

**Utopias in the Digital Age: Uncovering the Sociotechnical Imaginaries of Facial
Recognition**

Zimo Meng

Thesis submitted to the University of Ottawa in partial fulfillment of the
requirements for the degree of Master of Arts in Criminology

Department of Criminology

Faculty of Social Sciences

University of Ottawa

Table of Contents

Abstract.....	v
Acknowledgement	vi
Introduction	1
Chapter I: Literature Review	5
The Individual and Dividual.....	6
Surveillance and Privacy	8
Surveillance, Control, and Power Imbalance	10
CCTV Cameras.....	11
Online Surveillance.....	12
Facial Recognition Technology	13
The Mechanism: How Does it Work.....	14
Technological Optimism	15
The Social and Cultural Elements.....	17
Surveillance and Resistance: Sousveillance and Advocacy Groups	20
Technology, Surveillance, and Imaginaries.....	24
Conclusion.....	25
Chapter II: Theoretical Framework	27
Technological Determinism.....	27
Cultural Determinism	28
Articulation and Assemblage.....	29
Technology, Politics and Sociotechnical Imaginaries	31
Sociotechnical Imaginaries.....	35
A Unique National Sociotechnical Imaginary	36
Multiple National Sociotechnical Imaginaries.....	37
Sociotechnical Imaginaries as Dynamic and Contextual.....	39
Sociotechnical Imaginaries as Co-evolving.....	40
Sociotechnical Imaginaries as Sites of Power	41
Sociotechnical Imaginaries as Commodified by Corporate Actors	42
Conclusion	43

Chapter III: Methodology	45
Research Design	45
Sampling and Material	45
Characteristics of the Advocacy Groups	47
Material Analysis.....	48
Narrative Analysis and Russian Folktales.....	49
Stone and Causal Stories.....	49
Operationalization of Sociotechnical Imaginaries	49
Combining the Models.....	51
Chapter IV: Narrative Construction.....	58
Introduction	58
Narrative Construction	58
Fight For The Future.....	60
Big Brother Watch	66
Electronic Frontier Foundation.....	70
Surveillance Technology Oversight Project.....	74
Conclusion.....	79
Chapter V: Narrative Analysis.....	80
Introduction	80
Similarities among the Four Advocacy Groups' Narrative	80
Lack of Regulations, Transparency, and Oversight	80
Private Sector: Regulations or a Complete Ban?	83
Collaboration.....	85
FRT: the Algorithm and the Biases	86
The Evolution of Technology	89
Differences Among the Four Advocacy Groups' Narrative	90
The “Big Tech” and the Digital Space	90
Addressing the Dilemma.....	92
The Reliable Allies.....	97
Conclusion.....	98
Concluding Remarks	100

Dystopias and Utopias Present in the Narratives	101
BBW: Walking IDs in an Authoritative State.	101
EFF: Hiding from a Perpetual Facial Dragnet.	101
FFTF: Constant Surveillance of Disenfranchised Masses.	102
STOP: Mass Discrimination Fueled by Search for Profits.	103
Summary	103
Social Life	104
Social Order.....	108
Future Research: Avenues and Opportunities.....	109
References	111
Reference List for Empirical Materials	120
Appendix A: Propp’s 31 Functions and 8 Character Archetypes ...	126

Abstract

The concept and practice of surveillance has long existed in our society, yet with the development of technology, it has taken on new forms and capabilities. As a result, surveillance technology has become integrated in our society, influencing norms and shaping imaginaries surrounding it. While many existing studies have thoroughly examined people's experiences with surveillance technologies, there has been little attention paid to the efforts of advocacy groups in challenging and reshaping the mainstream imaginaries regarding surveillance technology. Using narrative analysis, this thesis aims to address this gap and explore the sociotechnical imaginaries surrounding facial recognition technology of four advocacy groups: a) Fight for the Future, b) Big Brother Watch, c) Electronic Frontier Foundation, d) Surveillance Technology Oversight Project. This study uncovers that these groups' shared sociotechnical imaginary aligns closely with modern liberal ideals, highlighting the possibility of separating public and private life, the necessity for not only moderate government intervention, but healthy commercial competitions, as well as public education. In other words, I argue that resisting against a particular technology and its associated power dynamics does not always represent a challenge to the fundamental power structure.

Acknowledgement

I would like to begin by expressing my deepest appreciation to my supervisor, Professor Dominique Robert. Your constant support, patience, and encouragement motivated me and gave me confidence to overcome the obstacles I encountered during this journey. Thank you for introducing me into Science and Technology Studies, I am immensely grateful for the guidance and mentorship you have provided throughout these two years, and it is truly an honor to be your student! I would also like to extend my gratitude to my examiners, Professor Maritza Felices-Luna and Professor David Murakami Wood, for the effort you dedicated to reviewing and providing insightful feedback and thoughtful questions during the thesis defense. Your comments prompted me to think from various perspectives and allowed me to strengthen my work.

To my dearest friends, thank you for the constant inspiration and support you have provided for me. To Grace, thank you for being there throughout the entire process, I am so glad to have you to count on!

Finally, I would like to express my sincere gratitude to my family. It is your love and great expectations for me that have given me this opportunity to study abroad; it is the support and affirmation you have provided that has filled me with the courage to move forward. Whenever I felt like giving up, thoughts of you would dispel any fear I had. I know that even though the journey ahead may be long and fraught with storms, my family will always be there for me. Grandma, Aunt, Uncle Wang and Zhang, and Mom, thank you for your unwavering love and support, I hope I can make you proud!

最后，我想向我的家人表达由衷的感谢。是您们对我无私的爱与厚望，让我有了这次留学的机会；是您们给予我的支持与肯定，让我充满了前进的勇气。每当我想要放弃的时候，我就会想起我的家人，然后我便不再怕了。因为我知道，纵使前路漫漫，风雨如磐，我的家人始终与我同在。姥姥，小姨，姨夫，大舅，妈妈，谢谢你们对我的爱与支持，我希望自己能成为您们的骄傲！

Introduction

The advancement of technology has brought us a great deal of convenience. Now thanks to the invention and innovations of smartphones, we can not only take pictures and videos and share them on social media for everyone to see, but also know how many steps we walked and how many calories we burned. We can now buy almost anything online, and interestingly, the internet seems to know what we want better than we do. Furthermore, in China, if you forget to bring your wallet, you can pay for your purchase by scanning your face at a vending machine. Indeed, everything appears to be much more convenient than it was twenty years ago, but there are also issues brought about by such seemingly harmless technologies.

The rapid development of technology is a crucial feature and driving force of Western modernity (Rahaman, 2022). We now enjoy the benefits of technological advancements yet at the same time, the process of modernity has reinforced the concept and practices of surveillance (Lyon, 2002). As a result, development of technologies has made mass surveillance much feasible and efficient. To put it differently, we have stepped into a “surveillance society” in which our actions, behaviours and information are constantly monitored, recorded, and analyzed (Murakami Wood, Ball, Lyon, Norris & Raab, 2006).

Despite the fact that initially criminal justice agencies introduced surveillance technology as a ‘techno-fix’ in many countries to address the rising crime rates and combat terrorism, these technologies are now re-designed and used by different agencies and corporations for various reasons, and that eventually, newly forged connections, relations, and problems are produced alongside the introduction of such technology (Kearon, 2012).

For instance, technical designs reveal to us how technology can be utilized to build power over others (Winner, 1986). When we look at the design and usage of surveillance technology, a power relation can be discovered between the surveiller (who use such technology to manage and control the majority of the population) and the surveilled (Williams, 2020).

However, just like Foucault once said, “where there is power, there is resistance” (1978, p. 95). Given surveillance technology’s utilization to target and discriminate against certain populations, along with the concerns raised by mass data collection, monitor, and analytics, many activists and advocacy groups have taken the initiative to resist the power imbalance

caused by surveillance and aim to protect people's freedom, autonomy, and privacy.

Much research has been conducted to examine the use and influence of surveillance technology, and people's experiences of living in the surveillance society. For instance, Kearon (2012) looks at how surveillance technology may lead to a decrease in public's confidence towards criminal justice agencies, and thus challenging its legitimacy; Van Oort (2019) reveals in her research that the use of surveillance in fast fashion retail has led to job insecurity and inequality in the workplace; Venkatesh (2021) argues that mass data collection and analytics have made the exploitation of internet users by surveillance capitalists possible; and Inoue (2019) concludes in his research that with the development of technology, campus police perceived themselves as both empowered and disempowered through the use of surveillance technology. However, not much research was done in relation to right advocacy groups that fought against the misuse of surveillance technology.

In an attempt to address this gap and explore how these groups challenge the mainstream imaginaries surrounding surveillance technology, in this case facial recognition technology (FRT), this thesis aims to examine the sociotechnical imaginaries (SI) of four different rights advocacy groups: The Big Brother Watch (BBW), Electronic Frontier Foundation (EFF), The Surveillance Technology oversight Project (STOP), and Fight For the Future (FFTF). While BBW is based in the UK, EFF, FFTF, and STOP are situated in the US. Yet, unlike the previous two groups, which focus on global surveillance issues, STOP focuses primarily on local surveillance incidents within New York City.

Using narratives analysis, I explored the futures they have envisioned with FRT, and mapped out the dystopias and utopias that populate the groups' positions. The choice of focussing on FRT is due to the fact that the increased demands for surveillance in society have led to the widespread utilization of biometric security solutions (Van der Ploeg, 2003). As a relatively new form of biometric data, facial biometrics are considered as non-intrusive and convenient when compared to other forms of biometrics. This is because the use of FRT does not require direct physical contact (Leong et al., 2020; Singh et al., 2019), while at the same time allowing a distanced and automated identification process (Purshouse & Campbell, 2022; Keenan, 2021; Fussey, Davies, and Innes, 2020).

Under promises like this, FRT is now widely used by both the public and private sectors (Raposo, 2022). Yet, despite these tempting benefits, researchers have pointed out that we must now pay attention to the impacts FRT may pose on society and be aware of the risks associated with its utilization (Ho et al., 2021; Chochia & Nässi, 2021; Raji et al., 2020). Therefore, by focusing on the advocacy groups' discussions of FRT, we can direct our attention to one specific technology, developing a greater and more nuanced understanding of the concerns and issues regarding this technology and what future it is embodying according to these groups.

The analysis shows that far from being subversive, the sociotechnical imaginary envisioned by these advocacy groups, as well as the dystopias and utopias that fuel it, align closely with modern liberal ideals: a tight separation between the public and private lives, moderate governmental involvements to safeguard civil liberty, commercial competition as adjuvants to human rights, and public education as guarantor of democracy. Most importantly, the research reveals that resisting a technology and the power imbalance that it contains and produces does not necessarily equate with resisting fundamental power structures.

Chapter 1 begins by establishing the notion of a surveillance society to demonstrate how surveillance technology has developed and been integrated into our daily lives, influencing the way we behave and the treatments we receive. Next, I highlight some of the concerns and problems that have arisen as a result of the implementation of general surveillance technologies, before focusing on the dilemmas brought by facial recognition technology. Following that, I introduce the concept of resistance towards surveillance technology, focusing on how activists organized as advocacy groups to resist against surveillance and fight to protect people's privacy, autonomy, and online freedom. Finally, I discuss briefly the imaginaries surrounding the concept of surveillance in our society and how such imaginaries may be inverted and challenged by creating new ones.

In Chapter 2, I introduce the theoretical framework utilized to analyze my materials. The introduction to this chapter begins with a discussion on how a deterministic perspective may be insufficient to address the problems associated with technology, and then point out the importance of paying attention to the interconnectedness of technology and society before introducing the concept of sociotechnical imaginaries.

Moving on to Chapter 3, I introduce the methodology used in this study, highlighting the sampling methods and my analytical schemes. I then provide an example of how I utilize such schemes to analyze the samples and construct several narratives for each advocacy groups.

The constructed narratives are showcased in Chapter 4, and later analyzed to reveal their similarities and differences in Chapter 5.

In the conclusion, I identify each group's overarching narrative as well as the dystopias and utopias that fuel them. I then return to the main concept of my theoretical framework and identify the sociotechnical imaginary around FRT shared by the groups under study and what it says about the type of resistance they undertake. The thesis concludes with a short discussion on the avenues and opportunities for future research.

Chapter I: Literature Review

In this chapter, we will first examine the concept of a “surveillance society”, highlighting three major problems brought by surveillance technology. Then, we will focus on the development and adoption of facial recognition technology (FRT) and explore the associated concerns and issues from two different perspectives. After that, we will shift our attention to resistance against surveillance technology, examining how activists may organize as an advocacy group to fight against the utilization of such technology. Finally, we will explore the mainstream imaginaries surrounding the concept of surveillance and how they may be challenged.

Surveillance Society

According to Giddens, how surveillance is practiced is a reflection of the modern way of life, and it is a crucial feature that defines and shapes modernity (Giddens, 1985, as cited in Lyon, 2002). As we enter into this era, we find ourselves in a surveillance society, where technological advancements as well as the state and corporations’ raising demands for controlling and managing the citizens facilitate new forms of surveillance. In this context, our every movement and action are monitored, recorded, and categorized (Marx, 1985).

Over the years, the concept of surveillance society has developed into a major topic that is frequently discussed and analyzed in surveillance studies (Murakami-Wood, 2006). Gradually, this discourse has expended beyond examining state and corporate entities’ utilization of surveillance cameras to monitor and track people’s behaviors in public contexts. Now Studies of surveillance society have extended its scopes to include how through acts of mass data collection, these entities can now gain access to a large amount of personal data and use it as a reference to make judgements and decisions that may influence our lives (Lyon, 2008).

Though some have argued that surveillance can be beneficial to law enforcement practices and social conduct, and that surveillance technology has made preventive policing possible (Walker-Munro, 2019); Living in a surveillance society can pose several problems:

1. **Data Double:** When individuals interact with technology, multiple copies of their “data double” are created. Following that, the state and corporate entities will profile, scrutinize, and judge individuals based on their combined data double (Deleuze, 1992).
2. **Privacy infringement:** When people are put under a constant surveillance gaze, there is

little room for privacy (Zhang, 2010).

3. Power Dynamics: The use of surveillance technology has produced power dynamics between the surveiller and the surveilled, and this may eventually lead to repression, control, discrimination and marginalization (Lyon, 2006).

In the following sections, I will first examine these three problems brought by surveillance society respectively, highlighting how personal data is collected by the state and private entities and then used as basis for decision-making, as well as exploring how these problems may be exemplified in the use of facial recognition technology, before moving on to a detailed introduction and analysis of the technology itself.

The Individual and Dividual

Deleuze once suggested in his 1992 essay that as we interact with technology, we are transformed from being individuals into dividuals; meaning that we are divided and reduced into data representations/simulations. As we keep using the technology (making changes to our applications, updating our information), multiple simulations will be generated, and ‘modulated’ or modified simultaneously. More importantly, our online data simulations will eventually displace us. The “data double” is what the corporations or institutions will look at/evaluate instead of the original one, we have ceased to matter or even to have a reality (Best, 2010).

For example, as Brusseau (2020) argues, it is not him who wants to purchase a “four-wheel drive Land Rover”, but the “fifty-year-old male, married, with incompletely attained professional aspirations wants that powerful vehicle” (p. 14). Additionally, our data doubles will not only replace who we are in reality, but they will also be recombined out of our control “based on the criteria deemed salient by those with access to the information, be the government officials or corporate marketers” (William, 2005, p. 108).

Best (2010) suggests that though individuals tend to underestimate the severity of being replaced by their dividuals online, the generation and recombination of dividuals affects our live chances significantly. For instance, she provided an example of how, if your actions are deemed by institutions as transgressive, they can simply refuse to provide you with their services (such as terminating your internet account, locking your credit cards, etc.). In this

sense, your freedom has been taken away without any actual physical interaction. However, a good proportion of the participants from her research expressed the idea that if the above-mentioned situation happened, they would simply move on to other service providers. Best explains that the participants usually expected a transparent decision-making process from the states, public institutions or corporations who have access to their data. What they did not realize is that the accuracy of their data collected online could not be guaranteed, yet that data is their representation in the cyber world, and the one that will be scrutinized, judged, and served as a reference for decision making. Furthermore, as previously stated, these data and information will be combined in ways out of our control, and sometimes what seems unharmed can be put together in ways to target and discriminate individuals (William, 2005).

For example, the collection of data now can be used to search out and correlate patterns from a large pool of data through the process of data mining. Best explained this process with an example of where correlations of data could be made between the preference of purchasing a certain color of sports car and the likelihood of “defaulting on one’s loan” (2010. p. 11).

Yang (2009) gives another example suggesting that when applying for American Visa, if the information you submitted was deemed as having several indicators for immigration intent by the visa officers, then your application would be denied. These ‘indicators’ are usually separate data and information, such as your gender, level of education, your current territory of residence, and your employment status etc. Yang explains that this separated information would be recombined by the visa officers to determine whether you have a higher inclination for immigration.

For instance, if you were a 30-year-old female who was planning to visit America for undergraduate study, then your application for the entrance visa was more likely to be denied by the visa officer than someone in their 20s planning to do the same thing. This phenomenon occurred because when combining your age, gender, and reason for visiting together, you were evaluated by the visa officer as more likely to have an immigration intent, disregarding what your intention for visiting really was.

Shifting our attention to FRT, when using FRT, our facial features will be analyzed and transformed into unique facial templates. These facial templates can then be used to conduct

identity verification or identification (Buckley & Hunter, 2011). However, as these generated facial biometrics are associated with a specific individual, they will simultaneously be integrated into an important part of the data double (Van der Ploeg, 2003). For instance, when FRT is used in various services and digital platforms, the produced facial information will then be associated with our online activities, allowing the construction of a more encompassing data double that can be used as the basis for decision-making (FFTF, 2021).

With these examples in mind, we can see how judgements are made based on a recombination of individual's data and information, and in this sense, we have no power or control over how, and on what grounds such combinations are made. As Best argues, the actions and judgements are made against the data double/simulations of us, rather than "any kind of transparent, grounded representation of the real" (2010, p.11).

Surveillance and Privacy

According to Zhang (2010), the collecting of personal data and information has infiltrated our lives with irresistible tendency and speed due to the development of technology, agencies' rising desire for control of personal information, and a pursuit of higher work efficiency. In China, the process of data collection and categorization began when a child was born since 1950. With the birth of a child, the household information and residence information are updated and stored; when signing a lease, you must provide both personal and family information to the property manager; and when paying for internet, electricity, and heat, among other services, personal information is once again required by the service providers. Moreover, even when you choose to stay at home and use the internet to pass the time, your data would be collected, stored and analyzed the moment you made an appearance online. During these actions and processes, what is considered private is passed around among service providers, and what should be our private spaces are being invaded and monitored.

It is worth noting that such surveillance is prevalent not only in private life, but also in the workplace, where employers adopt various surveillance technology to watch their employees and ensure that they will be fully productive during working hours (Fuchs, 2013). The following paragraphs are an example of how Chinese employers utilize such technology to monitor employee's work performance.

On November 17, an internal Gome Holdings Group Co., Ltd. document titled “Notice of Punishment for Violation of the Employee Code of Conduct” was circulated on the internet in China. The warning criticized 11 employees for indulging in non-work-related activities in the workplace, such as watching movies, playing video games, and listening to music. The warning even included specific traffic data, demonstrating that the majority of the employees spent more time “fishing” on Tencent Video and Jitterbug while at work (Southern Morning Post, 2021).

This document soon sparked a heated debate. What scared the netizens most was the fact that the surveillance software Gome used on its employees could even record the entire network data, which showed the exact amount of data usage each employee spent on a specific website or application. Many perceived the company’s actions as an infringement of individuals’ privacy. However, the controversy around this incident was soon resolved since there are no laws in China prohibiting companies from monitoring their employees or deeming such measures illegal (Southern Morning Post, 2021).

Another example of workplace surveillance can be seen in Fuchs’ 2013 work where he uses e-Surveiller, a product of SurveillanceTech LLC, as an example to demonstrate the functions and usage of such technology in the workplace. For instance, according to e-surveiller’s description listed on SurveillanceTech’s website, it allows the employers to measure “how much text each employee has written, if and when work time was used for private computer or internet use, how long each employee has worked, etc.” (2013, p. 10). Fuchs later explains that the description of e-surveiller did not mention anything about employees’ privacy, and that this technology can be used by employers as tools to measure each employee’s work performance, and that the data collected from e-surveiller can be used as a reference to fire those who are deemed unproductive. In this sense, Fuchs sees technology as more than just an invasion of individual privacy; he sees workplace surveillance as a means of control and class struggle between employers and employees, in which employers use surveillance to “strengthen capital’s power against workers,” ensuring that workers are always productive during working hours, and thus benefit from the surplus value generated during the process of production (2013, p.10).

When it comes to FRT, Kostka and Steinacker (2021) suggest that both government and

corporations perceive this technology as a powerful instrument, and they are now promoting its utilization to satisfy their own interests. However, it is important to note that the use of FRT has raised several ethical concerns. For instance, there are biases inherent in the algorithm itself, subjecting certain populations to the risk of being misidentified. Additionally, researchers have pointed out that when FRT is utilized secretly, without acquiring individuals' consent first, it also infringes upon people's rights and privacy (Kostka & Steinacker, 2021; Tene, 2011).

As previously mentioned, facial biometrics transformed and collected by different actors may eventually be associated with other personal data (Van der Ploeg, 2003). Such association has only worsened existing privacy concerns as if the databases containing our facial biometrics are hacked, the associated information is also at the risk of being stolen (Naker & Greenbaum, 2017).

We can see from these interactions that a power relation has been formed between those who use surveillance to manage, control, and benefit and those who are being surveilled. In the following sections, I will first provide a general overview of the power dynamic in our society produced by the employment of surveillance technology, and then demonstrate how a power imbalance between the surveiller and the surveilled can be formed and exacerbated by exploring two areas where power dynamics are strongly perceived by scholars: CCTV cameras, and online surveillance. After that, we will delve into a more complex technology – facial recognition technology (FRT). This will involve an exploration of the issues associated with its development and utilization from two unique perspectives.

Surveillance, Control, and Power Imbalance

As we interact with different technology, we have been turned into several 'dividuals' that contain a part of our information which is then collected and analyzed by various agencies and corporations (Deleuze, 1992). David Lyon (2010) explains that as our data/information is being monitored and analyzed, a category and social position will be assigned to us. To put it differently, discrimination and marginalization are embedded in technology. For instance, though the original aim for surveillance technology was to deter crime and fight terrorism, they have also been used as a method to sort "foreign workers, immigrants and asylum seekers" into two categories: the "desirable" and the "undesirable" (p. 10), in other words, instead of

everyone being affected by the act of surveillance equally, people are now sorted into those who need to be controlled, and those who are free from such control.

Adding to Lyon's statements, Smith (2016) states that the categories individual is assigned into (desirable or undesirable) will also influence the treatments he/she will receive in specific situations. In this sense, individuals are evaluated solely on the data and information collected on them, and different meanings are attributed to these data and information based on cultural assumptions and biases. During this process, social inequality will be maintained and exacerbated. One example of how surveillance technology reinforces the existing systematic discrimination can be seen in the use of CCTV cameras.

CCTV Cameras

In his 2005 research, Norris argues that the adoption of CCTV by law enforcement agencies was at first aimed to democratize the surveillance gaze, based on the fact that camera would not discriminate or differentiate between different social groups, and that electronic surveillance technology could help to eliminate corruption and discrimination. The reality, however, was much different from what had been anticipated. Instead of being an impartial "techno-fix" for the criminal justice agencies to deter and solve crimes, the use of CCTV cameras has intensified the existing categorizations and discriminations (Graham, 1998).

Norris reveals that most CCTV operators have a strict protocol to follow, which usually forbid them from tracking individuals on the street unless they are deemed "suspicious", but neither the protocol nor the training clarifies what actions might be classified as suspicious. Therefore, whether an action or behavior is seen as suspicious by the operators are entirely based on common sense or self-evident (2005). Furthermore, Norris and Armstrong's research discovers that young black males are more likely to be tracked and targeted by CCTV operators based on how they look and dressed rather than the way they behave. They argue that this bias may be attributed to the overrepresentation of young black males in prison populations, which in turn, leads to increased attentions received from CCTV operators (1999).

In conclusion, what CCTV operators consider suspicious is based on cultural assumptions and biases as a result of a lack of definition of what constitutes suspicious behaviour in their operating protocol and work training sessions. Therefore, instead of democratizing the

surveillance gaze, the use of electronic surveillance technology is instead perpetuating and reinforcing the long-existing systematic discrimination in our society.

Online Surveillance

Now turning our attention to online surveillance, Mark Andrejevic (2014) expresses the concerns that with us entering into the big data era, people are experiencing a lack of control and knowledge over their own data and information. This has led to a sense of powerlessness among those whose data is being collected and analyzed.

In her research, Best (2010) discovers a lack of concerns from her research participants regarding to how their data may be used by the data collectors. The majority of the participants believed that they were not a worth-while target for neither the state nor the corporations, and they argued that as long as they did nothing wrong, there would be no need to fear about surveillance or data collection.

Even after being informed about the potential harms associated with data collection and surveillance, the participants perceived a trade-off between these possible damages (i.e. privacy infringement) and the convenience provided by technology. In this case, despite the acknowledgement of potential risks, a significant number of participants chose to participate in the process of surveillance willingly. Such result has shown that people would comply with being surveilled if data collection and their participation in surveillance is a prerequisite for them to use the technology or services provided by different entities. Moreover, some also believed that it would be impossible to stop participating in the digital life, due to society's increased dependency on technology. From these statements, Best recognizes that the problem is not a lack of concerns for the risks associated with data collection and surveillance, but rather a lack of viable alternatives for people to choose from (2010).

Adding to Best's argument, Venkatesh (2021) gives an interesting analogy that draws a parallel between the roles of the workers and entrepreneurs in industrial society, and those of internet/technology users alongside the capitalists in contemporary surveillance society. On the one hand, workers sell their labor force as a commodity in exchange for wages to purchase necessities, and the surplus value they produced through working is exploited by the factory owners; on the other hand, internet/technology users sell their personal data to entrepreneurs

in exchange for the services they provide, and eventually, they are exploited for economic benefits by surveillance capitalists.

From these examples, we can see that the utilization of surveillance technology has led to a power dynamic between the surveiller and the surveilled: The surveilled individuals find their data exploited by those who conduct the surveillance, while being left with limited or no viable alternatives to choose from. In the meantime, the surveillers reap benefits from the collected data, whether in the form of commercial gains or claimed ‘increased security’, often disregarding the potential harms they may pose to the surveilled.

Facial Recognition Technology

In this section, we will move on from the use and influence of general surveillance technologies to a more advanced and complex one: facial recognition technology (FRT). It is important to note that, unlike general surveillance tools (such as CCTV cameras), which facilitate constant seeing and monitoring, FRT makes immediate recognition possible. As a result, according to Gray (2003), FRT may be able to “bring the disciplinary power of panopticon surveillance into the contemporary urban environment” (p. 314), and better identify and sort out dangerous individuals, offering increased security.

Purshouse and Campbell (2022) reveal that the development and utilization of FRT have exacerbated the power imbalance in society. They explain that the increased adoption of FRT by law enforcement has given rise to problems due to a lack of regulations and oversight. However, government and domestic courts often fail to acknowledge this issue. According to Purshouse and Campbell, FRT is now being used to further oppress and discriminate against the marginalized population. Police are found to utilize FRT at public gatherings, aiming to identify “persons of interest” (p. 3). This not only poses risks to individuals’ rights and privacy, but also turns the general public into targets of mass surveillance and identification, with no power to opt-out from this covert surveillance gaze.

Similarly, Leong (2019) has expressed concern that FRT provides the government and corporation with immense power to monitor, track, and even manipulate the general public without their knowledge or consent. It is even more concerning that FRT is not only used by authoritarian governments to reinforce their control over the citizens, but it is now visible in

democratic states, where FRT is used for oppression and discrimination, disregarding individuals' privacy and civil liberties.

As previously discussed, though FRT can be beneficial in some perspectives, much more problems are being pushed to the surface (Raposo, 2022; Purshouse & Campbell, 2021; Chochia & Nässi, 2021). In order to adequately assess the risks associated with FRT, Leong argues in her 2019 research on FRT and the future of privacy that we must first understand how the technology functions technically.

In the following sections, I will first introduce the mechanism of FRT, demonstrating how it works to extract facial features and identify individual's identity before moving on to examine how FRT is perceived by engineers (who focus primarily on analyzing and improving the algorithm/mechanism of FRT to solve the associated problems) and social scientists (who study the relationship between society and technology) respectively to reveal their perceived benefits, problems, and solutions to the issues brought on by FRT.

