies that show in practice how technological development is shaped by more forms of agency, change and causation that mesh the social and the technical. The case studies revealed a series of recurrent themes that developers, users and policy-makers shall take into consideration for a better management of risks related to technology adoption and creation.

Table of Contents

List of Figures

1 Introduction

PopAI is a 24 month Coordination and Support Action (CSA) project funded by Horizon 2020 and undertaken by a consortium of 13 partners from 8 European countries. PopAI aims at bringing together security practitioners, AI scientists, ethics and privacy researchers, civil society organisations as well as social sciences and humanities experts with the purpose of consolidating knowledge, exchanging experience and raising awareness in the EU area. The core vision of PopAI is to foster trust in AI for the security domain via increased awareness, ongoing social engagement, consolidating distinct spheres of knowledge (including theoretical & empirical knowledge by academics & non-academics) and offering a unified European view across LEAs, and specialised knowledge outputs (recommendations, roadmaps), while creating an ecosystem that will form the structural basis for a sustainable and inclusive European AI hub for Law Enforcement.

AI systems need to be considered "socio-technical" systems, meaning that their development, employment and impact depend on technical factors, such as the design, as well as social factors such as the cultural and political context in which the system is developed and employed. To create a sustainable and inclusive European AI hub for LEAs, it is important to look at how the social and technical factors of technology interact. To this end, this report presents the controversies and risks that have shaped innovation and will shape AI in the next 20 years.

1.1 Scope and objectives of the deliverable

Work Package 2 “Security AI in the next 20 years: trends, practices and risks” builds on the existing state of the art in relation to the use of AI by LEAs in Europe and elsewhere to identify:

1) the actual AI use and technical characteristics of AI tools in the security domain (T2.1);

2) the legal frameworks and recent court rulings (T2.2);

3) how controversies have shaped technology adoption in the security domain (T2.3);

4) the ethical principles and challenges that can inform a practical ethics toolbox (T2.4);

5) the organisational issues around AI implementation in LEA contexts (T2.5).

Task 2.3, "The Controversies and Risks that Have Shaped Innovation and Will Shape AI in the Next 20 Years" (D2.3), explores the "technology backlash," a situation in which technological innovation is being treated with skepticism by the populace, particularly in the security area. It is claimed that technologies that generate distrust frequently end up being abandoned at a significant reputational cost to its proponents. The history of innovation-related controversies is examined in this paper. Additionally, the most recent and important debates surrounding the use of technology by LEAs are

covered. In order to understand and record the various dynamics that emerge around various technologies, this scoping in particular attempts to make sense of the various scenarios and tensions that generate debates.

A robust understanding of how controversies have shaped technological adoption in the past and currently is an invaluable resource for those seeking to understand how technology evolves and is successfully integrated into policing practices. The work in the task is complemented by the work in WP3, where empirical research is conducted for a more dynamic understanding of the potential trends that will shape this space in the near future. For anyone interested in learning how technology develops and is successfully incorporated into policing tactics, a thorough understanding of how controversies have affected technological adoption in the past and currently is a useful resource. The work in WP3, where empirical research is undertaken for a more dynamic knowledge of the prospective trends that may shape this space in the near future, complements the work in the task.

1.2 Structure of the deliverable

This deliverable is organised into four main sections.

Section 1 introduces the main topic discussed in the deliverable, outlines its scope and explains how this work relates to other PopAI tasks and deliverables.

Section 2 explains why looking at social controversies is key to shaping tech imageries. Controversies help to understand technology and its development. They suggest challenges and risks, drive technological development and inspire new models of governance that help employ sustainable and responsible technologies that fit societal needs. The section shows how social controversies democratise technological development and how technology is socially constructed.

Section 3 shows in practice how social controversies open up the technology black box. The section presents current and past social controversies in the security domain and beyond, to demonstrate the interaction between the social and technological spheres and the significance of examining social controversies for effective technology development and governance. It also indicates recurrent debates across history, sectors and technologies. These controversies revolve around transparency, training, oversight, privacy, and discrimination.

Finally, section 4 provides a discussion and some key recommendations in terms of risk management.

1.3 Relation to other tasks and deliverables

This report is the outcome of task 2.3 "The Controversies and Risks that Have Shaped Innovation and Will Shape AI in the Next 20 Years". Overall, this study contributes to the PopAI project by explaining why and how it is crucial to consider social controversies when creating new security-related

technologies, introducing them, and building new governance models. It expands upon D3.1 Map of AI in Policing Innovation Ecosystem and Stakeholders, which provided early insights into current debates surrounding AI in crime prevention, crime investigation, cyberoperations, and migration, asylum, and border control. Task 3.3, "Citizen produced priorities and recommendations for addressing AI in the security domain," Task 3.4, "Stakeholder attitudes, priorities, and recommendations for addressing AI in the security domain in practice," and Task 3.5, "Foresight Scenarios for AI in Policing," are all supported by the controversies mentioned in this report. Additionally, the controversies identified in this task serve WP4's recommendations to civil societies, LEAs, and technology developers.

1.4 Methodology

D2.3 aims to examine the history of innovation-related controversies as well as the most recent and important debates surrounding the use of technology by LEAs. To this end, this report has been produced after a thorough review of both academic and grey literature to which all research partners contributed.

The sources of information can belong to broader five categories:

- **Scientific Publications**: Collection of publications in scientific journals, conference/workshops proceedings and scientific book chapters.
- **Gray literature**: magazines and newspaper articles.
- **Official report:** work published by public and private institutions in a report format.
- **Legal Frameworks**: Information related to regulations that regard technology and innovation.
- **Advocacy work**: work produced by organizations for advocacy purposes.

The collection of information was accompanied by the creation of case studies of recent and past social controversies that are discussed in the second section of the report. The identification of central themes discussed in section 3 emerged through a keyword exercise. When compiling the case studies, researchers noted recurrent keywords and the most used have been selected to shape the recommendations on risk management for LEAs.

2 Why do we need to look at social controversies?

We use the word "innovation" to describe brand-new inventions in technology, goods, and services (Chiesa & Frattini, 2011). However, prior to its connection to technology, innovation was a contentious concept that did not necessarily have a positive meaning in politics, art, philosophy, religion, and social affairs (Godin, 2015). In ancient Greece, novelties in arts and knowledge were accepted only when they did not change the natural order of things, but innovation (*kainotomia*) was not tolerated in any circumstances because it was linked to political subversion and instability (Godin, 2019). By the fourth century, the term "innovo" was introduced to the Latin vocabulary and became a positive concept used in religion, poetry and law to refer to the start of a new order without necessarily introducing anything new. With the Renaissance and the raise of awareness of people's capacity to change the course of history, innovating was seen as mean to achieve progress (Godin, 2015). However, In the 16th century following the English Reformation the term "innovo" shifted back to its negative connotation. For example, Edward VI, King of England, issued "A Proclamation against Those that Doeth Innovate" which admonished not to innovate and imposed a fine on offenders (Godin, 2010). In 1636 an English Puritan and royal official was accused of being an innovator, had his ears cut and was sentenced to life imprisonment. Innovation started to take hold as a term linked with science and industry in the nineteenth century, reflecting the forward march of the Industrial Revolution. With governments starting to frame research as a source of economic advantage and competitiveness, innovators were elevated as positive contributors to society. Godin argues that the word "innovation" assumed a positive connotation with the work of the Austrian-American economist Joseph Schumpeter (1942), who made the case in his 1942 book "Capitalism, Socialism, and Democracy" that technological innovation drives economic progress, causing processes of "creative destruction" that sweep aside dominant players and make room for new ones. The definition of innovation changed over time to mean the commercialisation of technological inventions. This was related to government support for Research & Development in foundations and laboratories (Godin, 2019). It was in between the 1950s to the 1980s that innovation started to be understood as a process that involved scientists and research from theoretical lab, followed by the development of new functionalities and eventually their commercialisation.

The history of innovation reveals that the concept is intrinsically controversial and ambivalent. In the field of technology, the extremes of this ambivalence are represented by technological optimism and technological pessimism (Basiago, 1994). While techno-optimism contends that technology promises positive advancements that will improve and reshape society (Krier & Clayton, 1985), techno-pessimism asserts that technology evolves also in negative ways, posing new threats and harms to society (Tigard, 2021). With the prevailing discourse on innovation being imbued by technological optimism (Birhane et al., 2022), those who show skepticism or oppose the adoption of new technologies are generally looked down on, as they seem to oppose a technological progress that brings more goods than harms (Hauschildt, 1999). This is partly explained by how we picture technological development. In the mainstream discourse, the word "technology" tends to be equated to something engineered and black boxed (Ada Lovelace Institute, 2020). Following evolutionism, we

tend to believe that technologies pass through two screens that automatically eliminate the worse contributions and allow the best to emerge (Noble, 1995). The first screen is the technical or scientific one, where the work of scientists scrutinizes all possibilities and rationally selects only the best solution to any given problem. The second is the economic filter that rules out all the non-economically viable technologies to leave those that are technically superior. We believe that this process make technology free of values and morals, we dignify technological innovations as the highest expression of technological progress, and we accept them as inevitable (Noble, 1995).
Nevertheless, the ambivalence toward technological progress is legitimised when we recognise that technological progress is not inevitable and value-neutral but reflects social, political and cultural values (Eubanks, 1018). Innovation and technologies are not neutral tools that facilitate efficiency and improve life quality but contested instruments that respond to specific needs and carry specific ideological preferences.

Technical tools have political qualities: for instance, at the beginning of the 20th century, bridges in New York were low by design to stop buses from poor black neighborhoods to access white middle-class areas (Winner, 2004). Technologies can pursue values that might harm or compromise some social groups and have been deployed to discriminate, threaten and maintain a power structure from the outset (O'Neil, 2016). Furthermore, technology can pursue different values at the same time that cannot be satisfied simultaneously and require a trade-off (Van den Hoven et al., 2012). A trade-off decision needs to carefully evaluate different viewpoints and meanings that technology acquires for different social groups. As such, opposition to technology is not only legitimate but it is also necessary. Opposition to new technologies allows citizens to participate in the development and introduction of new technologies, and identify new issues and potential solutions (World Economic Forum, 2018). By opposing technological innovations at different levels, citizens open controversies, give voice to their needs, defend their rights and envision desired alternatives to the current social and technological landscape. These imaginaries play a significant role in shaping technological progress by affecting the trajectory of new technologies, their acceptance, adoption, governance and tradeoffs decisions. By doing so, social controversies democratise technological development and are themselves a source of innovation. The sections below will explain why social controversies are important and how they shape the development of new technologies and their regulations.

2.1 The silver lining of technology backlash

Historically, technology and innovation have led to major disputes over their benefits and risks. Between the end of the 18th century and the beginning of the 19th century, Britain and France were stormed by violent movements against the promotion of mechanised production. In France, these movements discouraged entrepreneurs from introducing new technologies while in Britain, the revolts were repressed to support innovation (Horn, 2005). In Britain, between 1811 and 1816 the Luddites radically opposed the introduction of machines in the textile industry. They were attacking and burning factories, hoping that their action would have discouraged employers from buying new machines. Nowadays Luddite is used as a derogatory term to describe people who dislike new

technologies (Sykes & Macnaghten, 2013). The Luddite action was not seen as the result of a process of clear reasoning. However, their action had a profound rationale: technological innovation was leaving trained artisans unemployed and was consolidating the wealth and power in the hand of a small number of mechanised manufacturers (Binfield, 2004). Innovation was causing fear of unemployment and poverty which was fuelling social turmoil.

The innovations and technologies that we now take for granted have endured and have been shaped by times of social unrest and dispute. Yet, it is not only the arrival of a new technology that is characterised by social disputes. All stages of a technology's life cycle are marked by social debates, and as technology develops, so do the conflicts that surround it. The case of cell phones is a good example: in the 1990s, early models of mobile phones came with great concerns around health risks (Burgess, 2004) while now they are also a privacy battleground (Klosowski, 2022). We frequently overlook the social conflicts that accompanied technological adoption or demise and instead celebrate the innovations that have revolutionized the world (Halls, 2014). However, ignoring social controversies contributes to a black box vision of tech by ruling out citizens' voices and understandings from its processes. This is another reason why it is critical to examine the public debate and understand the drivers of acceptance or resistance. People resist technology for various reasons (Oreg & Goldenberg, 2015):

- Because of the individual's dispositional orientation toward change. For example, the innovation itself could make someone feel threatened.
- Because the innovation jeopardizes people's rights, security, or expertise. Innovation might pose a threat to civil rights (such as privacy), health as well as to jobs.
- Because of the quality of information around innovation and how the innovation is presented. Information around innovation might not be transparent enough or accessible. As a result, when innovations are introduced, individuals may not understand them, they might not recognise when and how advantages outweigh risks or they might not feel engaged.
- Because of the cultural societal and economic setting in which the innovation is introduced. This includes national regulations, norms, values and culture that can increase and decrease the perceived threat.

Technology and innovations often acquire special social meanings: they are the target of often unrealistic expectations and fervour that anticipate the emergence of a new social order characterised by greater equality, prosperity and harmony (Winner, 2004). Or they are seen as a dystopic alternatives that channel reality toward new challenges and risks (Winner, 1997). People envision new technologies as a potential solution or possible problem for society, and project many different hopes and fears into them (Sturken et al., 2004). New technologies chart people's aspirations and preoccupations that are translated into visions that affect how technologies are designed, employed, made sense of, and integrated into people's lives. Innovation can bring about new functionalities and abilities which can result in economic competitiveness, new jobs and consequently economic growth. Innovation brought society electricity, antibiotics, clean water, sanitation raising dramatically human life expectancy (Wei, 2012). However, innovation and

technology are not always positive in itself. There are many instances of innovation that at first glance appeared to be beneficial but eventually gave rise to moral problems such as insecticides containing DDT and construction materials containing asbestos. Therefore, seeing technology resistance with a negative outlook is generally very simplistic and prevents us from seeing its silver lining. Luddism, technology backlash and resistance are essential to identify new problems, challenge developers, organisations and users to create and employ sustainable and responsible technologies that fit societal needs. Controversies on new technology do not halt progress, but they enable public participation in the technological evolution (Horst, 2010). Public rejection of technology and controversies about ethical, legal negligence or harmful use emphasize what needs to change and allow new imaginaries that help to articulate the answers to ethical, legal and social risks, but most of all, they show that technology is socially constructed and therefore, socially carved.

2.2 The Social Construction of Technology

Many accounts of how technology and innovation develop treat the technological artefacts apart from the social. However, the design of new technologies is in constant interplay with the social arrangements that inspire or support their creation. Bikes, cars, mobiles, computers drugs, building materials and other artefacts would not be on the market without the network of social roles and practices that surround them. These include scientists, engineers, designers, big corporations, politicians, regulators, civil societies, patents, trials, studies, trademarks, advertisements, users and countless other actors and practices. Seatbelts for example were first used to keep people inside during bumpy rides and had little to do with safety (Gantz & Henkle, 2002). Through the 60s and 70s, the auto industry believed that the emphasis on safety would scare the public and deter from buying cars. Yet, a number of legislators and activists brought auto safety to the public eye. Sealtbelts were raising a number of controversies: they could cause internal injuries, they prevented easy escapes from cars, and the device frequently failed (Roos, 2020). As a response, carmakers agreed to add a release latch. In Europe, the European New Car Assessment Programme (Euro NCAP) was introduced in the late 90s and thanks to the car industry's response to it, the road death toll in EU-28 reduced by a quarter despite a growth in traffic volumes (van Ratingen et al., 2016). Therefore, the car as we know it is the result of the work of the car industry, regulators and the public debate.