The Mechanism: How Does it Work

Facial recognition is a biometric system that can identify an individual based on his/her unique physiology. To begin, facial recognition software detects individual faces in images or videos. Following the detection of a face, the individual's facial features will be measured and transformed into multiple nodes/facial landmarks (Hirayama, Iwai, and Yachida, 2003; Chou et al., 2017). According to Amazon Web Services' website on FRT (2023), these facial landmarks might include: "distance between the eyes", "distance from the forehead to the chin", "Distance between the nose and mouth", and so on.

Once the face has been mapped into a "template" based on the landmarks measured and extracted from individual's facial features, it will then be converted into binary codes and stored in the system. When a new image/person needs to be identified, the system will first scan the image/face before creating a template based on the measured facial landscapes. The template will then be converted into codes to be compared with the ones previously collected and identified in the database (Leong, 2019).

It is worth mentioning that different facial recognition programs will measure and convert these landmarks differently, yet the technique remains the same. In other words, regardless of

the program employed, three distinct processes are required: image acquirement and detection, facial features analysis, and identity recognition (AWS, 2023).

Technological Optimism

According to Islam, Toufiq, and Rhaman (2017), many researchers view biometrics as an effective solution to today's problems with user identification and security. They claim that FRT based personal identification has yielded some highly accurate results and created secured systems that are now used in a variety of practical fields. For instance, Carlos-Roca, Torres, and Tena (2018) suggest that, given the current state of internal security and terrorist threats, FRT has proven to be a more efficient and effective border control and management technique. It has reduced the time required for travellers to cross the border and the workload for the border control officers. Moreover, some researchers express the belief that comparing to other biometric characters, facial data and recognition are non-intrusive, easy to use without being noticed by the users or those being monitored (Singh et al., 2019; Leong et al., 2020).

Apart from collective use of FRT by the state and corporations, there is also an increase in personal use of such technology. For example, individuals can now unlock their phones via 'face id', increasing security and efficiency at the same time (Chambino, Silvia, and Bernardino, 2020).

While FRT has undoubtedly brought us with much convenience, problems have also occurred with the development and implementation of such technology. For instance, critics have pointed out the fact that the accuracy of FRT is subjected to multiple factors, such as lighting, shading, position, expression, occlusion etc. (McLindin, 2003; Li, Gong & Liddell, 2002; Hirayama, Iwai & Yachida, 2003; Singh et al., 2019). Researchers and scientists reveal that FRT algorithms are usually trained within a controlled environment, meaning that a good testing performance is achieved by using well-lit frontal face photos and images. However, the real-world application of FRT introduces unpredictable factor, leading to variations in algorithm performance (Ng, Tay & Goi, 2015; Li, Gong & Liddell, 2002).

Researchers have suggested several solutions to deal with the issues brought by these uncontrollable factors. For example, Chou et al. (2017) proposed a "robust real-time face recognition system that utilizes regression tree based method to locate the facial feature points"

(p.1), so that the recognition system will be able to better identify and recognize the face region and facial expression, and perform the analyses geometrically. Chou's team concludes that an accurate detection of facial image will increase the performance and accuracy of facial recognition and identification. Additionally, McLindin, Butavicius, and Meaney (2003) have acknowledged that because previous FRT tests were primarily conducted in a laboratory setting, the results of facial recognition may not be reliable once applied in an operational environment. In order to increase the accuracy of FRT, McLindin and their colleagues collected facial data from operational trials, so that the trained system will be able to provide a more accurate data in an uncontrolled environment (2003). To further increase the robustness of current facial recognition technology, Hirayama, Iwai, and Masahiko (2003) have proposed a facial recognition system composed of their "flexible matching and rapid parallel estimation of facial position and scale" (p. 3236). To put it differently, their system is able to measure the facial scale and position at the same time, and thus increasing the accuracy and efficiency of dynamic facial recognition.

It is worth mentioning that some scientists have acknowledged privacy and security issues raised by FRT and have offered various technological solutions to deal with these problems. For instance, according to Leong, Phan, Baskaran and Ooi (2022), their program removes identifiable facial information and relies solely on a "one-dimensional spatial information" (p. 11). In their case, the identification/verification is performed without individual's facial appearance being revealed to the public view, and thus privacy is preserved.

In conclusion, from a technological optimistic perspective, scientists and researchers see FRT as posing more benefits than problems. They consider the unstable accuracy of FRT to be a challenging problem and have identified lighting, positions, expressions etc. as factors that may influence the recognition results. To tackle these challenges, many researchers start from a technological deterministic perspective. Some of them argue that in order for FRT to be more accurate, facial data from environments other than controlled lab settings should be included to train the algorithm (Singh et al., 2019; Ng, Tay & Goi, 2015; McLindin, Butavicius, and Meaney, 2003). Others have proposed that improved algorithms can also be developed to solve these problems (Chambino, Silva, Bernardino, 2022; Chou et al., 2017; Islam, Toufiq, and

Rhaman, 2017; Goodall, Gibson & Smith, 2012; Hirayama, Iwai & Yachida, 2003; Li, Gong & Liddell, 2002).

In the next section, I will highlight how the issues with FRT are perceived by social scientists. In other words, how they balance the benefits and problems of FRT from a sociological perspective.

The Social and Cultural Elements

Both the engineers and the social scientists see FRT as a non-intrusive technique for performing recognition and identification tasks without being realized by the individuals under surveillance. However, while engineers see such non-intrusive nature of FRT as beneficial and efficient, believing that any problems brought by technology can be solved through analyzing and improving the algorithms (Singh et al., 2019; Leong et al., 2020), social scientists perceive it as problematic. They suggest that in order to tackle the problems, we must either focus on the causal relation between culture and technology or consider their interconnectedness (Raposo, 2022; Purshouse & Campbell, 2022; Chochia & Nässi, 2021).

To begin, Raposo (2022) argues that though FRT based authorization and authentication can provide consumers with many benefits, it has also facilitated mass surveillance. In the case of FRT, individual's biometric information (facial data) is being collected automatically, and no consent is given in these instances. Raposo further suggests that this situation has raised serious privacy concerns and created a power imbalance between the "data controller" and the "data subject" (p. 13).

Similarly, Chochia and Nässi (2021) express their concern that, apart from the convenience brought by FRT, the adoption of such technology also brought challenges to individual privacy, data security and human rights. They explain that FRT may lead to discrimination, meaning that the already marginalized populations in our society might be specifically targeted/identified under FRT without their consent, exacerbating the long-existing systematic discrimination.

What is more, Ho, Black, Agrawala and Li (2021) suggest that in order for academic and civil organizations to better evaluate and assess the benefits and risks of FRT, we need to first understand the accuracy of FRT in the precise context of its application. They not only highlight

the inadequacies of training FRT algorithm in a controlled environment, as identified by engineers, but also point out that FRT is integrated in a human system. Such integration implies that given the inherent biases within our society, users of FRT may selectively rely on the recognition results, using it to support their biased beliefs and conducts.

When such human bias is combined with a lack of diversity in the database used to train the algorithms, it will eventually lead to false identification, further marginalizing those who are already subjected to discrimination.

As exemplified in the previous discussions, one of the major differences between how engineers and social scientists perceive FRT related problems is that while engineers view the issues from a technological perspective and believe that these problems can be solved through technological innovation and advancement (technological determinism); social scientists see the problems with FRT as stemming from not only the technological domain but influenced by human/cultural factors, and that to solve these problems, technological solutions will not be enough. It is worth mentioning that even within the field of social science, researchers have expressed different opinions and proposed various suggestions regarding the adoption of FRT.

Contrary to the engineers, researchers in the field of social science evaluate FRT from either a cultural determinist's position or an angle that acknowledge the interconnectedness of the technology and the culture.

For example, Raposo (2022) and others (Purshouse & Campbell, 2022; Chochia & Nassim, 2021) argue that the privacy and security issues raised by FRT are the result of a lack of clear regulations regarding "how, when and for what purposes this technology can be used in specific fields" (Chochia & Nassi, p. 14, 2021), and that with appropriate regulations in place, we will finally be able to enjoy the benefits of FRT while avoiding the risks associated with it.

Additionally, according to Leong (2019), the invention of FRT did not cause discrimination or prejudice against certain populations. Rather, we need to acknowledge the fact that this technology is being "implemented into a world already facing the problems of biased human systems", and that FRT is just another "tool in the tech box" (p. 114) that allows the government to fulfill its desire to track, monitor and manage its citizens in a more advanced manner. Leong suggests that what the future will be like depends on how the society and culture react to

balance government efficiency and national security.

Unlike Leong's cultural deterministic approach to issues associated with FRT, which contends that once we fix the culture, we will automatically solve the problems brought about by technology, various researchers argue that in order to understand the situations with FRT, we have to pay attention to the interconnectedness of culture and technology.

According to Williams (2020), when analyzing a specific technology, we must look back to the historical moment in which it was designed and deployed. He explains that for some technologies, there are "prejudicial values" ingrained in "every aspect of their commission, design, and construction" (p. 580). Using FRT as an example, Williams argues that simply adding more diversity to the photos used to train the algorithms will not solve the problem of FRT's disproportionate impact on certain populations. The problems stem not only from the deficiency of the algorithm, but from the strong influence of the cultural context in which the technology is designed and used.

In this sense, FRT is more than just a neutral tool waiting to be used by state actors to meet their different needs. Rather, the flawed algorithm reflects the biases and values prevalent in our society while at the same time, reinforcing these biases through its utilization.

Similar to Williams' argument, in their research on police use of FRT, Fussey, Davies, and Innes (2021) suggest that instead of saying such technology is "automated", it should be "assisted" facial recognition. They explain that behind the design and use of FRT lies not just the algorithms. When thinking about facial recognition, we should keep in mind that its use constitutes a "socio-technical assemblage that both shapes police practices yet is also profoundly shaped by forms of police suspicion and discretion" (p. 327). In other words, Fussey and his colleagues argue that in order to avoid technological determinism, researchers must acknowledge the impact of human intervention and interpretation. For example, FRT's lower accuracy in recognizing female and people of color has led to a higher rate of false positives within these groups (p. 338). Once this factor is combined with the fact that police are often influenced by social biases and focus their attention mainly on racial minorities, the use of FRT by law enforcement will further intensify the societal issues with marginalization and discrimination.

What is more, Stark (2019) draws an analogy between FRT and Plutonium, claiming that, while some believe that FRT benefits society, the risks outweigh such advantages, just like how it is with nuclear technology. Stark explains that because of the flaws within the algorithm, the technology itself is harmful regardless of its creators' intention, and that its use will only exacerbate the problems in our society. However, apart from the technological flaws, it is important to note that FRT was invented and is used by human, thus the algorithm and the way FRT is utilized will also reflect the bias of the human system.

In conclusion, both the engineers and the social scientists have acknowledged the benefits and problems associated with FRT. However, while the engineers perceive FRT's problems from a technological deterministic perspective, the social scientists perceive such problems in two ways: as a cultural dilemma (cultural determinism), or propose that we need to recognize the interconnected nature of technology and culture. In other words, we must think about what such interconnectedness has revealed, and whether the technology in question can really be separated from the culture to be controlled and used safely and impartially.

Though Raposo (2022) and others argue that proper regulations will provide effective constraints on the use of FRT, there are still challenges when it comes to the definition and criteria of what constitutes "proper regulations". For instance, Purshouse and Campbell (2022) point out that while police use of FRT in Britain is controversial among the general public, the government and domestic courts still perceive such use as being properly regulated, thus ignoring the voice of the public. As many (Best, 2010; Venkatesh, 2021; Raposo, 2022) argue that there is a power imbalance between those who have access to our data (data controller) and those who are subjected under surveillance gaze (data subject). The data subjects may not even know that they are being exploited by the data controllers, and that they have little power to resist against the exploitation of their data since technology has been integrated into our lives. Therefore, now is the time for someone to speak up and raise people's awareness of the dilemma, as well as mobilize individuals to fight for privacy, security, and freedom.

Surveillance and Resistance: Sousveillance and Advocacy Groups

David Lyon (2007) once suggested that although the problems brought by surveillance technology has been widely explored by scholars located not just in the global north, but also

the global south, the idea of resistance and the activities of advocacy groups have yet to be fully examined. He suggests that though most of the time, these resistance and actions of the advocacy groups can not be described as a social movement, they do have the potential to influence certain political decisions. Therefore, it will be meaningful to see how these groups resist against what they perceive as inadequate use of surveillance technology.

Like many reveal (Leese, 2014; Introna & Gibbons, 2009; Andrejevic, 2014) the states' desire for control and management of their citizens have increased, particularly following the 9/11 incident. This has caused a power imbalance that needs to be addressed and solved in order to avoid problems caused by such asymmetrical relation.

For example, Best's (2010) research has shown the fact that there is an existing gap between public's knowledge on surveillance technology (how they think the technology work) and how these technologies are actually experienced. Adding to Best's findings, Andrejevic (2014) reveals that as individuals interact with technology and services provided by different agencies and corporations, a large amount of data will be generated and combined for analysis. However, the users themselves do not have access to this generated data and information. Andrejevic further claims that even if they are given such access, it will be impossible for the majority of the general public to understand or interpret this data/information, let alone make use of it. Together, these findings have revealed a major problem underlying the asymmetrical relation between those who monitor, collect, and analyze individual's data, and those who have been put under surveillance – a lack of information. To elaborate, most of the time, problems surrounding surveillance technology are not clearly made visible to the general public, and that individuals often lack sufficient information or education in this specific area.

Introna and Gibbons (2009) add that the increasing expansion of the installation of surveillance technology by states, alongside the lack of relevant information, have resulted in a decreased public's confidence towards government's ability of managing and securing the collected data. As a result, the idea for resistance has been pushed to the surface.

One way to address the power imbalance caused by surveillance is through 'sousveillance'. According to Mann and Ferenbok (2013), one of the challenges brought by modernity is the regulation and discipline of the majority. Foucault's Panopticon theory is often widely used as

“a power metaphor for the distribution of institutional power that works through the fear of being watched” (p. 23). They explain that in the panopticon system, each individual is ‘localized’ into different identities (docile bodies) and then watched by a prison guard who sees the bodies of the prisoners while remaining unseen. This characteristic of panopticon suggests that overtime individuals will learn to discipline themselves due to the fear of punishment, thus we have the idea of ‘the few watch the many’. However, with the development of technology and portable devices many argue that now surveillance technology does not just serve as an all-seeing eye of the panopticon, where the few watch the many, it has also made ‘sousveillance’ possible, where by using different technology, the many now have the ability to watch/surveill the states, and expose potential harms in their practices (Newell, 2020; Brucato, 2015; Mann & Ferenbok, 2013).

According to Brucato (2015), the release of the Rodney King video in 1991 shocked the public sphere since police violence was not recognized as a critical issue, and it was challenging to prove prior to the invention and usage of videotapes or mobile recording devices. The Rodney King case demonstrated the power of technology and mobile recording, showing that no one could escape from the surveillance gaze. Furthermore, with the help of social media, video recordings of police misconducts can now be widely disseminated and made visible to the public sphere (Mann & Ferenbok, 2013). In this sense, sousveillance attributes a portion of power to the surveilled, contributing to balancing the asymmetrical power between the states and the general public.

Apart from the idea of sousveillance, Introna and Gibbons (2009) state that advocacy groups that aim for social, economic and political change are the most suitable actors to engage in the action of sousveillance. They explain that one of the key elements for resistance is “the ability of different actors to make visible the variety of state surveillance practices and the connections between such practices” (p. 237). They propose that resistance becomes possible for the general public only when advocacy groups consisting of various actors step forward to “expose and make visible” the potential harms and practices brought by the adoption of surveillance technology (p. 234).

Similarly, Venkatesh (2021) proposes that we can learn from the workers’ strategies in the

industrial society and create a “data union” to aid in educating people about data collection and surveillance. In this way, people will gain a better understanding of how surveillance works and will be alerted to potential threats they may not be aware of before. Raising people’s collective consciousness is crucial, because it is only when they realize their shared predicament will they stand together to fight for their common good. What is more, once we develop a collective consciousness within the data union, we will be able to negotiate with those who have access to our data, bargaining for more benefits and thus working together to address the power imbalance caused by surveillance technology.

One example of how the advocacy groups addressed the problems of surveillance technology can be seen in the case of the banning of Amazon’s facial recognition technology – Rekognition.

Williams & Lynch (2018) indicate that on May, 29th, 2018, Electronic Frontier Foundation (EFF) joined a coalition formed by privacy/civil right advocacy groups in the fight against the use of Rekognition by law enforcement agencies. They argue that the use of facial recognition system will lead not only to an infringement to individual’s privacy, but also exacerbate discrimination against the racial minorities. For instance, without receiving any form of consent or giving prior knowledge, Rekognition was used by Immigration Customs Enforcement to scan state driver’s license with the purpose of identifying undocumented individuals (Aboulafia, Fritzius, Mears, & Nix, 2021).

On June 11th, 2020, as a result of the concerns and protests raised by privacy/civil right advocacy groups and the ongoing police brutality against racial minorities, Amazon decided to ban law enforcement use of their FRT for one year (Greene, 2020). Later in 2021, Amazon announced that it would extend this ban indefinitely until the problems associated with police utilization of FRT are properly addressed with regulations (Harwell, 2021).

Additionally, in both the UK and the US, several advocacy groups have formed coalitions to fight against states mass surveillance after the event of the Snowden leaks (Wascher, 2017; Dencik, Hintz, Cable, 2016). Dencik et al. argue that in the UK, the voice of advocacy groups is very significant and hold an important position in the debate over the use of surveillance technology. They state that advocacy groups “have formulated fundamental critiques of

surveillance practices, but they have also, increasingly, been recognized as a legitimate participant in policy debates that holds relevant expertise” (2016, p. 4). In this sense, it shows that the efforts put up by advocacy groups were not in vain, their materials and information online have equipped people with relevant knowledge around surveillance, and they organize together with a common interest to protect people’s privacy, freedom, human right, and autonomy in this surveillance society.

Though advocacy groups have proven to be effective in addressing issues caused by surveillance technology and protecting individuals from the surveillant gaze, there are still imaginaries prevalent in our society that limit people’s awareness of the potential of resistance. In the next section, I will present the dominant imaginaries surrounding surveillance technology and how such visions can be challenged and replaced.

Technology, Surveillance, and Imaginaries

As technology advances, the concept of surveillance becomes increasingly integrated into our daily lives. As Lyon (2017) suggests, certain imaginaries surrounding surveillance technology have dominated the general public’s perceptions and reactions to it.

In his research, Kearon (2012) reveals that every time surveillance technology fails to deliver what we expect, people choose to blame those who operate or implement the technology, rather than the technology itself. Kearon explains that such belief is prevalent because the concept of surveillance and technology is culturally created and maintained. People tend to imagine that machines are objective, neutral, impartial, and capable of bringing significant changes to society. In this sense, the symbolic meaning of surveillance technology is more important than its ability, as technology is often perceived as a force “outside of social and political influences” (Sturken and Thomas, 2004, as cited in Kearon, 2012, p.425).

Adding to Kearon’s arguments, Lyon (2017) states that now we are living in a surveillance society, where the presence of surveillance has become naturalized. Similar to Best’s (2010) findings, Lyon suggests that with an increased integration of surveillance technology into our lives, people perceive that it is impossible to avoid being surveilled by the states or corporate entities. Therefore, instead of resisting against surveillance, people tend to comply with it. This widespread imagination of surveillance technology being the all-seeing eyes of the panopticon

has been planted deep inside the minds of the general public, leaving little room to imagine an alternative future or possibility.

However, just like Kazansky and Milan (2021) propose, these seemingly unchangeable imaginaries are now being challenged by advocacy groups. They strive to shed light on problems and information surrounding surveillance technology and offer guidance and technical interventions to help the general public resist against surveillance technology and promote positive social change. According to Kazansky and Milan, these imaginaries represent collectively held visions by groups of people which contain shared ideals and beliefs about technology. Therefore, analyzing the sociotechnical imaginaries that populate the activists mind enables us to see how advocacy groups work to invert the dominant imaginaries surrounding surveillance technology and gain insight into their vision of a future utopia without (or with limited utilization of) such technology.

Conclusion

The advancement of technology has brought us numerous comforts, but also the integration of electronic surveillance into our daily lives. Though surveillance technology was initially adopted by law enforcement agencies to fight terrorism and severe crimes, the widespread use of it has also exacerbated and made prevalent many existing problems in our society.

Like many suggest that since the concept of surveillance has been naturalized in people's perception, it is seen as unavoidable in our daily routine (Lyon, 2017; Kearon, 2012). However, as we will explore in the next chapter, the understanding of surveillance varies on the conceptual level, depending on whether the analysts adopt a technological or a cultural determinist position or choose to avoid both. The literature on sociotechnical imaginaries might be a way out of the cultural vs technological determinism. For example, Kazansky and Milan (2021) argue that now we have various advocacy groups who are trying to invert the dominant imaginaries by offering guidance and technique to help the general public defend themselves in this hyper-surveillance society, as well as producing and imagining a new future where people are empowered to fight for their rights and privacy. The rationale behind their thinking, which also serves as the driving force for my research, will be further developed in the following chapter. Once again, my thesis will delve into the sociotechnical imaginaries of four

different advocacy groups (BBW, EFF, STOP., and Fight For the Future) by analyzing the materials posted on their official websites to explore the dystopia and utopia that populate their imaginaries, and examine how they constructed such visions.

Chapter II: Theoretical Framework

With a thorough review of the existing literatures on surveillance society, the issues associated with different surveillance technologies, as well as the idea of resistance and imaginaries, we will now move on to explore the theoretical framework that guide my understanding and analysis of the collected materials.

Overtime, researchers in the field of Science and Technology Studies (STS) have investigated the historical and social contexts of and relationships with science and technology, and various explanations for technology-related problems have been presented and addressed. These explanations can be classified into two categories:

1. Problems are caused by the technology.
2. Problems are caused by the cultural/social/economic system.

In the following sections, I will first examine these two perspectives in terms of technological and cultural determinism respectively, and then introducing a third perspective which focuses on the interconnected nature of technology and society/culture.

Technological Determinism

According to Winner (1986), a technological deterministic perspective suggests that technology is separate from and independent of society, in that it will mold society to “fit its patterns” (p. 20). In other words, the shape and form that a society takes is the result of the adaptation to technology.

Similar to Winner’s claim that society changes according to technology, Slack and Wise (2005) state that technological determinism considers technology as a force that causes effects which lead to cultural change. To put it differently, technology is seen as having the ability to impose effects and changes on society, and that social, historical, and cultural contexts are deemed irrelevant.

Inoue’s 2020 research on the concepts of surveillance and sousveillance is one example of technological determinism. Elaborating on Palmer’s (2016) statement on body-worn cameras, Inoue suggests that the development and adoption of body-worn cameras has made both the “governing of and governing by police” possible (p. 233). For instance, during his ethnographic research with the University of Kentucky Police Department, Inoue learned that police are

required to turn on their cameras whenever they interact with the public.

The recording of police-public interactions has enabled *sousveillance* (governing of police), it ensures police misconducts are recorded on tape, and in some instances the recorded videos are uploaded to the internet with open access, allowing the public to view these videos. The use of body-worn cameras has also made surveillance (governing by police) possible, because as it records every interaction between the police and the public, it protects the police from false accusations by the public.

As previously mentioned, Slack and Wise (2005) propose that technological determinism views technology as causing different effects in society, and that it may eventually lead to cultural change. When we look at Inoue's research on surveillance and *sousveillance*, we see that body-worn camera (the technology) has enabled both surveillance and *sousveillance* (the effect), and that it transforms Foucault's concept of Panopticon, in which the watcher is invisible, to a model of "new governance" (p. 250), where the "watcher" (body-worn camera) is made visible and integrated into society. As a result, instead of the idea of "watching without being watched" (p. 250), a mutual surveillance (surveillance and *sousveillance*) is encouraged and has become a social norm.

Cultural Determinism

Unlike technological determinism which holds that technology shapes society, cultural/social determinism suggests that as society/culture develops, it needs new technology to achieve its goals. To put it differently, society's needs and desires are reflected through the development and adoption of various technologies (Slack & Wise, 2005). Therefore, when we look at technology-related problems in society, we must focus our attention on the social/cultural system in which these technologies are embedded, rather than the technologies themselves (Winner, 1986).

In his 2013 research on political economy and surveillance theory, Fuchs explores how surveillance technology is tied to the capitalist economy. He explains that the increasing desire for economic gain in the capitalist society has led to a heightened need for surveillance. For example, Fuchs suggests that surveillance technology is used in the workplace to monitor and control workers' behaviors. It is used as a convenient tool by the employers to measure

employees' work performance and ensure maximum profit. Furthermore, Fuchs mentions that technology has made monitoring and evaluating consumer data much easier for corporations. As a result, it has led to a phenomenon known as "social sorting", in which services are provided and promoted to certain users based on an analysis of personal data collected in various ways.

In conclusion, whether it is workplace surveillance or social sorting in the fields of advertising and service providers, they are not the results of the adoption of various technologies (or as the effects caused by technology). Rather, modern society is built on the concept of constant surveillance, and the phenomenon of social sorting has long existed in our society (Fuchs, 2013). Because of society's/culture's growing desire for effective control and management of its citizens, technologies are being developed and adopted as tools to facilitate the monitoring and management process. Therefore, instead of focusing on technology, a cultural/social deterministic perspective argues that we must focus our attention on the cultural/social system in which these technologies are embedded (Winner, 1986; Slack & Wise, 2005).

Articulation and Assemblage

According to Slack and Wise (2005), both technological and cultural deterministic perspectives view technology and culture in a casual relation as specified in previous sections. They have also contended that viewing them in this way is insufficient because reality is more complicated than the cause-effect model envisioned by deterministic perspectives. In this section, I will introduce a non-deterministic perspective proposed by Slack and Wise (2005) to assist in the analysis of technology-related issues.

To begin, it is crucial to consider the interconnectedness of technology and culture. In other words, technology should not be considered a separate and independent entity from society. the development of a technology is in fact, influenced by the society and culture in which it is designed and used. This in return, shapes and transforms the culture itself. Therefore, instead of technology and culture, it should be considered as "technological culture" (p. 129).

Culture is made up of various connections and relationships in society, and Slack and Wise describe these connections as "articulations" (p. 112). They explain that these articulations are

not static but dynamic and can move in different directions; they are contested in some instances yet corresponding in others, and that eventually, these articulations form into an “assemblage” (p. 126). To be more specific, when we look at articulations, we are examining and exploring connections and relations among various “practices, representations, and experiences” (p. 126) that composed the society we live in; on the other hand, when we investigate the assemblage, we are seeking to scrutinize the “structured nature and work” (p. 126) of the articulations that made up such assemblage. In other words, the articulations are formed by the interactions between different actors, and the assemblage is the final network composed by such interactions and connections.

Let us now return our attention to technological issues. Unlike deterministic perspectives which consider technology and culture in a causal relation, Slack and Wise suggest that we need to view technology in terms of articulation and assemblage, because technology is not only interconnected with the materiality of the society, but also “practices, representations, experiences, and affects” (p. 128). When we consider technology in terms of both articulation and assemblage, we are paying attention not only to the connections and relations that influence and constitute the technology (what are the connections), but also how these connections are articulated into a particular form.

To use FRT as an example to demonstrate Slack and Wise’s concept of articulation and assemblage, we must first keep in mind that FRT is interconnected with the culture, and these connections are what considered to be articulations (whether it is the materiality of FRT, the state’s desire to monitor its citizens, or business sector’s cooperation with the state); these articulations are dynamic and fluid, and eventually form into an assemblage. However, once new articulations are established, this assemblage may be rearticulated. For example, when new regulations on FRT are introduced into society, the public and private sectors will respond accordingly (e.g., it may lead to new business practices, and depending on the regulations, it may either improve or decrease public confidence towards the state), and eventually, new articulations will be constituted, resulting in a different or slightly different assemblage.

It is worth mentioning that articulations are contingent; some may be more tenacious and thus more difficult to disarticulate, whereas others are much easier to be taken apart or

rearticulated. Using surveillance as an example, Slack and Wise argue that rather than trying to persuade people that their beloved technology poses severe risks to their privacy and rights, it will be easier and faster to appeal to their commitment to the Bill of Rights. They suggest that the Bill of Rights “hits home affectively in the mainstream heart of the United States” (p. 132), and that with an affective and collective response, it may eventually lead to the enactment of laws, regulations, and oversight to protect people’s privacy and rights.