The question of whether technology is causing society or whether people are causing technology has long been the focus of studies on technological development (e.g. Morison, 1968) and is central to The Social Construction of Technology (SCOT). SCOT derives from Science and Technology Studies (STS) and contends that human behaviour, in conjunction with the social, economic, and political context, shapes technology (Pinch & Bijker, 1984). In other terms, there is no technology without humans. Society and technology are mutually dependent, and social and technical factors interact to determine the trajectory of new developments and innovations (Law & Callon, 1988). Technologies and innovations shape the world we live but it is the individual who creates the technology and decides its purpose, utility, meaningfulness and its acceptance. Based on individual and socio-cultural factors, people interpret technologies in different ways and their interpretations direct technological

development to fruition or defeat (Chiesa & Frattini, 2011). This perspective on technological development resists technological determinism, which holds that technology develops in accordance with its own inherent logic of efficiency, influencing societal change and the formation of the social structure (Bimber, 1994).

Understanding the social context and controversies around artefacts is crucial for comprehending why and how technology is or should be developed, governed, adopted, or rejected, as well as how, as a result, technology changes. Without focusing on how technology is integrated into the social context, it is hard to comprehend how technology evolves and how it is used. The social context around technology is defined by a number of social groups that hold a stake in that technology (Pinch & Bijker, 1984). Social groups include institutions (e.g. academia, governments), organisations (e.g. civil societies) or organised or unorganised groups of individuals (e.g. women, children, the elderly). Each social group share a meaning attached to a specific artefact that is influenced also by the wider socio-cultural and political situation (Mohamed et al., 2020). These social groups include citizens, users, politicians, technologists, scientists, developers and may more (Geels, 2004).

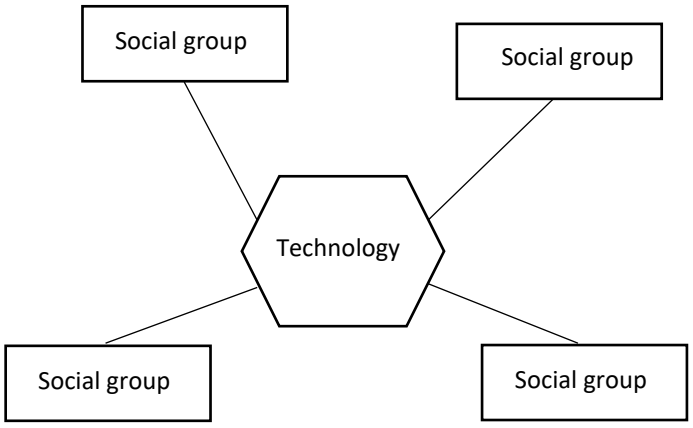

Figure 1: Each social group interpret a new technology in different ways. Adapted from Pinch & Bijker, 1984.

For each social group, the innovation will play a specific function and each social group will interpret the innovation with different problems and solutions while attaching to it specific meanings (Pinch & Bijker, 1984). These meanings interact to drive and shape the progress and adoption of new technologies through their acceptance, rejection, and governance.

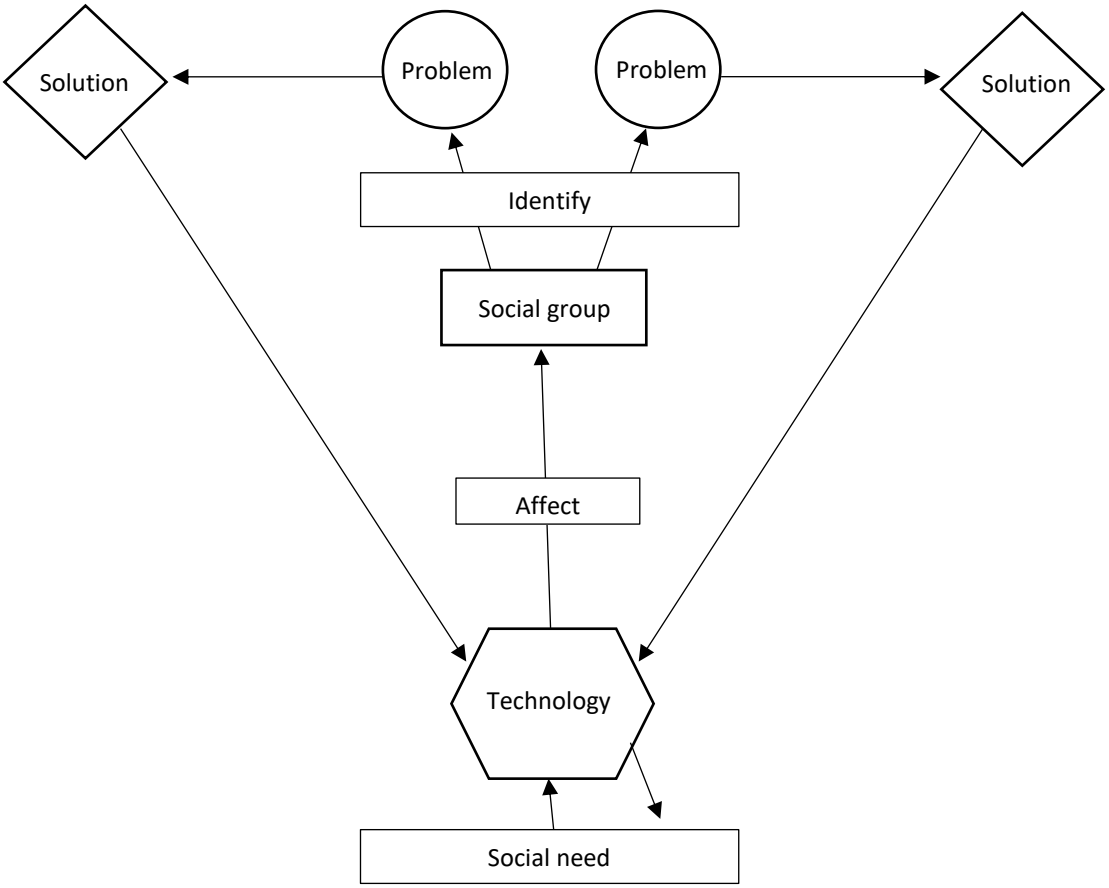

Figure 2: How a social group shape technological development. Adapted from Pinch & Bijker, 1984.

The interplay of the meanings attached to technologies by different social groups sparks social controversies that reveal the interpretative flexibility of innovation. With interpretative flexibility, SCOT suggests that new technologies can be interpreted, thus shaped, in different ways (Pinch & Bijker, 1984). Therefore, studying the controversies around emerging technologies demonstrates that technological artefacts are socially and culturally constructed from their design to their employment. There is not just one possible way or one best way of designing an artefact since different social groups of users and developers have radically different interpretations of it. Finding the relevant social groups for a new technology and looking into how the meanings they attribute to technology interacts are crucial steps to understand how technology evolves. This method aids to bring out all the viewpoints on technical difficulties (e.g. difference in error rates for gender classification in facial recognition), their social causes and effects (e.g. discrimination), and the moral and legal standards they have to comply with (e.g. privacy, transparency, non-discrimination).

Different resolutions to these conflicts and issues are feasible from both a technological and a moral perspective. Strategies to resolve controversies involve developers to redesign the system, and users, citizens, technologists, regulators considering new governance models and marketing campaigns (Pinch & Bijker, 1984). In this way, technological development is shaped by more forms of agency, change and causation that mesh the social and the technical. The social and the technical world exists in a constantly shifting network of relationships and change (Latour, 2005). Interpretations of technology cannot be separated from the technology itself, otherwise, we objectify the technology (Latour, 2005). Acknowledging that technology is culturally and socially construed empowers people because it distributes agency (Callon, 1984; Latour, 1987). Applying the controversy perspective to the dominant understanding of technology draws attention to the relationship between the social and the technical and allows to act more efficiently on the technical. Social controversies around technology are far from being a barrier to technological adoption. Instead, they are an active part of the innovation process and they allow to:

1. **Examine** technological progress through the analysis of multiple meanings attached to technologies;
2. **Challenge** the conception of technology as an antidemocratic force that self-regulates following its internal logic,;
3. **Identify** the trends and patterns around technological progress;
4. **Rethink** technology as a social process of co-creation;
5. **Tackle** issues arising from new technologies more efficiently;
6. **Inspire** new projects under development and new model of governance;
7. **Manage** risk.

In the next section, we will provide a range of case studies showing in practice how the social and the technical shaped each other in the security field and beyond. This exercise highlight recurrent social interpretation of new technologies and emphasize how they affected their development, governance, adoption, and demise.

3 Case studies

This section presents key current and past social controversies to demonstrate the interaction between the social and technological spheres and the significance of examining how society responds to technology for effective development and governance. It also indicates that there are persistent debates that are frequently discussed across a variety of views, sectors, technologies, and timeframes. The recurring themes will be discussed in the conclusion section of this report.

3.1.1 Google Glasses

Google Glass (GG) is a brand of smart glasses developed by X - formerly GoogleX, a research lab specialized in technological innovation. On its website, X is advertised as a creator of "radical new technologies to solve some of the world's hardest problems" and a "diverse group of inventors and entrepreneurs who build and launch technologies that aim to improve the lives of millions, even billions, of people"[1]. Yet, GG fueled the privacy debate when they were first launched in the US in 2012. Prior to GG launch, Google CEO Eric Schmidt said "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place" (Esguerra, 2009). By 2011, Google had already been several times at the center of the debate when privacy groups asked regulators to investigate how privacy was protected in Google mailing service (Orlowski, 2004) and in Google data collection for Street view mapping (Epic, 2007).

In April 2012 a "Project Glass" account appeared on Google Plus[2]. The first post of this account unveiled the purpose of the project: to build a wearable computer that help to "explore and share the world". Initially Google advertised GG as experience augmentation where people could share their experience with others (Google Developers, 2012). Then, Google added some user-friendly information icons appearing on screen (Google, 2012). GG was a wearable, voice and motion-controlled Android device that resembled a pair of eyeglasses and showed information to the user. GG could show text messages, maps, reminders, video chats, provide directions, take photos and video through voice commands (Google, 2012). The first product was made exclusive: in June 2012 Google opened the pre-orders to the Google Glass Explorer Edition only to developers at the price of $1,500 with the delivery planned for early 2013 (Savov, 2012) but some prototypes were made available in late 2012 (Stern, 2013). Developers, could wear them and test them around the city and some of them were spotted in New York (Davies, 2012). Google called these developers "Glass Foundry" and said to be looking forward to see what they would do with GG (Stern, 2013). Following this first test, in February 2013 Google launched a social media campaign "If I had Glass" asking Twitter and Google+ users what they would do if they had a Google Glass (Souppouris, 2013) and people with the best answers would have been selected to have the opportunity to buy for $1,500 the Explorer edition of GG (Bean, 2013). In May 2013, Google released 2000 more test versions to

[1] https://x.company
[2] https://plus.google.com/111626127367496192147/posts/aKymsANgWBD

developers and another 8000 people winning the contest were planned to receive them (Streitfeld, 2013). The consumer version became available in 2014 (Stein & Turrentine, 2013)

GG had been made available to the general public when smart devices and button-free commands became the highlight of the debate in the tech industry as they were offering a hand-free tool to perform tasks. However, GG initial plan failed on the market. Reduced sales and public controversies led Google to abandon the GG plan as it had been imagined at the outset. GG was considered by the public a form of ubiquitous recording: the camera on GG could be activated by users at any time without people around knowing it because there was no external light indicator to show when GG was recording (Soper, 2013a). Consumers were also worried about the device collecting data from them, making them vulnerable to hacking. GG also provoked a series of negative reactions from the public and bans that made their way to news headlines (Soper, 2013a). While glasses were not yet available for purchase In March 2013 a bar in Seattle was the first to ban the use of GG. The owner of the bar explained that "First you have to understand the culture of the 5 Point (...). People want to go there and be not known, and definitely don't want to be secretly filmed or videotaped and immediately put on the Internet." He said: "Part of this is a joke, to be funny on Facebook, and get a reaction. But part of it's serious, because we don't let people film other people or take unwanted photos of people in the bar, because it is kind of a private place that people go to." (Soper, 2013b). Customers were kicked out from cafes (Soper, 2013a) and in several states, GG was not allowed in casinos (Parry, 2013). In May 2013 a petition was put together asking White House to ban the devices until regulations could be put in place (Maxham, 2013). In December 2013 in Florida a person wearing GG having breakfast in a bakery was confronted by a stranger asking whether they would have been comfortable with him recording a video violating their privacy (Kelly, 2013). In January 2014 a person wearing GG was interrogated in an Ohio movie theater by the FBI for wearing GG. He had been accused of recording the movie on his device. He claimed he was not recording but he was not believed. The FBI downloaded the GG content in the computer and after checking all of them they concluded he did not do anything wrong. In June 2014 the Alamo Drafthouse, a movie theater chain, banned GG use for piracy problems (Matyszczyk, 2014). In October 2014 The Motion Picture Association of America and the National Association of Theatre Owners officially banned the use of GG and other wearable recording devices in the cinema as part of an updated "anti-theft policy" (Gayomali, 2015). In January 2014 A woman speeding in San Diego was fined for wearing GG while driving as the device was considered a distraction like any other monitor (Graham, 2014). In December 2013 Illinois was considering banning GG in cars (Servantes, 2013).

A group called Stop the Cyborgs offered free anti-glass icons on their website for businesses that wanted to notify customers that the technology was not allowed. Stop the Cyborgs was also concerned about the massive collection of data through GG. In their page they said that the issue was the control over the data. They pushed against GG to stop a future in which "privacy is impossible and central control total" (Farivar, 2013).

In January 2015, only three years after their launch, Google stopped selling Glassesand In January 2016 it erased all the social media channels dedicated to GG and in X, the failures of the launching program are not mentioned (Collins, 2016). The central objection to GG was moved by privacy-related concerns (Arthur, 2013). Others pointed to the lack of clarity on why the product existed and what solutions was giving to users, their aesthetical unappeal, and bad marketing (Leonard, 2022).Today, Glass is advertised on the X website as a "lightweight wearable computer with a transparent display for hands-free work"[3] so X re-targeted the device to businesses that want to improve the quality of their output and "help their employees work smarter, faster and safer". There is voice-activated assistance and they are advertised for helping workers to stay focused, to improve accuracy and collaborate with co-workers in real time.

3.1.2 Smart Meters

Despite Smart meters for electricity have received acclaim as a device that would help to attain more sustainable and resilient electricity consumption, the public opposed to this device in several countries like Canada and North America, Austria, The Netherlands, The UK, Italy, Spain (Hess, 2014). The main issue was that the devices were distributed and developed without a proper legal framework and an assessment on the potential impacts of this technology on people privacy.

Smart grids are defined as “an electricity network that can cost efficiently integrate the behaviour and actions of all users connected to it – generators, consumers and those that do both – in order to ensure economically efficient, sustainable power system with low losses and high levels of quality and security of supply and safety”[4]. Smart meters are key component of smart grids as they allow to measure the consumption of energy and potentially transmit the information to utilities companies[5]. Smart meters are installed in homes and provide power companies with an accurate and streamlined method of monitoring reading and controlling a home's power usage. Smart Meters are able to measure energy consumption by appliance every 12 minutes or even less -even on a minute basis-, capturing information on how people spend the energy on a real time basis. The monitoring can occur by room, appliance and outlet and it is estimated to monitor between 750 and 3000 data point per month. Appliances like heating, cooling systems, refrigerators, pc, toasters account for the majority of residential energy usage, managing this energy consumption can impact the energy load at any time of the day. This is why manufactures have begun to enable these appliances to communicate with smart meters. Appliances continually send their energy usage labeled as consumption by that appliance. The smart meter reads that communication from all smart appliances and can generate a load signature for each home. Users can see their consumption and anyone with access to residents' display or website can determine the time a person arrives and leave home, if the security system is activated, if someone use microwave or stove, or how much television is watched. Smart meters are

[3] https://www.google.com/glass/start/
[4] https://s3platform-legacy.jrc.ec.europa.eu/smart-grids#:~:text=A%20Smart%20Grid%20is%20an,and%20security%20of%20supply%20and
[5] http://ec.europa.eu/growth/tools-databases/mandates/index.cfm?fuseaction=search.detail&id=475#

also able to recognise electric vehicles so if someone charge the car to a frined house this would be registered by the smart meter.

With smart grids and smart meters, the energy traffic is two ways making the communication among consumers, households or companies, other grid users and energy suppliers interactive. and have been defined as "the backbone of the future decarbonised power system"[6].
However, frequent smart meter data collection comes at the cost of user privacy: smart meters systems can be vulnerable to viruses, malware, phishing, and user errors that compromise integrity (Luthra et al., 2014). In fact, the information collected on electricity consumption can also be used to estimate the composition and behavior of individual households (NIST, 2010) and with a two way communication is two ways, utility companies are enabled to remotely control smart appliances within homes. The consumption reveals details of personal life in the most privacy sensitive place: the home. Additionally, smart meters are related to an address. Therefore, data sent from the meters is personally identifiable.

With the rush to install residential smart meters, privacy experts and governmental agencies in the early 2010s were alerting to be cautious until privacy implications for smart meters could have been addressed. While the legal framework was being shape, smart meters started to be developed and rolled out in several countries. The Legal and social challenges of implementing smart grid technology in Europe were the lack of regulatory framework for the technology and the privacy of the data and low public awareness(Luthra et al., 2014). The public objections to Smart meters suggested that privacy cannot be underestimated and that a privacy by design approach and a privacy impact assessment are vital for new devices to be accepted by the public and to comply with Data protection laws.

In 2009 the European Union enacted the Electricity Directive and the Natural Gas Directive which recommended the installation of smart meters to promote energy efficiency and to help to meet Europe 2020 goals on reducing emissions and energy consumption[7]. To advise on policy and directions for the installations of Smart Grids in Europe, the EC set up a Smart Grids Task Force to set up the foundations for smart grids in Europe. The Smart Grids Task Force had to set of regulatory recommendations to ensure EU implementation of smart grids[8]. If the balance between costs and benefits for markets and consumers was positive after an economic assessment by September 2012, the Electricity Directive stipulated that at least 80% of consumers shall be equipped with smart meters by 2020. In 2011 it was also planned to develop legal and regulatory framework in

[6] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0202:FIN:EN:PDF
[7] Directive 2009/72/EC concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC. http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:211:0055:0093:EN:PDF and https://www.ceer.eu/documents/104400/3751729/E09-EQS-30-04_SmartGrids_10+Dec+2009_0.pdf/c481db2a-3cfb-6d6f-4b58-da3dee68de4a?version=1.0

[8] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0202:FIN:EN:PDF

collaboration with the European Data Protection Supervisor to protect consumer privacy and make it easier for them to access and control the data that third parties are processing about them.

The Dutch Senate blocked two smart meter billings in 2009 (Cuijpers & Koops, 2013). To comply with the EC directive, in 2008, two smart meters bills in the Netherlands proposed the mandatory introduction of Smart meters in every Dutch household. According to this bills, refusing to install the smart meter was sanctioned with a fine up to 17000 euro or imprisonment for 6 months. Data would have been collected hourly for gas and quarter-hourly for electricity and forwarded to energy suppliers. The Dutch proposals included the signaling function which would have enabled providers to detect energy quality and the switching function, which enable network operators to switch capacity on and off for fraudulent customers or in case of disasters. THE DDPA (Dutch Data Protection Authority) had been involved in the case after some privacy concerns were raised after the bill was submitted. The DDPA deemed the proposal for the Dutch metering act to violate the Dutch Data Protection Act as it was not clear who hwould have processed and accessed the data. The Minister of Economic Affairs amentded the proposal including that data would have been transfered to energy supliers if consumers had given the consent, the DDPA adeemed the legislation compliant with the DDPA and in 2008 the second chamber passed both smart metering bills without any further privacy debate.

The Dutch consumer Union was not convinced about the privacy issues and commisioned a study to test whether the smart metering legislation was in conformity with article 8 ECHR. The report, published in October 2008 highlighted that quarte-hourly/hourly daily detailed smart meter readings were able to suggest information about lifestyle and presence or absence and number of persons and this was an infringement to privacy. Smart meters were challenging principles of informational privacy and the right to inviolability of the home and right to respect for family. The report concluded that the generaion and trasmission of quarter-hourly/hourly readings to grid managers, the daily readings to managers and suppliers and the compulsory roll out of smart meters were not proven to be necessary in a democratic society. The introduction of smart meters was violating article 8 of the ECHR. To meet the privacy compliance test there needed to be more empirical ebidence about the prevalence of energy fraud. It was also not clear how SM contributed to saving energy and why consumers needed to go on the computer to view their meter readings instead of seeing them on the device at home. To justify the breach of involability more empirical data requested.

The Dutch first Chamber discussed the outcome of the report and all concerns raised by the media. The chamber was not convinced and in 2009 decided not to accept the proposed legislation unless with changes. In 2010 the novelles (amendments) were introduced. Grid operatos could not collect a continuous stream of measured data but they had to attain a standard measurement regime. One of the major changes was to grant consumers the right to refuse a smart meter without fines or imprisonement. Moreover, they were granting the right to ask operators to shut down the smart meter which would have allowed stop reading data of an end user. Furthermore, the collection of consumers metering data was made explicitly tied to their legally prescribed task such as belling

by suppliers and network management by the grid operator. The novellas was passed in Novemebr 2010 and was accepted by the first chamber in February 20011.

As highlighted by (Cuijpers & Koops, 2013) the main issues related to the rejection of the bills were:

1. the very detailed readings of smart meters and the transfer of these readings from consumer to grid operator and (of less but still) detailed readings from operator to energy supplier;
2. the compulsory nature of the roll-out, sanctioned by a hefty fine or even imprisonment.
3. a lack of substantiation why the privacy infringement and the compulsory roll-out were necessary;
4. the combination of different functionalities in one smart meter, creating a complex hybrid involving new risks and also confusing the argumentation for the necessity of such a smart metering system.

In the UK People have organised campaigns against Smart Meters for different reasons: information privacy, radio waves, economy, and inaccuracy[9]. Some initiative against smart meters were: Stop Smart Meters! (UK)[10], Smart Meter Dangers[11]. With the public pressure, the UK Government required energy suppliers to install smart meters for their customers and set out rules around: data access, security, technical standards for the smart metering equipment, meeting the needs of vulnerable customers. In the UK smart Meters will be rolled out as standard across the country by 2024 but there will be no legal obligation on individuals to have one unless the existing meters is faulty. In terms of consumer privacy, consumers will have a choice about how the energy consumption data is used, apart from where it is required for billing and other regulated purposes such as theft detection. Consumers will be able to see the real-time energy consumption data on the display. The electricity stores 13 months of measurements data taken at half hourly intervals which are available to llook at. Custmoers are able to share data with third parties if customers want advices on best tariff.

[9] https://www.smartme.co.uk/campaigns-against.html
[10] https://stopsmartmeters.org.uk/
[11] https://smartmeterdangers.org/

3.1.3 Early controversies on Biometrics: from Anthropometry to Dactyloscopy

This section dives into history to discuss the development of and controversies around two technologies that appeared in the late 19th century with the promise of identifying criminals. The first one is Anthropometry, the science of physical measurement of the size and proportions of human bodies for identification. The second is Dactyloscopy, or the science of fingerprint identification. These two innovations were developed around the same time to solve similar problems in different socio-political contexts and under different premises. While anthropometry was first created in Europe, fingerprinting developed in the colonies of the Western imperial states (Cole, 2002). These two different origins and the sociocultural meanings attached to them shaped the initial development and adoption of the two innovations.

3.1.3.1 Anthropometry

The first instance of a biometric identifying system was documented in France in the 1800s when Alphonse Bertillon created his anthropometric system, named Bertillonage, for categorizing and comparing criminals using body measurements. In the middle of the 19th century, France seemed to have a high rate of recidivism, but it was impossible to access information and search for offenders in long lists of names if multiple jurisdictions, with lots of alias no other information (Sekula, 1986). In 1851, The French government created a law to exile recidivists to the colonies and Bertillon invented his identification and categorisation system to enforce the law. With his system, providing that a person had been Bertillonaged before, any repeat offender could be identified, and their criminal record retrieved. Bertillonage had a wide success because it was facilitating the identification of suspects and was adopted in England, Austria, Russia, Canada, Argentina and in a variety of states in the US. Part of its success was due to the fear of political radicalism and anarchist terrorism (Quinn, 2016). In 1898, at the International Anti-Anarchist Conference in Rome, organised in response to a wave of political assassinations that saw the death of the
President of France, the prime minister of France, the king of Italy, and the empress of
Austria, a highly secret committee of police chiefs and representatives endorsed Bertillonage to create a standardized identification system across Europe in order to track international terrorists and radicals. By 1899 Germany, Belgium, the Netherlands, Spain, Italy, Russia, Sweden, Norway, Turkey, Monaco, Luxembourg, Romania and Switzerland had all adopted an anthropometric identification. Anarchists were
targeted, surveilled, and arrested across European borders through a police apparatus that
operated through a nodal network

The Bertillon system was based on a variety of physical measures, taken with designed tools and by trained "Bertillon operators" (Rhodes, 1956). The assumption underlying Bertillonage was that when "accurately measured, no two people will ever show the same dimensions" (Fosdick, 1915). Measurements comprised the left middle finger, trunk, foot length, the width of the skull, height among others. These measurements were noted on a standardised card along with distinctive

features (e.g. scars) and other features such as hair and eye colours, attitude, voice and the front and side photos of the suspect. All these characteristics were described with a standardised language. The measurements were then used to categorise the cards following a tripartite system (Bertillon & McClaughry, 1896). After separating the cards by sex, Bertillon classified them according to whether the head was small, medium or large. From there, the cards were then sub-classified by head breath, then by middle finger length and so on. The method was categorising more than 100,000 cards into 12 categories. This system was first proposed by Bertillon in 1897 but started to be employed only in 1883 following a change of leadership in the Paris prefecture. The system appeared to be effective as by 1884 Bertillon identified 241 recidivists. In 1888 the Paris police created a Department of Judicial Identity with Bertillon at his head and the number of recognitions grew to 680 by 1892 (Cole, 2002).

At the time, the system was celebrated for having an "amazing accuracy" as it was soundly based on "scientific principles" (Fosdick, 1915). The scientific measurement approach was the basis for claims of technical neutrality: unlike physiognomy the aim was to identify faces, no facial types. With Bertillonage, recidivism was a new criminal punishable category justified by this scientific method (O'Brien, 1982). However, the system had several drawbacks: it could not be applied to children, it did not account for changes in measurements of adults due to age or diseases, it was not considered suitable for women (Cole, 2002), it was technically difficult to take accurate and replicable measurements and have properly trained officers. The results were highly susceptible to error and the measurement was time consuming.

Bertillion had imagined a standardised systems that could be applied in different social and cultural contexts but with its diffusion abroad, Bertillonaged started to change. Users outside France modified the design of the tools, the number and type of measurements, changed categories, the measuring scale from metric to English. Furthermore, Bertillon's system was not always met with enthusiasm abroad because it was playing a unique role in population control and monitoring in different regions of the world. People were suspicious of this new system and for example, in New York, detectives were reluctant to replace their traditional professional practices (Piazza, 2011). People in colonies were also protesting against Bertillonage as a form of oppression and disciplinary practice (Piazza, 2011).As for its intended purpose, the reasons for Bertillon System usage changed depending on context necessities. While some police officers were using it to identify recidivists, others applied it to modernise the immigration and border control system, or for judicial purposes (Piazza, 2011). Bertillonage was employed across the globe by "Anthropometric labs", "Anthropometric identification departments", "Offices in Criminal Identification and "Offices of forensic identification".

Because the system was undergoing through different changes depending on the context, the transmission of specialised knowledge of Bertillonage became an issue addressed in a multiple ways (Piazza, 2011). Department using Bertillonage were monitored, and r egulated training courses were organised to transmit a rigorous, replicable and consistent application of Bertillonage. Through

training, officers interiorised these new practices that treated the body as a target and scholars have argued that Bertillonage introduced the new role of the expert officer who grounds his work in the scientific knowledge (Spaun, 2009).

Bertillon was in fact urging users to avoid changing any procedure and at times he was struggling to have his instructions followed and enforced (Cole, 2002). With the system expanding, users realised that Bertillon measurements were not unique, and cases of mistaken identity showed that there were common physical characteristics that appeared to be identical. This was the case of Will West, an African-American man, who arrived in 1903 at the Leavenworth, Kansas, U.S. Penitentiary and denied any previous incarceration (Farebrother & Champkin, 2014). As per standard procedure, identification clerks took his Bertillonage which was found to match those of a William West who was previously incarcerated. However, after an inquiry the clerks discovered that William West was actually a completely different individual who was actually serving a life sentence for murder at the same prison (Farebrother & Champkin, 2014). Bertillon and other law enforcement officials had deemed it implausible for the two males to have the same measurements but the names, photographs and Bertillon measurements were dramatically similar (FBI, 1991). Over the years, authors justified the switch to fingerprinting with Will West story and invented that clerks fingerprinted the two men and they were completely different so they declared the end of Bertillonage (Smyth, 1980).

3.1.3.2 Dactyloscopy

After only 20 years from its first use, Anthropometry was gradually replaced by Dactyloscopy, the science of fingerprinting identification. During the 7th century in China, thumbnails were impressed in documents and used as signatures and the practice spread to Japan, Tibet and India (Hoover, 1971). Antique Palestinian pottery also signed their creations with fingerprinting (Hoover, 1971). Fingerprinting identification was used in the British Colonies (India), where British colonial officials at the end of the 19th century were using fingerprinting for civil identification. Fingerprinting was considered an efficient and cost-effective way to strengthen control over a large colony with a small number of civil servants (Cole, 2002). The use of fingerprinting was said to be used in colonies to prevent fraud and impersonation in handling pensioners and in the property registration offices (Singha, 2000). In colonies, Indian natives were also required to stamp their fingerprint on contracts (Hover, 1971). Evolutionary theories and biological determinism in combination with this new technology were then used to legitimise colonial racism. Fingerprinting was proposed as an identification system for criminals to be used across India, where colonial ethnographers were believing that Indian castes represented racial types (Hinchy, 2020), with lower castes being considered hereditary criminal castes (Tolen, 1991). The Criminal Tribes Act for example, was a regulatory project to register, surveil and control those who were considered criminal tribes (Tolen, 1991). Bertillonage was in use but in the colonies it had multiple issue. Under the colonial eyes, people looked homogeneous and this was making identification more difficult (Cole, 2002). Secondly, in the colonies it was hard to have trained officials, making measurements were more prone to error

(Cole, 2002). The issue with fingerprinting was that there was the need of a new system of classification because comparing one fingerprint to the whole database was impossible and too time consuming.