Although Slack and Wise argue that we can target this weakest link in the articulations to promote the desired change, they do not suggest that it is crucial for us to always target such articulations to solve the associated problems faced by society. Rather, Slack and Wise state that we must map out the assemblage created by various articulations and pay attention to the tenacity of the articulations we are trying to dis/rearticulate.

To summarize, technology should never be separated from the cultural/social context in which it is embedded; technological articulations are constantly disarticulated and rearticulated as a result of technology and culture’s interconnectedness; and a new assemblage will be formed once new articulations are made (or unmade). Therefore, “if you don't like what you see, don't blame the tech or the culture; understand the assemblage that maps technological culture” (Slack & Wise, 2005, p. 132).

While the concept of articulation and assemblage has provided a fundamental framework that guided my understanding of the interactions between culture/society and technology, highlighting how different elements are interconnected and eventually form into a unique socio-technological network, it was utilized as a theoretical lens for me to examine and understand FRT, rather than being the primary focus of my analysis.

Technology, Politics and Sociotechnical Imaginaries

Similar to Slack and Wise’s (2005) perspectives on technology and cultural determinism, Winner (1986) contends that analyzing technology from a deterministic perspective is insufficient for understanding its associated issues or phenomena. He explains that when we look at a technology, we must at the same time identify and analyze its political properties. Therefore, we should look beyond the fact of how technology is used and focus our attention on its design. For instance, a certain technology may be beneficial to some (give them more

power and control over others), yet harmful to others. In the case of FRT, although it has become much easier for the state to monitor and manage its citizens, the general public perceives it as an invasion of individual privacy and a sign of oppression and authoritarianism (Chochia & Nässi, 2021). However, it was not in FRT's original design intention to infringe people's privacy or oppress certain populations. Rather, such phenomena have reflected an interaction between technological innovation and the state's raising desire for efficient surveillance and management of its citizens, and these different factors "reinforces each other in deeply entrenched patterns, patterns that bear the unmistakable stamp of political and economic power" (Winner, 1986, p. 27). Drawing a parallel to Winner's example of how tomato harvester may influence small farmers and larger growers differently, those who oppose the use of FRT/artificial intelligence are labeled as "anti-technology", "anti-progress" or "anti-innovation" (Bartoletti, 2020, p. 66), and in this sense, FRT resembles and embodies a social order in which proponents of FRT are empowered and are able to enjoy the benefits brought by its utilization, while opponents are marginalized and discredited (Winner, 1986). Most importantly, Winner contends that such embodiments of social order reveal to us the world constructed by the adoption of certain technologies.

To examine a technology, Winner (1986) suggests that we must venture beyond its associated policies, regulations, and ideologies and look at the technology itself. Because different values, patterns and power are embedded in the materiality of a technology, and once we choose a particular technology, we are at the same time choosing a "particular form of political life" (p. 29). Winner explains that the selection and adaptation to a certain technology influences the "form and quality of human associations" (p. 33). To put it differently, technology has an impact on the social order and social life that we choose to maintain. For instance, because of the unstructured and decentralized nature of solar energy, it can be easily managed by local communities. As a result, supporters of solar energy perceive it as "more compatible with a democratic, egalitarian society" (p. 32). On the other hand, because of its structured and centralized nature, by choosing nuclear power, we accept a centralized government that manages and safeguards nuclear facilities and materials. Therefore, Winner argues that technology has political qualities, and that by examining the materiality of a

technology, we will also discover how power and authority are structured around such technology.

Adding to Winner's (1986) statement on the importance of analyzing the design of technology, Latour (1992) argued that technological design has the ability to impact human action and shape the way we behave and react. He stated that by designing a technology, we have not only delegated certain forces to that technology, but also various "values, duties, and ethics" (p. 157). As Latour stated, these different values and political goals may be discovered by analyzing the development and implementation of a technology. For instance, the use of surveillance cameras and facial recognition technology in China has revealed government's desire to build a "smart city" in which citizens are simplified into "human subjects" (Jasanoff & Kim, 2009, p. 122, as cited in Bareis & Katzenbach, 2021, p. 19), so that they can be monitored, governed and managed more efficiently, and allow a "intelligent monitoring and early warning and control system" to be established (Bareis & Katzenbach, 2021, p. 19). In other words, people are reduced into data and subjects, devoid of their agency, and subjected to constant monitoring, identification, and tracking.

What is more, living in a "smart city" has significantly altered and shaped people's actions and lives. For example, FRT is currently being used as an access control system in an increasing number of neighborhoods in China. Instead of speaking with the security guard who usually sits near the entrance (who may or may not be present when you need to enter the neighborhood), residents must scan their faces at the front of their neighborhoods in order to enter the building complex. According to Zhang and Luo (2022), while neighborhood FRT is now commonly used in China for its convenience, it has transformed people's ways of living and exposed residents to various risks. Now residents are faced with the risks of privacy infringement and illegal collection of their biometric information, due to not only the absence of AI (artificial intelligence) regulations in China, but a lack of transparency in the algorithm and the inadequacy of law enforcement.

In conclusion, it is insufficient to perceive technology from a deterministic perspective, because technological innovations are imbued with political qualities and are influenced by existing cultures and values. At the same time, the utilization of these technologies shape and

influence people's actions and lives (Winner, 1986; Latour, 1992). When we look at technology, each design reveals to us how it may be used to build power and control over others. Such notions of "power over others" may be intentional, unintentional, or a mixed of both, and in order to understand such dilemma, we must pay attention to how technology is arranged in society, as well as the social actors who are influenced by these arrangements. Furthermore, technology has an impact on the form of social order and social life that individuals choose to uphold, and examining technology and its arrangement reveals the associated "institutionalized patterns of power and authority" (p. 38). In this sense, by choosing a specific technology/technical system, we are at the same time choosing the political lives/structures embodied by it.

Furthermore, when considering the political qualities of technology, it is important to distinguish between the politics made possible by technology and the politics embedded within technology. In the case of FRT, the characteristics of this technology enable the act of identification. Ideally, law enforcement may use FRT to help identify criminals and even prevent crime, thus ensuring safety in society. However, there are also biases and political values inherent within FRT. For instance, FRT may be used to exacerbate systematic discrimination in society, infringing on people's privacy and rights, and ultimately pose a threat to democracy.

Now when we consider sociotechnical imaginaries (SI), a concept developed by Jasnoff and Kim (2009), we can see some similarities. Winner's (1986) perspectives on technology and politics have emphasized the importance of venturing beyond determinism and focusing on the design of technology, its patterns, encompassing values, social structures and power. Accepting and adapting to one technology/technical system represents the acceptance of a specific social order and social life. Similarly, SI are visions that reveal how the choice of a specific technology might constitute a collectively imagined future. In other words, by choosing a specific technology, individuals have envisioned a future in which that technology works well to benefit society (Schmid, 2021).

In the following section, I will introduce the concept of SI in detail, highlighting how it is understood and operationalized by different scholars, before introducing my own

operationalization of this concept.

Sociotechnical Imaginaries

Sheila Jasanoff and Sang-Hyun Kim proposed the concept of sociotechnical imaginaries (SI) in their 2009 research on national policies and nuclear energy, and later redefines SI as “collectively held, institutionally stabilize, and publicly performed visions of desirable futures, animated by shared understandings of forms of social life and social order attainable through, and supportive of, advances in science and technology” (2015). SI has since been used by various researchers to explore the relationships between technology and state policies, specifically how technological policies are structured around society’s shared vision of the future. However, as more researchers use the concept of SI to investigate the collectively held imaginaries surrounding a technology, new interpretations of SI are proposed and added to Jasanoff and Kim’s original definition.

In this theoretical section, I will first examine different researchers’ interpretations and applications of the concept of SI, highlighting how they evolve from the original definition, before introducing my own operationalization of the concept. I have classified these various interpretations of SI into two types based on researchers’ different views and approaches to SI (Consensual view V.S. Conflictual view), and then within these two types, building on Mager and Katzenbach’s summary (2020), I will introduce six different subtypes of SI, four that fit in the consensual type and two that fits in the conflictual type. These six subtypes are listed as follows:

Type 1: Consensual View on Sociotechnical Imaginaries

Subtypes:

1. Each country has one leading sociotechnical imaginary.
2. Sociotechnical imaginaries are multiple and dynamic: state actors may have various SI for a particular technology to help inform policies and decision-making process.
3. Sociotechnical imaginaries will not only vary according to groups, but also change over time.
4. Sociotechnical imaginaries are dynamically interconnected, they influence and shape one another and evolve together through time.

Type 2: Conflictual View on Sociotechnical Imaginaries

Subtypes:

5. Sociotechnical imaginaries are contested: they can be produced by a variety of actors (nation states, public institutions, advocacy groups, etc.), competing for dominance or seeking resistance.
6. Sociotechnical imaginaries can be commodified by corporate actors (Corporations create/facilitate a specific imaginary to promote and sell their products).

The first type expresses a more functional view of society, where imaginaries negotiate peacefully. On comparison, the second type focuses on force and dominance of imaginaries, emphasizing power dynamics between contested SI. In the following sections, I will explore and explain the aforementioned six subtypes in these two types separately.

A Unique National Sociotechnical Imaginary

The idea of sociotechnical imaginaries was originally proposed by Jasanoff and Kim during their 2009 research which examines and compares America and South Korea's SI surrounding the use of nuclear energy. They explain that current science and technology studies (STS) tend to undertheorize the relationship of science and technology to political power, as a result, they introduce the concept of sociotechnical imaginaries to fill the gap.

Jasanoff and Kim define SI as “collectively imagined forms of social life and social order reflected in the design and fulfillment of nation-specific scientific and/or technological projects” (p. 120). They state that imaginaries describe the attainable future envisioned and desired by states and practitioners. By analyzing these imaginaries and visions, researchers will be able to understand how policies can be built upon dominant imaginaries and how these visions influence technological development and preference. In other words, to understand why certain policy is preferred over others, we need to identify imaginaries that populate the policymaker's mind and examine how such imaginaries are stabilized.

For instance, the US and South Korea entered the atomic age differently, with the US being the first country that developed and launched the atomic weapons and South Korea being a newcomer to such technology. As a result, these two nations have positioned themselves differently. On the one hand, the US perceives itself as the peaceful protector of nuclear energy,

thus measures concerning radiation release containment are of primary concern to the state. On the other hand, South Korea is guided by the vision of ‘developmental nationalism’ (p.134), which sees nuclear energy as a means to achieve national development and self-sufficiency, therefore policies usually focus on promoting the use of nuclear energy and building domestic capacity. In conclusion, Jasanoff and Kim’s study reveal how different imaginaries around nuclear energy affect national political cultures, in other words, they have shown how “technoscientific and political orders are co-produced” (p. 123).

Similarly, in her 2021 research, Schmid shows how the choices for specific nuclear reactors constitute a particular sociotechnical order and reflect a collectively imagined future. She explains that there are different visions and expectations behind each choice of the nuclear reactor design, and that these imaginaries reveal how institutions feel the world should function and their expectations of how such technology would transform the society we live in.

For instance, in the 1970s, the RBMK reactor model “was neither the cheapest nor the technologically most sophisticated design available, nor did it have the most substantial track record” (p. 1320), yet by choosing RBMK as the national nuclear reactor, Soviet Russia had envisioned a future in which RBMK is capable of providing the society with unlimited power supply, which is considered as a sign of advancement and modernity, and is believed to be capable of accelerating the progress of Communism.

Furthermore, Schiolin (2020) provides an example of a leading national SI in Denmark. He explains that by adopting the concept of the fourth industrial revolution (4IR) as its national imaginary, technology is seen as revolutionary, capable of bringing positive change to society, and that the future with 4IR is depicted as inevitable. According to this depiction, policies in Denmark strive to ensure a smooth transition to this inevitable future. Actions and modes of being congruent with the techno-positive aspect of 4IR are encouraged, while others are marginalized/discouraged. As a result, such hegemony in the Danish government has led to a neglect of democratic and ethical value.

Multiple National Sociotechnical Imaginaries

Other than the idea that each country has one leading SI, the works of many researchers have revealed that state actors can have various SI for a particular technology to help inform policies

and decision-making process.

In the context of the fourth industrial revolution (4IR), many argue that technology is revolutionary, capable of bringing about inevitable change in society. As a result, in order to succeed in the coming global competition, countries must adopt and adapt to the 4IR rhetoric, as well as make decisions and allocate funds accordingly (Schiolin 2020; Vivente and Dias-Trindade, 2021). Similarly, the growing prominence of the “Big data” discourse has led the European Commission (EC) to perceive an upcoming global competition driven by big data rhetoric. Therefore, in order to maintain its global competitiveness and ensure a leading position in the global market, the commission has decided to fully embrace this digital trend (Rieder, 2018).

Instead of a single leading SI that informs the policies within EC, Rieder has identified three SI envisioned by the commission. EC’s first SI depicts the big data trend as a perfect opportunity to boost the union’s economy, and in order to do so, it is perceived that regulations should not constrain the development and innovation of technology. Second, big data is viewed as a means for the government to provide improved social services, because it is believed that by incorporating technology and big data management into the administrative process, it increases “government efficiency and effectiveness” while reducing the costs (p. 5). Third, big data is envisioned as capable of providing evidence-based policies and informing the decision-making process.

These three SI co-exist peacefully and together guide the European union’s (EU) policies and the direction of its development. The economy is viewed as a crucial factor that will influence the Union’s position in the global competition driven by the big data rhetoric. To ensure a leading position, risks associated with technology are downplayed, and it is argued that regulations should make space for technological innovation.

Mager’s 2017 research on search engine imaginary is another example of multiple national SI. According to Mager, the European Union perceived information and communications technology (ICT) to be beneficial for economic development; however, with an increase in incidents and controversies surrounding ICT (such as the Snowden leak and the Google Street

view incident in Austria¹), state and public discourse have shifted from a techno-euphoric attitude to one that emphasizes citizens' fundamental rights. As a result, the EU envisions itself as the "guardian of citizens' personal data" (p. 249), and that policies and regulations should be designed towards privacy protection (protecting citizens from the control and influence of multinational ICT corporations such as Google and Microsoft). However, instead of being a homogenous entity, Mager argues that Europe is envisioned as a "multiply imagined community" (p. 255), with policies and decision-making process shaped by different member's ICT imaginaries.

For instance, while some members believe ICT technology violates citizens' privacy and that strict legislation is required to ensure privacy and safety, such vision and belief are perceived by other EU members as posing a negative impact on national economy, overlooking the argument that this emphasis on the economy and the call for lenient regulation has resulted in "high costs and competitive disadvantages for European companies" (p. 254). These different imaginaries may appear to be conflicting, yet instead of competing for dominance, they collectively contribute to the negotiations of the EU's data protection policies and legislations.

In conclusion, as Mager writes, "sociotechnical imaginaries should not be seen as monolithic or stabilized, but rather as multi-faceted and dynamic" (p. 256).

Sociotechnical Imaginaries as Dynamic and Contextual

Indeed, state actors may have various SI to help inform policies, this section reveals that SI can not only vary according to groups but change over time.

In their 2022 research on how newspapers construct and shape the sociotechnical imaginaries around digitally mediated touch and communication technologies. Mackley and Jewitt state that news media is considered as an indispensable part of people's social lives, and that by revealing the sociotechnical imaginaries shaped and disseminated by news media, they will be able to see how the development and adoption of certain technologies create a collectively held vision of the future while shaping the societal response at the same time.

¹ Google's Street View project was banned for violation of privacy when it was discovered to have illegally collected WiFi data in Austria in 2010 (Mager, 2018).

More importantly, since Mackley and Jewitt focus on the historical context of discourse and knowledge, their research has shown how the SI around certain technologies varies over time. For instance, Mackley and Jewitt argue that prior to Covid-19, the imaginary around remote touch/communication technologies expressed concern that the development of such technologies may one day replace the desire for human touch. During the pandemic, however, the imaginary changed from a “threatening replacement” to a “bridge for interpersonal connection” because of the elements associated with Covid-19 (such as segregation, isolation, long-distance relationship, and lack of personal touch and intimacy etc.).

Yang, Szerszynski, and Wynne’s 2018 research on energy futures and power shortages in Taiwan is another example of how SI may change over time. They argue that though renewable energy is initially presented as a solution of power shortage, it is portrayed as “immature and unviable” when nuclear energy enters the big picture. Contrary to renewable energy, nuclear energy is depicted as “cheap, reliable, and safe” (p. 278), and is envisioned by the government actors to be a better solution to Taiwan’s energy shortage. However, with the anti-nuclear movement in Taiwan and the closure of Nuclear Power Plant 4 in 2015, nuclear energy, which was once envisioned as “the only feasible way of solving this imminent power shortage” (p. 278), is now faced by debate and controversies.

Sociotechnical Imaginaries as Co-evolving

Previous subgroups of SI have pointed out the existence of multiple SI co-existing within a national context, which may also vary across different scenarios. In this section, we will explore how multiple SI may be dynamically interconnected, influencing and shaping one another, and ultimately evolving through time.

In their 2021 research on electrification and biogas fuel imaginaries in Sweden, Mutter and Rohrache focus their attention on the relationship of different SI and how four crucial qualities of SI (spatial bondedness, materiality, contested nature, and temporality) have all contributed to the co-evolution of the sociotechnical imaginaries surrounding electric vehicles and biogas. They explain that biogas was at first imagined as a way to not only provide clean energy to society and help to reduce pollution, but also to contribute to economic development and waste management. However, Mutter and Rohrache argue that since biogas is more tied to regional

development because of its materiality (it is transported via undersea transnational gas pipeline, and is usually mixed with natural gas), the imaginary around biogas is more “fragmented and unstable” (p. 94). Similarly, although electrification is recognized as an alternative national energy supply to biogas, and its associated imaginary is less fragmented and more stable, there are still issues attached to its imaginary. For instance, many people in Sweden have expressed concerns that electrification alone may not be sufficient in many parts of the nation, and that a regional supplement is needed. Therefore, Mutter and Rohrache argue that SI around biogas and electricity should be seen as complementary, as they have together created a “new types of imagined future transport systems” (p. 99), with biogas being imagined as “local imaginaries of a sustainable regional future” (p. 104), and electric vehicles as national imaginaries indicating advancement, sustainability and modernity. In this sense, we can see that instead of competing for dominance or seeking resistance, these two different visions have shaped each other, co-evolved through time, and together influenced the envisioned energy future in Sweden.

Sociotechnical Imaginaries as Sites of Power

Moving on to the conflictual view on SI, researchers have demonstrated through their works that SI can be contested, produced by a variety of actors competing for dominance or seeking resistance.

Polleri’s 2020 research on nuclear controversies in post-Fukushima Japan reveals to us that there can be confronting SI existing in society, and they may eventually lead to a power imbalance. Polleri identifies two confronting sets of sociotechnical imaginaries around the use of nuclear energy: one from the METI (the Ministry of Economy, Trade and Industry) and the other from nuclear energy protesters. While state actors promote the use of nuclear energy, framing it as an economic backbone of the society and a symbol of modernity and independence; protesters compare nuclear energy to “akuma” (p. 582), a demonic force/energy that will lead to the detriment of democratic values, and that instead of providing equal electricity, protestors believe that nuclear energy will be used by militaries to build nuclear weapons.

By analyzing these two confronting SI, Polleri states that there is a clear power-imbalance

between the state and protesters (general public), and that such imbalance allows us to see how the state uses its power to depoliticize the uncertainties raised by the activists/protesters, framing these uncertainties as invalid or of minor importance. In this sense, the state is limiting activists' political engagement in order to advance the SI preferred by the authority. To put it another way, by looking at different SI of various actors, we can now see how power is distributed unequally among actors and how this power-imbalance plays a crucial role in advancing a particular imaginary while limiting others.

According to Smallman (2020), such a power imbalance between the state actor and the general public is also visible in the UK's policy-making institutions. She explains that the technoscientific viewpoint that informs the decision-making process in the UK depicts technology as a problem-solver for societal issues. Guiding by the elite SI of "science to the rescue" (P. 6), it has influenced the knowledge production process and caused a democratic backlash. For instance, while policymakers separate science from societal/ethical issues, perceiving the latter as "epiphenomena" (p. 4), public imaginaries express the concern that such separation is impossible. The public imaginary insists that we have to consider the problems produced by using science as a solution to societal issues during the policy-making process. However, since the policymaking structures are shaped by the elite SI, such complexity is regarded as a hinderance. As a result, imaginaries, knowledge, and perspectives of science that do not fit with the elite SI are framed as unprofessional and illegitimate. In order for public imaginaries to be incorporated into the policy-making process, they have to be assimilated into the dominant SI. In this case, we can see how power is exercised by controlling which types of knowledge/perspective are legitimate to advance an elite imaginary while marginalizing or assimilating conflicting ones.

Sociotechnical Imaginaries as Commodified by Corporate Actors

SI may also be commodified by corporate actors, meaning that corporations may create and facilitate specific imaginaries to promote and sell their products.

According to Bareis and Katzenbach's 2021 research on narratives and imaginaries on national AI strategies, various studies on media discourse have revealed an increasing presence of business and corporate actors in promoting positive discourse around AI and emphasizing

the benefits it may bring to the society. Similarly, Vicente and Dias-Trindade (2021) point out in their analysis of Portuguese news media discourse of the fourth industrial revolution (4IR), that corporate actors contribute almost half of the information sources in 4IR news. They state that corporate actors have expressed an elite SI in which technology is seen as inevitable and framed as a solution to economic problems. Furthermore, Vicente and Dias-Trindade discovered that 17% of the collected news articles are sponsored by corporate actors, and that some of the 4IR news coverage is related to industrial products. They argue that such “product-placement logic” in the news media has made the concept of 4IR into a brand (p. 718), and that the associated SIs (such as techno-fix) have been commodified to promote corporate interests.

Conclusion

Though the original concept of sociotechnical imaginaries focuses on one leading national imaginary and was developed for analyzing technological policies in a certain nation, over time various researchers utilize the concept of SI to analyze not only national policies, but media discourse, corporate documents, or marketing materials. This has widened the scope of SI, and the concept itself has been further developed by integrating different interpretations to its original definition. As a result, instead of being “monolithic, linear visions of future trajectories that are primarily enacted by state actor” (Mager and Katzenbach, 2021, p. 226), SI are multiple and dynamic; state actors may have various SI for a particular technology to help inform policies and decision-making process; SI can also be contested, produced by a variety of actors competing for dominance or seeking resistance; and corporate actors may also commodify certain SI to promote their own benefits. It is worth mentioning that SI will not only vary according to groups but will also change over time. Finally, when we look closely at the relationship between different SI, we may notice that they are dynamically interconnected. These SI influence and shape one another, and ultimately co-evolve through time.

In my case, I acknowledge that SI are both multiple and dynamic. By analysing the similarities and differences in these SI, we will be able to understand each group’s unique perspective and emphasis with FRT. Instead of solely examining how a nation’s attitudes, policies, or social norms may influence advocacy groups’ imaginaries related to FRT, my analysis went beyond specific geographic boundaries. It explored diverse social perspectives,

ethical considerations, suggested solutions, and future visions surrounding FRT across different advocacy groups. As a result, the characteristics of these groups' narratives make it possible to subsume their imaginaries into a more encompassing one. The examination of this collectively imagined SI not only reveals the groups' universally recognized dilemmas brought by the technology, but also how they perceive these problems, shedding light on the values and ideals that drive their advocacy, as well as the envisioned pathways for the future of FRT.

Chapter III: Methodology

In this chapter, I will introduce my sampling methods and explain how I combined three different models to serve as my analytical framework. After that, I will demonstrate how this framework is utilized to analyze the materials.

Research Question and Goals

This research aims to explore the sociotechnical imaginaries (SI) of four advocacy groups (Big Brother Watch (BBW), Electronic Frontier Foundation (EFF), The Surveillance Technology Oversight Project (STOP), and Fight for the Future (FFTF)) regarding facial recognition technology (FRT), as well as how they construct such imaginaries. In order to sketch out their SI, I analyzed the materials on their official websites, and used narrative analysis to identify how they envision a future with FRT. In other words, I examined the narratives they had developed for their fights against FRT, as well as the roles they assigned to various actors that occurred in their stories to reveal their goals and desired futures.

Research Design

The first step of my research design was to identify four different privacy advocacy groups. Although there were many advocacy organizations to choose from, I prioritized organizations with a higher level of online presence and more readily available information and materials, as this would provide me with more details to delve into for my analysis.

Second, these four groups offered me diversified samples. For instance, although FFTF is considered an independent advocacy organization, it has a strong connection with the Silicon Valley, as it is often backed by technology companies (Levine, 2018). In comparison to FFTF, which primarily focuses on the US, EFF operates at a global level, collaborating with various international organizations to protect human rights and civil liberties worldwide. Conversely, STOP and BBW provided me with a more extensive view on local and national issues surrounding the use of FRT in the United States and United Kingdom, respectively. In this way, I was able to acquire a more comprehensive understanding of various attitudes toward FRT and its relating issues and concerns.

Sampling and Material

To begin, since the focus of my analysis is on how different privacy advocacy groups envision

a future with/without the use of FRT, I specifically selected materials (blogs, press release, newsletters, and project descriptions) from their websites that discussed issues with FRT. To use EFF as an example, I used the search function located at the top right corner of the homepage and entered “Facial recognition” as my keywords to access relevant materials. The results were presented in a sorted order based on the relevance of their titles and contents to the prompted keywords, and then I reviewed each source carefully, double-checked its relevance, removed duplicated or repetitive materials, and transferred the contents into a word document, which was then imported into QDA Miner for analysis. It should be noted that while it was possible to sort these materials by date, such sorting option yielded articles that mentioned FRT in general but were focused on a different technology.

It is worth mentioning that though FFTF’ website did not have a search function for accessing archived materials, there was a section featuring news articles written by its members. In order to search for articles on FRT, I used my browser’s (Chrome) search function (CTRL + F) and entered the keywords “Facial recognition”, prompting the browser to highlight all matches on the page. I then reviewed each highlighted article for relevance and copied the contents into a word document.

As a result of my material collection, a total of 38 articles were collected, the detailed information is shown in Table 1.

TABLE 1

Article Collection

Name of the Advocacy Group	# of Articles Collected	Word Count	Search Order	Total Word Count
Big Brother Watch (BBW)	10	6265	Chronological (default option, no alternatives)	25,597
Electronic Frontier Foundation (EFF)	10	6748	Relevance (as sorting by date would not ensure the articles’ relevance to FRT)	

Fight for the Future (FFTF)	9	6213	Chronological (default option, no alternatives)	
The Surveillance Technology Oversight Project (STOP)	9	6371	Chronological (default option, no alternatives)	

To organize my research materials, I created a separate word document for each of the four advocacy group. After reviewing the contents on their website, I transferred relevant materials to their respective documents. This way, when I imported these documents into QDA Miner, each group had their own section, making it easier to analyze their discourse separately.

Characteristics of the Advocacy Groups

Before delving into the analysis, I believe it would be beneficial to first familiarize ourselves with the characteristics of these advocacy groups (BBW, EFF, FFTF, and STOP). Because it is only when we understand their motivations, goals, drives, and values, can we situate their narratives into appropriate context.

To begin, we will review some of the common characteristics shared among these groups, and then move on to explore the differences in their focuses.

Upon reviewing their “About US” section, we can see that all groups are determined in their fight for people’s rights and civil liberties in this digital age. They are independent, non-profit organizations composed of individuals from diverse backgrounds, aiming to empower the general public with knowledge regarding current technologies and their own rights. Their goal is to provide measures and opportunities that enable the public to defend their own privacy and civil liberties. In other words, the groups’ missions extend beyond fighting solely for the interests of the public. They aim to foster the emergence of a collective consciousness, where individuals will be able to come together and fight for their rights and freedom.

In addition, these groups all employ multiple yet similar measures to advocate for people’s rights, including but not limited to:

1. Using internet and media to communicate their findings to the public.

2. Engaging in Parliamentary/Congressional conversation.
3. Attending legal proceedings
4. Launching public campaigns.

What is more, these groups recognize the importance of collaborating with other rights advocacy groups and organizations, and they have received help from actors across various fields.

After exploring their shared characteristics, now let us move our attention to their differences. First, though they all aim to safeguard people's privacy and rights in the face of rapid technological advancement, their focuses differ slightly.