A new system of classification was propsed by Faulds, a British colonial physician who submitted a letter to Nature (1880) proposing fingerprinting as a mean of identification and the use of printers' ink as a method for obtaining fingerprints. In his letter, Faulds was talking about the identification of criminals, but he was also hoping that fingerprinting could have contributed to explain the evolution of the human species. The scientific community readily accepted the method that was quickly picked up by Francis Galton, the creator of eugenics, the pseudoscience that tried to prove hierarchical differences between races and that over century, have been used to justify colonial violence and oppression (Levine, 2010). Those were the years of the Darwinian revolution when science was dedicated to tracing the trajectory of human evolution, understanding the relationship between human and primates and investigating the role of heredity in explaining intelligence, personality and other features. Anthropometry and fingerprinting were used to affirm assumptions about the differences between people, the superiority of some races and classes and to support the marginalisation of some social groups. In 1892 Galton published a book with the results of his studies testing how fingerprinting could contain genetic information to prove differences in temperament and intelligence between people of different races and class (Galton, 1892). His studies could not support his hypothesis, but he created a new classification system based on three categories and he was convinced that fingerprints were inherited. Galton believed that fingerprinting was a tool of colonial governance and could address colonies' issues (Waits, 2016). Yet, the idea of hereditary fingerprinting was undermining the work of dactylographer in law enforcement as it was casting doubts on the uniqueness of all human fingerprint patterns which was crucial to the judicial application of fingerprinting (Cole, 2002). Heredity meant that the likelihood of accidental matches between members of the same family was higher. Because of this, links of fingerprinting to eugenics have been instrumentally forgotten to render fingerprinting an empty and neutral identification technique (Cole, 2002).

In late 20th century, Victorian cities were expanding and so did crime rate. Identifying suspects was increasingly important and in October 1893, Home Secretary Asquith established a committee to investigate the best method available for identifying habitual criminals because relying solely on photograph or distinctive marks was ineffective and labour intensive. Under Chairman Charles Troup, the committee examined both anthropometry and fingerprinting. In deciding which system or combination of systems to adopt, the Troup Committee established the three criteria (Gates, 2011):

- Descriptors of measurements should be taken with sufficient accuracy
- The classification of the descriptions must be such that on the arrest of an old offender who gives a false name his record may be found readily and with certainty
- When the case is found in the classification, convincing evidence needs to be afforded.

The committee wanted the system to be practical, to avoid misidentification and to economize the need of labour. At the beginning of the 20th century fingerprinting and Dactyloscopy were used in

combination in law enforcement and dactyloscopy was regarded as the technique of the future (Dastre, 1907) because it was quicker, cheaper, and it was overcoming the barriers of dactyloscopy. Fingerprinting was first applied in law enforcement on bodies that were considered invisible to anthropometry: those of colonial natives, women, African-Americans ethnic minorities and immigrants. All these so Fingerprinting and its classification system were exported to America during the first two decades of the 20th century and was used to identify immigrants (Finn, 2009). The wide adoption of fingerprints was again linked to racial biases. Fingerprints were thought to offer a valid option to be able to identify people of other ethnicities, which at the beginning of the 19th century were thought to lack enough individuality (Hawthorne Wilder, 1902). Beyond the prejudiced idea of homogeneity of populations other than white, the discriminatory idea of a lack of individuality had historical roots and was due to slavery, when legally, African Americans could not have surnames (Foster & Eckert, 2003). The switch from anthropometry to fingerprinting was first met with resistance because the practice was not seen as scientific enough. Prejudice was also stopping people from using fingerprinting: it had eastern origins and because it was related to colonial governance, it was associated with control and surveillance and considered appropriate only for non-white people (Ramakers, 1905). furthermore, if fingerprinting was suddenly adopted all the anthropometry databases would have become useless and inaccessible. Despite these drawbacks, because it was cost-effective the US started to use it to identify people enrolling in the army and to detect "repeaters," deserters or who had been dishonourably discharged yet wanted to reenlist (Cole, 2002). Later on, fingerprints would be used to identify the deceased and as well as to monitor pension payments.

In the US, the first time fingerprinting was used in the criminal justice system was in 1910 on prostitutes in New York. This occurred because identification experts often complained about the difficulties of using anthropometry to identify women. For example, it was requiring physical intimacy between the operator and the prisoner's body which was not considered appropriate for female prisoners (Fosdick, 1915). People also believed that Bertillonage did not work on women because of their hairstyles and the changes in the size of the female body over the course of the menstrual cycle. In 1916, a law passed that extended the collection of fingerprints to minor offenders and for the first time, American citizens objected to it (Cole, 2002). Citizens were worried that after being fingerprinted, people would have been permanently branded as criminals. Protests and public hostility forced to change policy and reduce the number of minor offences for which people would have been fingerprinted. These for example included jostling, mashing, riotous conduct, offences involving injuries to persons or property, and begging. Two years later, the New York City Health Commissioner proposed to fingerprint also people living with addiction to drugs (Cole, 2002). As fingerprinting was fast and less expensive than Bertillonage, it extended state control over minor offenders and allowed also to map their recidivism.

By 1915, progressive law enforcement officials and advocates were pushing for a widespread adoption of fingerprinting. At the first International Criminal Police Congress held in Monaco in 1914, it was predicted that all European criminal identification files would soon be classified according to

fingerprint patterns. Attendees also expressed the intention to create an international identification system -which then became INTERPOL- and a centralised international record (1st International Criminal Police Congress, 1914) to facilitate the cooperation on solving crimes. Bertillonage offered the opportunity to standardise and systematise knowledge about suspects, but it was becoming increasingly hard to use the database efficiently (Hoover, 1971). Furthermore, Bertillonage was allowing to identify repeat offenders but not criminal suspects. The potential of fingerprinting for forensic identification emerged in 1902 when Bertillon matched a bloody fingerprint at a crime scene with a fingerprint available in a criminal file (Cole 2002). Also in Europe, fingerprints were used with hesitancy as they were seen as less scientific.

Fingerprinting gradually overtook Bertillonage as the primary mean for identifying criminals over the first two decades of the 20th century. Despite fingerprinting having origins in evolutionism and colonialism, it offered an opportunity to avoid racial typing because it did not necessarily involve any other information on skin tone as Bertillonage did. However, fingerprinting ended up reifying racial categories. In 1922, for example, the New York Police Department Identification Bureau created a separate “yellow file” for fingerprints to go along with the “black” and “white” files to categorise people by race (Cole, 2002). Fingerprinting thus allowed individualised identification while maintaining a discriminatory physiognomically based, tripartite (white, black, yellow) system of racial classification.

As compared to Antropometry, fingerprinting had a mechanical property that replaced the human observation with the objective gaze. Anthropometry relied upon the meticulous, trained operator while fingerprinting relied upon a mechanical process that transferred a bodily inscription onto a paper record. This mechanical appeal was more in line with the emerging rhetoric of industrialisation and was used to advocate for its accuracy and objectivity. Fingerprinting evoked the efficiency of mass production and police officials were comparing the process of recording fingerprints to emerging technologies of duplication, such as the letterpress, and carbon paper. Like these technologies, fingerprinting promised to provide more accurate, and faster, representation by eliminating the human element from copy work (Cole, 2002). In other words, fingerprinting seemed like part of the new era of technocracy, it emphasized quantity, efficiency and economic advantage. Fingerprinting brought identification back to visual imagery.

3.1.4 Facial Recognition

The logic behind encoding identities in bodies led to Facial Recognition technology. The development of photography and the use of mug shots for criminal justice and in Bertillonage paved the way for developing technologies that were able to automatically apply quantification to visual materials. Woody Bledsoe, Helen Chan Wolf, and Charles Bisson were among the first pioneers of facial recognition. Bledsoe, Wolf, and Bisson started working on computer-based facial recognition in 1964 and 1965. Bledsoe tried to match suspects' faces to mugshots. He measured the separations between various facial characteristics in printed photos and input those measurements into a computer program that had to match one of the image records to the photograph (Raji & Fried, 2021). Because

the project was funded by an unnamed intelligence agency, much of their work was never published. Authors have claimed that photography and visual recognition has fulfilled what Craig Robertson Called a "Documentary Regime of Verification" where practices of trust and face to face recognition are replaced by standardised identification documents and their verification (Robertson, 2009). Standardised identification documents created a wide archive of state memory while disembodying authority and trust, fulfilling citizens' needs of anonymity and privacy (Caplan & Torpey, 2001). Yet, the public was initially reluctant to add their photo to their passport because of the criminal connotation of the mug shots (Caplan & Torpey, 2001).

Facial-recognition systems analyze a face geometry to create a faceprint, a biometric marker that can be used for verification, identification or classification purposes. First, the system locates the face in a given image. Next, landmarks (eyes, nose and mouth) are located within the face. Then, the face is artificially aligned into a frontal and well-lit view and the geometrical features of the face are extracted. In the verification process, the faceprint is matched with a stored example (one-to-one comparison). Examples of this use are: unlocking smartphones or travelling through a passport gate. When the face-print is used to identify people, the face-print is compared to a database (one-to-many comparison) to discover identity. People can be scanned in crowds. When facial recognition is used for classification purposes, the AI system will infer human characteristics from the faceprint like age, gender, emotion.

Between the 80s and the 90s automated facial recognition was still in an early stage of development but was promising a number of advantages over other types of biometrics: technology's supporters said that consumers would find it less intrusive because it simply recognized persons by looking at their faces, like the way that humans do (Gates, 2004). In addition to this, facial recognition had also the practical advantage of being able to build on the norms and practices of facial identification and its technology relied on the fact that billions of people were already photographed for their documents so there was a great deal of data available (Caplan & Torpey, 2001). In the 90s research in facial recognition increased and made advances in computational methods for locating the face in an image, segmenting it from background, and automatically extracting features (Magnet, 2011). Increasing amounts of computing power facilitated faster techniques and accommodated larger, higher-quality images, and in greater quantities. The research sector found social actors both from the private and public sector with an interest in capitalising in this technology that helped to legitimise its use and development. For example, in 1993 the Department of Defense Counterdrug Technology Development Program Office began and sponsored over five years the Face Recognition Technology (FERET) program (NIST, 2011). The purpose of FERET was “to develop automatic face recognition capabilities” that could be employed “to assist security, intelligence, and law enforcement personnel in the performance of their duties” (NIST, 2011). Accuracy of Face Recognition was part of the early debate on this technology and the program was designed to assess the viability of the technology for use by government agencies through research and evaluation. FERET created a standard database of face imagery to test the accuracy of facial recognition algorithms and demonstrated that, although some systems performed better than others, automated facial recognition appeared to be developing as a technology, at least with respect to still

photographs shot (Gates, 2011). Government testing not only sparked new research but also motivated creators to start using the real world as their testing ground by integrating prototypes into surveillance identification systems (Magnet, 2011). Around the time of the initial FERET experiments, new businesses emerged that were focused on creating and marketing face recognition technologies (Gates, 2011). In this, US law enforcement agencies seem to have adopted facial recognition about a decade earlier than EU countries. In the 1990s, law enforcement organizations in the US started implementing face recognition and other biometrics as techniques for managing the rapidly growing jail population, and for border control (Gates, 2011). In 2001, MIT's *Technology Review* named biometrics one of the top ten technologies that would change the world, further legitimising the use and development of this technology[12] and NIST, building of FERET begun to build the Face Recognition Vendor test, aimed at quantifying the accuracy of face recognition systems (NIST, 2020). In the meantime, the company Visage was closing a number of contracts with several US states to provide a facial recognition technology for law enforcement. In 2001, the system was tested during SuperBowl XXXV in Tampa. Attendees were scanned, analysed and cross-referenced against a database of wanted suspected criminals without being aware of it. A few days after the event, the media and the American Civil Liberties Union shared the news with great concerns about surveillance and condemned the system as privacy invasive (ACLU, 2001). Legal experts were saying that the technology was raising "novel questions about the relationship between technology, the law and the future of police surveillance" while critics were saying that Facial recognition could "put everyone in a police line-up"(McCullagh, 2001). Others were saying that the practice could not be deemed as unconstitutional because in a public event there is no legitimate expectation of privacy (McCullagh, 2001). The technology was used by Florida and other states to meet operational needs, for investigation and for an inmate booking system (Welsh, 2001). Facial recognition made it to the headlines also in 2015 after Willie Allen Lynch, an African American man, was accused of selling cocaine as the facial recognition system suggested him, together with other four people, as a likely match (Valentino-DeVries, 2020). The use of this technology was never mentioned in initial warrants or affidavits and the man learnt late in the process that he had been accused because of a positive FR match. The man, who is serving an eight year prison sentence, claimed to be misidentified and sought the images of the other possible matches but a Florida appeals court ruled against it. Privacy advocates and lawmakers said that the use of facial recognition by law enforcement was Orwellian and unconstitutional because it was scanning Americans with no criminal histories via driver's license and ID photo databases (Valentino-DeVries, 2020). A 2016 study found that one in two American adults is in a law enforcement Facial recognition network (Gavie et al., 2016).

In 2018, the Gender shades project (Buolamwini & Gebru, 2018) revealed that facial recognition was also perpetuating racial bias. The research project assessed several face recognition software and revealed a bias in gender classification error rates between groups. Overall, the Facial recognition product used by IBM, Microsoft and Face++ appeared to have a relatively high accuracy spanning from 87.9% for IBM to 93.7% for Microsoft but there were differences in the error rates between different groups.

[12] https://www.technologyreview.com/10-breakthrough-technologies/2001/

All companies performed better recognizing males than females with 8.1% to 20.6% difference in error rates.
Additionally, all companies better recognised lighter-skinned subjects than darker subjects with 11.8%-19.2% difference in error rates. When the analysis is intersectional -darker males, darker females, lighter males, lighter females- all companies perform worst on darker females. IBM had the largest gap and after receiving the performance results said to be making changes to the Watson Visual Recognition API (IBM, 2018). In June 2020 the Association for Computing Machinery in NY city urged a suspension of both private and governmental use of facial-recognition technology because of a "clear bias based on ethnic, racial, gender, and other human characteristics recognizable by computer systems" (ACM U.S Technology Policy Committee, 2020) which compromise the rights of individuals that are part of specific demographic groups.
The gender Shades project findings have been supported by NIST in 2019: faces in NIST's database classified as African American or Asian were between 10 to 100 times more likely to be misidentified than those classified as white by most facial recognition systems with variations across algorithms. False positives -incorrectly finding matches- were also more likely for women than men (Grother et al., 2019).

Face recognition misidentifications let to a number of renown several wrongful arrests of three African-American men. In January 2020 Robert Williams, was wrongfully arrested by the Detroit police (Ryan-Mosley, 2021) and held in prison overnight under accuse of stealing from a luxury store. He had been arrested because of a wrong match from the Detroit Police Department's facial recognition system. The American Civil Liberties Union and the University of Michigan Law School's Civil Rights Litigation Initiative filed a lawsuit on behalf of Robert Williams, alleging that the arrest violated his Fourth Amendment rights and was in defiance of Michigan's civil rights law (Chicklas, 2021). Similarly in 2019, Michael Oliver was wrongly arrested in Detroit with the accusation of a felony for supposedly reaching into a teacher's vehicle, grabbing a cell phone, and throwing it, cracking the screen and breaking the case (Anderson, 2020). He was another victim of a wrong match of the facial recognition system used by the Detroit police. In 2019, Nijeer Parks was accused of shoplifting and trying to hit an officer with a car. He was arrested and spent 11 days in jail, while innocent, because of a wrong match and he learnt about the face recognition evidence only after his release (General & Sarlin, 2021) .

In the Europe, Germany started to employ facial recognition for forensic purposes as early as 2008 while there are other nineteen[13] countries that are expected to use or are using Facial Recognition for law enforcement. The main controversy with facial recognition is that it gives authorities the ability to track people and collect their personal data which is considered incompatible with democracy because it raises moral questions, compromises privacy, leads to mass surveillance and infringes civil liberties. Generally, human rights campaigners and civil societies say that this

[13] Latvia, France, Slovenia, Hungary, The Netherlands, Italy, Greece, Lithuania, Finland, Austria, Croatia, Czech Republic, Romania, Spain, Sweden, Cyprus, Estonia.

technology might be easily abused to spy on societies and marginalised individuals like migrants, people of colour, or residents in low-income neighbourhoods

Similarly to the Superbowl case discussed above, Leicestershire (UK) Police used facial recognition to scan people who attended a music festival in 2015 and check them against a list of wanted criminals. Big Brother Watch was concerned about the state surveillance (BBC, 2015, p. 201).
Facial recognition is used by London Metropolitan Police (MET) to" prevent and detect crime, find wanted criminals, safeguard vulnerable people, and to protect people from harm – all to keep the people we serve safe." (MET, 2020). MET says that Live Facial Recognition is focused on specific areas and is not a ubiquitous tool that uses lots of CCTVS cameras across London to track all people movements. The system contains a watchlist. They say "It is a carefully deployed overt policing tactic to help locate a limited number of people the police need to find in order to keep London safe." MET is also set to expand its facial recognition capabilities by employing Retrospective Facial Recognition (RFC). While Live Facial Recognition compares live images with those in a watchlist, RFC allows the police to check against broader list (e.g. images captured by cameras at burglaries, assaults, crimes, images shared or submitted by the public).
In 2020 MET said that they were "updating the technology we will use for Retrospective Facial Recognition. We are currently working to integrate the updated capability and develop a suite of documents to ensure we have the right controls and safeguards in place to use the technology" (MET, 2020). At the end of August 2021, the Mayor of London approved a proposal allowing MET to use Retrospective Facial Recognition (Woodhams, 2021) with a 3 million 4 years deal with NEC Corporation, a Japanese firm. In the approval, it is explained that: "The RFR use case is very different to Live Facial Recognition and seeks to help officers identify persons from media of events that have already happened and does not involve members of the public walking past the system 'live time'. As such it would be a tool that helps aid the investigative process, by analysing still images or images that have been specifically extracted from a media source. The result of this analysis will present investigators with additional leads to consider." Retrospective Facial Recognition is used by six police forces in England and Wales (HMICFRS, 2021). The European Digital Rights group and The Big Brother Watch expressed their concern on the RFR as it further undermines people privacy and exacerbate racial discrimination. The Ethics panel, an independent scrutiny group for the London Police is reviewing the RFR use for MET. There are also political pleas to regulate technology (Dearden, 2019). The Data Protection Impact assessment on RFR is not ready yet. A briefing note by the South Wales Police shows that they used RFR system to process 8,501 images between 2017 and 2019 and identified 1,921 potential offenders in the process. However, the use of this technology cause dabate because it avoided avoided both public and legal scrutiny (Woodhams, 2021).

A new EU funded Biomtric program raised serious concerns of civil rights advocates in Greece. The system was supposed to scan people's faces and fingerprints and was deemed inconsistent with international human rights standards on privacy and likely to amplify discrimination. Under the EU-funded program, the police would use hand-held devices to gather biometric information from people on a vast scale and cross check it against police, immigration, and private sector databases

primarily for immigration purposes(HRW, 2020). Recently, Clearview AI made it to the newspaper for devising a facial recognition software that is considered to end privacy as we know it. Clearview AI is a facial recognition platform that contains more than 3billion images scraped from the web - Facebook, Twitter, Instagram, Linkedin[14] often without the platforms' consent. against which is compared a picture provided by the user. It has been used by both the public and private sectors and by LEAs to identify offenders (Castro, 2020). In 2020 600 LEAs were using it without scrutiny but Clearview declined to provide a list (Hill, 2020). In Sweden, the data protection authority fined the Local Police 250.000 euro for unlawful use of Clearview AI as it was employed without proper training, prior authorization and without a data protection impact assessment (see D2.2). Clearview was also accused to have violated Canadian Privacy laws by collecting photos and highly sensitive biometrics of people without their knowledge or permission. However, Clearview declared that Canada's privacy law does not apply because the company do not have a real and substantial connection to the country (Whittaker, 2021). According to Buzzfeed (Mac et al., 2021), LEAs from 24 countries outside the US used Clearview AI - up to February 2020. Data show that police, prosecutors' offices, universities and interior ministries from around the world run about 14000 searches on the software. In the European Union, authorities are assessing whether the use of Clearview violate the General Data Protection Regulation (GDPR) and has been already fined or banned by several Data Protection Authorities (see D2.2). Clearview has been also used by Ukraine's Defense Ministry to uncover Russian assailants, combat misinformation and identify the dead (Paresh & Jeffrey, 2022).

3.1.5 CCTVs

In the 90s, CCTVs systems were quickly becoming problematic. With the increased memory capacity, the amount of work required to monitor these systems increased exponentially. In addition to being boring work, surveillance and identification procedures presented a labour issue. Managing thousands of hours of footage required a lot of labor, which put a significant strain on both public law enforcement agencies and the expanding private security industry (Cavoukian, 2009). Entrepreneurs trying to market facial recognition technology saw an economic opportunity and proposed the concept of "Smart CCTV"—the incorporation of automated facial recognition with video surveillance—as a viable remedy to these issues of surveillance labor and video overload (Yeganegi et al., 2020). Automated facial recognition and other "algorithmic" surveillance techniques such as license plate recognition and "anomaly detection," along with other computer vision technologies, held the promise of automatically managing the massive amount of video data produced by CCTV systems without the need for hundreds of human observers. The first metropolitan area in the US to have a Smart CCTV system installed on its public streets was Ybor City, Tampa's "Latin Quarter," a historic entertainment zone in Florida, in June 2001 (Danner, 2003). Visionics Corporation and the Tampa Police Department (TPD) began a project to integrate FaceIt, the company's automatic facial recognition tool, with the TPD's present 36-camera CCTV system, which covers a number of streets in Ybor City. This brand-new, high-tech method of video

[14] https://www.clearview.ai/

surveillance, which Visionics installed for free, was intended to ensure security for a region targeted for urban renewal and to assist central Ybor City become a more appealing tourist and shopping destination. The system was designed to automatically search digitized images of faces grabbed from video feeds against a watchlist database of wanted individuals, enabling the police to target those specific individuals for exclusion from the area.

However, the experiment did not go as expected. The announcement of the system's installation sparked a contentious discussion that took place in the halls of the Tampa city administration as well as on the streets of Ybor City and in the local and national press. Protetestors were demonstrating in the streets against the installation of facial recognition to defend civil liberties (Danner, 2003). While detractors objected that it was too Orwellian, that it had a Big Brother feel in it and would destroy the distinctive and colorful nature of the neighborhood, supporters said that facial recognition technology would help the police make Ybor City a safer place and so bring new life and commerce to the region. Others claimed that the equipment did not work, making it at best a harmful diversion of police resources and at worst a time waster. The system's supporters struggled to prove that it was a viable "security solution" for Ybor City because of the conflicting claims made about it. The Tampa Police gave up on the project to incorporate computerized facial recognition with the Ybor City CCTV system in August 2003 after a two-year free trial period, citing its inability to locate even a single wanted person.

CCTV in policing dates back to the 1960s in Britain (Goold, 2004) . However, the use of closed-circuit television by law enforcement and private security companies in both the United States and Europe to monitor urban areas, gated communities, workplaces, and capital-intensive spaces like banks, shops, and casinos increased exponentially in the 1980s and 1990s (Goold, 2004). The installation of CCTVs in the city was advertised as the solution to the crime problem, which generally makes it hard for the public to contest the technology. The debate around CCTVs has been prompted in part by the work of sociologists, legal scholars, and other critical observers who have questioned the reasons behind the growth of CCTVs and its social and political ramifications (Kruegle, 2011). This body of research (Goold, 2004; Kruegle, 2011) suggests that the ostensibly obvious justifications police give for using CCTV obscure more nuanced connections between the spread of video surveillance, the social function of the police in contemporary societies, the material and symbolic uses of police power, and the social construction of crime and disorder (Leverentz, 2012). The use of CCTV by the police and their continued adoption of new technologies that claim to make CCTV a "smarter" and more effective surveillance devices are best understood in the context of these more nuanced relationships. Extensive use of CCTVS has been related to the normalisation of crime (Garland, 2001). As a result, criminal justice systems are experimenting with new methods of managing crime rather than believing that addressing the social factors that contribute to crime can reduce or even completely eradicate it (Garland, 1996). Garland contends that the normalisation of crime and the issues of police legitimacy and work overload, have conducted to the adoption of strategies of crime control that seek to off-load responsibilities for crime prevention onto individuals and non-state actors, making the avoidance of crime a part of everyday life. In both the United States and Britain,

police officials and policy-makers began to realize in the 1980s that public fear of crime was somewhat disconnected from actual crime rates (Manning et al., 2022). As a result, they started to take actions aimed at changing public perceptions, regardless of their effect on actual crime (Ratcliffe et al., 2009). As a result of this new approach to crime control CCTVs are now often hovering over urban centers, extending the action of law enforcement or private security throughout those areas and frequently substituting for the authorities themselves.

CCTVs have been contested not only for their invasion of privacy, but also for the lack of transparency in their installation and their consequences on the citizen living in the neighborhoods. In 2010, another controversy stormed Birmingham (UK) citizens who saw a number of CCTVs installed in a Muslim area (Lewis, 2010). People initially suspected that they were automatic number plate reading (ANPR) cameras used to track drivers and protesters sprayed cameras with messages against a "1984" state. Citizens who asked what the cameras were for were reassured that it was a traffic control initiative. However, an inquiry from The Guardian newspaper revealed that cameras were installed to monitor extremists that "the police knew to be living among the city's Muslim population. Additionally, the cameras appeared at 81 sites without consultation, after being requested by West Midlands police counterterrorism unit more than two years in advance. They include around 150 ANPR cameras, 40 of which have been classified as "covert", and are thought to be concealed in walls and trees by the side of the road. The initiative was sponsored by the Terrorism and Allied Matters fund and one of the criteria to participate was to prove that a project will "deter or prevent terrorism or help to prosecute those responsible". Cameras were positioned in a way that no one could enter or leave the neighborhood without being tracked. Data were then transferred to the database BOF2 and stored for 2 years. Citizens felt they did not know why CCTVs were that they were having misleading information. The community felt victimised and felt that the message was that" if you live in a predominantely Muslim area, you're a suspected terrorist." and that cameras threatened the trust between Muslim citizens and the community. Briefing documents given to councillors made only fleeting references to counterterrorism, and in parts sought to play down its importance. The only reference the document came in a paragraph, which stated that an added advantage of the cameras is that they will "provide support and reassurance to communities considered to be vulnerable to violent extremism".

3.1.6 Encryption

Encryption is the conversion of information or data into a code to protect information and prevent unauthorized accessand since the 1990s, it has become an essential component of societies. Encryption protects everything from confidential data to financial transaction and private communication. In Europe, encryption is perceived in two conflicting ways: as a tool for privacy and security, but also as a key obstacle to law enforcement activities. In 2014, in response to Snowden revelations about the US mass surveillance programme, the EU Parliament called on member states, the EU commission and the European council to develop and support EU technologies and standards for cybersecurity and encryption to achieve higher independence in the IT sector and to protect

citizens' rights to privacy (European Parliament, 2014). However, the series of terror attacks that involved different European states between 2015 and 2016 sparked the EU policy debate around encryption. After these attacks, EU member states called for collective measures to prevent and counter such terrorist activities and demanded EU to create a law that would facilitate LEAs to access encrypted data (Stupp, 2016). In 2016 Europol Internet Organised Threat Assessment pointed to encryption as a threat to the detection, investigation and prosecution of such criminal activity (EUROPOL, 2016). LEAs see encryption as an obstacle to criminal investigation and a threat to security in cases of trafficking, organized crime, terrorism, child abuse, corruption, cyber crime. Moreover issues with encryption in investigations vary from one member state to the other as access policies and capabilities differ among member states (Koomen, 2021). On the other hand, the EU Fundamental Rights Agency described encryption as a means to reinforce security and privacy (FRA, 2017) as it allows people - including journalists, activists as well as ordinary people- to shield their communication and safeguard unauthorized access or leaks. Academics, business associations and civil societies (Access now, European Digital Society Rights) have been advocating for the defense of encryption as a need to protect individual rights, intellectual property and data from cyber-attacks (EDRi, 2017).

In 2016 France and Germany interior ministers asked for an European solution to ease the access to encrypted communication and oblige communication operators to cooperate to intercept terrorists (Reuters Staff, 2016). In September of the same year, the Slovak Presidency to the Council of the European Union shared with council members a questionnaire that was asking members to provide details about any national legislation they had on encryption. Initially, this legislative process was kept behind closed doors with the questionnaire and answers being kept private, excluding important members that were part of the debate like academic, civil societies and business organisations. Under the pressure of Access Now and Bits of Freedom[15] some of the countries made their response public. An open letter was signed by organisations, companies, experts, and individual form more than 50 countries asking governments to reject laws, policies and practices that would have undermined encryption.

The leaked questionnaires revealed that member states ministers agreed that encryption should be protected and EU countries struggled with encryption and security protocols to varying degrees[16]:

1. VPN, SSH, PGP, and Tor, as well as Telegram, Signal, and WhatsApp were repeatedly reported as an issue, and as tools used by “suspects”.
2. Law enforcement lacked specific knowledge to deal with cases with electronic evidence. They lacked the “technical capability” as well.
3. Law enforcement used commercially available decryption tools.
4. The principle of territoriality seemed to be inadequate, given the cross-borders nature of the internet.

[15] https://securetheinternet.org/
[16] https://www.asktheeu.org/en/request/input_provided_by_ms_on_question?nocache=incoming-11727#incoming-11727

5. Court orders were necessary in order to request data from telecommunications providers or wiretap a connection.
6. Italy allowed wiretapping of encrypted data flows through the so-called Trojan inoculation technique, on the basis of a court order.
7. Most states indicated a need for a European platform for decryption, to be used by law enforcement.
8. Data needed by law enforcement could be decrypted with the help of private industry third parties.
9. Data decrypted or obtained in such a way may help the investigation, but was not admissible in court.

In October 2017 the EU commission announced its position of encryption with its recommendations on "to support law enforcement and judicial authorities when they encounter the use of encryption in criminal investigations" (European Commission, 2017). The position was announced in the anti-terrorism package. In this document, the commission recognized encryption as an essential way to ensure cybersecurity and the protection of personal data. However, in the context of criminal investigation encryption was deemed as a challenge to LEAs. Therefore, the commission published a set of measures to support law enforcement and judicial authorities when they encounter the use of encryption by criminals in criminal investigations. This included both legal and technical measures aiming to support member states authorities (European Commission, 2017) in accessing cross border information, establishing a network of experts on encryption, create a toolbox for member state authorities of alternative investigation techniques to obtain needed information encrypted by criminals, training programmes for law enforcement and judicial authorities.