For instance, BBW and STOP prioritize the problem of surveillance in society. They suggest that as more technologies are developed and adopted by various sectors, it has created a complex surveillance network, subjecting individuals under constant monitoring and tracking. STOP pays particular attention to the impact of surveillance on BIPOC communities, highlighting the trauma caused by "anti-Black policing" (STOP, 2023). The group argues that these communities are disproportionately affected by government use of surveillance technology, and that they have firsthand experience with such technology and understand its impacts. Therefore, their voices need to be amplified and empowered to lead the movement against government's mass surveillance practices.

On the other hand, EFF and FFTF focus more on the relationship between the technology and society. For instance, they suggest that despite the problems brought by technological advancement, technology can be used to benefit society when used properly and responsibly (STOP also has a similar suggestion).

With a basic understanding of the groups' positions, goals, and values, now is time for us to explore the analysis of the materials.

Material Analysis

In order to analyze my materials, I combined Propp's (1968) model of analysing folktale, Stone's (1989) concept of causal stories, and components related to my own operationalization of SI. This allowed me to create multiple narratives for the groups' discourse on FRT, while gaining a better understanding of how they envisioned and constructed a future utopia. I will first provide a brief overview of my analytical schemes before explaining how I combined them

together to reveal the narratives and the constructed futures.

Narrative Analysis and Russian Folktales

To understand the structure of folktales and shed light on historical study, Propp reviewed 100 Russian folktales (1968, p. 123) and identified 8 “sphere of actions”/character archetypes (p. 79) and 31 functions. He believed that these 31 functions are essential components of folktales, and that by analyzing these functions and character archetypes, researchers will be able to discover the fundamental structure of the tale, the unique role of each character, and how they interact to advance the story. Additionally, by conducting narrative analysis, it reveals to the researchers the values, beliefs, and norms of the culture in which these stories are composed. In other words, by analyzing Russian Folktales, researchers will be able to explore the culture as well as the social settings during the time these stories were composed. A list of Propp’s 31 functions and 8 character archetypes is provided in Appendix A.

Stone and Causal Stories

According to Stone (1989), politicians frame issues in ways that benefit their conditions to gain public support. She explains that political actors create their own “causal stories”, in which they portray harmful events as being caused by certain organizations or individuals in order to build support for their own policies. In response, the opposing parties will attempt to shift the blame away by creating a new causal story to argue about and identify the “true cause” (p. 283). However, as Stone suggested, political conflicts are never about finding a “true cause”, but rather about gaining support and control by explaining why things happened in ways that benefit their positions, and attributing responsibility for the outcomes. Therefore, by analyzing these causal stories, researchers will be able to understand how public policies are shaped by the ways narratives are uttered and delivered to influence public opinions.

Apart from exploring causal stories to analyze formal policy, in my case, identifying the causal stories behind the dilemmas associated with FRT will allow me to understand how the advocacy groups under study assign responsibility to different actors, as well as how these groups utilize these causal stories to support their claims and proposals.

Operationalization of Sociotechnical Imaginaries

To help me in identifying advocacy groups’ SI surrounding FRT, I developed a SI operationalization table (SIO). The table was composed of three major sections: the dimensions,

the components, and the indicators (see Table 2).

This table was produced by combining Jasanoff and Kim’s 2015 definition of SI with various researchers’ understandings and applications of this concept in their respective fields of study. In the following paragraphs, I will first explain how I created my table before explaining the way I combined all three models (Narrative analysis, Causal stories, and SIO) to assist me in analyzing advocacy groups’ discourse on FRT, constructing multiple narratives, and revealing the futures they have envisioned.

To begin, Jasanoff and Kim (2015) define Sociotechnical imaginaries (SI) as “Collective held, institutionally stabilized and publicly performed visions of desirable futures, animated by shared understanding of forms of social life and social order attainable through, and supportive of, advances in science and technology”. According to this definition, there are two crucial elements: a shared understanding of ideas in society (social life), and a shared societal understanding of the roles and functions of actors and mechanisms (social order). These elements served as the dimensions of my operationalization table, as they provided the underlying structures of SI. Within each dimension, there were different components, each of which was defined by specific indicators. For example, on the one hand, social order was composed of various actors and mechanisms of society (state, government, law, Industry, and economy, etc.). On the other hand, social life was constituted by a diverse set of beliefs and ideas (futures promoted and fought; goals, values, affects promoted and fought, etc.). To identify and analyze these components, I created a list of questions (indicators) such as “what is the role and involvement of the state actors” and “what is public good”. This allowed me to analyze the components and dimensions of the advocacy groups’ SI systematically and shed light on the futures they envisioned.

TABLE 2

Sociotechnical Imaginaries: Operationalization

Dimension	Components	Indicators
Social Life (ideas)	Futures predicted	What would the future look like if FRT was continuously used in its current way?

	Futures promoted and fought	What are they? Why are they important?
	Goals, values, affects promoted/fought	What is public good?
	Obstacle/problems encountered	What are they?
	Solutions/designs/measures to address the problems	What are they? How do they work? What are their characteristics? What are their risks or dangers? Feasibility of their conception, implementation, and adoption.
	Rapport to change/innovation/science	What speed? Promoting continuity or rupture with the past or the present?
Social Order (actors and mechanisms)	Public/organized groups such as activist groups	What are their roles and involvement?
	State/government/laws	What are their roles and involvement?
	Industry/economy	What are their roles and involvement?
	Decision process regarding the technology	Who makes the decision? How do they make the decision?
	Monitoring/Safeguarding/Oversight of the technology	Who overlooks the technology? How do they do that?

Combining the Models

As previously mentioned, I combined Propp's (1968) model of analysing folktale, Stone's (1989) concept of causal stories, and my SIO to analyze the advocacy groups' discourse.

To begin, I used Propp's 31 functions of Russian folktale, 8 character archetypes, and my SIO table to help me determine the plot of the story, the role of each character, as well as their interactions.

To accomplish this, I divided Propp's 31 functions into four major parts based on Brusentsev, Hitchens, and Richards' (2012) traditional grouping methodology:

1. Functions 1 to 8: These functions together signify the beginning of the story, where the

villain has created a dilemma² that requires the hero to address.

2. Functions 9 to 11: The situation is made known to the hero, and the hero is sent out to remedy the dilemma. In my analysis, this section is about the hero recognizing the dilemmas presented by the villains and providing proposals and suggestions for counteractions.
3. Functions 12 to 19: The hero faces/is tested by the villains and fights them. This section is about the sequence of events. In other words, it reveals how the villains present the dilemma and how the hero fights against the villains and the challenges they pose.
4. Functions 20 to 31: The hero has addressed the dilemma and is determined to fight against any other dilemmas brought by the villains³.

Together, these functions reveal to us who the characters are, what happened in the story and how the story advanced.

To use FFTF as an example, after reading one of their articles on FRT, I got a general idea of what happened/was happening and who the relevant characters were. Then, based on my SIO and the grouping strategy, I identified the roles of the participants and organized the discourse into a general story arc. Again, the key point in this step was to sketch out the underlying structure of the story by answering the WHO and WHAT question. To put it differently, at this stage I aimed at examining the dilemmas created by the villains (Functions 1 to 8), the heroes' counteractions (Functions 9 to 11: what did the heroes propose/do to address the dilemmas), as well as the results of their counteractions (Functions 20 to 31).

With a general understanding of the structure of the story, the next question to answer was HOW: How did the story advance? In other words, I needed to identify the sequence of events – namely, how the villains presented the challenges and how the heroes remedy the dilemmas. I used my SIO to help me navigate through the discourse, because each indicator of a specific

² A dilemma in my case refers to a situation in which different actors' development and utilization of FRT pose risks to individuals' privacy and civil liberties.

³ It is worth mentioning that, according to Brusentsev, Hitchens, and Richards (2012), the original definition of function 20 to 31 focuses on how the hero defeats the villain, returns, and is rewarded for their actions. However, the fight against different actors' development and utilization of FRT is often a prolonged process with no immediate results. Therefore, the groups express the commitment to keep advocating for robust regulations governing the use of FRT, while urging for a complete/partial ban on its utilization across various sectors.

component reveals the key factors that require me to identify. For example, by answering the indicators for advocacy groups (as one of the components of social order), I would not only be able to confirm the role I assigned to each character in the story, but also their involvement (i.e., how did FFTF fight against the use of FRT). It is worth mentioning that the answers to the HOW question revealed the details of Functions 12 to 19.

As of this stage, I have sketched out the entire plot of a story based on how Propp's 31 functions depict the storyline of Russian folktales. However, unlike folktales, exploring the reasons behind the heroes' actions is crucial for understanding the motivations behind each advocacy group's activities (i.e., the values and beliefs that motivate them).

In other words, once we knew what happened and how it happened, the next question was WHY certain things happened. To answer this question, I referred to Stone's (1989) concept of causal stories. Instead of examining the sequence of events, the aim was to explore the intentions and motivations that led to the outcome. To that end, I needed to identify the causal factors for an action. For example, I could ask "why did FFTF fight against the use of FRT". Identifying different causal factors allowed me to understand the reasons behind FFTF's fight (their explanations of why it was crucial to ban the use of FRT), and their attribution of responsibility to different actors.

When putting the answers to the WHO, WHAT, HOW and WHY questions together, the entire plot of the story was unfolded. In the case of FFTF, now I would understand not only the dilemma they faced and who/what caused this situation (who/what FFTF chose to blame), but also how and why FFTF fought against the use of FRT. It is worth mentioning that the storylines or plot generated by answering these four questions would only provide me with different analytical structures for each group. These structures would later be reorganized into distinct narratives, so that we could get a better look at how the story around FRT is told and presented. More importantly, by sketching out the story and constructing the narrative, I had discovered the social life and social order held and imagined by FFTF, as well as the future they envisioned with/without the use of FRT.

In the following pages, I will first demonstrate how I produce a storyline for FFTF, and then move on to the details of narrative constructions.

First, after reading FFTF's articles, I reorganized them according to Propp's 31 functions and Brusentsev, Hitchens, and Richard's (2012) traditional grouping methodology as introduced earlier to identify "what happened" and "who are involved". During this process, I used my SI operationalization table (SIO) to help me navigate through the discourse, assigning roles to different characters, and identifying the sequence of events ("how it happened"). The following section showcases the result for the analysis of one article.

Article Name:

- Congress needs to stop messing around and ban facial recognition

Characters:

- Villain: Facial recognition companies, Law enforcement agencies (LEA), Clearview AI (CAI), FRT
- Hero: FFTF, civil rights advocacy groups, university students
- Helper: Congress/lawmakers= not so helpful helper, European Union, and many US states

Functions 1 to 8: These functions together signify the beginning of the story, where the villain has created a dilemma that requires the hero to address (What happened 1).

- Clearview (CAI) is selling its FRT to law enforcement agencies, which has raised various concerns regarding the potential impact on individuals' rights and privacy.

Functions 9 to 11: The situation is made known to the hero, and the hero is sent out to remedy the dilemma. In my analysis, this section is about the hero recognizing the dilemmas presented by the villains and providing proposals and suggestions for counteractions (What happened 2).

- FFTF believes that the utilization of FRT by law enforcement, government agencies, as well as both the private and public sectors should be banned when it is used for the purpose of public surveillance.

Functions 12 to 19: The hero faces/is tested by the villains and fights them. Again, this

section is about the sequence of events. In other words, it reveals how the villains present the dilemma and how the hero fights against the villains and the challenges they pose (How it happened).

- FFTF and many students from 50 universities are calling on the banning of FRT at college campus.
- The European Union and several US states are considering and promoting a moratorium on FRT.
- Activists are now working together to slow down the spread of FRT.
 - For instance, FFTF, in collaboration with many other civil rights advocacy groups, has launched a campaign (BanFacialRecognition.com) urging for a moratorium on Law enforcement and government use of FRT.
- FRT vendors have start marketing their technology to state, private and public sectors.
- FFTF publicly performed a facial recognition process using Amazon's Rekognition software to show the problematic aspects of this technology.
- Technology industry and Law enforcement agencies are pushing for a "industry-friendly regulatory framework" for FRT.
- Apart from banning the technology, FFTF also supports a restriction of "egregious" use of FRT, such as the utilization of FRT at public housing.

Functions 20 to 31: The hero has addressed the dilemmas and is determined to fight against any other challenges brought by the villains (What happened 3).

- The campaign launched by FFTF, along with other rights advocacy groups, has led to the rejection of FRT in many US cities. FFTF states that it will keep fighting against the establishment of an "industry-friendly regulatory framework" regarding tech industry and law enforcement use of FRT. At the same time, FFTF continues to advocate for a ban on governmental use of FRT.

After organizing FFTF's articles based on both the traditional grouping methodology and my SIO, now we have a clear depiction of the characters featured in the stories, along with their

respective roles, the dilemmas created by the villains, the measures proposed by FFTF to address the situation, and how the group proceeds to remedy the dilemmas. The next step is to attribute causal factors⁴ for FFTF's actions. For instance, when examining the second part of the grouping (Function 9 to 11), this section reveals the actions suggested by FFTF to different actors to address the dilemmas posed by the villains. If FFTF argues that the Internal Revenue Service (IRS) must terminate its contract with ID me, then, using Stone's (1989) concept of causal stories, we are looking for causal factors that explain the rationale behind FFTF's proposals and actions. Additionally, we will be able to identify to whom FFTF assigns responsibility. Here is a list of the causal factors I have identified for the same article as exemplified above:

- a) Why should the government ban the use of FRT by law enforcement, government agencies, as well as the private and public sectors if it is used for the purpose of public surveillance.
 - 1. According to FFTF, “weak, industry-friendly regulation” of FRT will only help the adoption of the technology to spread further.
 - 2. FRT poses threats to “public safety and basic liberty”.
 - 3. It has also threatened individual's privacy and human rights.
 - 4. The technology must be banned because it can never be used safely.
 - 5. The algorithm is biased, and the use of FRT only exacerbates pre-existing discrimination.
 - 6. FRT is “a software for tyranny”.
 - 7. FFTF's public demonstration of Rekognition's capability has shown the fact that FRT is “invasive and dangerous when it works”, but it is equally dangerous when it does not work.

After identifying these four factors (what, who, how, and why), now we have a general

⁴ Causal factors are the underlying elements that provide explanations for the occurrence of a particular incident or an individual's action. In our case, we are looking at the reasons behind different advocacy groups' proposals and actions. For example, we can explore the factors that explain these groups' belief that the utilization of FRT by different actors should either be banned or regulated.

structure/storyline of FFTF's narratives. However, this general structure can be quite confusing since it encompasses a mixture of all the characters present in my collected materials for FFTF. In order to establish some distinct narratives, the next step is to separate and categorize the storyline of these 10 articles based on the villains and their relationships as identified by FFTF.

To be more specific, we can deduce from this general storyline that FFTF has identified the state, private sectors as the villains of the story, and the group perceives the collaboration between these two sectors as problematic. In order to make the narrative construction process easier, this general storyline is divided into 3 types of stories: a) State sector as the villain, b) Private sector as the villain, c) Collaboration.

The new storylines are organized in the chronological order of what happened, how it happened, and why it happened. It is worth mentioning that the constructions of these storylines for all groups followed the same manner. Ultimately, with the help of these storylines, we will be able to craft some distinct narratives.

To conclude, the organized storylines for each group reveal that, unlike STOP, who does not identify the private sector as a potential villain in the story, the remaining groups (EFF and BBW) share the same three storylines as FFTF. It is worth mentioning that while BBW also identifies some members from the public sphere as villains (such as publicly funded research institutions) in some instances, such discourse is primarily centered around the problematic aspects of collaboration between the state and private/public sectors. Therefore, I categorized this type of discourse into the aforementioned collaboration category shared by the other three groups. In the next chapter, I will showcase the constructed narratives for each group based on these storylines to examine how they present and address the dilemmas associated with FRT.

Chapter IV: Narrative Construction

Introduction

In this chapter, I demonstrate that although the four advocacy groups (FFTF, BBW, EFF, and STOP) in this study all have expressed a negative attitude towards the utilization of facial recognition technology (FRT) by different sectors, all the groups maintained a clear separation between the public and private life, as exemplified in how they differentiate and treat public and private surveillance⁵ differently. Additionally, they emphasize the necessity of commercial competition, as well as highlight the needs for public education to ensure privacy and democracy. Notably, instead of challenging the fundamental power structure, the groups' positions and imaginaries align with and reinforce modern liberal ideals.

As a reminder, this study aims to answer two questions: a) what are the sociotechnical imaginaries (SI) of different advocacy groups regarding FRT, and b) how did the groups construct such imaginaries? By addressing these questions, I aim to understand how the groups advocate to invert the dominant imaginaries surrounding FRT and surveillance, as well as to map out the utopias that populate their imaginaries.

In order to find answers to these questions, I combined Propp's (1968) narrative analysis, Stone's (1989) casual stories, and my own SI operationalization table (SIO) to analyze the materials posted on the official websites of these advocacy groups.

In the following pages, we will construct three unique narratives for each of the following groups under study, FFTF, BBW, and EFF, and two for STOP. In other words, this chapter presents the results of my vertical analysis for each group.

Narrative Construction

As demonstrated in the methodology chapter, after analyzing each groups' discourse on FRT, I organized each of their general story structure into three distinct storylines⁶. Two of these storylines feature a distinct villain, while the third focuses on the relationship between the

⁵ According to the advocacy groups, while the use of FRT for public surveillance must be banned to safeguard the general public, its utilization for private surveillance is perceived as more acceptable and only requires robust regulations and privacy protection measures.

⁶ It is worth mentioning that STOP has only two storylines. In the selected articles, the group focuses exclusively on the utilization of FRT by state actors and the collaboration between the state and private sector.

villains previously identified by the advocacy groups under study. These villains include state actors (i.e., the metropolitan police, the NYPD, the Home office), private actors (i.e., FRT company), and public actors (i.e., public research institutions).

In the following sections, I will first provide a reminder of the basic analytical structure for each story, along with a brief description (Who are the characters? What happened? How it happened? Why it happened?)⁷ before putting together a narrative for each storyline⁸.

In my analysis, a well-crafted story is composed of four important components: the characters, the events that occurred (what happened), the ways these events unfold (how it happened), and the underlying reasons behind the events (why it happened). Though these four parts are seemingly independent of each other, together they create a complete picture of a story and illuminate its significance.

1. Characters: The characters of a story play an essential role in advancing the plot. Each character is distinct and has a unique role. They have goals, ideals, and values that may sometimes clash with other characters', leading to conflicts in the story.
 - Villain = the actors who are producing /using FRT in ways that results in causing harms to the general public during the process.
 - Hero = Individuals/organizations that fight against/disclose concerns regarding the use of FRT.
 - Helper = The allies or supporters of the hero
2. What happened: This is the base of the story. By answering "what happened" in the story, it reveals to us the basic structure of the story and it offers us a summary of the events that happened in the story.
3. How it happened: This is the sequence of events, by answering the HOW question, it shows us the key stages in the narratives and reveals to us the ways these events are presented to the readers.

⁷ Please refer to Appendix B-I for detailed construction processes.

⁸ While the narrative is about how the story is told and presented, the storyline is the analytical structure I put together for each article. It highlights the events and their sequence within a story, as well as the causal relations among different actors and events in the story. In other words, the storyline reveals the basic structure/progression of a narrative.

4. Why it happened: In order to answer this question, our aim is to identify the casual factors that led to the events in the story. By answering the WHY questions, we can uncover the underlying motivations and fundamental reasons behind the events.

When we put all four elements (who, what, how, why) of the story together, different narratives unfold before us. We will start with the three narratives that I extracted from Fight For The Future (FFTF), an American advocacy group that states its mission as ensuring technology is used as a force to empower people.

Fight For The Future

Narrative 1: State Sector. One of the major dilemmas identified by the hero, FFTF, is the systematic discrimination within law enforcement agencies. There have been several instances where police targeted and mistreated people of color, causing further harms to the marginalized population. Now with the advancement of technology, law enforcement agencies are provided with a range of “high-tech” tools to incorporate into their practices. Regrettably, despite the original design purposes of these technologies, some are being used in ways that exacerbate the pre-existing discrimination in society, while others possess inherent characteristics that enable and lead to its misuse. According to FFTF, FRT is a technology just like this, and as such it is an opponent to the quest for unbiased identification practices.

The hero reveals that FRT has enabled certain forms of surveillance. For instance, now law enforcement and various government agencies have turned into villains who utilize FRT to constantly surveil millions of Americans without their consent or knowledge. It is even more problematic that the use of FRT by law enforcement is often without strict regulations or guidelines. Many police departments use FRT without informing their superiors, highlighting a lack of transparency in police conduct and the missing of proper oversight. Additionally, police have been found to utilize FRT during public demonstrations to identify and track protesters. As a result, this has threatened people’s freedom of expression and civil liberties.

Furthermore, apart from identifying the state actors as the villains of the story, the hero also emphasizes how the unique characteristics of FRT have turned the technology into another villain. The hero acknowledges that the algorithm is “racist, biased, and discriminatory” (FFTF,

2021), as it has a higher misidentification rate for women and especially people of color. This has led to wrongful arrests and imprisonments of many innocent people, and FFTF argues that it may even lead to physical harms or death. FRT is described as “authoritarian and dangerous” (FFTF, 2020) as the technology is perceived as an “Orwellian technology”, capable of constant monitoring and identification of a large number of individuals, eventually turning the society into the one portrayed in George Orwell’s fiction, 1984.

Another concerning qualities of this algorithmic villain is its “toxicity”. FFTF argues that the technology’s dangerous and invasive nature have not only sparked many political controversies, but also infiltrated into our society slowly and unknowingly, causing irreversible harms like toxic gas.

Additionally, the hero draws an analogy between FRT and nuclear/biological weapons. This implies that there is no way to provide proper guidance regarding the utilization of FRT while ensuring the safety of the general public. In other words, even with strict regulations, nuclear or biological weapons are at risk of being misused, and the consequences of such misuse are dreadful and unthinkable. FFTF believes that the situation with FRT is similar, and that it may be impossible to properly regulate this technology when it is applied in public contexts.

Taking into account of these dilemmas, many lawmakers have expressed concerns regarding the impacts of FRT. However, the hero suggests that these potential helpers must now take concrete steps by banning the use of FRT by state actors. What is more, it is worrying that some lawmakers attempt to align with the perspectives of the villains, such as the “Big Tech” companies and law enforcement, necessitating and justifying the utilization of FRT in certain incidents or on certain populations (i.e., to identify and arrest the protestors during the Capitol Attack).

Under situations like this, FFTF expresses the concern that if we allow the widespread use of FRT continues, we may step into a future where we will be constantly oppressed and controlled.

In order to address the problems brought by FRT, the hero, FFTF, contends that it is crucial to recognize that the issues lie not only with the technology itself, but also with the individuals

who use it. The algorithm of FRT is equally problematic as the manner in which it is utilized in police practices. In order to tackle the dilemmas, the group has launched several campaigns along with other rights groups advocating for the banning of FRT in the state sector, and it has achieved many successes in its fights. FFTF states that it will continue to fight to protect people's privacy, security, and civil liberties from the invasive use of FRT.

Narrative 2: Private Sector. Not only the state sector, but the private sector has also started using FRT to surveil the general public. Unsurprisingly, private sector is another villain identified by the hero, FFTF.

To begin, FFTF points out that many retailers use FRT to monitor and discipline their employees, making sure they always stay productive. Additionally, as soon as the customers enter a store with FRT installed, they will be immediately subjected under constant surveillance and identification, posing a risk to individual's privacy and rights.

What is more, there are risks that FRT in store may be used in discriminatory ways, such as the targeting of members from BIPOC (Black, Indigenous, and People of Color) communities, and the profiling of customers. It is worth mentioning that these dilemmas are not only results of human biases, but rather a combination of human's biased decision-making and the biases inherent within the algorithm. For instance, FRT has a higher misidentification rate, especially for the BIPOC community. When relying on FRT for identification purposes, the biased algorithm will affect individuals from these communities disproportionately, eventually leading to targeting and discriminatory treatments.

The hero argues that it is unethical and authoritarian for retailers to subject their employees and customers to constant, covert and potentially discriminatory monitoring and identification. Their use of FRT is deemed "un-American" and "unwarranted" as such utilization infringes upon individuals' privacy and human rights, contradicting the democratic values the U.S. is aligned with.

To address these dilemmas, FFTF, along with various rights advocacy groups, have launched a campaign⁹ to call on U.S. retailers to stop the use of FRT on shoppers and employees. As a result, many retailers have acknowledged the public's negative attitudes

⁹ The campaign, "Ban Facial Recognition in Stores", was launched on July 14, 2021.

towards FRT and confirmed that they would refrain from using it in stores. The hero states that it will keep mobilizing the public to reach out to other retailers.

Apart from the retailers, FFTF reveals that FRT vendors often present their technology as a means to bring convenience and “personalization” (FFTF, 2021) into people’s daily lives. These corporate villains seize every opportunity (i.e., the COVID 19 pandemic) to promote their technology and maximize profits, without considering the impacts of FRT on people’s rights and safety.

Furthermore, the hero utilizes the controversies and incidents around Facebook’s (FB) facial recognition program to highlight the inherent self-centered and greedy nature of the “Big Tech” companies. For instance, even though FB announced that it would stop using FRT for its “Tag Suggestions” feature, the technology continues to be adopted in other platforms and services owned by FB¹⁰. At the same time, though FB is ordered to delete the database that contained its users’ facial biometrics, due to a lack of independent oversight and assessment, it would be impossible to know whether the data was really deleted.

Additionally, in order to promote the idea of a “metaverse”, where individuals are able to interact in virtual realities, FB/Meta¹¹ sells equipment like headsets that can track the wearer’s eye movements and facial information.

FFTF argues that the situation with FB/Meta is concerning, because first of all, FB has dominated the digital world and it exerts a great influence over people’s choice of social media platforms. This dominance/monopoly enables the sharing of data across its various platforms, leading to the collection of a large amount of personal data. This situation has raised a significant risk to individuals’ privacy and online security.

Moreover, as individuals interact in the metaverse, the production and collection of more personal data become inevitable. People’s’ biometric information is collected, analyzed, and stored unknowingly, which further exacerbating concerns about users’ privacy and the potential of data misuse.

The hero suggests that in order to put an end to private sector’s misuse and abuse of FRT,

¹⁰ Such as Meta, Instagram, and Oculus, etc.

¹¹ On October 28, 2021, Facebook rebranded itself as “Meta”.

and safeguard people's rights and privacy, Congress must now enact more Federal data privacy legislations, and allocate sufficient resources to make sure such legislations can be enforced properly. The hero further argues that it is crucial to ban the private sector's use of FRT in a public context, and insist that when such technology is deployed, the acquirement of individuals' consent is a prerequisite.

Furthermore, FFTF suggests that to address the dilemma with Big Tech's monopolization of the digital space (such as FB and its multiple social platforms), it is necessary to enact legislation that provides opportunities for smaller companies to compete and offer "alternatives to major platforms" (FFTF, 2021). In other words, fostering competition gives rise to more services and choices for individuals to choose from. By bringing equality to the digital space, smaller companies will be able to innovate and offer unique services to suit different user's needs and preferences. Moreover, addressing such monopoly also reduces the Big Tech's ability of conducting mass data collection and analytics. As competition increases, Big Tech companies may face more inquiries and pressures to prioritize their users' privacy and data protection. As a result, people may be empowered by being able to choose services and platforms based on their preferences and gaining more control over their own data.

Narrative 3: Collaboration. The widespread utilization of FRT in both the state and private sectors has spurred a collaboration between them. This collaboration between the two previously identified villains has also introduced certain dilemmas into the picture.

In order to gain more profits, FRT vendors such as Clearview AI (CAI) all start marketing their products to state actors "aggressively", while disregarding the negative impacts their technology may have on the general public. For instance, CAI has exploited the COVID-19 pandemic to promote and sell its technology. The company suggests that incorporating their facial recognition program into existing CCTV networks is crucial for more effective contact tracing and public safety during the pandemic. However, according to the hero, FFTF, such measure will subject individuals to constant monitoring, identification, and tracking. It not only grants police access to individuals' health information, but also their locations, posing a threat to people's privacy and civil liberties.

Apart from capitalizing on the pandemic, some corporate villains resort to lies to promote

their technology. FFTF reveals that under pressure from heroes like rights advocacy groups, FRT vendors tend to advertise their algorithms as verification¹², instead of recognition¹³, so to distance their technology from the controversial FRT. However, ID.me was found to be lying about not only the algorithm of its matching strategy, but also the number of unemployment benefit fraud cases, with the intention of securing more government contracts. Together, these incidents indicate that certain FRT vendors, like ID. me, are willing to prioritize their profits at the cost of their integrity, reputation and people's privacy and rights.