Facebook in 2019 announced the adoption of end-to-end encryption which alarmed LEAs and child protection organizations which started to insert in the European agenda on encryption the debate on online child abuse (Koomen, 2021). In response, EU commissioner for Hime Affairs Ylva Johansson called for a technical solution to the problem of encryption "Encryption is a problem for detection. Internet companies can't detect child sexual abuse material if it's encrypted. Encryption is a problem for investigation and prosecution. A warrant will give access to a suspect's home. But not to the encrypted hard-drive"[17]. In July 2020 the EU commission launched two strategies which pointed to encryption from a public safety and security standpoint as a tool that hides perpetrators identity and criminal actions[18]. The strategy to fight Child sexual abuse highlighted the role of private sector and called on companies to detect and report child abuse in end-to-end encrypted communications. The EU Security Union Strategy confirmed that the EU would have explored and supported balanced technical, operational and legal solution to maintain the effectiveness of encryption while providing an effective response to crime and terrorism. However, a leaked draft of the EU discussion paper

[17] https://ec.europa.eu/commission/commissioners/2019-2024/johansson/announcements/speech-commissioner-johansson-webinar-preventing-and-combating-child-sexual-abuse-exploitation_en
[18] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0605&from=EN and https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0607&qid=1634899236324

revealed that the technical solution [19] proposed a least bad option which would have put the privacy, safety and security of people at risk making everyone more vulnerable to online crimes. Under the pressure of online communication becoming subject to strict confidentiality requirements of the EU privacy framework, the EU Commission presented a proposal to allow tech companies to derogate from these rules, with the aim to enable them to continue detecting and removing child sexual abuse material, however the proposal was rejected as did not lived up to EU privacy rules.

The issue is creating a balance between strong encryption and the right to access to encrypted content. On one hand, LEAs ask for more access to data, on the other civil society, academia and industry ask for stronger encryption to protect privacy. Another challenge is that data access policies and capabilities differ among member states so problems with encryption vary from one state to the other. These differences between member states and insufficient legal assistance were the problem that pushed the encryption debate at the EU level (Koomen, 2021). This risk to render an EU legislation ineffective as it would rely on the capabilities of LEAs that in some context, are lacking.

From a technical standpoint any solution would break or undermine encryption. Solutions proposed this far have varying degrees of feasibility, effectiveness, privacy, security, transparency. In any case, these solutions are considered to break end-to-end encryption as they pre-filter messages before they are encrypted and sent. This undermines users' fundamental rights and the crucial technological safeguard of encryption as Diego Naranjo outlined in a letter to Ursula Von der Leyen[20].

3.1.7 Body Cameras

A body camera is a wearable audio, video, or photographic recording system. Body cameras are used to varying degrees across the European Union, with Denmark credited as the first country to use body cameras (Thompson, 2020). Challenges include police accountability, training, privacy, storage and the use of recordings the judicial system (Wasserman, 2015). On one hand, body cameras are considered to address blind spots in police oversight and a source of better evidence and transparency in policy conduct. They have been proposed as a way to reduce police force and assaults against officers especially after cases of killings by the police (Ariel et al., 2016). On the other, data collection and retention become problematic in terms of privacy. However, recent studies showed that bodycams had no effect on police use of force and increased the rates of assaults against police (Ariel et al., 2016). Recent controversies on data retention shed a light on how recordings can infringe data protection law. Body cameras were unlawfully used in Stockholm's public transport by ticket inspectors with the purpose of "preventing threatening situations, to document incidents that have occurred and to ensure that the right person is fined for having travelled with public transport without a valid ticket". The Swedish Authority for Privacy Protection found that the body cameras were continuously registering images and sounds, and travellers were at risk of being recorded. The Swedish Authority for Privacy Protection stated that Ticket inspectors should only press the button to activate their camera 15 seconds before wanting to turn it on and only need an image and not

[19] https://www.politico.eu/wp-content/uploads/2020/09/SKM_C45820090717470-1_new.pdf
[20] https://edri.org/wp-content/uploads/2020/10/20201020-EDRi-Open-letter-CSAM-and-encryption-FINAL.pdf

sound. Moreover, passengers were not informed about this camera surveillance with sound, with the Authority for Privacy Protection highlighting a lack of transparency in the use of body cameras in this case. The transport company was fined for these shortcomings (European Data Protection Board, 2021).

The Irish Garda Siochana Digital Recording Bill 2021 stated that body cameras will only be activated by Gardai (Irish National Police) in certain situations rather than recording all the time. Gardai will wear a highly visible camera on the chest and will have to signal when they are going to record and justify their decision. Footage will be stored in a way where it cannot be edited or altered to preserve its integrity in case it is needed for court evidence (Gallagher, 2021). The Irish Council for Civil Liberties has criticised the deployment of bodycams due to the potential impingement on citizens' privacy rights (Bracken, 2021). The rollout of bodycams in An Garda Siochana will commence in 2022, as it remains one of the few national police forces in Ireland that has not rolled out bodycams.

In 2019, it was reported that German police were storing bodycam footage on the Amazon Cloud which sparked controversy over security and privacy issues. The Federal Police stated that they are using the cloud service from Amazon as it is the only one in Germany with a certificate from the Federal Office for Information Security. The interior ministry echoed this informing that storing data on Amazon's servers is in compliance with German data security standards. A lawmaker from the political party, Free Democrats, raised concerns over the risks of storing highly sensitive data with a private company. Although the servers are located in Germany, US security and intelligence could potentially access the data. A chairman from the Greens parliamentary group also noted privacy concerns as Amazon sells facial recognition software to the US police for analysing bodycam videos. The deputy chairman of the Police Union raises the additional concern that the German authorities' reliance on one single company leads to "competition and practical issues", while also acknowledging that complete state control is desirable but may not be affordable (Winter, 2019).

3.1.8 Security Scanners

Body scanners have been used in airports over the past 20 years, yet there is still controversy surrounding the privacy and social injustice issues that this form of AI may cause. The first x-ray scanning machines to check baggage were introduced in the 1970s and before that, checks were carried out manually. Until the 1990s, passengers were only checked with an electronic magnetometer and later through metal detectors. In the early 1990s, the first body scanner model was developed consisting of a very low-dose backscatter X-ray security screening system (Airport Industry Review, 2020).

As a consequence of the 9/11 terrorist attacks, airport security became a global controversy and full-body scanners started to be introduced with the first being deployed at Amsterdam Schiphol Airport in 2007 (Reuters Staff, 2007). From 2010 onwards, body scanners were introduced in various airports across Europe as a measure against terrorism (Shirbon, 2010). At the time, two models were available: the millimetre wave scanner and the backscatter x-ray screener. The backscatter x-ray

scanners were not in the market for long due to being labelled as too revealing and therefore resulting in privacy concerns, as well as potentially harmful due to the radiation emitted. Backscatter x-ray scanners were phased out from the majority of airports in 2013 (Airport Industry Review, 2020).

From the mid-2010s, most airports were equipped with millimetre wave scanners, fitted with a privacy software, Automatic Target Recognition, that identifies suspicious objects. In recent years, body scanning machines have seen improvements such as a decrease in scanning times and greater detection capabilities in line with new terrorist threats. Research on body scanners is often slow and reliant on the investment it receives. Some researchers are trialling alternative body scanners which use space technology to detect human body heat (Airport Industry Review, 2020).

Body scanners are portrayed as increasing security, preventing future terrorist attacks, and as a threat to privacy and civil liberties (Gregoriou & Trullinou, 2012). They are seen as a weapon to be employed in the war against 'terrorism', with technology deemed superior to humans, or as an invasive practice that infringes human rights (Gregoriou & Trullinou, 2012). In past controversies around body scanners, specific social groups have been discriminated against and linked to terroristic threat (Gregoriou & Trullinou, 2012).

Travellers face gender discrimination as a result of body scans used at border control points in airports and stations. Some scanners that are used in the UK, and all of those used in the US, have to be programmed according to sex and staff are alerted if the scans show a prothesis, chest bindings or a body part that security guards do not associate with the gender indicated on their travel document (Tims, 2017). Therefore, security staff may misgender individuals when inputting individuals' sex into binary gender body scanners. This may also lead to security staff questioning individuals on their gender identity in public in front of other passengers leading to distress, humiliation and discrimination (Tims, 2017). In 2017, a transgender woman filed a civil rights complaint with the Transportation Security Administration for invasive search after being flagged by a full body scanner that was designed to detect potential threats that are not necessarily metal but the machine can't tell if the machine detects a weapon or a body part that the scanner was not programmed to associate with a woman (Waldron & Medina, 2019). Body scanners were also found to be prone to false alarms for turbans, wigs, and hairstyles popular among women of colour (Medina & Frank, 2019. The Transportation Security Administration (TSA) requested vendors to "improve screening of headwear and hair in compliance with Title VI of the Civil Rights Act." which bars federally funded agencies and programs from discriminating — even unintentionally — on the basis of race, colour or national origins (Medina & Frank, 2019). Furthermore, images produced by a body scanner, depending on the depth of scanning, may reveal intentionally concealed physical features or medical information which people might prefer not to be revealed.

3.1.9 Drones

Drons are unmanned aerial vehicles (UAV) or aircraft without a human pilot on board. The drone's flight can be managed manually by a controller on the ground or automatically by computers on board. Drones are used for aerial photography and videography and give rise to a series of controversies as they are perceived as surveillance equipment that raises significant privacy and civil liberties concerns. Some of these controversies relate to the lawfulness of the technology, whereas others relate to the circumstances and ways in which such technology is being used. In May 2020, the use of drones by police in Paris to monitor demonstrations and gatherings on public roads was prohibited (Desai, 2020). However, despite the ban, the Paris Police was found to monitor large-scale demonstrations on public roads. La Quadrature du Net (LQDN), an advocacy group promoting digital rights, filed several complaints against the Paris police's continuous infringement of privacy by flying drones. LQDN argued that this activity was in violation of privacy rights and freedom of expression and used to track individuals rather than keep the peace (Desai, 2020). Of particular concern was the capturing, recording and transmission of images. The police blurred the photographs taken by surveillance drones using AI and was justifying their use of drones on an order which allowed the use of flying cameras if the requirements of public order and safety justify it (Desai, 2020). However, a media investigation revealed that it was simple to "unblur" the photographs that were obtained. The Council of State rejected the case made by the Police and ruled that drone surveillance of protests should have been stopped right away as "the Minister does not provide any evidence to establish that the objective of guaranteeing public safety during gatherings of people on the public highway could not be fully achieved, in the current circumstances, without the use of drones" (Statewatch, 2021). According to data protection law, surveillance devices' usage cannot be authorized without a sufficient justification of its need and proportionality. Furthermore political opinions expressed at protests are considered sensitive data, thus to be legitimately deployed, the device need to be absolutely necessary.

In the UK drones have also been used to monitor political protests including those organised by Black Lives Matter and by animal rights advocates (Dodd, 2021). The Campaign group Drone Wars used freedom for information requests to ask the police information about their use of drones which was perceived as not transparent and a form to "silence dissent". One of the issues was that the police adopted the technology with little oversight or consent from the public and little control over how data were gathered (Dodd, 2021).

Drones have been used for border control and to intercept migrant boats crossing the Mediterranean (Mazzeo, 2021). In this context, they have been linked to risk of dehumanisation and criminalisation of migrants as well as a way to evade humanitarian responsibility toward those in distress (Burt & Frew, 2020). The use of drones and aircraft for border control in the Mediterranean has been seen as a tool that "allows (...) to gain knowledge of the presence of boats in distress and their position without having to engage in rescue activities" violating migrants' fundamental rights (Alarm Phone et al., 2020).

Drones have been widely used in several European states to enforce social distancing (Holroyd, 2020). Earlier in 2020, the French court also banned the use of drones by police in relation to security rules imposed during the COVID-19 lockdown (Drago, 2020). Hundreds of drones had been used to monitor and capture images of people in the street potentially infringing lockdown rules. The appeal presented to the court was based on the absence of any legal framework concerning the use of images captured by these drones (Drago, 2020). The French Highest Court ruled that the use of drones by the police in the context of monitoring compliance with Covid19 lockdown measures was unlawful. According to the decision, images and videos taken by drones flying at a low altitude were personal data to the extent that individuals were identifiable. Therefore, using drones for law enforcement purposes amounted to data processing and was covered by French data protection law. According to the French data protection law, any data processing activities must be authorized by legislation statute or executive order and be accompanied by a public review by the French Commission on Information and Liberties. In regards to the employment of drones, none of these actions has been performed. The Court ordered to suspend all drone surveillance activities related to monitoring compliance with Covid-19 measures until the requirements set by the data protection law were met. In the US the adoption of drones for law enforcement purposes created a series of issues because their deployment happened in a culture of "secrecy" and with a lack of transparency (Boussios, 2017). Drones capabilities to execute targeted killings also raised numerous legal questions (Boussios, 2017). In 2012, Pew Research surveyed people in 20 countries worldwide and found that in 17 countries, more than half participants disapproved the US conducting drone strikes to target extremists (Drake, 2013).

4 Discussion, recommendations, and conclusions

The history of innovation reveals that the concept is intrinsically controversial and ambivalent. Focusing on techno-optimistic narratives transforms technology and innovation into a black box because it prevents from seeing how technology is socially and culturally constructed (Latour, 1987). Social controversies are a key tool that allows to open-up the black box. They afford to track the evolution of technology, image alternatives, identify challenges and risks and enable the creation of new technologies and new models of governance that fits societal needs. By looking at controversies it is easier to identify assumptions underlying tech development and adoption, technical difficulties, their social causes and effects, and the moral and legal standards. In this, social controversies reveal how the social and the technical are meshed and they challenge the value-neutrality attributed to new technologies by the mainstream discourse. Value-neutrality impedes technological development as it prevents us from seeing and acting upon important issues embedded in technology (e.g. discrimination). Therefore, social controversies are a tool of empowerment that enable to identify and forecast challenges and act upon them. This in turn allows a better and more efficient technological development and adoption.

Across the different technologies analysed above, there are several recurrent themes. These are:

- **Transparency**: the case studies reviewed above indicate that a lack of awareness by the public on the use of new technologies raises distrust and delegitimise technology use. This theme was raised in the CCTVs, and facial recognition as well as in the drone case where people felt excluded from the technology process and or misled by decision-makers.
- **Privacy** is one of the human rights that are particularly salient in most of the case studies. When new technologies that involve people's data are adopted, citizens feel that their right to have a private life is at stake.
- **Training** of users has been a key part of the debate since early times. As Bertillonage case indicated, it seemed to start with the introduction of the "expert" figure in law enforcement. Lack of training and wrong cultural adaptations to instructions pose a serious risk to a rightful and fair technology adoption. This type of controversy emerged also in the facial recognition and encryption case.
- **Safeguards:** on the wave of tech optimism, often new technologies have been adopted without proper legal and moral safeguards into place. This led to cases of errors and misuses that made citizens question the safety and legality of these technologies.
- **Intended purpose**. The case studies indicate that the concept of **intended purpose** is particularly problematic as technologies assume different meanings in different contexts and places and for different social groups. This directly affects how and why technology is used and the consequences it has for people.
- **Discrimination and bias**: as the fingerprinting and Bertillonage cases showed, new technologies have been historically tested and used on marginalised groups and have also arisen from biased preconceptions. Discrimination can arise from biased data, biased assumptions, biased functioning and application of the technology, or biased bureaucracy

that makes categories like gender, social class, geography and race tangible. This can have severe consequences for citizens, exacerbate structural discrimination and further marginalise some communities.

- **Datafication and surveillance**: early controversies demonstrated that surveillance issues as early as the expansion and use of standardised documents. Thus, controversies about surveillance have been a constant in technological development and, as the Google Glass and the Smart Meter cases show, have led to technological change and development.
- **Context.** The controversies reviewed highlighted that the same technology (e.g. drones) used in different contexts (protests vs. border) creates different risks.

This suggests that to mitigate risk and for a more efficient technology development and adoption law enforcement agencies should:

- build awareness of values and morals embedded in the technology they might want to adopt or develop.
- consider contextual, social and cultural factors when adopting or developing a new technology.
- assess how the technology under consideration has been used before, where it has been developed and used and citizens' reactions to it.
- develop proper training programs enabling a full understanding of the functioning, use, risks and consequences of the technology under consideration.
- adopt clear communication strategies that make the public aware of what technologies are adopted, why they are used, how they work and how the benefits outweigh risks.
- ensure that the technology and its application do not discriminate against social groups.
- ensure that proper legal, ethical and moral safeguards are in place, known and understood before any technological adoption.

To sum up, social controversies allow an insight into technological processes that are otherwise considered obscure. In this, they enable people to imagine new strategies to address key issues related to technological development and adoption before risks materialise. Thus, more generally, we strongly encourage embedding social controversy analysis in any risk management plan.

5 References

1st International Criminal Police Congress. (1914). *Summary of the Wishes Expressed at the Session or Assemblied held on 15, 16 and 18 April 1914*.

ACLU. (2001). *ACLU Calls for Public Hearings on Tampa's "Snooper Bowl" Video Surveillance*. https://www.aclu.org/press-releases/aclu-calls-public-hearings-tampas

ACM U.S Technology Policy Committee. (2020). Statement on Principles and Prerequisites for the development, EValuation and Use of Unbiased Facial Recognition Technologies. *ACM*. https://www.acm.org/binaries/content/assets/public-policy/ustpc-facial-recognition-tech-statement.pdf

Ada Lovelace Institute. (2020). *Examining the Black Box: Tools for assessing algorithmic systems*. Ada Lovelace Institute.

Airport Industry Review. (2020). *Timeline: The History of Airport Body Scanners.* https://airport.nridigital.com/air_mar20/timeline_the_history_of_airport_body_scanners

Alarm Phone, Borderline Europe, Mediterranea - Saving Humans, & Sea-Watch. (2020). *Remote control: The EU-Libya collaboration in mass interceptions of migrants in the Central Mediterranean*. https://www.borderline-europe.de/sites/default/files/readingtips/RemoteControl_Report_0620.pdf

Anderson, E. (2020). Controversial Detroit facial recognition got him arrested for a crime he didn't commit. *Detroit Free Press*. https://eu.freep.com/story/news/local/michigan/detroit/2020/07/10/facial-recognition-detroit-michael-oliver-robert-williams/5392166002/

Ariel, B., Sutherland, A., Henstock, D., Young, J., Drover, P., Sykes, J., Megicks, S., & Henderson, R. (2016). Wearing body cameras increases assaults against officers and does not reduce police use of force: Results from a global multi-site experiment. *European Journal of Criminology*, *13*(6), 744–755. https://doi.org/10.1177/1477370816643734

Arthur, C. (2013). Google Glass: Is it a threat to our privacy? *The Guardian*. https://www.theguardian.com/technology/2013/mar/06/google-glass-threat-to-our-privacy

Basiago, A. D. (1994). The limits of technological optimism. *The Environmentalist*, *14*(1), 17–22. https://doi.org/10.1007/BF01902656

BBC. (2015). *Download festival: Leicestershire Police defend facial recognition scans*. https://www.bbc.com/news/uk-england-leicestershire-33132199

Bean, D. (2013). Google Glass: Some Winners of "If I Had Glass" Contest Disqualified. *ABC News*. https://abcnews.go.com/blogs/technology/2013/03/google-glass-some-winners-of-if-i-had-glass-contest-disqualified

Bertillon, A., & McClaughry, R. W. (1896). *Signaletic instructions including the theory and practice of anthropometrical identification.* Werner Company.

Bimber, B. (1994). Three Faces of Technological Determinism. In *Does technology drive history?: The dilemma of technological determinism* (Fourth printing, 1998). MIT Press.

Binfield, K. (2004). *Writings of the Luddites*. The Johns Hopkins University Press.

Birhane, A., Kalluri, P., Card, D., Agnew, W., Dotan, R., & Bao, M. (2022). The Values Encoded in Machine Learning Research. *2022 ACM Conference on Fairness, Accountability, and Transparency*, 173–184. https://doi.org/10.1145/3531146.3533083

Boussios, E. G. (2017). Drones in War: The Controversies Surrounding the United States' Expanded Use of Drones. *Contemporary Voices*. https://cvir.st-andrews.ac.uk/articles/10.15664/jtr.1337/

Bracken, A. (2021). Gardaí will wear body cameras under new laws. *Independent.Ie*. https://www.independent.ie/irish-news/gardai-will-wear-body-cameras-under-new-laws-40272488.html

Buolamwini, J., & Gebru, T. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Proceedings of Machine Learning Research*, 1:15. http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

Burgess, A. (2004). *Cellular Phones, Public Fears, and a Culture of Precaution*. Cambridge University Press.

Burt, P., & Frew, J. (2020). *Crossing a line: The use of drones to control borders*. https://dronewars.net/wp-content/uploads/2020/12/DW-Crossing-a-Line-WEB.pdf

Callon, M. (1984). Some Elements of a Sociology of Translation: Domestication of the Scallops and the Fishermen of St Brieuc Bay. *The Sociological Review*, *32*(1_suppl), 196–233. https://doi.org/10.1111/j.1467-954X.1984.tb00113.x

Caplan, J., & Torpey, J. (2001). *Documenting Individual Identity: The Development of State Practices in the Modern World*. Princeton University Press.

Castro, A. (2020). ICE just signed a contract with facial recognition company Clearview AI. *The Verge*. https://www.theverge.com/2020/8/14/21368930/clearview-ai-ice-contract-privacy-immigration

Cavoukian, A. (2009). *Privacy by design, take the challenge*.

Chicklas, D. (2021). Farmington Hills father sues Detroit police department for worngful arrest based on faulty facial recognition technology. *ACLU Michigan*. https://www.aclumich.org/en/press-releases/farmington-hills-father-sues-detroit-police-department-wrongful-arrest-based-faulty

Chiesa, V., & Frattini, F. (2011). Commercializing Technological Innovation: Learning from Failures in High-Tech Markets. *Journal of Product Innovation Management*, *28*(4), 437–454. https://doi.org/10.1111/j.1540-5885.2011.00818.x

Cole, S. A. (2002). *Suspect Identities: A history of Fingerprinting and Criminal Identification*. Harvard University Press.

Collins, K. (2016). Google Glass goes dark on social media. *CNET*. https://www.cnet.com/tech/computing/google-glass-goes-dark-on-social-media/

Cuijpers, C., & Koops, B.-J. (2013). Smart metering and privacy in Europe: Lessons from the Dutch case. In *European Data Protection: Coming of Age*, (pp. 269–293). Springer.

Danner, T. A. (2003). Violent Times: A Case STudy of the Ybor City Historic District. *Criminal Justie Policy Review*, *14*(1). https://doi.org/10.1177/0887403402250926

Dastre, A. (1907). Des empreintes digitales comme procédé d'identification. *Comptes Rendus Des Séances de l'Academie Des Sciences*, *145*, 47–42.

Davies, C. (2012). *Google Glass spotted in wild with prescription lenses*. https://www.slashgear.com/google-glass-spotted-in-wild-with-prescription-lenses-31262620

Dearden, L. (2019). *Facial recognition: Labour vows to regulate "lawless" technology if it wins power in next elections*. https://www.independent.co.uk/news/facial-recognition-technology-police-general-election-a9111026.html

Desai, S. (2020). *Paris police banned from using surveillance drones. Anadolu Agency*. https://www.aa.com.tr/en/europe/paris-police-banned-from-using-surveillance-drones/2085728

Dodd, V. (2021). Drones used by police to monitor political protests in England. *The Guardian*. https://www.theguardian.com/uk-news/2021/feb/14/drones-police-england-monitor-political-protests-blm-extinction-rebellion

Drago, M. (2020). *France: First victory against police drones. European Digital Rights*. https://edri.org/our-work/france-first-victory-against-police-drones/

Drake, B. (2013). *U.S. Use of Drones, Under New Scrutiny, Has Been Widely Opposed Abroad* [Pew Research]. https://www.pewresearch.org/2013/02/06/u-s-use-of-drones-under-new-scrutiny-has-been-widely-opposed-abroad/

EDRi. (2017). *Encryption Workarounds*. https://edri.org/files/encryption/workarounds_edriposition_20170912.pdf

Epic. (2007). Investigations of Google Street View. *Epic.Org*. https://epic.org/documents/investigations-of-google-street-view/

Esguerra, R. (2009). *Google CEO Eric Schmidt Dismisses the Importance of Privacy*. https://www.eff.org/deeplinks/2009/12/google-ceo-eric-schmidt-dismisses-privacy

Eubanks, V. (1018). *Automatin Inequality. How high tech tools profile, police, and punish the poor*. St Martin's Press.

European Commission. (2017). *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL AND THE COUNCIL Eleventh progress report towards an effective and genuine Security Union*. https://home-affairs.ec.europa.eu/system/files/2020-09/20171018_eleventh_progress_report_towards_an_effective_and_genuine_security_union_en.pdf

European Data Protection Board. (2021). *Unlawful use of body cams in Stockholm's public transport.* European Data Protection Board. https://edpb.europa.eu/news/national-news/2021/unlawful-use-body-cams-stockholms-public-transport_en

European Parliament. (2014). *Resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs*. https://www.europarl.europa.eu/doceo/document/TA-7-2014-0230_EN.html?redirect

EUROPOL. (2016). *IOCTA 2016 Internet Organised Crime Threat Assessment*. https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2016

Farebrother, R., & Champkin, J. (2014). Alphonse Bertillon and the measure of man: More expert than Sherlock Holmes. *Significance*, *11*(2), 36–39. https://doi.org/10.1111/j.1740-9713.2014.00739.x

Farivar, C. (2013). “Stop the Cyborgs” launches public campaign against Google Glass. *Ars Technica*. https://arstechnica.com/tech-policy/2013/03/stop-the-cyborgs-launches-public-campaign-against-google-glass/

Faulds, H. (1880). On the Skin-Furrows of the Hand. *Nature*. https://www.nature.com/articles/022605a0

FBI. (1991). *Identification Division of the FBI - A Brief Outline of the History, the Services, and the Operating Techniques of the World’s Greatest Repository of Fingerprints*. https://www.ojp.gov/ncjrs/virtual-library/abstracts/identification-division-fbi-brief-outline-history-services-and

Finn, J. (2009). *Constructing the Criminal in North America*. University of Minnesota Press.

Fosdick, R. B. (1915). Fosdick, R. B. (1915). Passing of the bertillon system of identification. J. Am. Inst. Crim. L. & Criminology, 6, 363. *Journal of Criminal Law and Criminology*, *6*(3). https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1374&context=jclc

Foster, G. S., & Eckert, C. M. (2003). Up From The Grave: A Sociohistorical Reconstruction of an African American Community From Cemetery Data in the Rural Midwest. *Journal of Black Studies*, *33*(4), 468–489. https://doi.org/10.1177/0021934702250027

FRA. (2017). *Fundamental Rights Report 2017*. https://fra.europa.eu/en/publication/2017/fundamental-rights-report-2017

Gallagher, C. (2021). Garda body cameras likely to be used only in potential confrontations. *The Irish Times*. https://www.irishtimes.com/news/crime-and-law/garda-body-cameras-likely-to-be-used-only-in-potential-confrontations-1.4547228

Galton, F. (1892). *Finger Prints*. MacMillan and Co. http://www.biometricbits.com/Galton-Fingerprints-1892.pdf

Gantz, T., & Henkle, G. (2002). *Seatbelts: Current issues*. http://www.preventioninstitute.org/traffic_seatbelt.

Garland, D. (1996). THE LIMITS OF THE SOVEREIGN STATE: Strategies of Crime Control in Contemporary Society. *The British Journal of Criminology*, *36*(4). https://www.jstor.org/stable/23638075

Garland, D. (2001). *The Culture of Control: Crime and Social Order in Contemporary Society*. University of Chicago Press.

Gates, K. (2004). The past perfect promise of facial recognition technology. *ACDIS Occasional Paper*.

Gates, K. (2011). *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance*. New York University Press.

Gavie, C., Bedoya, A., & Frankle, J. (2016). *The perpetual line-up*. https://www.perpetuallineup.org/

Gayomali, C. (2015). Why Google Glass' privacy concerns are grossly overstated. *The Week*. https://theweek.com/articles/464216/why-google-glass-privacy-concerns-are-grossly-overstated

Geels, F. (2004). From sectoral systems of innovation to socio-technical systems. Insights about dynamics and change from sociology and institutional theory. *Research Policy*, *33*, 897–920.

General, J., & Sarlin, J. (2021). A false facial recognition match sent this innocent Black man to jail. *CNN*. https://edition.cnn.com/2021/04/29/tech/nijeer-parks-facial-recognition-police-arrest/index.html

Godin, B. (2010). "Meddle Not with Them That are Given To Change": Innovation as Evil. *Project on the Intellectual History of Innovation*. http://www.csiic.ca/PDF/IntellectualNo6.pdf

Godin, B. (2015). *Innovation contested: The idea of innovation over the centuries*. Routledge.

Godin, B. (2019). *The Invention of Technological Innovation*. Edward Elgar.

Google (Director). (2012). *Project Glass: One day...* https://www.youtube.com/watch?v=9c6W4CCU9M4

Google Developers (Director). (2012). *Project Glass: Live Demo At Google I/O*. https://www.youtube.com/watch?v=D7TB8b2t3QE

Goold, B. J. (2004). *CCTV and policing: Public area surveillance and police practices in Britain. Oxford University Press on Demand, 2004.* Oxford University Press.

Graham, M. (2014). California woman who drove with Google Glass beats traffic ticket. *Reuters*. https://www.reuters.com/article/us-usa-googleglass-trial-dismissal-idUSBREA0F1XR20140117

Gregoriou, C., & Trullinou, P. (2012). Scanning Bodies, Stripping Rights? How Do UK Media Discourses Portray Airport Security Measures? In *Constructing Crime*. Palgrave Macmillan.

Grother, P. J., Ngan, M., & Hanaoka, K. (2019). *Face Recognition Vendor Test Part 3: Demographic Effects*. NIST. https://www.nist.gov/publications/face-recognition-vendor-test-part-3-demographic-effects

Halls, J. (2014). *Inventions that didn't change the world*. Thames & Hudson.

Hauschildt, J. (1999). Opposition to innovations—Destructive or constructive? In K. Brockhoff, A. K. Chakrabarti, & J. Hauschildt (Eds.), *The Dynamics of Innovation* (pp. 213–236). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-03988-5_9

Hawthorne Wilder, H. (1902). Palms and Soles. *American Journal of Anatomy*.

Hess, D. J. (2014). Smart meters and public acceptance: Comparative analysis and governance implications. *Health, Risk & Society*, *16*(3), 243–258. https://doi.org/10.1080/13698575.2014.911821

Hill, K. (2020). The Secretive Company That Might End Privacy as We Know It. *The New York Times*. https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

Hinchy, J. (2020). Conjugality, Colonialism and the 'Criminal Tribes' in North India. *Studies in History*, *36*(1), 20–46. https://doi.org/10.1177/0257643019900103

HMICFRS. (2021). *Getting the balance right? An inspection of how effectively the police deal with protests*. https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/getting-the-balance-right-an-inspection-of-how-effectively-the-police-deal-with-protests.pdf

Holroyd, M. (2020). *Coronavirus: Italy approves use of drones to monitor social distancing*. https://www.euronews.com/2020/03/23/coronavirus-italy-approves-use-of-drones-to-monitor-social-distancing

Hoover, J. E. (1971). The role of identification in law enforcement: An historical adventure. *John's L. Rev.*, *46*, 613.

Horn, J. (2005). Machine-Breaking in England and France during the Age of Revolution. *Labour / Le Travail*, *55*, 143–166.