When moving our focus to the collaboration between the villains from both the state and private sectors, the hero points out that due to a lack of regulations and oversights on private sector's collection and processing of users' personal data, the collaboration may pose a risk to individuals' privacy and data security. Additionally, the use of FRT in government services presents challenges for marginalized communities due to issues with "accessibility and accuracy" of the technology. For instance, FRT has a high misidentification rate among people of color, and incorporating FRT into government services may result in wrongful identification and subsequent account lockouts for users from BIPOC communities. What is more, "economically disadvantaged" individuals may face difficulties accessing ID.me, as it requires smart phones or computers with high-quality cameras.

Uniting as heroes in the cause of safeguarding people's privacy and civil liberty, FFTF, along with other rights advocacy groups, have launched a campaign¹⁴ advocating for a ban on government and law enforcement use of FRT. The campaign later also urges the private and public sector to stop utilizing FRT to surveil the general public in public contexts or without the consent of affected individuals. Although the IRS terminated its contract with ID.me regarding the utilization of FRT in its online services due to the pressure received from a 2022 petition organized by FFTF and various rights groups, similar collaborations can still be seen in other government agencies. Our hero, FFTF states that it will keep fighting against the

¹² A "one-to-one" matching strategy which compares the two photos uploaded by service users.

¹³ A "one-to-many" matching strategies which compares the photos uploaded by the service user with the photos stored in the database. This is often perceived as more harmful and invasive, as the algorithm has received a lot of criticisms regarding its high misidentification rate for members from the BIPOC communities.

¹⁴ "Ban Facial Recognition", launched in July, 2019.

government use of FRT and advocate for regulations to govern private sector's utilization of this technology.

In the following pages, we will examine three narratives that I constructed for BBW, a UK advocacy group that aims to fight for a “free future” (BBW, 2023), and safeguard people's privacy and freedoms during the time of technological change.

Big Brother Watch

Narrative 1: State Sector. According to the hero, BBW, police are given far too much discretion in making policy decisions that may influence the lives of UK citizens. They have the authority to decide what technology to use to police the country, as well as how that technology will be used. This has posed serious threats to democracy. One of the most controversial problems at hand is police use of FRT.

Now, the police are using this intrusive technology to surveil and identify UK citizens without their consent, with a particular focus on protestors and individuals with mental health conditions. This has led to innocent people being subjected to constant surveillance, effectively transforming them into walking ID cards, ready to be identified by the police. Additionally, the algorithm of FRT is not without blame. With a high misidentification rate for women and people of color, it exacerbates the discrimination of marginalized population. However, police have refused to subject their facial recognition software to bias testing and have rejected any opposing voices to their use of FRT. Additionally, police even justify the inaccuracy of FRT by claiming that there is no perfect algorithm, disregarding the negative implications posed by the risks of misidentification to society.

Furthermore, when combining these algorithmic flaws/biases with existing human biases, FRT becomes an intrusive and authoritarian police tool, ready to surveil and identify the individuals at any instance and transform UK into a dystopian police state. In this sense, police have been turned into an uncontrollable villain, using the biased technology (FRT) as they see fit.

What has made the situation even worse is the fact that, instead of acknowledging the problematic aspects of police's use of FRT, the Home Office (HO) has supported and defended such usage. However, their plans and claims are misleading and false according to BBW: how

do you build a board to oversee FRT and ensure police use this technology in line with guidelines if there are no safeguards regulating its utilization, or guidelines for them to follow? The HO has claimed that FRT is just an evolution of “super recognisers”, but are these human experts capable of identifying millions of individuals across time and space everyday, as FRT can? The HO has clarified that all facial data gathered will be deleted immediately if no matches are found in the database, yet evidence suggests that such claim is simply untrue, as every facial photo captured unknowingly is stored in police database for up to 1 year. In addition, though HO argues that it would be too expensive to delete all of the collected photos, they still awarded the South Wales Police Department £2 million to deploy FRT. Ultimately, according to our hero BBW, HO has transformed into yet another villain, posing threats to democracy.

BBW suggests that, considering the biases inherent in the law enforcement and the algorithm, instead of funding the police for the integration of more advanced technology into their practices, they should use their existing resources to fulfill their duties.

According to BBW, the UK police use of FRT is problematic, as it has violated UK citizens’ right to privacy, freedom of expression, and created a “democratic vacuum” (2019 b) in the society. In 2018, acting together as heroes, BBW launched a legal campaign against the use of FRT by police, with the support of more than 15 rights advocacy groups. They also publicly support the Ethic group’s statement that facial biometrics should receive the same level of attention from the government as other forms of biometric data (i.e., fingerprints). More importantly, BBW argues that we must not only bring police illegitimate use of FRT into democratic inquiry, but at the same time, advocating for a moratorium on this technology before it turns society into a dystopian police state.

Narrative 2: Private Sector. Indeed, the utilization of FRT by state actors has brought about certain dilemmas, yet the responsibility also lies with those who develop and provide such technology.

Our hero, BBW has expressed concerns over the unauthorized and unethical collection and processing of people’s facial biometrics by private actors. For instance, Clearview AI, an American facial recognition company, was found to be secretly collecting and making available UK citizens’ facial data to the highest bidder in 2022. The company was fined by Information

Commissioner's Office (ICO) over £7.5 million for its illegitimate collection and processing of personal data and was ordered to delete all previously collected and stored data. Similarly, a few months later, an online facial recognition search engine named PimEyes was found to be unlawfully processing millions of UK citizens' facial images collected across the Internet, without proper safeguards to prevent their technology from being used for surveillance purposes. While PimEyes asks the users to use their service ethically, there are no limitations on the type of photos users can use on their website, posing privacy risks to the individuals in those photos.

Private sector's handling of personal biometrics is problematic, and the cases of Clearview AI and PimEyes are only the tip of the iceberg. According to BBW, the lack of transparency surrounding the data collection and handling practices of these companies are concerning, because without knowing how personal data is collected, handled, and used, people have lost control over their own data, and it poses serious privacy risks to the data subjects. These unregulated practices have clearly violated UK citizen's human rights, and it ends anonymity in society.

Similar events will continue to occur with this lack of transparency and the absence of effective laws to properly regulate and safeguard private sector's development and utilization of FRT, as well as their handling of personal data. In order to battle the mishandling of individual's personal data and to protect UK citizens' privacy right, uniting as heroes in this narrative, BBW has filed a legal complaint with the ICO against PimEyes for its violation of data protection law, and BBW proposes that now the ICO must take on the role of the hero to protect the citizens from "these dangerous facial recognition tools" (2022).

Narrative 3: Epidemic of FRT (Collaboration). In addition to the state and private sectors, the public sectors have also started to develop and employ FRT, and their utilization is similarly concerning.

In 2017, the Bristol Robotics Laboratory planned to use FRT at train stations to enhance travel experience. In this sense, instead of train tickets, people are able to use their facial biometrics as tickets, avoiding the need to wait in line to enter or exit the barriers. This seems to be quite convenient, and Professor Lyndon Smith at the laboratory believes that in the future,

individuals' faces will be the key to doing whatever they want in the modern world. However, such convenience is not free of concern. The hero, BBW argues that the use of FRT by the public sector may encourage and lead to collaboration between the private/public actors and the state actors, and such collaboration between the previously identified villains may eventually introduce certain dilemmas into society. BBW has warned the government that this collaboration, as well as the lack of regulations, monitoring and transparency regarding data collection practices in the private and public sector, may raise some privacy concerns. However, the UK government paid no attention to their warning.

According to our hero, we are faced with an epidemic of FRT, and it is eroding our democratic values and threatening our right to privacy. Many private and public actors perceive government's inaction regarding FRT as a greenlight for their illegitimate development and deployment of the technology. Looking back on the use of FRT at train stations, BBW argues that our faces are no longer private to us. They were reduced to binary codes and stored in the system. Once we give the private and public sectors access to our facial data, it may not only be shared with the state for policing and safety purposes, but it also poses serious risks to security and privacy. We are constantly monitored, tracked and identified whenever we appear under a CCTV camera, and unlike password, which we can change at will, facial biometrics are unique to each individual. Therefore, if the database containing our facial information is breached or lost, this data could be used for identity theft. Eventually, we may end up living in a society where there is no right to privacy.

Though some argue that the collected data will be encrypted and thus safe from security breaches, BBW expresses the concern that, given the government's history of weakening and abandoning encryption measures, the group does not trust the government's ability or claim to secure citizens' personal data.

BBW states that with this epidemic of FRT, the UK is gradually transforming into a surveillance state, and is on the path of becoming "the most surveilled democracy in the world" (2019a). According to BBW, regulations regarding FRT are insufficient to pull us out of this democratic vacuum and will only provide the private sector with a defined space to conduct public surveillance and monitor the citizens. Under a situation like this, BBW states that we

must subject the use of FRT by different sectors and their handling of personal information to democratic investigation and proper oversight, while advocating for a ban on any use of FRT for the purpose of public surveillance. It is only then can we ensure that our society does not transform into an authoritarian state devoid of privacy and democracy.

Moving on to the narratives of the next advocacy group under study, EFF is an American based NGO who states its mission as to ensure that technology is utilized to support “freedom, justice, and innovation for all people of the world” (EFF, 2023).

Electronic Frontier Foundation

Narrative 1: State Sector. In 2011, the FBI announced that it would build a “bigger, faster and better” (EFF, 2013) biometric database, including an updated facial recognition program. This database was designed to be shared across different agencies and with foreign countries, with the inclusion of innocent people’s facial images. These plans alone raised some serious concerns regarding the infringement of people’s privacy and civil liberties, as they would enable massive and yet covert monitoring, identification, and tracking of not only suspects but innocent people.

What makes the situation worse is the FBI’s unshakable determination to roll out this database and its facial recognition program, despite the lack of thorough review regarding the potential technological impacts on the general public¹⁵. EFF, along with other rights advocacy groups, have united as the heroes and demanded that the villain, FBI, release relevant information regarding this new database and have argued that a public debate is needed to determine its acceptability. However, against many opposing voices, the database was eventually deployed and gradually enhanced over the years, enabling a massive surveillance network.

As time goes by, an increasing number of government agencies have also started to adopt FRT into their practices, leading to various dilemmas in its utilization.

To begin, FBI’s Next Generation Identification system (NGI) has created a shared facial biometric database that allows different government agencies to access and share their own collection of individuals’ facial images. For instance, the Department of Motor Vehicles (DMV)

¹⁵ FBI has not updated its Privacy Impact Assessment (PIA) for several years.

can share driver's photos with the NGI database, allowing law enforcement agencies to conduct facial verification and identification of suspects. However, due to a lack of regulations and guidelines, these facial biometrics are at risk of being misused, raising concerns for people's privacy and rights. Moreover, this unrestricted access to and sharing of facial biometrics facilitates a "perpetual facial dragnet" (EFF, 2018), enabling the large-scale collection, identification, and storage of individuals' facial biometrics.

When focusing our attention on another villain identified by our hero, law enforcement agencies, they may argue that such high-tech equipment will help solve and even prevent crimes. However, the reality differs from these claims.

For instance, people should have the freedom to participate in peaceful gatherings and demonstrations and express their beliefs openly. Yet, police have been found to frequently utilize FRT to identify and track protesters during peaceful demonstrations, causing harm to individuals' civil liberties.

What is more, though the San Diego police department's drafted policy requires the officers to obtain individual's consent before taking a photo, many officers choose to rely on their "spidey senses"¹⁶ (EFF, 2015). In other words, if an officer instinctively perceives someone as "suspicious", they will choose to utilize FRT without regard for the policy's guidelines.

Now, moving on to the technology itself, the algorithm of FRT is equally flawed and problematic, as it is prone to errors and misidentifications, especially for women and people of color. However, the problems escalate when we combine the manner in which FRT is used by government agencies and the algorithm itself.

For example, in order to produce a match through the algorithm, police analysts may edit the photo by modifying individual's facial expressions, adding special effects to improve the quality of the image, or using 3d modeling to create non-existent facial features in the photo etc. Yet, these editing all increased the risks of misidentification. Moreover, the accuracy of identification results can also be influenced by the database used by police. This is to say that

¹⁶ Spiderman's ability to be hyper-aware of the surroundings, sensing and preventing dangerous before it happened.

when conducting facial recognition, police may utilize their own criminal databases. However, because of an already biased police practices, mugshots stored in these databases are composed mainly of individuals from over-policed and marginalized communities. In this sense, individuals from these communities are more likely to be affected by the resulting misidentification. As a result, police use of FRT may further exacerbate the pre-existing discrimination in society.

Additionally, since FBI's NGI facial recognition program is used by all levels of government agencies, it is essential for the FBI to ensure the accuracy of their recognition system and take measures to prevent FRT from being used in a manner that may result in innocent people being falsely identified as suspects by its external partners. Unfortunately, the FBI has done none of these.

As the hero, EFF has also highlighted the lack of transparency in police use of FRT. For instance, police keep the specific processes of their FRT utilization and the adopted facial recognition algorithm secret. This lack of knowledge has posed a challenge when it comes to questioning police utilization of FRT, such as assessing the validity and the trustworthiness of the identification results. It is also worth mentioning that once potential matches are identified by the algorithm, human reviewers may still be influenced by their own biases when making judgements and decisions.

To address these dilemmas and safeguard people's rights and civil liberties, our hero argues that lawmakers and regulators must now act to limit the collection of individuals facial biometrics and subject FRT to independent oversight. It is also crucial to make transparent law enforcement agencies' development and adoption of FRT. Additionally, EFF urges the public to be concerned about the government's plan to enhance the ability of their facial recognition system and be aware of its potential impacts. By doing so, people will be able to properly assess the situation and together oversight the development and utilization of FRT.

Narrative 2: Private Sector. Apart from the state sector, there has been an increase in private sector's use of FRT. According to the hero of this narrative, EFF, actors in this sector recognize the potential benefits that the adoption of FRT can offer. They are willing to subject individuals to constant surveillance, causing privacy concerns in the process, all in pursuit of

greater profits. Despite the existence of bills and regulations that aimed to safeguard people's privacy rights, such as the "Illinois Biometric information Act", various members from the private sector are attempting to repeal bills like this and promote a more "industry-friendly" framework (2016). In this sense, private sector is another villain identified by the hero.

Additionally, in a meeting organized by the National Telecommunications and Information Administration for the drafting of a "voluntary code of conduct" regulating the utilization of FRT by private companies, the industry stakeholders rejected proposals put forth by privacy advocates, such as the requirement for consumers' consent prior to the collection of their biometric data.

These instances reveal that when it comes to their own profits and interests, corporate villains are willing to sacrifice their consumers' privacy, security, and rights in exchange for their own benefits. In other words, they prioritize their self-interest above all else.

To address this dilemma, EFF has joined forces with other privacy advocacy groups to advocate for new regulations and bills that protect people's privacy and rights from private sector's invasive use of FRT, while defending existing privacy bills from being attacked and repealed by corporate actors.

Narrative 3: Collaboration. So far, we have seen the adoption of FRT by both the state and private sectors, which has resulted in the establishment of a massive surveillance network. However, as time goes on, a collaboration between these two types of villains has been pushed to the surface.

According to our hero, EFF, corporate villains often describe the technology as a "silver bullet". This implies that FRT vendors and advocates present the technology as a quick, easy, and almost magical solution for law enforcement. However, EFF argues that FRT does not work as advertised, and the reality is far more complex.

One example of this collaboration is the partnership between the Internal Revenue Service (IRS) and ID.me. EFF highlights the lack of regulations and privacy restrictions governing the private sector's collection and handling of personal data. As a result, the IRS' collaboration with a third-party FRT company has posed privacy risks to its service users.

Our hero argues that apart from the collaboration, FRT itself is a dangerous technology with the potential to become one of the most pervasive and intrusive surveillance technologies. When such a technology is incorporated into government services, individuals are forced to give up their privacy in exchange for accessing these services. This is dangerous and unnecessary, especially when the companies that provide this technology are not bound by federal rules and laws that regulate state actor's use of FRT. In this sense, when forcing individuals to entrust their biometric data to a third party, their personal information is at risk of being misused.

The collaboration between the IRS and ID.me has received critiques from not only the public (such as rights advocacy groups like EFF), but from various branches of government. Consequently, the IRS terminated its contract with ID.me. However, EFF contends that many state and local government agencies still use or plan to use FRT for user identity verification under the guise of ensuring "safety". The hero states that it will keep fighting for a ban on government use of FRT.

Finally, let us now shift our attention to STOP, an American-based rights advocacy group that primarily focuses on issues related to surveillance and surveillance technology in New York City. The organization's works highlight the discriminatory impacts of surveillance on marginalized populations, and it fights to ensure that technology is used ethically and with proper regulation and safeguards.

Surveillance Technology Oversight Project

Narrative 1: State Sector. With the advancement of technology, there has been a surge in AI-powered surveillance technology. Among these technologies, FRT is one of the most controversial surveillance tools utilized by law enforcement. According to our hero, STOP, police have slowly incorporated FRT into their practices to aid their investigations. Yet, dilemmas have occurred along with its utilization, and these problems originated not only from the technology itself, but the manner in which police utilize it.

Firstly, contrary to the powerful and accurate tool advertised by many technology companies, FRT is biased and dangerous. The accuracy of the algorithm depends not only on the quality of the photo provide for identification, but also the inherent qualities of the

algorithm.

Our hero suggests that when a technology is developed, a series of “decisions and assumptions” are made that can influence the reliability of the technology. These choices and assumptions not only affect the technological accuracy but also introduce biases into the algorithm. Consequently, these fundamental factors significantly influence the functioning of the technology.

For instance, STOP highlights a lack of diversity¹⁷ in the photos used to train the algorithm of FRT. As a result, it has a higher misidentification rate for women and people of color. This has led to many wrongful arrests and imprisonments of innocent individuals, further exacerbating discrimination against marginalized population in society.

To expand on the problems inherent to the algorithm, it is crucial to examine its real-world applications and impacts. According to the hero, FRT has facilitated a new form of surveillance, infiltrating our lives and subjecting us to constant identification and tracking without our awareness. This invasive technology has become a driving force behind the establishment of a “dystopian surveillance state” (STOP, 2020). Now, shifting our attention to the law enforcement, it becomes evident that the problems arise not only with the inherent qualities of the algorithm of FRT, but also with its users. STOP has identified law enforcement as one of the villains that utilizes FRT as a tool, bringing certain dilemmas into society. Our hero has specifically highlighted a lack of transparency and oversight in police conduct, emphasizing how the use of FRT by law enforcement may exacerbate the infringement on our privacy and civil liberties.

For example, though FRT has been shown to have a higher misidentification rate for people of color, police continue to use this biased technology to target the already over-policed communities. This effectively transforms individuals’ bodies into “government tracking devices” (STOP, 2021), all while using fundings and donations to purchase more surveillance tools without City Council oversight. What is more, when the photo of a suspect is of low quality, police analysts may resort to editing the photo using software like Photoshop to force

¹⁷ Stop reveals that the algorithms of FRT are usually trained with photos of “middle-aged white men”. This decision has introduced biases and limitations to the performance of the algorithms.

a match through the algorithm ¹⁸ . However, such edits only increase the risks of misidentification and wrongful arrest.

Moreover, due to the impacts of the Capitol Attack incident, even those who once criticized police practices have begun promoting and justifying the use of FRT, arguing that it is crucial to empower the police. Yet, according to STOP, this perspective is misguided.

The hero argues that the police already possess enough power – perhaps too much power. They have the discretion to decide when, how, and on whom FRT is used, without any oversight body to assess and regulate their use of such invasive technology. In addition, despite public criticism of police use of FRT, law enforcement not only rely on the algorithm to make decisions for them, but also use the results of FRT as evidence to support their biased beliefs and conduct. What is more, NYPD even refused to disclose relevant information regarding the FRT it has used, such as how the technology works, when it is used, and the accuracy of the algorithm. Such disregard for transparency may further exacerbate systematic discrimination in society.

STOP asserts that FRT is treated by the law enforcement as nothing more than an advanced toy, indicating a lack of awareness within police departments regarding the inherent biases and potential negative effects associated with this technology. When such unawareness is combined with an already biased system, it threatens individuals' privacy, human rights, and civil liberties, and may eventually lead to the erosion of democracy.

In light of this dilemma, our hero contends that instead of giving police more surveillance technology to target and surveil marginalized communities (figuring out how to empower police), it is crucial to not only address the systematic discrimination within law enforcement agencies, but also establish a civilian oversight board to evaluate the surveillance technologies purchased and used by police and protect the general public from police misuse of these technologies, while advocating for a ban on invasive technology like FRT.

In order to achieve such a goal and safeguard people's privacy and civil liberties, STOP, along with other rights advocacy groups, united as the heroes and launched a global campaign in 2021 to call for the banning of FRT not only in New York, but several other cities over the

¹⁸ Such as adding special effect to improve the quality of the image.

world. Moreover, due to collected efforts¹⁹, the “Public Oversight of Surveillance Technology” (POST) was passed in 2020, which requires transparency in police policies and practices, and establishes a civilian surveillance oversight board in New York to govern police use of surveillance technology. Similarly, many cities in the U.S. have also passed the “Community Control Over Police Surveillance” (CCOPS) laws, requiring police surveillance technology to be evaluated and monitored by civilian. However, despite these successes, STOP suggests that this is only the first step, as they will keep advocating for a ban on law enforcement utilization of FRT, and safeguard people’s privacy, civil liberties, and democracy.

Narrative 2: Collaboration. According to our hero, STOP, there is a growing global demand for FRT, and many companies have recognized the potential benefits they may gain in this industry. However, as more and more companies enter into the FRT market, the competition has intensified. Now in order to stay ahead of their rivals (such as gaining more government contracts), companies are expected to introduce innovative features of their FRT products. Nevertheless, many of these innovations are invasive in nature and have brought certain dilemmas into the picture.

For instance, the hero reveals that Wolfcom, a company that specializes in manufacturing bodycams, is now proposing the idea of “live facial recognition” by integrating FRT into bodycams. However, such incorporation raises a threat to individuals’ privacy and the democratic values that the U.S. upholds. It enables real-time analysis of live video feeds captured by body-worn cameras, subjecting not only suspects but innocent bystanders to constant monitoring and identification. Their facial biometrics are collected and analyzed automatically without consent whenever they appear in front of the camera.

Apart from the unique dangers posed by live facial recognition, STOP highlights the fact that Wolfcom fails to clarify the source of their FRT and the database it uses for identification. It remains unclear whether the technology is designed and developed by itself or obtained from a third party. Without this information, it is challenging to assess the reliability of the algorithm and determine who has the access to the collected data, ultimately posing a threat to individuals’ privacy and civil liberties.

¹⁹ The majority of the City Council, public advocates, and the New York Times editorial board.

Similarly, many U.S. FRT vendors present their technology as an effective solution for tackling societal issues, such as the increasing occurrence of unemployment benefits fraud. As a result, more and more government agencies have begun incorporating FRT into their online services.

While some argue that government agencies employ FRT solely for the purpose of verification, a one-to-one matching technique commonly used in smartphones, instead of identification, making it less invasive, STOP has a different stance. The hero asserts that verification is as dangerous and biased as identification, as the use of it has led in delays or even denials of unemployment benefits applications. Moreover, due to a lack of regulations and oversight concerning corporate actors' collection and processing of individuals' personal data, the use of FRT by government agencies has posed a risk to people's privacy and rights.

In addition to privacy concerns associated with government use of FRT, STOP argues that incorporating FRT into government services may exacerbate inequality and marginalization within US society, contributing to the "digital divide" (STOP, 2021). One example can be seen in the IRS' contract with ID.me, where the economically disadvantaged users may experience difficulties accessing IRS' service due to the requirement of owning a phone or computer with a high-resolution camera.

Taking into account the aforementioned dilemmas, the hero states that though the use of FRT is common for consumer devices, the government should never incorporate this kind of technology into its services. Such incorporation is authoritarian in nature, as government use of FRT will subject citizens to constant surveillance, identification, and tracking, building a pervasive surveillance network. To address the dilemma, STOP has collaborated with other rights advocacy groups to launch several campaigns against law enforcement and government use of FRT. Fortunately, many state actors and corporate actors have recognized the risks associated with FRT and have taken on the role of heroes. For instance, California, along with Oregon and New Hampshire, banned police use of FRT on body cameras in 2020, and Google has also paused its development of FRT programs for government use. Despite these successes, STOP states that it will keep advocating for a ban on law enforcement and government use of FRT, with the aim of safeguarding people's privacy, rights, and democracy.

Conclusion

Using Propp's (1968) narrative analysis, Stone's (1989) casual stories, and my own SI operationalization table (SIO), I have constructed three narratives each for FFTF, BBW, and EFF, as well as two for STOP. These narratives were created based on the villains identified by the groups in their discourse and the relationships between these villains. To elaborate, FFTF, BBW, and EFF all recognize the state and private sector as villains in the story, and perceive their collaboration as problematic, calling for it to be addressed. In contrast, STOP focuses primarily on the state sector and its collaboration with the private sector. Similar to the previous three groups, STOP also emphasizes the need to end such collaboration due to the potential threats it may pose to the general public.

Additionally, all groups assume the role of the heroes and acknowledge the importance of collaborating with other actors to safeguard privacy and civil liberties of the general public.

In the following chapter, we will analyze these narratives, exploring their similarities and differences, before delving into their envisioned futures.

Chapter V: Narrative Analysis

Introduction

After constructing distinct narratives for each advocacy group, the similarities and differences in these narratives have all been pushed to the surface. We will begin by exploring the common problems that all four advocacy groups have identified and agreed upon: the lack of regulations, transparency, and oversight; the issues rising from the collaboration between the main stakeholders on FRT; and the inherent problems and potentialities with the technology itself as well as its combination with existing devices. Next, we will discuss the differences found in the narratives of the four advocacy groups under study: the place attributed to Big Tech companies; and the means the advocacy groups deployed to meet their goals including the relationship developed with their allies. Finally, we will examine the futures they predicted and envisioned under the influence of different sectors' utilization of FRT.

Similarities among the Four Advocacy Groups' Narrative

Lack of Regulations, Transparency, and Oversight

As Marx (1985) argued, technological advancements have led to not only the state but corporate actors to employ various surveillance tools for their own purposes. As a result, the general public has been transformed into the subject of surveillance, giving rise to various problems associated with the adoption of these technologies. When focusing our attention on the state and private sectors' utilization of FRT, the narratives presented by all four advocacy groups have emphasized the lack of regulations, transparency, and oversight in both the use of FRT by law enforcement and the collection and processing of personal data by technology companies.

The groups' narratives all point out that first, there are inherent biases within the legal system. Without proper regulations and oversight, police have been found to utilize FRT as they see fit, while justifying their practices with the results produced by an equally biased technology (which we will discuss later). As Chochia and Nässi (2021) argue, such misuse and abuse of FRT may eventually lead to an intensification of the existing marginalization and discrimination. Notably, these narratives reflect Ho et al.'s (2021) concerns regarding FRT. The researchers have warned that apart from the flawed technology, the inherent biases within

society may lead users of FRT to selectively rely on the recognition result and reinforce their biased conducts and beliefs.

For example, EFF and STOP's narratives highlight that police have been using editing tools such as Photoshop to enhance the quality of the images they use for identification, or even employing 3D modeling software to add non-existent facial features to facilitate a match in the database when using FRT. This has increased the rate of misidentification and may lead to the exacerbation of systematic discrimination²⁰.

In addition, FFTF's narrative suggests that some police departments use FRT without informing their superiors, while EFF, STOP and BBW argue that police now have too much power/discretion in deciding how and on whom FRT is used, and that they refuse to neither reveal the details of the FRT they used, nor subject the algorithm to bias-testing. Similarly, Purshuse and Campbell (2022) highlight that the British legal framework has granted police too much discretion in deciding how to utilize FRT, and whether such utilization is "proportionate and necessary" (p. 17). The researchers point out that such excessive discretion reflects a "structural deficiency" (p. 22) in British law, and they argue that FRT should never be used by law enforcement without strict regulations and ethical evaluation. It is worth mentioning that Purshuse and Campbell suggest that with a rapid technological advancement, it may become challenging, if not impossible, to predict new innovations and tailor regulations accordingly to safeguard the general public from law enforcement misuse and abuse of such technology. Rather, the researchers propose that we must at least begin addressing the problems within the legal system. Therefore, they contend that it is now crucial to regulate police practices and tackle the power imbalance between law enforcement and the general public.

Furthermore, BBW and STOP point out that such lack of regulations and oversight in police practices have resulted in a diminishing of police accountability. They argue that instead of providing police with more fundings for the incorporation of FRT into their practices, in an attempt to empower them, as some suggested²¹, all police need to do is to use the existing

²⁰ EFF reveals that due to systematic racism, police databases are composed of images of individuals from over-policed and marginalized communities. Therefore, members from these communities are more likely to be affected by the resulting misidentification (EFF, 2022 b).

²¹ UK: The Home Office awarded the South Wales Police Department £2 million to deploy FRT (BBW, 2018 b).

resources to do their jobs.

Using the Capitol Attack incident in 2021 as an example, STOP suggests that what is “infuriating” (STOP, 2021 a) is not the attack, but rather the lack of accountability displayed in police unwillingness to act. In this sense, the police failed to take proper action to deescalate the situation during the attack, indicating a failure to fulfill their duty and responsibilities as law enforcement officers. STOP states that such lack of accountability may eventually lead to the erosion of democracy.

Indeed, the lack of regulation and oversight in law enforcement utilization of FRT has also been widely identified and discussed by many scholars (Raposo, 2022; Chochia & Nassi, 2021; Stark, 2019). They have revealed how such lack of regulation and excessive police discretion may result in an infringement of individuals’ rights and privacy. It is worth mentioning that Brad, Yesberg, Jackson and Dawson (2020) highlight a correlation between an individual’s level of trust towards police and their acceptance of police utilization of FRT. They explain that the higher an individual’s trust level in the police is, the more legitimacy they will assign to police use of FRT, and the more likely they will accept such technology.

On the contrary, when there is a low level of trust in police, less legitimacy will be assigned to police conduct, and there will also be a heightened concern for individuals’ privacy. Such findings are in line with our advocacy groups’ narratives surrounding police conduct. These narratives have shown the groups’ uncertainty towards police utilization of FRT. To be more specific, they have not only questioned police excessive discretion and their legitimacy of utilizing FRT, but also raised concerns regarding its impact on people’s privacy and rights. In this sense, it has revealed the lack of confidence and trust in the groups’ narratives towards the police. Therefore, all groups have emphasized the necessity of having more robust regulations to govern and oversee law enforcement utilization of FRT, and ultimately, they advocate for a ban on the police use of such technology.

Similar for the corporate actors, the absence of regulations and oversight has led to a lack of transparency regarding private sector’s collection and processing of individuals’ facial

US: some lawmakers believe that it is important to empower police by providing them with more advanced tool to aid in their practices.

biometrics, posing risks to people's privacy and security. According to BBW, Clearview AI (CAI) has been secretly collecting millions of UK citizens' facial images and prepared them for sale without individuals' consent. Additionally, Raposo (2023) points out that due to the lack of regulations in the private sector, CAI was found to illegitimately collect and process people's photos gathered from various companies, such as "Facebook, YouTube, Venmo and millions of other websites" (P. 7), without the consent and agreement from these involved companies. Leong (2019) points out that FRT has provided corporate actors with immense and unregulated power to surveil and even manipulate the general public unknowingly. This has raised concerns that such unregulated utilization of FRT may eventually lead to more oppression and discrimination.

In conclusion, the narratives of those groups all emphasize that the absence of regulations, transparency, and oversight in law enforcement practices and private sector's activities have resulted in an infringement to citizen's privacy, human rights, and civil liberties. As BBW puts it, unregulated police conduct, along with corporate actors' illegitimate collection and processing of personal biometrics have punched a hole in democracy.

Private Sector: Regulations or a Complete Ban?

Indeed, the groups' narratives have all emphasized the importance of implementing proper regulations and oversight for both the state and private sector's utilization of FRT. However, there is a divergence in these narratives. On the one hand, they suggest that regulations alone are insufficient to safeguard the general public from the inherent risks associated with both the technology and the biased legal system, therefore a ban on law enforcement and governmental use of FRT is crucial. On the other hand, the narratives reveal that it is not necessary to call for a complete ban on the private sector's utilization of FRT.

This differentiation in their positions has raised a contradiction in some of the groups' narratives. For instance, similar to Stark's position (2019), though FFTF also draws a parallel between FRT and nuclear/biological weapons, highlighting the fact that such technology is dangerous and can never be properly regulated. Yet, instead of advocating for a complete ban on private sector's use of FRT (as they did for the state sector), the group calls for a partial

ban²², demanding that the private sector stop using FRT in public for surveillance purposes or without the affected individuals' consent.

Such a stance may seem contradictory at first, but if we recall the characteristics of the groups, the answer becomes evident. According to FFTF, STOP, and EFF, they believe that when used properly, technology can become a force to “empower people” (FFTF, 2023), allowing the general public to gain more access to knowledge and information so that they can be more aware of their own situations, and challenge the dilemmas that concerns them. In other words, the groups have recognized the potential benefits of technological advancement. For instance, such access to technology enables individuals to educate themselves on issues that may affect their rights and well-being. What is more, technology provides people with spaces (such as social media platforms) where they can express their believes and ideas freely. As a result, their voices can reach a wider audience and have a greater impact.

In terms of FRT, when incorporated into consumer devices, it does provide the users with much convenience. However, the groups' narratives reveal that such incorporation also enables mass surveillance.

Similar to several scholars' suggestions (Roposo, 2022; Purshouse & Campbell, 2022; Chochia & Nassim, 2021), the groups acknowledge that with proper regulations and oversight, we will be able to enjoy the benefits brought by technological advancements without having our rights and freedom taken away from us. However, another question arises: if the groups believe that instead of a complete ban, regulations and oversight can ensure the responsible use of FRT by the private sector, why have they all expressed the necessity to ban state sector's use of FRT? To put it differently, both state and private use of FRT facilitates a distinct form of surveillance, yet one form is considered unacceptable and needs to be banned, the other is perceived as acceptable, as long as there are strict regulations and legislations to regulate the utilization of FRT. We will discuss this seemingly confusing separation in greater detail later.

²² Similar to FFTF, BBW states that the use of FRT for public surveillance is a human rights issue. In this sense, regulations will only provide corporate actors with a defined space to surveil the general public. To put it differently, the group argues that the use of FRT by private sector for public surveillance purposes must be banned.

Collaboration

All four groups' narratives identify the existing (or potential) collaboration between the state and the private sector. According to EFF, FFTF, and STOP, FRT vendors tend to advertise their technology as not only a powerful and accurate tool for law enforcement, but also an effective tool for other government agencies to address existing societal problems (Ho, Black, Agrawala & Li, 2021). For instance, EFF, FFTF, and STOP use IRS' contract with ID.me as an example to highlight the risks and harms associated with such collaborations. More specifically, though some government agencies claim that they incorporate FRT into their online services for "safety" purposes, the groups argue that safety problems are posed exactly by forcing individuals to subject their data to a third party that is not regulated by strict privacy laws.

Similarly, BBW's narratives also reveals the possibility that once individuals subject their facial biometrics to the private or public sector by using their services, their data may be collected and shared with law enforcement for policing and safety purposes. Likewise, Purshouse and Campbell (2022) reveal that law enforcement sometimes may also provide individuals' images to private entities to use when deploying FRT. They argue that with a lack of regulation and transparency in both the state and private sector's processing of personal data, people's data are at risk of being misused and abused, posing risks to individuals' privacy and data security. Gray (2003) has also expressed that such collaboration between the state and private entities raises ethical concerns due to a lack of oversight and regulations, yet such problem is seldomly examined. More importantly, Gray argues that this collaboration may eventually lead to a shrinking of private space and an expansion of surveillance spaces.

According to the groups' narratives, the sharing of facial data between different sectors provides the state with an opportunity to use or even merge facial biometrics collected by the private sector with its own databases, establishing a complex surveillance system and network. In this sense, the collaboration between law enforcement and private entities also enables police to extend the scope of their surveillance to online platforms and activities, building a more encompassing and intrusive data double of the affected individuals (Van der Ploeg, 2003). Ultimately, with the lack of regulations and transparency in both the state and private sector, we have no idea how our data is collected and combined. As a result, the combined data may

be used as a reference for biased decision-making (William, 2005).

Furthermore, such collaboration gives the government access to millions of people's facial biometrics, and BBW expresses a level of disbelief in government's ability to prevent the collected data from undergoing security breaches due to its history of insufficient and irresponsible encryption measures. In a similar light, researchers (Introna and Gibbons, 2009) have observed a decline in public confidence regarding the government's ability of managing and securing the collected data.

It is worth mentioning that regarding issues of identity theft, both BBW and EFF suggest that when faced with data breaches, we can change our passwords. However, our facial biometrics are unique to us, and thus can not be changed. In this regard, the uniqueness of our facial biometrics has made us more vulnerable to the risks posed by data breaches.

FRT: the Algorithm and the Biases

Different sectors' utilization of FRT has led to not only an infringement of our privacy, rights, and civil liberties, but also a threat to democracy (Chochia & Nässi, 2021; Willam & Lynch, 2018). Indeed, all four groups' narratives have identified the inherent biases within law enforcement, and that due to a lack of regulations and oversights, FRT is treated by police as a tool to justify their discriminatory conduct. At the same time, the private sector attacks existing privacy protection bills, asking for a more "industry-friendly" framework, and continues to collect and process our facial biometrics illegitimately. With all that being revealed, the fault seems to be with the users of the technology. However, the groups contend that while it is true that FRT is used in a way that exacerbate the discriminations in society, the technology itself is also problematic.

For instance, the groups' narratives suggest that the unique qualities of FRT have facilitated a particular form of surveillance. In other words, FRT has not only made constant monitoring possible, but also enables covert identification and tracking (Singh et al., 2019). While FRT engineers perceive such characteristics of FRT as non-intrusive since most of the time, it does not require direct contact with the affected individuals (Singh et al., 2019; Leong et al., 2020), BBW and EFF argues that when confronted with such technology, it will be challenging for us to safeguard our privacy and rights if we are not even aware of being watched and identified.

Furthermore, there are biases inherent in the algorithm (Williams, 2020). The groups point out that the algorithm has a higher misidentification rate for women and people of color (William & Lynch, 2018; El Khiyari & Wechsler, 2016). When such flawed algorithm is combined with an already biased system, it exacerbates discrimination against the marginalized populations. More specifically, as STOP highlights, when a technology is designed, there will always be a series of “decisions and assumptions” (2019, b) embedded within the algorithm. These factors not only introduce biases into the algorithm, but at the same time influence its accuracy, ultimately leading to the intensification of pre-existing discrimination in society. It is worth mentioning that many researchers have also pointed out these problems with FRT. They suggest that it is crucial to not only address the flaws with the algorithm, but also be aware of the societal context in which FRT is deployed (Fussey, Davies & Innes, 2021; Ho et al., 2020).

One example of such embedded decisions and assumptions can be seen in the training of FRT. The groups’ narratives have all pointed out the lack of diversity in the photos used to train the algorithm, similar to that mentioned by Ho, Black, Agrawala and Li (2021). This choice not only increases the rate of misidentification for women and people of color, but also reflects the inherent biases prevalent in society²³. To put it differently, FRT is developed under the influence of existing human biases, and at the same time, the utilization of this biased technology within an already biased society further amplifies the oppression and discrimination experienced by marginalized populations. Therefore, as William (2020) argues, such dilemma cannot be solved by simply adding more diversity to the photo galleries used to train the algorithm. Because given the mutual influence between technology and society, it is crucial to examine not only the technology, but the society and culture in which FRT is designed and used; otherwise, the problems associated to the algorithm can never be properly addressed.

Fussey, Davies, and Innes (2022) also suggest that instead of being a tool to be used by police, the utilization of FRT constitutes a “socio-technical assemblage” (p. 327). Such an assemblage is composed of various articulations, including not just the material aspects of the technology, but also the practices, values, and ideals within law enforcement and society. In

²³ According to STOP, most FRT algorithms are trained with photos of white men. Such choice also reflects the problematic aspect of people’s assumptions about the “default” representation/indication of people.

this sense, the use of FRT has shaped police practices and is at the same time shaped by “forms of police suspicion and discretion” (p. 327).

From the previous discussion, we can see a mutual existence and influence between the politics made possible by FRT and the politics embedded within FRT. As mentioned in Chapter 2, Winner (1986) emphasizes the importance of looking beyond how a technology is utilized and focusing on its design when exploring the issues associated with technology.

In terms of the politics made possible by FRT, the groups’ narratives reveal that the characteristics of FRT have enabled covert and constant identification of individuals. On the one hand, police are now using this technology to identify and monitor suspects to enhance public safety (Purshouse & Campbell, 2022), and the incorporation of FRT into border control and management has increased the work efficiency for border control officers (Carlos-Roca, Torres & Tena, 2018). On the other hand, while the idea of “safety enhancement” may be the original design purpose of FRT, such design, at the same time, has facilitated a massive and invasive surveillance of the general public, causing privacy concerns during the process of its utilization.

Moving beyond the effects caused by the design of FRT, the groups’ narratives and many scholars (Fussey, Davies & Innes, 2021; Ho et al., 2020; Williams, 2020) all point out that the values, ideals, and cultures within a society will influence its design (politics embedded within technology). In other words, there are inherent biases within the technology itself, as it is not designed and deployed in a value-free society. Therefore, as the groups’ narratives suggest, these inherent biases within FRT have led to not only an infringement of individual privacy, but also an exacerbation of oppression and discrimination experienced by certain populations, posing a threat to civil rights and democracy.

In conclusion, when we combine these two perspectives together, we see not only how the use of FRT causes various effects in society (what is enabled by the technology), whether it is increased workflow for border control officers, or the facilitation of public mass surveillance, but also how the design of FRT is influenced by societal values and ideals, and again reinforcing those values through its utilization.

The Evolution of Technology

Apart from FRT, an interesting phenomenon that emerges in the groups' narratives is the evolution of technology. According to STOP and EFF, in order to stay ahead of their rivals in the competition that takes place in the FRT market, companies are expected to improve upon their FRT products. This is when Wolfcom introduced the concept of "live facial recognition", which combines FRT with police body cameras, enabling constant and automated facial recognition.

This phenomenon is interesting yet concerning. It demonstrates how a new technology is developed through the combination of existing technologies. This combination not only brings new possibilities to police practices, but also introduces new risks and concerns for individuals.

Similarly, the combination of CCTV with FRT²⁴, as proposed by Clearview AI (FFTF, 2020b), marks another evolution of technology, as such innovation facilitates new forms of surveillance.

To be more specific, when we combine CCTV network with FRT, we enable a surveillance network with the capacity of constant seeing and identifying. As we combine bodycams with FRT, the technology further evolves. Now police not only have a portable panopticon with them, but this panopticon also has the ability to automatically assign an identity to every individual that comes before it. In this sense, FRT continues to evolve into increasingly invasive and accessible forms, facilitating various forms of surveillance and identification of individuals within society.

Though these are the only two combinations discussed by the advocacy groups, such combinations are quite common in our society. Some of these combinations can appear to be invasive and concerning, like the aforementioned ones, yet they may also conceal their invasiveness under the disguise of safety and convenience. For instance, now you can unlock your smartphone by simply scanning your face, and there are vending machines that have built-in FRT, meaning that you do not even need to bring your wallet with you when you want to grab something to drink (Chambino, Silvia, and Bernardino, 2020; Zhao, 2022). These

²⁴ BBW (2018) has also warned about the possibility and risks of how the incorporation of FRT into the CCTV network may pose threats to people's privacy and rights.

evolutions of technology seem to provide us with so much convenience, yet behind their seemingly innocent nature lie risks and threats to our privacy and rights (Raposo, 2023). Therefore, we must pay attention to the constantly evolving technologies, and consider the impacts they may have on our lives.

Differences Among the Four Advocacy Groups' Narrative

After discussing the shared similarities in the groups' narratives, we will now explore some differences and variations in their narratives in the following pages. We will begin by emphasizing FFTF's focus on the importance of addressing digital monopolization. Next, we will compare the means and strategies that the groups deployed or suggested to achieve their goals, as well as examine their relationships with their allies.

The "Big Tech" and the Digital Space

The groups' narratives have all addressed the problems with illegitimate collection and processing of our personal data by the private sector, emphasizing the need for regulations and privacy protection bills to safeguard people's privacy and rights. However, FFTF also highlights the Big Tech's monopoly of the digital space. The group explains that such monopoly has limited opportunities for smaller and start-up companies to compete and offer platforms and choices other than the major ones owned by the Big Techs.

For example, FFTF points out that Meta has monopolized the digital space by offering various platforms and services for individuals to utilize and engage with. However, as we interact with these platforms, our data are collected, analyzed, and shared across multiple Meta-owned platforms unknowingly. During this process, we have lost the ownership and knowledge over our own data, raising significant privacy and security concerns (Andrejevic, 2014). Moreover, Best (2010) and Brusseau (2020) have warned that the data collected from individuals and shared among different actors and across various platforms will be recombined out of our control. The recombined data will then be used as a basis to make decisions that may influence our life chances. Chochia and Nassi (2021) further argue that once database containing our facial biometrics are breached, the data associated with these faces may also be hacked.

According to FFTF's narratives, in order to provide people with more alternatives in the

digital space, it is necessary to enact legislations that provide opportunities for smaller companies to compete, eventually bringing equalities to the digital space. By doing so, consumers are empowered by being able to choose platforms that suit their preferences and prioritize user privacy and data protection. In addition, with more privacy protection bills, it may also pressure the Big Tech companies to give priority to their users' privacy and data protection. Notably, FFTF's narratives reveal that this monopoly has created a power dynamic. Due to the lack of competition in the digital space caused by the monopoly, the Big Tech companies can exert a great influence and limitations on the information we will be able to access, as well as the services available to us (Best, 2010). What is more, this monopoly may also lead to a limitation of individuals' freedoms, particularly the freedom of speech and expression online. When this situation is combined with the lack of regulations and safeguards regarding private sector's collection and processing of personal data, we find ourselves losing control over our data. In a similar light, Hull (2021) argues that such imbalance between data companies and individuals have led to the "death of the data subject" (p. 1), in which individuals are disempowered due to their lack of legal standing, resources and influences compare to the data companies. Hull suggests that in order to ensure people's privacy and rights, it is crucial to address this power asymmetry.

Furthermore, this narrative on monopoly also reveals a unique aspect of FFTF's sociotechnical imaginaries (SI). As mentioned earlier, FFTF's goal is to fight for a future where technology empowers people and serve as "a force for good" (FFTF, 2023). This indicates that the group recognizes the potential benefits and opportunities that technology may bring to the picture, such as increased accessibility of knowledge and information. Therefore, by addressing the Big Tech companies' monopoly of the digital space, it may not only promote competition, innovation, and provide more choices for the general public, but also balance the power dynamic between the Big Techs and the consumers.

Ultimately, such effort can lead us to regain control over our data and ensure the protection of our privacy and rights. In this sense, FFTF is fighting for a future where instead of being used as a tool to discriminate and exacerbate inequality, technology is utilized to serve the interests of the general public and promote democracy. In other words, technology is imagined

by FFTF as having the potential to empower people and promote positive social change. However, in order to achieve such vision, this narrative has revealed that we must first work towards creating a society where there is an equal distribution of opportunities, so that power and resources will not be monopolized by the few in power.

Addressing the Dilemma

In order to tackle the problems brought by different sectors' use of FRT, all groups' narratives suggest that the government must now act to ban law enforcement and governmental use of FRT due to the negative effects it has posed to the general public. As for the private sector, their narratives reveal that strict privacy protection bills and regulations are necessary to safeguard the public from corporate actors' illegitimate collection and processing of data. However, it is worth mentioning that there are also some distinctions and variations in the groups' suggestions.

To begin, although all groups' narratives argue that governmental use of FRT must be banned, they have slightly different strategies to achieve this goal, and their attitudes towards private sector's use of FRT also varies. We will start with examining the approaches of their advocacies before moving on to their attitudes towards the private sector.

In order to safeguard people from police use of this invasive technology, STOP suggests that there must be an independent civilian board to oversee law enforcement use of FRT, and the group has launched various campaigns and participated in congressional conversations to facilitate the establishment of such oversight.

As mentioned earlier, the groups' narratives have all emphasized the biases, lack of transparency, and accountability within law enforcement. Therefore, having an independent civilian board will enable an impartial evaluation of police utilization of surveillance technology.

Additionally, involving citizens in the oversight process allows them to engage in protecting their own interests and rights. This increased involvement can foster a greater confidence in the oversight process.

The building of a civilian board also helps to shift some power away from the law enforcement and empower citizens. According to Bragias, Hine and Fleet (2021), a healthy public-police relationship is crucial for democratic society. To be more specific, the researchers

suggest that it is essential for the general public to have confidence in police utilization of new technology, such as FRT. Therefore, by participating in the oversight process, it not only adds transparency to how surveillance technology is deployed and used by police, but also increases people's confidence in police practices.

Many researchers (Purshouse & Campbell, 2022; Bragias, Hine & Fleet, 2021; Bradford, Yesberg, Jackson & Dawson, 2020; Gray, 2003) reveal that individuals are usually unaware of the influence of FRT, they have no access to the information collected on them, and that there is very little known about the general public's attitudes towards FRT. Therefore, to ensure public safety and rights, we must raise people's awareness of the utilization and potential influence of FRT, and that the implementation of any surveillance technology and system needs to be publicly scrutinized to ensure such technology is used ethically and properly.

For their part, EFF suggests that the public at large must stay vigilant and informed regarding state's development and adoption of FRT. Because it is only by staying engaged and aware that we can properly assess the technology and situation, and collectively oversee the development and utilization of FRT. The group has also filed several Open Record requests, demanding that law enforcement agencies disclose the details of their use of FRT. EFF believes that by bringing transparency to police conduct, it enables us to challenge their use of such technology.

Comparing the strategies proposed by STOP and EFF, we can see that while STOP emphasizes the importance of addressing the problems associated with police utilization of surveillance technology with an independent civilian board, EFF highlights the cruciality of sensitizing the public with knowledge regarding surveillance technology.

These differences in strategies may be due to the fact that STOP focuses primarily on surveillance issues within New York City. In other words, the group places a greater emphasis on local concerns. In contrast to STOP, EFF is mostly concerned with surveillance problems on a broader national level. Therefore, while STOP aims to directly address the immediate concerns with surveillance technology (such as police illegitimate use of FRT) through the implementation of a civilian board, EFF takes a long-term approach by focusing on educating the public and raising awareness about the utilization and implications of surveillance

technology. By doing so, EFF aims to equip the general public with the knowledge necessary for people to actively participate in challenging and shaping the mainstream discourse surrounding surveillance technology. At the same time, this strategy aims to mobilize the public to advocate for necessary changes in policies and regulations, so that they will be able to safeguard their own privacy and rights.

Similarly, BBW argues that the government has constantly ignored their warnings regarding the utilization of FRT, and the risks associated with state sector's utilization of FRT are often overlooked. BBW's concerns are in line with Purshouse and Campbell (2022) who point out that despite the controversy surrounding police use of FRT in the UK, the government and domestic courts still perceive the technology as being properly regulated, thus disregarding the voice of the general public. Once again, such narrative and emphasis on authorities' unwillingness to properly regulate the use of FRT highlight a lack of oversight over how decisions are made by those in power, thus pointing to a power imbalance between the authority figures and the general public. According to BBW's narratives, we must now bring police illegitimate use of FRT into democratic inquiries, shedding light on not only the algorithm, but also the manner in which police utilize it.

It is worth mentioning that the government tends to justify the incorporation of FRT into their online services under the guise of safety. For instance, some argue that such incorporation will better prevent issues with identity theft. However, as mentioned earlier, FFTF and EFF's narratives suggest that it is equally dangerous to subject people's personal data and biometrics to unregulated third parties.

Additionally, STOP's narratives state that instead of incorporating FRT into government services to combat identity fraud and subject people to automated system, the implementation of a "secure digital ID system" (STOP, 2021 e) may be a better option. Though the group acknowledges that this ID system may not be the ideal choice, it argues that there is no perfect solution. According to STOP, any system capable of proving individuals' identity consistently should be considered as a "mass surveillance tool". However, the group contends that the use of such a universal ID system can, at the very least, save us from the biased algorithm. In this sense, STOP has proposed a solution to address the dilemma of identity fraud, aiming to avoid

the potential exacerbation of discrimination caused by the biased FRT algorithm. However, the group's narratives also suggest that in order to implement this solution (a universal ID system), people need to be willing to make compromises and accept to live with certain risks in society (such as the adoption of certain mass surveillance tool like the aforementioned ID system). In other words, STOP perceives a trade-off between addressing the issues regarding identity theft, and accepting the risks brought by increased surveillance in society.

Now focusing our attention on the private sector, all four groups advocate for strict regulations and privacy protection laws to govern the private sector's utilization of FRT, and demand that the government allocate more resources to ensure proper enforcement of such regulations and laws. However, BBW and FFTF's narratives suggest that regulations alone are insufficient if FRT is used by private sector for public surveillance.

BBW emphasizes that instead of defining a standard to be used as a globally accepted norm for new technologies, human rights are the only standards we need. Similar to other groups' positions described in their narratives, BBW's narratives also highlight the authoritarian and discriminatory implications associated with the use of FRT for public surveillance. Therefore, as depicted in their narratives, public surveillance is "first and foremost a human rights issue" (BBW, 2019 a). The implementation of more regulations regarding public surveillance will only provide the private sector with a defined space to spy on us.

For their part, apart from advocating for a ban on state sector's utilization of FRT, FFTF also started a campaign calling for a ban on the use of FRT in universities, music concerts, and stores etc. According to FFTF's narratives, using FRT in these publicly accessible spaces may not only jeopardize individuals' privacy, but also pose threats to people's civil liberties.

These narratives and examples have indicated that these two groups believe in the necessity of banning FRT to address the risks and harms associated with its utilization by the private sector in publicly accessible areas.

From the previous discussions, we can observe a separation between public and private surveillance from the group's narratives. This distinction revolves around whether affected individuals are able to opt-out of the surveillance. To be more specific, the state sector's utilization of FRT is recognized by the groups as a form of public surveillance, in which

individuals are subjected to scrutiny without their consent or an option to opt-out. When it comes to private surveillance, the groups' narratives reveal that individuals do have the choice to choose whether to be surveilled (by trading their data in exchange for services from the service providers) or not. In order to ensure people's data is not exploited by the data collectors, we need more robust regulations to govern private surveillance.

In conclusion, as depicted by all four groups' narratives, there is an ongoing power struggle between the general public and the state as well as the private sectors. With the use of FRT, we are being constantly monitored, identified, and tracked unknowingly. As we interact with different technologies and utilize various services provided by corporate and state actors, our data and facial biometrics are collected, analyzed, and stored without our consent. This dilemma has created a power imbalance between the surveiller and the surveilled. Eventually, this power dynamic may lead to the exacerbation of the repression and discrimination experienced by already marginalized populations (Lyon, 2006).

As Best (2010) and Venkatesh (2021) argue, the power dynamic described above is often the result of the general public's lack of attention and knowledge regarding surveillance and surveillance technology. Therefore, the groups' narratives have revealed their shared objective: to educate the general public about surveillance, thus raising awareness about the dilemmas they face. Once the public has developed a collective consciousness regarding their own situation, the groups advocate for mobilizing the public and forming alliances with other actors (i.e. advocacy groups, researchers, law makers, and public institutions, etc.). Together, they aim to safeguard people's privacy and civil liberties.

More specifically, the groups' narrative suggest that this process empowers the public by equipping them with awareness and knowledge about their own situations. Such empowerment would enable them to join the fight against illegitimate utilization of FRT and the unlawful collection and processing of personal data. As a result, a portion of the power would be shifted to the surveilled. In addition, the four groups' narratives have also revealed their belief that it is possible to separate private and public surveillance and treat them accordingly. By doing so, we will be able to enjoy the benefits brought by technological advancements without compromising our privacy and rights.

The Reliable Allies

Along the road of addressing the problems associated with FRT, there are multiple helpers/allies that appear in the groups' narratives. For instance, the groups have all collaborated with other advocacy groups and organizations to launch campaigns advocating for the protection of people's privacy and rights. Apart from the grassroots organizations, they have also received support from actors in various sectors, including researchers, law firms, and journalists.

It is worth mentioning that while BBW, EFF, STOP, and FFTF's narratives all suggest that lawmakers/congress now need to pass more privacy protection bills and ban governmental use of FRT, FFTF's narratives depict them as somewhat "unhelpful" allies. The group's narratives suggest that although lawmakers often acknowledge the problems associated with the technology, and express concerns accordingly, they are not willing to act upon those concerns. Similar to FFTF's narratives, Purshouse and Campbell (2022) contend that even though police use of FRT have raised public protest, and many advocacy groups and organizations have joined force and launched several campaigns to call for a ban on police utilization of FRT, lawmakers have refused to listen to these calls for actions.