Horst, M. (2010). Collective Closure?: Public Debate as the Solution to Controversies about Science and Technology. *Acta Sociologica*, *53*(3), 195–211. https://doi.org/10.1177/0001699310374904

HRW. (2020). *Greece: New Biometrics Policing Program Undermines Rights*. https://www.hrw.org/news/2022/01/18/greece-new-biometrics-policing-program-undermines-rights

IBM. (2018). *IBM Response to "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification."* http://gendershades.org/docs/ibm.pdf

Kelly, H. (2013). Google Glass users fight privacy fears. *CNN Business*. https://edition.cnn.com/2013/12/10/tech/mobile/negative-google-glass-reactions/index.html

Klosowski, T. (2022). How Mobile Phones Became a Privacy Battleground—And How to Protect Yourself. *The New York Times*. https://www.nytimes.com/wirecutter/blog/protect-your-privacy-in-mobile-phones/

Koomen, M. (2021). The Encryption Debate in the European Union: 2021 Update. *Carnegie Endowment for International Peace*. https://carnegieendowment.org/2021/03/31/encryption-debate-in-european-union-2021-update-pub-84217

Krier, J. E., & Clayton, P. G. (1985). The Un-Easy Case for Technological optimism. *Michigan Law School Scholarship Repository*, 405–429.

Kruegle, H. (2011). *CCTV Surveillance: Video practices and technology*. Elsevier,.

Latour, B. (1987). *Science in Action: How to Follow Scientists and Engineers Through Soiety*. Open University Press.

Latour, B. (2005). *Reassembling the Social: An Introduction to Actor-Network Theory*. Oxford University Press.

Law, J., & Callon, M. (1988). Engineering and Sociology in a Military Aircraft Project: A Network Analysis of Technological Change. *Social Problems*, *35*(3), 284–297. https://doi.org/10.2307/800623

Leonard, J. (2022). 5 Reasons Why Google Glass was a Miserable Failure. *Business 2 Community*. https://www.business2community.com/tech-gadgets/5-reasons-google-glass-miserable-failure-01462398

Leverentz, A. (2012). Narratives of Crime and Criminals: How Places Socially Construct the Crime Problem1: Narratives of Crime and Criminals. *Sociological Forum*, *27*(2), 348–371. https://doi.org/10.1111/j.1573-7861.2012.01321.x

Levine, P. (2010). Anthropology, Colonialism and Eugenetics. In *The Oxford Handbook of the History of Eugenetics* (pp. 43–61). Oxford University Press.

Lewis, P. (2010). Surveillance cameras spring up in Muslim areas-the targets? Terrorists. *The Guardian*. https://www.theguardian.com/uk/2010/jun/04/birmingham-surveillance-cameras-muslim-community

Lomas, N. (2021). *Sweden's data watchdog slaps police for unlawful use of Clearview AI*. https://techcrunch.com/2021/02/12/swedens-data-watchdog-slaps-police-for-unlawful-use-of-clearview-ai/

Luthra, S., Kumar, S., Kharb, R., Ansari, Md. F., & Shimmi, S. L. (2014). Adoption of smart grid technologies: An analysis of interactions among barriers. *Renewable and Sustainable Energy Reviews*, *33*, 554–565. https://doi.org/10.1016/j.rser.2014.02.030

Mac, R., Haskins, C., & Pequeño IV, A. (2021). Police In At Least 24 Countries Have Used Clearview AI. Find Out Which Ones Here. *BuzzFeed.News*.

Magnet, S. A. (2011). *When Biometrics fail: Gender, Race and the Technology of Identity*. Duke University Press.

Manning, M., Fleming, C. M., Pham, H.-T., & Wong, G. T. W. (2022). What Matters More, Perceived or Real Crime? *Social Indicators Research*, *163*(3), 1221–1248. https://doi.org/10.1007/s11205-022-02924-7

Matyszczyk, C. (2014). Movie theater chains bans Google Glass use. *CNET*. https://www.cnet.com/culture/movie-theater-chain-bans-google-glass-use/

Maxham, A. (2013). *White House Petition for Project Glass to be Banned Surfaces; Would You Sign it?* https://www.androidheadlines.com/2013/05/white-house-petition-for-project-glass-to-be-banned-surfaces-would-you-sign-it.html

Mazzeo, A. (2021). Border surveillance, drones and militarisation of the Mediterranean. *Statewatch*.

McCullagh, D. (2001). Call It Super Bowl Face Scan I. *Wired*. https://www.wired.com/2001/02/call-it-super-bowl-face-scan-i/

Medina, B., & Frank, T. (2019). TSA Agents Say They're Not Discriminating Against Black Women, But Their Body Scanners Might Be. *ProPublica*. https://www.propublica.org/article/tsa-not-discriminating-against-black-women-but-their-body-scanners-might-be

MET. (2020). *Facial Recognition*. https://www.met.police.uk/advice/advice-and-information/fr/facial-recognition/

Mohamed, S., Png, M.-T., & Isaac, W. (2020). Decolonial AI: Decolonial Theory as Sociotechnical Foresight in Artificial Intelligence. *Philosophy & Technology*, *33*(4), 659–684. https://doi.org/10.1007/s13347-020-00405-8

Morison, E. (1968). *Men, Machines, and Modern Times*. MIT Press.

NIST. (2010). *Guidelines for Smart Grid Cyber Security*. https://csrc.nist.gov/publications/detail/nistir/7628/archive/2010-08-31

NIST. (2011). *Face Recognition Technology (FERET)*. https://www.nist.gov/programs-projects/face-recognition-technology-feret

NIST. (2020). *Face Recognition Vendor Test (FRVT)*. https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt

Noble, D. (1995). *Progress Without People: New Technology, Unemployemnt, and the Message of Resistance*. Between The Lines.

O'Brien, P. (1982). *The Promise of Punishment*. Princeton University Press.

O'Neil, C. (2016). *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (1st edition). Crown.

Oreg, S., & Goldenberg, J. (2015). *Resistance to Innovation. Its Sources and Manifestations*. The University of Chicago Press.

Orlowski, A. (2004). Google mail is evil—Privacy advocates. *The Register*. https://www.theregister.com/2004/04/03/google_mail_is_evil_privacy/

Paresh, D., & Jeffrey, D. (2022). Exclusive: Ukraine has started using Clearview AI's facial recognition during war. *Reuters*. https://www.reuters.com/technology/exclusive-ukraine-has-started-using-clearview-ais-facial-recognition-during-war-2022-03-13/

Parry, W. (2013). Las Vegas casinos, others ban gamblers from using Google Glass. *Las Vegas Review Journal*. https://www.reviewjournal.com/business/casinos-gaming/las-vegas-casinos-others-ban-gamblers-from-using-google-glass/

Piazza, P. (2011). Bertillonage: The international circulation of practices and technologies of a system of forensic identification. *Criminocorpus, Revue Hypermédia*. https://doi.org/10.4000/criminocorpus.2970

Pinch, T., & Bijker, W. E. (1984). The Social Construction of Facts and Artifacts: Or How the Sociology of Science and the Sociology of Technology might benefit from Each Other. *Social Studies of Science, 14*(3), 399–441.

Quinn, A. (2016). *The Long Red Scare: Anarchism, Antiradicalism and Ideological Exclusion in the Progressive Era*. UVM ScholarWorks. https://scholarworks.uvm.edu/cgi/viewcontent.cgi?article=1581&context=graddis

Raji, I. D., & Fried, G. (2021). *About Face: A Survey of Facial Recognition Evaluation*. https://doi.org/10.48550/ARXIV.2102.00813

Ramakers, L. (1905). A New Method of Identifying Crimi- nals. *Scientific American*.

Ratcliffe, J. H., Taniguchi, T., & Taylor, R. B. (2009). The Crime Reduction Effects of Public CCTV Cameras: A Multi-Method Spatial Approach. *Justice Quarterly*, *26*(4), 746–770. https://doi.org/10.1080/07418820902873852

Reuters Staff. (2007). *Amsterdam airport deploys body-scanning machines*. https://www.reuters.com/article/us-dutch-airport-security-idUSL1569798620070515

Reuters Staff. (2016). France, Germany press for access to encrypted messages after attacks. *Reuters*.

Rhodes, H. (1956). *Alphonse Bertillon: Father of Scientific Detection*. Abelard-Schuman.

Robertson, C. (2009). A DOCUMENTARY REGIME OF VERIFICATION: The emergence of the US passport and the archival problematization of identity. *Cultural Studies*, *23*(3), 329–354. https://doi.org/10.1080/09502380802016253

Roos, D. (2020). When New Seat Belt Laws Drew Fire as Violation of Personal Freedom. *History*. https://www.history.com/news/seat-belt-laws-resistance

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

Savov, V. (2012). Google announces Google Glass Explorer Edition, $1,500 pre-order shipping next year. *The Verge*. https://www.theverge.com/2012/6/27/3121288/google-glass-explorer-edition-announcement

Schumpeter, J. (1942). *Capitalism, Socialim and Democracy*. Harper & Brothers.

Sekula, A. (1986). Sekula, A. (1986). The Body and the Archive. October, 39, 3–64. *October*, *39*, 3–64. https://doi.org/10.2307/778312

Servantes, I. (2013). Illinois Might Ban Using Google Glass While Driving. *Complex*. https://www.complex.com/sports/2013/12/illinois-google-glass-ban

Shirbon, E. (2010). London's Heathrow airport deploys body scanners. *Reuters*. https://www.reuters.com/article/us-security-britain-scanners-idUSTRE6102O220100201

Singha, R. (2000). Settle, mobilize, verify: Identification practices in colonial India. *Studies in History*, *16*(2), 151–198.

Smyth, F. (1980). *Cause of Death: The STory of Forensic Science*. Van Nostrand Reinhold.

Soper, T. (2013a). Get out, Glasshole: Seattle geet kicked out of restaurant for wearing Google Glasses. *GeekWire*. https://www.geekwire.com/2013/seattle-geek-kicked-restaurant-wearing-google-glass/#:~:text=and%20tech%20workers-,Get%20out%2C%20Glasshole%3A%20Seattle%20geek%20kicked%20out%20of,restaurant%20for%20wearing%20Google%20Glass&text=Seattle%20restaurant%20owner%20Dave%20Meinert,his%205%20Point%20Cafe%20restaurant.

Soper, T. (2013b). Seattle bar that banned Google Glasses has its own surveillance cams. *GeekWire*. https://www.geekwire.com/2013/seattle-bar-banned-google-glasses-surveillance-cams/

Souppouris, A. (2013). *Google expands Glass pre-orders to "creative individuals" with #ifihadglass competition*.

Spaun, N. A. (2009). *Facial comparisons by subject matter experts: Their role in biometrics and their training*. 161–168.

Statewatch. (2021). France: Court bans drone surveillance of demonstrations. *Statewatch*. https://www.statewatch.org/news/2021/january/france-court-bans-drone-surveillance-of-demonstrations/

Stein, S., & Turrentine, L. (2013). Hands-on with Google Glass: Limited, fascinating, full of potential. *CNET*. https://www.cnet.com/reviews/google-glass-preview/

Stern, J. (2013). *Google's Project Glass is Ready, but for Developers' Eyes Only*. https://abcnews.go.com/blogs/technology/2013/01/googles-project-glass-is-ready-but-for-developers-eyes-only/

Streitfeld, D. (2013). Google Glass Picks Up Early Signal: Keep Out. *The New York Times*. https://www.nytimes.com/2013/05/07/technology/personaltech/google-glass-picks-up-early-signal-keep-out.html?_r=0

Stupp, C. (2016). *Five member states want EU-wide laws on encryption*. https://www.euractiv.com/section/social-europe-jobs/news/five-member-states-want-eu-wide-laws-on-encryption

Sturken, M., Thomas, D., & Ball-Rokeach, S. J. (2004). *Technological Visions: The Hopes and Fears that Shape New Technologies*. Temple University Press.

Sykes, K., & Macnaghten, P. (2013). Responsible Innovation. In *Responsible Innovation*. John WIley & Sons.

Thompson, C. (2020). All police in France will wear body cameras by July 2021. *The Connexion France*. https://www.connexionfrance.com/French-news/All-police-in-France-will-wear-body-cameras-by-July-2021-says-Gerald-Darmanin-minister-interior

Tigard, D. W. (2021). There Is No Techno-Responsibility Gap. *Philosophy & Technology*, *34*(3), 589–607. https://doi.org/10.1007/s13347-020-00414-7

Tims, A. (2017). Trauma as travellers face a gender issues going through security. *The Guardian*. https://www.theguardian.com/money/2017/sep/11/travellers-gender-issue-security-checks-airports-how-staff-respond

Tolen, R. (1991). Colonizing and Transforming the Criminal Tribesman: The Salvation Army in British India. *American Ethnologist*, *18*(1), 106–125.

Valentino-DeVries, J. (2020). *How the Police Use Facial Recognition, and Where It falls Short*. https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html

Van den Hoven, J., Lokhorst, G.-J., & Van de Poel, I. (2012). Engineering and the Problem of Moral Overload. *Science and Engineering Ethics*, *18*(1), 143–155. https://doi.org/10.1007/s11948-011-9277-z

van Ratingen, M., Williams, A., Lie, A., Seeck, A., Castaing, P., Kolke, R., Adriaenssens, G., & Miller, A. (2016). The European New Car Assessment Programme: A historical review. *Chinese Journal of Traumatology*, *19*(2), 63–69. https://doi.org/10.1016/j.cjtee.2015.11.016

Waits, M. R. (2016). The Indexical Trace: A Visual Interpretation of the History of Fingerprinting in Colonial India. *Visual Culture in Britain*, *17*(1), 18–46. https://doi.org/10.1080/14714787.2016.1147978

Waldron, L., & Medina, B. (2019). When Transgender Travelers Walk Into Scanners, Invasive Searches Sometimes Wait on the Other Side. *ProPublica*. https://www.propublica.org/article/tsa-transgender-travelers-scanners-invasive-searches-often-wait-on-the-other-side

Wasserman, H. (2015). Moral Panics and Body Cameras. *Washington University Law Review*. https://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=6136&context=law_lawreview

Wei, J. (2012). *Great inventions that changed the world*. Wiley.

Welsh, W. (2001). *Florida County Gives Viisage $2.7 Million Award*. https://washingtontechnology.com/2001/08/florida-county-gives-viisage-27-million-award/350370/

Whittaker, Z. (2021). *Clearview AI ruled "illegal" by Canadian privacy authorities*. https://techcrunch.com/2021/02/03/clearview-ai-ruled-illegal-by-canadian-privacy-authorities/

Winner, L. (1997). Technology today: Utopia or dystopia? *Social Research*, 989–1917.

Winner, L. (2004). Sow's Ears from Silk Purses. In *Technological Visions: The Hopes and Fears that Shape New Technologies*. Temple University Press.

Winter, C. (2019). German police storing bodycam footage on Amazon. *DW*. https://www.dw.com/en/german-police-storing-bodycam-footage-on-amazon-cloud/a-47751028

Woodhams, S. (2021). London is buying heaps of facial recognition tech. *Wired*. https://www.wired.co.uk/article/met-police-facial-recognition-new#:~:text=The%20UK's%20biggest%20police%20force,bid%20to%20track%20down%20suspects.

World Economic Forum. (2018). *Why we need to embrace the tech backlash*. https://www.weforum.org/agenda/2018/01/embrace-the-tech-backlash/

Yeganegi, K., Moradi, D., & Obaid, A. J. (2020). Create a wealth of security CCTV cameras. *Journal of Physics: Conference Series*, *1530*(1), 012110. https://doi.org/10.1088/1742-6596/1530/1/012110