Additionally, FFTF's narratives reveal that some lawmakers even choose to align themselves with corporate actors, justifying the governmental use of FRT under the guise of safety and convenience. FFTF states that these lawmakers must now "get off their butts, do their jobs" (FFTF, 2020 a), by banning law enforcement utilization of FRT immediately.

Another important point to highlight is BBW's relationship with the Information Commissioner's Office (ICO). According to its narratives, the group constantly urges the ICO to investigate various incidents associated with the adoption of FRT, and the group states that whether it is police illegitimate utilization of FRT, or private sector's unlawful collection and processing of personal data, ICO must take the responsibility to safeguard UK citizens' privacy, civil liberties, and democracy (Purshouse and Campbell, 2022). This indicates that the ICO plays a significant role in safeguarding the general public's privacy and data security, and that there is a mutual influence/collaboration between the ICO and the BBW.

By urging the ICO to start investigating in unlawful use of FRT, and enforcing data

protection laws, BBW is at the same time advocating for the ICO to act according to their shared goal – safeguarding people’s privacy and protecting democracy from being eroded by the misuse/abuse of surveillance technology.

Similarly, STOP’s narratives suggest that as more and more civil society groups unite in their efforts to combat the use of FRT, greater support from state actors may facilitate the progress. In other words, STOP calls for state actors to join forces with local activists to address concerns regarding FRT and push for bans and restrictions on its usage.

From these narratives, the government has a tendency to downplay the dangers and risks associated with the use of FRT. FFTF’s narratives have also highlighted that some lawmakers have even chosen to align with corporate actors’ perspectives and justify state actors’ utilization of FRT. In this sense, the responsibility to bring awareness to the state actors who refuse to perceive the reality seems to lie on the advocacy groups’ shoulder.

Conclusion

Through the analysis of the groups’ constructed narratives, we have discovered both similarities and differences shared in these narratives.

On the one hand, the groups have all identified a lack of regulations, transparency and oversight in the utilization of FRT by both the state and private sectors. Their narratives reveal a belief in the possibility of separating the public and private life through the enforcement of different strategies to address the problems associated with FRT in these sectors separately. In addition, the groups’ narratives highlight the dilemmas associated with the collaboration between the state and private/public sector on FRT, the technology itself, as well as how it may evolve through a combination with existing devices, facilitating new forms of surveillance in the process.

On the other hand, the groups’ narratives differ in the place they attribute to Big Tech companies (FFTF: addressing Big Tech’s digital monopoly), the strategies they suggest to tackle the dilemmas, and their relationships with their allies.

In the following and concluding pages, based on the analysis of previous narratives, we will establish four overarching narratives for each advocacy group. We will explore the dystopian background portrayed in these narratives, as well as the groups’ envisioned utopian

futures. After that, we will examine the social life and social order present in these overarching narratives to get a clear image of the groups' SI regarding FRT.

Concluding Remarks

This research explored the sociotechnical imaginaries (SI) of four rights advocacy organizations that advocate against the use of FRT. The study discovered that the underlying values and beliefs driving these groups' advocacy align closely with modern liberal ideals. Their shared SI highlights the importance of separating public and private life, the necessity for moderate government intervention to regulate different sectors' utilization of FRT, promoting public education to raise people's awareness about issues affecting their rights and civil liberties, and encouraging healthy commercial competition in the digital realm for more alternatives. In this context, instead of advocating for an overhaul of the current system, the groups act to reinforce the existing power structure.

To serve as a reminder, Jasanoff and Kim (2015) define sociotechnical imaginaries as “collectively held, institutionally stabilize, and publicly performed visions of desirable futures, animated by shared understandings of forms of social life and social order attainable through, and supportive of, advances in science and technology” (2015).

Based on this definition, I have documented the two dimensions of SI: social life and social order. Each dimension is composed of various components. Social life encompasses a set of ideas, such as the futures predicted by advocacy groups, or the goals and values the groups fight for. Social order, in contrast, is composed of various actors and mechanisms in society (state, private, and general public), and relate to their roles, weaknesses, strengths, and involvement in the decision-making processes regarding the technology²⁵. By documenting the actors and mechanisms, we can not only explore how various actors (both human and non-human) interact and contribute to shape the imaginaries, but also the power relation between various actors. Ultimately, once we identify and piece all the components together, we can unravel the SI behind the groups' narratives.

By analyzing the similarities and differences presented in the narratives of FFTF, BBW, EFF and STOP, we have uncovered various components of the SI envisioned by these advocacy groups. In the following pages, I will first briefly describe the overarching narratives of the four groups as well as the dystopian background used to promote the utopian future present in

²⁵ Please refer to my SI operationalization table for details.

those narratives. Afterward, conceptually, I will explore the components of social life identified by the advocacy groups, before delving into the dimension of social order present in their narratives.

Dystopias and Utopias Present in the Narratives

Based on the selected and limited material that I have subjected to the analysis, the overarching narrative on FRT envisioned by each advocacy group, including the dystopian background and utopian future they propose can be synthesized in the following way.

BBW: Walking IDs in an Authoritative State.

BBW argues that when using FRT, people are put under covert monitoring and identification. Such constant surveillance has transformed the general public into “walking ID card” (BBW, 2018, 2019 a, 2019 b, 2022 a), ready to be surveilled and identified. During this process, it ends anonymity in society, people have lost the control over their own data and their right to privacy. In this sense, BBW has described a future, where the use of FRT ends up transforming society into an authoritarian police state, devoid of privacy, rights, and democracy, similar to the dystopian state portrayed in George Orwell’s novel “1984”.

Alternatively, in BBW’s imagined future, people are no longer “walking ID card”, and the ability to remain “anonymous” has finally been returned to them. Now the UK government has not only recognized the importance of treating facial biometrics on par with other forms of biometrics (i.e. fingerprints), but also acknowledged the potential harms that may arise from their collaboration with other sectors (private and public). As a result, the government has decided to enact strong regulations governing different sectors utilization of FRT and the sharing and processing of data, while allocating enough resources and oversight to ensure the enactment of these regulations. Furthermore, in order to better protect people’s personal data and facial biometrics from data breaches, the government has strengthened their data encryption level and measures. Now there are not only transparency within law enforcement and government practices, but also an increased accountability. BBW, alongside the ICO, remains committed to safeguard the privacy and rights of the UK citizens in this utopian future.

EFF: Hiding from a Perpetual Facial Dragnet.

EFF contends that the use of FRT has created a “perpetual facial dragnet” (EFF, 2018 b),

meaning that it enables a massive yet covert form of surveillance. Under such situation, we are heading towards a future where we must constantly worry about being falsely identified as someone else due to FRT's flawed algorithm. We must be concerned about potential data breaches and the unauthorized use of our facial biometrics by identity thieves. We must also be wary of our every move being monitored and tracked whenever we appear in front of a camera. In this hyper-surveillant society, we have lost our right to stay anonymous. We must constantly expose our faces to others, all the while worrying about how our facial biometrics are captured and subjected to FRT. During this process, how will our privacy and rights be affected?

Similar to BBW, in the utopian future society imagined by EFF, we can once again remain anonymous. There is no need to worry about our facial biometrics being captured and searched unknowingly without our consent. Furthermore, the sharing of data and facial biometrics between different sectors is strictly regulated or even postponed, preventing them from being misused by different agencies or the creation of a "perpetual facial dragnet" (Ibid).

FFTF: Constant Surveillance of Disenfranchised Masses.

Moving on to FFTF, FRT is an "Orwellian technology", capable of conducting constant monitoring and identification of a large number of individuals. There are not enough regulations to govern different sectors' utilization of this technology, and the collaboration between the private and state sector has exacerbated the situation. As the group argues, under such surveillance, we have lost ownership of our data, and our facial biometrics are "weaponized" against us (FFTF, 2021 b). Police use this technology to target and discriminate against marginalized populations, while Big Tech companies seek every opportunity to advertise their technologies at the expense of our privacy and rights. With all the concerns raised by FFTF, it becomes clear that we are heading towards a future where we are subjected to constant and potentially discriminatory surveillance. Our every move is monitored and tracked without our consent. Additionally, the digital space is dominated by major Big Tech companies, leaving us with no choice but to entrust our data to them, hoping that it remains safe and secure. Ultimately, we have lost the ownership of our own data and biometrics.

In the utopian future imagined by FFTF, the digital space is no longer monopolized by Big Tech companies. Smaller and start-up companies all have an equal chance to participate in

online competitions and have offered various alternatives to the major platforms owned by the Big Tech companies. We are empowered with the ability to choose platforms that prioritize our privacy and data security. In a society like this, we have reclaimed ownership of our data. Hopefully, with increased competition and the enforcement of strong privacy protection laws, the Big Techs may also feel the needs to pay attention to their users' data security and privacy.

STOP: Mass Discrimination Fueled by Search for Profits.

Slightly different from the previous groups, STOP primarily focuses on the marginalized population in society. The group suggests that when the already biased law enforcement is combined with a biased algorithm, the use of FRT will only further the discrimination in our society. Additionally, due to the lack of regulations, transparency, and safeguard in not only police practices, but private sector's collection and processing of personal data and biometrics, our privacy and rights are infringed, and we are turned into "government tracking devices" (STOP, 2011). With an increased reliance on technology provided by tech companies, the decision-making power regarding the utilization of FRT is also placed in their hands. If we allow this situation to continue, STOP argues that we may end up in a society where technology companies suggest and decide how FRT can be used to "assist" in police conduct, while police utilize such technology to justify their biased practices and perpetuate discrimination in society.

Conversely, in the ideal future imagined by STOP, there are independent civilian oversight boards across the country, tasked with evaluating any new technology purchased by law enforcement and overseeing their practices and conduct. State actors have also joined forces with local activists to address concerns regarding FRT, and advocate for bans and regulations on its usage. Furthermore, apart from banning and regulating the flawed technology, the government also begins to address biases within law enforcement. They finally realize that in order to tackle the problems brought by FRT, simply "fixing" the technology is far from enough. The real problem lies within both the algorithm and its users. It is only when we address the problems with the technology and the discrimination within the system, can the US truly become a "beacon of world democracy" (STOP, 2021).

Summary

According to the dystopian character of those narratives, our society has already been

transformed by the rapid advancement of technology. The utilization of FRT by various sectors is gradually turning our society into a surveillance state, where we are subjected to a constant surveillance gaze without even being aware of the dangers and risks associated with FRT. Ultimately, what was once considered private is now made public and exploited by various actors. As FRT and similar surveillance technologies are used continuously without proper regulations and oversight, we are stripped of the ownership over our own data and biometrics, rendering us powerless and vulnerable to pervasive surveillance. Privacy and civil liberties have become remnants of the past.

When moving to the collectively imagined utopia, this is a future where law enforcement use of technology is strictly regulated and subject to oversight. Technologies that are deemed invasive, discriminatory, or potentially harmful to society (such as FRT) are prohibited from being incorporated into police practices and governmental services. In other words, the technologies they choose to incorporate in their services must not enable massive surveillance.

At the same time, the private sector is regulated by strict privacy protection bills. Their utilization of FRT and the collection of individuals' personal data must obtain people's consent first, and that it is prohibited for private actors to use FRT for the purposes of public surveillance.

Eventually, people are no longer subjected to constant monitoring, identification and tracking. There is no need to worry about the possibility of being misidentified as someone else, or having our data used against us. In this envisioned future, we have regained control over our data, and the complex surveillance network has been partially dismantled. With support from various sectors, the advocacy groups will continue to safeguard our privacy, rights, and democracy whenever new challenges arise.

Conceptually, the groups' narratives share enough similarities for us to be capable of subsuming them under one sociotechnical imaginary. Indeed, we can contend that, at the root, the four groups promote a similar vision of the social life and social order.

Social Life

In this section, we will start with a brief discussion on the goals and values pursued by the four advocacy groups and their perceptions of technological influence on society. Then, we will

explore the problems the advocacy groups associate with FRT itself and how this technology is utilized by various actors, highlighting the groups' shared belief in the separation of private and public surveillance. Next, we will investigate the problems of collaboration between different sectors before examining STOP's unique ways of addressing the issues with FRT.

The constructed narratives have revealed that all four groups are determined in their fight for the privacy and rights of the general public, as well as the protection of the democratic values that the US/UK aligns with. These narratives suggest that the world we live in has already been transformed by technological advancement, making the problems associated with FRT concrete realities.

Furthermore, the groups have all acknowledged the inherent biases present not only within law enforcement, but also within the algorithms of FRT. The biased nature of this technology has resulted in disproportionate wrongful arrests and the unjust imprisonment of members from the BIPOC community. Police have also been found to use FRT as they see fit, sometimes justifying their biased conduct. The narratives of these groups display that the fault lies with both the technology and the users, as there exists a mutual influence between the technology and society. Therefore, as suggested by these narratives, it is crucial to ban the state sector's utilization of FRT. In addition, the groups' narratives point out the concerns behind the evolution of technology, noting that sometimes the combination of existing technologies may lead to the development of new ones. However, we must remain vigilant about such evolution, as new technologies may conceal their dangers and harmful effects under the guise of safety and convenience.

It is worth mentioning that there is a distinction in the groups' attitudes towards the state and private sector's utilization of FRT. While the narratives identify a lack of regulations and oversight in both sectors' utilization of this technology, on the one hand, the narratives place particular emphasis on the importance of banning state actors use of FRT. On the other hand, the private sector's utilization of FRT is deemed to require robust regulations and strict oversight²⁶. Such divergence in their attitudes reveal the groups' belief that it is possible to

²⁶ BBW and FFTF's narratives also display the necessity for a partial ban, arguing that the use of FRT by the private sector must be banned if it is used for the purpose of public surveillance.

separate private and public surveillance²⁷.

Moreover, FFTF's narratives depict a monopoly of the digital space by Big Tech companies. The group argues that it is necessary to promote market competition, so that people may be provided with more alternatives to the services offered by the Big Tech. At the same time, individuals may also be empowered by the possibility to choose services that prioritize their interests and rights. Most importantly, promoting competition in the digital space helps ensure that power and resources are not monopolized by the few in power.

Apart from the state and private sector's utilization of FRT, all four groups' narratives have depicted a collaboration between the state and private sector, and they all contend for the termination of the collaboration between these two sectors. It is possible that this objection arises from the perception that such collaboration blurs the line that separates public and private surveillance.

According to our groups, though ID.me's FRT program was initially developed and used for commercial purposes by the private sector, collaborating with the government means that state sector can now utilize ID.me's service for public surveillance. Additionally, BBW suggests that such collaboration facilitates data sharing between the state and private/public²⁸ sector. This provides the state with an opportunity to use or even merge data collected by the private sector with its own databases, establishing a complex surveillance system and network²⁹. Additionally, the collaboration between the state and private sector may lead to the facilitation of a more pro-surveillance legal framework. FFTF and STOP point out that in the US, law enforcement and private sector are now trying to push for a more industry-friendly framework to promote the use of surveillance technology like FRT.

²⁷ While the use of FRT for public surveillance (the form of surveillance that is usually associated with state sector) must be banned, private surveillance is perceived as more acceptable, and only requires proper regulations and oversight.

²⁸ Such as public transport and schools.

²⁹ According to FFTF, police were found to have used ID. me's commercial database to perform facial searches. Furthermore, due to the service and platform monopolization happening in the digital space, FFTF suggests that people's data and facial biometrics are shared across platforms held by Big Techs, such as Meta. Though this data is initially collected for commercial purposes (private surveillance), the collaboration between the private and state sector enables state actors to utilize it for their own purposes. In this sense, we can see an overlap between private and public surveillance.

With the aforementioned examples in mind, we can see that the line between public and private surveillance has become blurred. Regulations alone are no longer sufficient to ensure that such collaboration may be effectively regulated and overseen. As previously discussed, collaborating with third parties has resulted not only in an exacerbation of the discrimination experienced by marginalized populations, but has also posed risks to individuals' privacy, online securities, and civil liberties. As the line continues to blur, the groups argue that it is necessary to stop these collaborations.

Another component that deserves attention is STOP's proposal to address the issue of identity theft. As previously mentioned, STOP's narratives recognize the biases inherent in both the technology and legal system. Therefore, in order to mitigate the risks associated with the biased FRT algorithm, STOP has proposed the idea of implementing a universal ID system to combat identity theft. Though the group does acknowledge that such a system could also be considered as a tool for mass surveillance, its narratives suggest that in order to solve a dilemma (in this case, identity theft), we need to be willing to accept the accompanying risks of increased surveillance in society.

In addition, STOP's narratives depict the necessity of establishing an independent civilian board to evaluate and oversee police utilization of surveillance technology. By involving the general public in the oversight process, according to the advocacy group's narratives, this approach not only enhances transparency in police conduct, but also has the potential to empower the public.

Finally, all the groups have expressed their concerns regarding the futures we may step into. Their narratives suggest that if the widespread utilization of FRT is not regulated and stopped, the US/UK society may eventually be transformed into an authoritarian surveillance state, devoid of democracy.

In conclusion, the social life depicted in the groups' narratives is characterized by a clear distinction between public and private life, a reliance on commercial competition as well as a belief in the education and empowerment of the public. These ingredients are deemed essential for the protection of the public, especially minorities, from abuse and the preservation of democracy for all. Contrary to being subversive, the social life imagined by these advocacy

groups aligns closely with liberal ideals.

Social Order

We will start our discussion on social order by exploring the roles and involvements of the state and private sectors. We will then examine how these four advocacy groups position themselves in their narratives, as well as the approaches they take to fulfill that role.

Regarding the components of social order as depicted in the groups' narratives, it is important to note that all groups identify the state and private sectors as the villains. According to their narratives, state actors often downplay and overlook the dangers and risks associated with FRT and surveillance technology. Some of these actors, such as law enforcement agencies, have refused to disclose details of the FRT programs they use and justified their utilization under the guise of justice and security, ignoring the lack of regulations and oversight. Similarly, BBW's narratives also point out the UK government's tendency of weakening and abandoning encryption measures for the data and biometrics collected from the general public.

In terms of the private sector, the groups point out that the expansion of the FRT market has led to more innovations. Industry actors strive to improve upon their FRT products in the hope of securing more contracts across different sectors. FFTF and EFF's narratives reveal that many corporate actors are willing to sacrifice the consumers' rights and interests in exchange for their own benefits, and STOP's narratives also highlight that with an increased reliance on technologies provided by tech companies, the decision-making power regarding the utilization of FRT is concentrated in their hands.

These narratives underline a power dynamic between the state/private sector, who possesses the power and resources to influence and decide how FRT may be used, and the general public, who are often unaware of the invasive use of FRT.

In order to address this power imbalance, all groups position themselves as the "heroes" of the story. They bear the responsibility to "awaken" different actors in society (the general public and state actors, such as law makers, etc.), making them aware of the issues associated with FRT. The groups' aim is to urge actions to address the dilemmas, and together safeguard people's privacy and rights. In order to fulfill their tasks, the groups have all joined forces with other advocacy groups and actors from various sectors to tackle the issues related to FRT.

Notably, the groups' narratives all emphasize the importance of educating and sensitizing the general public about surveillance and surveillance technology. Because it is only when people are aware of their own situation and the harms they face, can they actively engage in safeguarding their rights and privacy, and collectively oversee the development and utilization of FRT.

In their sociotechnical imaginary, the four groups boil down the social order into three major components: a) a state that needs to be sensitized to the issues posed by FRT to produce better regulations, b) a private sector that pursue innovative enhancements and combinations of technology without much care and need to be reined in, c) a public that requires awakening and defending by the advocacy groups. These groups act as protectors and efficient moderators, mediating between the state, the private sector and the public. Here again, the sociotechnical imaginary promoted by the advocacy groups under study is rather conventional and in line with liberalism. Rather than presenting an alternative, the proposed SI reinforces the current social life and social order prevalent in the western democracies. While advocacy groups might be seen as agents of resistance to the power imbalance that exist, this study shows that resisting a technology does not necessarily mean resisting fundamental structures of power.

Future Research: Avenues and Opportunities

It is important to note that the four advocacy groups under study are all organizations that mainly focus on surveillance issues in the Global North, emphasizing how technological advancements may lead to an erosion of democracy. It may therefore be worthwhile for future research to investigate the narratives of privacy advocacy organizations that focus on a similar issue in the Global South. By shifting our attention on the Global South, it allows us to acquire a more diverse understanding of the impacts of surveillance and technological advancements on society. In other words, such research enables us to see how different cultures, politics, and social settings may lead to varying perspectives on the issues with surveillance and technology.

In addition, the groups under study all focus on how the utilization of FRT may undermine democracy, yet I believe it would be valuable for future research to examine organizations that investigate how FRT is used to further build and support authoritarianism in different countries. In this sense, instead of emphasizing on the potential impact of FRT on

individuals' privacy, rights and democratic values, the attention is shifted to how FRT is utilized and incorporated into various systems and services to reinforce authoritarian government's control on their people.

Furthermore, due to a time limitation, this research only examined advocacy groups' narratives surrounding FRT. However, future research could benefit from an analysis of the narratives of FRT vendors. By analyzing their narratives, researchers will be able to see how providers of this technology perceive and market their FRT programs. Such as how they may emphasize the benefits of their products while downplaying or ignoring the risks and limitations. In this way, it reveals to us how these FRT programs were originally intended to be used, the abilities of these technologies, as well as the targeted customers. By comparing the advocacy groups and FRT vendors' narratives, it may help the researchers to better identify and understand the patterns in the advocacy groups' narratives and the futures they envisioned.

References

- Aboulafia, A., Fritzius, G., Mears, T., & Nix, M. (2021). The Price of Prime—Consumer Privacy in the Age of Amazon. *Mitchell Hamline Law Journal of Public Policy and Practice*, 42(1), 4.
- Amazon Web Services. (2023). *Amazon Rekognition*. <https://aws.amazon.com/rekognition/>
- Andrejevic, M. (2014). Big data, big questions| the big data divide. *International Journal of Communication*, 8, 17.
- Bareis, J., & Katzenbach, C. (2022). Talking AI into being: The narratives and imaginaries of national AI strategies and their performative politics. *Science, Technology, & Human Values*, 47(5), 855-881.
- Bartoletti, I. (2020). *An artificial revolution: On power, politics and AI*. Black Spot Books.
- Best, K. (2010). Living in the control society: Surveillance, users and digital screen technologies. *International Journal of Cultural Studies*, 13(1), 5-24.
- Bradford, B., Yesberg, J. A., Jackson, J., & Dawson, P. (2020). Live facial recognition: Trust and legitimacy as predictors of public support for police use of new technology. *The British Journal of Criminology*, 60(6), 1502-1522.
- Bragias, A., Hine, K., & Fleet, R. (2021). ‘Only in our best interest, right?’ Public perceptions of police use of facial recognition technology. *Police Practice and Research*, 22(6), 1637-1654.
- Brusseau, J. (2020). Deleuze’s Postscript on the Societies of Control: Updated for Big Data and Predictive Analytics. *Theoria*, 67(164), 1-25.
- Burr, V. (2015). *Social constructionism*. Routledge.
- Carlos-Roca, L. R., Torres, I. H., & Tena, C. F. (2018, July). Facial recognition application for border control. In 2018 *International Joint Conference on Neural Networks (IJCNN)* (pp. 1-7). IEEE.
- Chambino, L. L., Silva, J. S., & Bernardino, A. (2020). Multispectral facial recognition: a review. *IEEE Access*, 8, 207871-207883.
- Chateau, Z., Devine-Wright, P., & Wills, J. (2021). Integrating sociotechnical and spatial imaginaries in researching energy futures. *Energy Research & Social Science*, 80, 102207.

- Chhabra, S., Banati, N., Gupta, G., & Gupta, G. (2020, January). Target identity attacks on facial recognition systems. In *IFIP International Conference on Digital Forensics* (pp. 233-252). Springer, Cham.
- Chochia, A., & Nässi, T. (2021). Ethics and emerging technologies–facial recognition. IDP: *revista de Internet, derecho y política= revista d'Internet, dret i política*, (34), 6.
- Chou, K. P., Li, D. L., Prasad, M., Pratama, M., Su, S. Y., Lu, H., ... & Lin, W. C. (2017, November). Robust facial alignment for face recognition. In *International Conference on Neural Information Processing* (pp. 497-504). Springer, Cham.
- Cobern, W. W. (1993). Constructivism. *Journal of Educational and Psychological Consultation*, 4(1), 105-112.
- Deleuze, G. (1992). Postscript on the Societies of Control.” 1990. Cultural Theory: An Anthology, 139-142.
- Dencik, L., Hintz, A., & Cable, J. (2016). Towards data justice? The ambiguity of anti-surveillance resistance in political activism. *Big Data & Society*, 3(2), 2053951716679678.
- Edley, N. (2001). Unravelling social constructionism. *Theory & Psychology*, 11(3), 433-441.
- El Khiyari, H., & Wechsler, H. (2016). Face verification subject to varying (age, ethnicity, and gender) demographics using deep learning. *Journal of Biometrics and Biostatistics*, 7(323), 11.
- Foucault, M. (1990). The history of sexuality: An introduction, volume I. *Trans. Robert Hurley*. New York: *Vintage*, 95.
- Fuchs, C. (2013). Political economy and surveillance theory. *Critical Sociology*, 39(5), 671-687.
- Fussey, P., Davies, B., & Innes, M. (2021). ‘Assisted’ facial recognition and the reinvention of suspicion and discretion in digital policing. *The British Journal of Criminology*, 61(2), 325-344.
- Galbin, A. (2014). An introduction to social constructionism. *Social research reports*, 6(26), 82-92.
- Giddens, A. (1985) *The Nation-State and Violence*. Cambridge: Polity Press.

- Goodall, T., Gibson, S., & Smith, M. C. (2012, July). Parallelizing principal component analysis for robust facial recognition using CUDA. In *2012 Symposium on Application Accelerators in High Performance Computing* (pp. 121-124). IEEE.
- Gragg, S. (1997, January). Facial Recognition at the CIA. In *Terrorism and Counter-Terrorism Methods and Technologies* (Vol. 2933, pp. 43-47). SPIE.
- Gray, M. (2003). Urban surveillance and panopticism: will we recognize the facial recognition society?. *Surveillance & Society*, 1(3), 314-330.
- Graham, S. (1998). Towards the fifth utility? On the extension and normalisation of public CCTV. *Surveillance, Closed Circuit Television and Social Control*. Aldershot: Ashgate, 89-112.
- Greene, J. (2020, June 10). Amazon bans police use of its facial-recognition technology for a year. *The Washington Post*.
<https://www.washingtonpost.com/technology/2020/06/10/amazon-rekognition-police/>
- Harwell, D. (2021, May 18). Amazon Extends Ban on Police Use of its Facial Recognition Technology Indefinitely. *The Washington Post*. Retrieved from
<https://www.washingtonpost.com/technology/2021/05/18/amazon-facial-recognition-ban/>.
- Hirayama, T., Iwai, Y., & Yachida, M. (2003, August). Facial recognition system using efficient methods for facial scale variations. In *SICE 2003 Annual Conference (IEEE Cat. No. 03TH8734)* (Vol. 3, pp. 3236-3241). IEEE.
- Ho, D. E., Black, E., Agrawala, M., & Fei-Fei, L. (2020). Evaluating facial recognition technology: a protocol for performance assessment in new domains. *Denv. L. Rev.*, 98, 753.
- Inoue, M. (2020). Between Surveillance and Sousveillance: Or, Why Campus Police Feel Vulnerable Precisely Because They Gain Power. *Journal of Contemporary Ethnography*, 49(2), 229-256.
- Introna, L. D., & Gibbons, A. (2009). Networks and Resistance: Investigating online advocacy networks as a modality for resisting state surveillance. *Surveillance & Society*, 6(3), 233-258.

- Islam, M. R., Toufiq, R., & Rahman, M. F. (2012, December). Appearance and shape based facial recognition system using PCA and HMM. In *2012 7th International Conference on Electrical and Computer Engineering* (pp. 1-4). IEEE.
- Jasanoff, S., & Kim, S. H. (2009). Containing the atom: Sociotechnical imaginaries and nuclear power in the United States and South Korea. *Minerva*, 47, 119-146.
- Kaur, P., Krishan, K., Sharma, S. K., & Kanchan, T. (2020). Facial-recognition algorithms: A literature review. *Medicine, Science and the Law*, 60(2), 131-139.
- Kazansky, B., & Milan, S. (2021). "Bodies not templates": Contesting dominant algorithmic imaginaries. *new media & society*, 23(2), 363-381.
- Kearon, T. (2013). Surveillance technologies and the crises of confidence in regulatory agencies. *Criminology & Criminal Justice*, 13(4), 415-430.
- Kostka, G., Steinacker, L., & Meckel, M. (2021). Between security and convenience: Facial recognition technology in the eyes of citizens in China, Germany, the United Kingdom, and the United States. *Public Understanding of Science*, 30(6), 671-690.
- Latour, B. (2003). The promises of constructivism.
- Latour, B. (1992). Where are the missing masses? The sociology of a few mundane artifacts. *Shaping technology/building society: Studies in sociotechnical change*, 1, 225-258.
- Latour, B. (1990). Technology is society made durable. *The sociological review*, 38(1_suppl), 103-131.
- Leder Mackley, K., & Jewitt, C. (2022). Sociotechnical imaginaries of remote personal touch before and during COVID-19: An analysis of UK newspapers. *New Media & Society*, 14614448221113922.
- Leese, M. (2014). The new profiling: Algorithms, black boxes, and the failure of anti-discriminatory safeguards in the European Union. *Security Dialogue*, 45(5), 494-511.
- Leong, S. M., Phan, R. C. W., Baskaran, V. M., & Ooi, C. P. (2020). Privacy-preserving facial recognition based on temporal features. *Applied Soft Computing*, 96, 106662.
- Leong, B. (2019). Facial recognition and the future of privacy: I always feel like... somebody's watching me. *Bulletin of the atomic scientists*, 75(3), 109-115.

- Levidow, L., & Raman, S. (2020). Sociotechnical imaginaries of low-carbon waste-energy futures: UK techno-market fixes displacing public accountability. *Social studies of science*, 50(4), 609-641.
- Levine, Y. (2018). All EFF'd Up: Silicon Valley's astroturf privacy shakedown. *The Baffler*, (40), 44-64.
- Li, Y., Gong, S., & Liddell, H. (2003). Constructing facial identity surfaces for recognition. *International Journal of Computer Vision*, 53(1), 71-92.
- Lyon, D. (2002). Surveillance Studies: Understanding visibility, mobility and the phenetic fix. *Surveillance & society*, 1(1), 1-7.
- Lyon, D. (2008, September 28). Surveillance Society [Speech transcript]. Retrieved from http://www.festivaldeldiritto.it/2008/pdf/interventi/david_lyon.pdf
- Lyon, D. (2010). Surveillance, power and everyday life. In *Emerging digital spaces in contemporary society* (pp. 107-120). Palgrave Macmillan, London.
- Lyon, D. (2017). Digital citizenship and surveillance| Surveillance culture: engagement, exposure, and ethics in digital modernity. *International Journal of Communication*, 11, 19.
- Mager, A., & Katzenbach, C. (2021). Future imaginaries in the making and governing of digital technology: Multiple, contested, commodified. *New Media & Society*, 23(2), 223-236.
- Mager, A. (2017). Search engine imaginary: Visions and values in the co-production of search technology and Europe. *Social Studies of Science*, 47(2), 240-262.
- Marx, G. T. (1985). The Surveillance Society-The Threat of 1984-style Techniques. *Futurist*, 19(3), 21-26.
- McLindin, B. A., Butavicius, M. A., & Meaney, K. (2003, July). Gallery image effects on facial recognition systems. In *Proceedings EC-VIP-MC 2003. 4th EURASIP Conference focused on Video/Image Processing and Multimedia Communications (IEEE Cat. No. 03EX667)* (Vol. 2, pp. 455-460). IEEE.
- McLindin, B. A. (2003, July). Baseline illumination variables for improved facial recognition system performance. In *Proceedings EC-VIP-MC 2003. 4th EURASIP Conference focused on Video/Image Processing and Multimedia Communications (IEEE Cat. No.*

- 03EX667) (Vol. 1, pp. 417-422). IEEE.
- Mutter, A., & Rohrer, H. (2022). Competing transport futures: tensions between imaginaries of electrification and biogas fuel in Sweden. *Science, Technology, & Human Values*, 47(1), 85-111.
- Ng, C. B., Tay, Y. H., & Goi, B. M. (2015). A review of facial gender recognition. *Pattern Analysis and Applications*, 18(4), 739-755.
- Norris, C., & Armstrong, G. (2020). *The maximum surveillance society: The rise of CCTV*. Routledge.
- Norris, C. (2005). From personal to digital: CCTV, the panopticon, and the technological mediation of suspicion and social control. In *Surveillance as social sorting* (pp. 263-295). Routledge.
- Poller, M. (2020). Post-political uncertainties: Governing nuclear controversies in post-Fukushima Japan. *Social Studies of Science*, 50(4), 567-588.
- Propp, V. (1968). *Morphology of the Folktale*. University of Texas Press.
- Purshouse, J., & Campbell, L. (2022). Automated facial recognition and policing: a Bridge too far?. *Legal Studies*, 42(2), 209-227.
- Rahaman, M. S. Western Modernity: The Origin, Development and the Limitation.
- Raposo, V. L. (2022). (Do not) remember my face: uses of facial recognition technology in light of the general data protection regulation. *Information & Communications Technology Law*, 1-19.
- Raposo, V. L. (2022). The Use of Facial Recognition Technology by Law Enforcement in Europe: a Non-Orwellian Draft Proposal. *European Journal on Criminal Policy and Research*, 1-19.
- Rieder, G. (2018). Tracing big data imaginaries through public policy: The case of the European Commission. In *The politics of big data* (pp. 89-109). Routledge.
- Schiølin, K. (2020). Revolutionary dreams: Future essentialism and the sociotechnical imaginary of the fourth industrial revolution in Denmark. *Social Studies of Science*, 50(4), 542-566.
- Schmid, S. D. (2021). From “Inherently Safe” to “Proliferation Resistant”: New Perspectives

- on Reactor Designs. *Nuclear Technology*, 207(9), 1312-1328.
- Singh, S., Ramya, R., Sushma, V., Roshini, S. R., & Pavithra, R. (2019, December). Facial recognition using machine learning algorithms on raspberry Pi. In *2019 4th International Conference on Electrical, Electronics, Communication, Computer Technologies and Optimization Techniques (ICEECCOT)* (pp. 197-202). IEEE.
- Smallman, M. (2020). 'Nothing to do with the science': How an elite sociotechnical imaginary cements policy resistance to public perspectives on science and technology through the machinery of government. *Social Studies of Science*, 50(4), 589-608.
- Smith, G. J. (2016). Surveillance, data and embodiment: On the work of being watched. *Body & Society*, 22(2), 108-139.
- Sovacool, B. K., Bergman, N., Hopkins, D., Jenkins, K. E., Hielscher, S., Goldthau, A., & Brossmann, B. (2020). Imagining sustainable energy and mobility transitions: Valence, temporality, and radicalism in 38 visions of a low-carbon future. *Social studies of science*, 50(4), 642-679.
- Stark, L. (2019). Facial recognition is the plutonium of AI. XRDS: Crossroads, *The ACM Magazine for Students*, 25(3), 50-55.
- Stone, D. A. (1989). Causal stories and the formation of policy agendas. *Political science quarterly*, 104(2), 281-300.
- Sturken, M., Thomas, D., & Ball-Rokeach, S. (Eds.). (2004). *Technological visions: The hopes and fears that shape new technologies*. Temple University Press.
- Su, Z., Cheshmehzangi, A., McDonnell, D., Bentley, B. L., Da Veiga, C. P., & Xiang, Y. T. (2022). Facial recognition law in China. *Journal of Medical Ethics*.
- Van der Ploeg, I. (2003). Biometrics and Privacy A note on the politics of theorizing technology. *Information, Communication & Society*, 6(1), 85-104.
- Van Oort, M. (2019). The emotional labor of surveillance: Digital control in fast fashion retail. *Critical Sociology*, 45(7-8), 1167-1179.
- Venkatesh, N. (2021). Surveillance Capitalism: a Marx-inspired Account. *Philosophy*, 1-27.
- Vicente, P. N., & Dias-Trindade, S. (2021). Reframing sociotechnical imaginaries: The case of the Fourth Industrial Revolution. *Public Understanding of Science*, 30(6), 708-723.

- Walker-Munro, B. (2019). A Case for Systemic Design in Criminal Law Techno-Regulation. *Criminal Law Journal*, 43(5), 306-324.
- Wark, W. (2021, September 1). The 9/11 Effect and the Transformation of Global Security. *Council of Councils*, Retrieved from <https://www.cfr.org/councilofcouncils/global-memos/911-effect-and-transformation-global-security>
- Wäscher, T. (2017). Framing resistance against surveillance: Political communication of privacy advocacy groups in the “Stop Watching Us” and “The Day We Fight Back” campaigns. *Digital Journalism*, 5(3), 368-385.
- Williams, R. W. (2005). Politics and Self in the Age of Digital Re (producibility). *Fast capitalism*, 1(1).
- Williams, D. P. (2020). Fitting the description: historical and sociotechnical elements of facial recognition and anti-black surveillance. *Journal of Responsible Innovation*, 7(sup1), 74-83.
- Winner, L. (1986). Do Artifacts have Politics? From The Whale and the Reactor. *Chicago: University of Chicago Press*. Winner, L.(1993), “Upon opening the black box and finding it empty: social constructivism and philosophy of technology', *Science, Technology & Human Values*, 18(3), 362-78.
- Winner, L. (1983). Technologies as forms of life. *Epistemology, methodology, and the social sciences*, 249-263.
- Wood, D. M. (2009). The Surveillance Society: Questions of History, Place and Culture. *European Journal of Criminology*, 6(2), 179-194.
- Wood, D. M., Ball, K., Lyon, D., Norris, C., & Raab, C. (2006). A report on the surveillance society. *Surveillance Studies Network, UK*.
- Yang, C. Y., Szerszynski, B., & Wynne, B. (2018). The making of power shortage: The sociotechnical imaginary of nationalist high modernism and its pragmatic rationality in electricity planning in taiwan. *East Asian Science, Technology and Society: An International Journal*, 12(3), 277-308.
- 黄玮杰 & 吕欣忆 Huang, W & Lv, X. (2021). 政治经济学批判视角下的当代西方社会监控批判 [A Critique of Contemporary Western Social Surveillance in the Light of the

- Critique of Political Economy]. *贵州师范大学学报(社会科学版)* (01),18-25.
- 监控员工上网 怎么做到的? 侵犯隐私吗? [*Should Workplace Surveillance be Considered an Invasion to Individual's Privacy?*] (2021, November, 19). The Southern News. http://news.sohu.com/a/502047061_417915
- 杨晔 Yang, Y. (2009). 详解美国留学签证中的“移民倾向” [A Detailed Review of “Immigration Intent” When applying for American Visa and Study Permit]. *留学生*, (10),48-49.
- 张敏 & 罗雨 Zhan, M. & Luo, Y. (2022) 住宅小区人脸识别门禁系统的应用风险及其法律规制 [The Risks and Legal Regulations of the Application of Facial Recognition Entrance Systems in Residential Communities]. *江西科技师范大学学报*, 205(03), 39-48.
- 张慧子 Zhang, H. (2011). 新媒体时代公民隐私的侵害与保护研究 [An analysis of Privacy Infringement and Protection in the Age of New Media] (博士学位论文 Doctoral Dissertation, 华中科技大学).
- 赵婉辰 Zhao, W. (2021). 基于人脸识别的自动售货系统设计 [*Facial Recognition Based Vending System*](硕士学位论文, 哈尔滨理工大学, Master Thesis).<https://kns.cnki.net/KCMS/detail/detail.aspx?dbname=CMFD202201>

Reference List for Empirical Materials

- Big Brother Watch Team. (2023). About Big Brother Watch. *Big Brother Watch*. Retrieved from <https://bigbrotherwatch.org.uk/about/>.
- Big Brother Watch Team. (2022 a, November 8). Big Brother Watch Files Legal Complaint Against Facial Recognition “Search Engine”, Pimeyes. *Big Brother Watch*. Retrieve from <https://bigbrotherwatch.org.uk/2022/11/pimeyes-press-release/>.
- Big Brother Watch Team. (2022 b, June 17). Statement On Cheshire Police Facial Recognition. *Big Brother Watch*. Retrieve from <https://bigbrotherwatch.org.uk/2022/06/statement-on-cheshire-police-facial-recognition/>.
- Big Brother Watch Team. (2022 c, May 23). Mailonline – ‘Orwellian’ Facial Recognition Firm Clearview Ai Fined £7.5m. *DailyMail*. Retrieved from <https://www.dailymail.co.uk/news/article-10845123/Orwellian-facial-recognition-company-used-UK-police-forces-fined-7-5M.html>.
- Big Brother Watch Team. (2019 a, August 23). Regulation Would Be A Life Raft For Live Facial Recognition — We Need A Ban. *Big Brother Watch*. Retrieve from <https://bigbrotherwatch.org.uk/2019/08/regulation-would-be-a-life-raft-for-live-facial-recognition-we-need-a-ban/>.
- Big Brother Watch Team. (2019 a, August 5). DEBATE: Should We Be Worried About Police Use of Facial Recognition Technology? *City A.M.* Retrieved from <https://www.cityam.com/debate-should-we-be-worried-about-police-use-of-facial-recognition-technology/>.
- Big Brother Watch Team. (2019 b, July 10). Are China’s Facial Recognition Trials Really the Example The Met Police Want To Follow? *OpenDemocracy*. Retrieved from <https://www.opendemocracy.net/en/opendemocracyuk/are-chinas-facial-recognition-trials-really-the-example-the-met-police-want-to-follow/>.
- Big Brother Watch Team. (2018 b, May 15). Police Facial Recognition Is An Authoritarian And Oppressive Surveillance Tool. *Huffington Post*. Retrieved from https://www.huffingtonpost.co.uk/entry/facial-recognition_uk_5afabdc2e4b044dffb5c41c?qho.
- Big Brother Watch Team. (2018 a, April 19). Misleading, Incompetent and Authoritarian: The

- Home Office's Defence Of Facial Recognition. *Big Brother Watch*. Retrieve from <https://bigbrotherwatch.org.uk/2018/04/misleading-incompetent-and-authoritarian-the-home-offices-defence-of-facial-recognition/>.
- Big Brother Watch Team. (2017 a, October 31). Home Office Not Listening To Ethics Group On Custody Images And Facial Biometrics. *Big Brother Watch*. Retrieve from <https://bigbrotherwatch.org.uk/2017/10/home-office-not-listening-to-ethics-group-on-custody-images-and-facial-biometrics/>.
- Big Brother Watch Team. (2017 b, July 27). Facial Biometrics Instead Of Train Tickets? Don't Even Go There. *Big Brother Watch*. Retrieve from <https://bigbrotherwatch.org.uk/2017/07/facial-biometrics-instead-of-train-tickets-dont-even-go-there/>.
- Electronic Frontier Foundation. (2023). About EFF. *Electronic Frontier Foundation*. Retrieved from <https://www.eff.org/about>.
- Electronic Frontier Foundation. (2022 b, September 30). EFF to NJ court: Give defendants information regarding police use of facial recognition technology. *Electronic Frontier Foundation*. Retrieved from <https://www.eff.org/deeplinks/2022/09/eff-nj-court-give-defendants-information-regarding-police-use-facial-recognition>.
- Electronic Frontier Foundation. (2022 a, February 9). Victory! ID.me to Drop Facial Recognition Requirement for Government Services. *Electronic Frontier Foundation*. Retrieved from <https://www.eff.org/deeplinks/2022/02/victory-irs-wont-require-facial-recognition-idme>.
- Electronic Frontier Foundation. (2019, October 23). Facial Recognition. *Electronic Frontier Foundation*. Retrieved from <https://www.eff.org/document/facial-recognition>.
- Electronic Frontier Foundation. (2018 b, March 5). Biometrics: Facial Recognition. *Electronic Frontier Foundation*. Retrieved from <https://www.eff.org/document/biometrics-facial-recognition>.
- Electronic Frontier Foundation. (2018 a, February 15). Law Enforcement Use of Face Recognition Systems Threatens Civil Liberties, Disproportionately Affects People of Color: EFF Report. *Electronic Frontier Foundation*. Retrieved from

<https://www.eff.org/press/releases/law-enforcement-use-face-recognition-systems-threatens-civil-liberties>.

Electronic Frontier Foundation. (2016, June 7). The Danger of Corporate Facial Recognition Tech. *Electronic Frontier Foundation*. Retrieved from <https://www.eff.org/deeplinks/2016/06/danger-corporate-facial-recognition-tech#:~:text=The%20Illinois%20Biometric%20Privacy%20Statute,strongest%20protection%20of%20biometric%20privacy>.

Electronic Frontier Foundation. (2015, August 13). San Diego's Facial Recognition Program Shows Why We Need Records on Police Use of Mobile Biometric Technology. *Electronic Frontier Foundation*. Retrieved from <https://www.eff.org/deeplinks/2015/08/san-diegos-facial-recognition-program-illustrates-why-we-need-information-police>.

Electronic Frontier Foundation. (2013, June 26). EFF Sues FBI For Access to Facial-Recognition Records. *Electronic Frontier Foundation*. Retrieved from <https://www.eff.org/press/releases/eff-sues-fbi-access-facial-recognition-records>.

Electronic Frontier Foundation. (2012, August 2). FBI's Facial Recognition is Coming to a State Near You. *Electronic Frontier Foundation*. Retrieved from https://www.eff.org/deeplinks/2012/07/fbis_facial_recognition_coming_state_near_you.

Fight For The Future. (2023). The Future is Ours. *Fight For The Future*. Retrieved from <https://www.fightforthefuture.org/about>.

Fight For The Future. (2022 c, February 7). BREAKING: under pressure from activists & lawmakers, IRS drops plan to use facial recognition. *Fight For The Future*. Retrieved from <https://www.fightforthefuture.org/news/2022-02-07-breaking-under-pressure-from-activists-lawmakers-irs-drops-plan-to-use-facial-recognition>.

Fight For The Future. (2022 b, January 29). Groups Call on IRS to Dump ID.me and Reject All Facial Recognition. *Fight For The Future*. Retrieved from <https://www.fightforthefuture.org/news/2022-01-29-groups-call-on-irs-to-dump-id-me-and-reject-all-facial-recognition>.

Fight For The Future. (2022 a, January 26). ID.me Lied About the Facial Recognition Tool it Sold to the IRS. *Fight For The Future*. Retrieved from <https://www.fightforthefuture.org/news/2022-01-26-id-me-lied-about-the-facial-recognition-tool-it-sold-to-the-irs>.

Fight For The Future. (2021 d, November 22). Facebook's Announcement About Facial Recognition Is a Misleading Distraction. *Fight For The Future*. Retrieved from <https://www.fightforthefuture.org/news/2021-11-22-facebooks-announcement-about-facial-recognition-is-a-misleading-distraction>.

Fight For The Future. (2021 c, August 5). 24 Major U.S. Retailers Added To The List That's Tracking Stores Using Facial Recognition On Customers. *Fight For The Future*. Retrieved from <https://www.fightforthefuture.org/news/2021-08-05-24-major-us-retailers-added-to-the-list-that's>.

Fight For The Future. (2021 b, July 14). Civil Rights Groups Call on Stores to Reject Facial Recognition. *Fight For The Future*. Retrieved from <https://www.fightforthefuture.org/news/2021-07-14-civil-rights-groups-call-on-stores-to-reject>.

Fight For The Future. (2021 a, July 13). Facial Recognition Is Doing Harm Right Now. Lawmakers Need to Stop Dragging Their Feet And Pass The Biometric Technology Moratorium Act. *Fight For The Future*. Retrieved from <https://www.fightforthefuture.org/news/2021-07-13-facial-recognition-is-doing-harm-right-now>.

Fight For The Future. (2020 c, November 18). This Is Why We Need Legislation That Bans Facial Recognition: LAPD Officers Exposed Using Clearview Without Permission. *Fight For The Future*. Retrieved from <https://www.fightforthefuture.org/news/2020-11-18-this-is-why-we-need-legislation-that-bans-facial>.

Fight For The Future. (2020 b, April 29). “Absolutely The Fuck Not.” Fight For The Future Issues Official Statement On Clearview AI's Absurd Proposal To Use Facial Recognition For COVID-19 Response. *Fight For The Future*. Retrieved from <https://www.fightforthefuture.org/news/2020-04-29-absolutely-the-fuck-not-fight-for>.

the-future.

Fight For The Future. (2020 a, February 5). Congress Needs To Stop Messing Around And Ban Facial Recognition. *Fight For The Future*. Retrieved from <https://www.fightforthefuture.org/news/2020-02-05-congress-needs-to-stop-messing-around-and-ban>.

Surveillance Technology Oversight Project. (2023). About Us. *Surveillance Technology Oversight Project*. Retrieved from <https://www.stopspying.org/our-vision>.

Surveillance Technology Oversight Project. (2021 e, June 9). WIRED-Facial Recognition Won't Fight Fraud. *Surveillance Technology Oversight Project*. Retrieved from <https://www.stopspying.org/opeds/2021/6/9/wired-facial-verification-wont-fight-fraud>.

Surveillance Technology Oversight Project. (2021 d, February 8). Ban 'Digital Stop-And-Frisk': Facial Recognition Technology Too Prone to Errors. *Surveillance Technology Oversight Project*. Retrieved from <https://www.stopspying.org/opeds/2021/3/10/ny-daily-news-ban-digital-stop-and-frisk-facial-recognition-technology-too-prone-to-errors?rq=facial>.

Surveillance Technology Oversight Project. (2021 c, February 5). Fast Company - The U.S. Can't Rebuke Global Tyranny When Our Companies Sell Tools That Enable It. *Surveillance Technology Oversight Project*. Retrieved from <https://www.stopspying.org/opeds/2021/3/10/fast-company-the-us-cant-rebuke-global-tyranny-when-our-companies-sell-tools-that-enable-it?rq=facial>.

Surveillance Technology Oversight Project. (2021 b, January 26). Gotham Gazette - Expand the School Ban, End the Use of Facial Recognition in New York. *Surveillance Technology Oversight Project*. Retrieved from <https://www.stopspying.org/opeds/2021/3/10/gotham-gazette-expand-the-school-ban-end-the-use-of-facial-recognition-in-new-york>.

Surveillance Technology Oversight Project. (2021 a, January 26). The Capitol Attack Doesn't Justify Expanding Surveillance. *Surveillance Technology Oversight Project*. Retrieved from <https://www.wired.com/story/opinion-the-capitol-attack-doesnt-justify-expanding-surveillance/>.

- Surveillance Technology Oversight Project. (2020, June 16). A Long Overdue Curb on NYPD Spying. *Surveillance Technology Oversight Project*. Retrieved from <https://www.stopspying.org/opeds/2021/1/6/new-york-daily-news-a-long-overdue-curb-on-nypd-spying?rq=facial>.
- Surveillance Technology Oversight Project. (2019 b, October 17). The Daily Beast - Facial Recognition Tech Is a Blatant Misuse of Police Bodycams. *Surveillance Technology Oversight Project*. Retrieved from <https://www.stopspying.org/opeds/2021/1/6/the-daily-beast-facial-recognition-tech-is-a-blatant-misuse-of-police-bodycams>.
- Surveillance Technology Oversight Project. (2019 a, April 17). Face it: Recognition technology isn't close to ready for prime-time. *Surveillance Technology Oversight Project*. Retrieved from <https://www.stopspying.org/opeds/2021/1/6/ny-daily-news-face-it-recognition-technology-isnt-close-to-ready-for-prime-time>.

Appendix A: Propp's 31 Functions and 8 Character Archetypes

Propp's 31 Functions (Propp, pp. 26-65, 1968)

Function 1-8: These functions together signify the beginning of the story, where the villain has created a dilemma that requires the hero to address.

1. One of the members of a family absents himself from home. (Definition: absention)
2. An interdiction is addressed to the hero. (Definition: interdiction)
3. The interdiction is violated (Definition: violation)
4. The villain makes an attempt at reconnaissance (Definition: reconnaissance)
5. The villain receives information about his victim. (Definition: delivery)
6. The villain attempts to deceive his victim in order to take possession of him or of his belongings. (Definition: trickery)
7. The victim submits to deception and thereby unwittingly helps his enemy. (Definition: complicity)
8. The villain causes harm or injury to a member of a family. (Definition: villainy)
- 8a. One member of a family either lacks something or desires to have something. (Definition: lack)



Functions 9 to 11: The situation is made known to the hero, and the hero is sent out to remedy the dilemma.

9. Misfortune or lack is made known; the hero is approached with a request or command; he is allowed to go or he is dispatched. (Definition: mediation, the connective incident)
10. The seeker agrees to or decides upon counteraction. (Definition: beginning counteraction)
11. The hero leaves home. (Definition: departure)



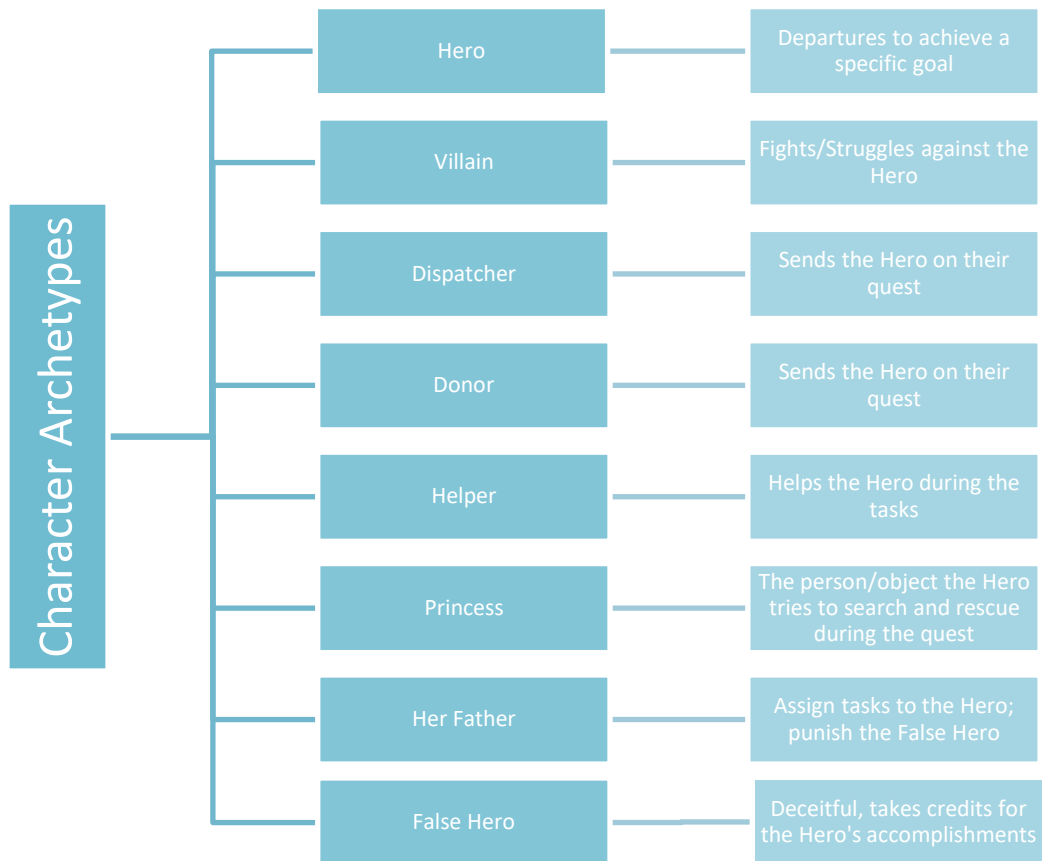
Functions 12 to 19: The hero faces/is tested by the villains and fights them.

12. The hero is tested, interrogated, attacked, etc., which prepares the way for his receiving either a magical agent or helper. (Definition: the first function of the donor)
13. The hero reacts to the actions of the future donor. (Definition: the hero's reaction)
14. The hero acquires the use of a magical agent. (Definition: provision or receipt of a magical agent)
15. The hero is transferred, delivered, or led to the whereabouts of an object of search. (Definition: spatial transference between two kingdoms, guidance)
16. The hero and the villain join in direct combat. (Definition: struggle)
17. The hero is branded. (Definition: branding, marking)
18. The villain is defeated. (Definition: victory)
19. The initial misfortune or lack is liquidated. This function, together with villainy, constitutes a pair. The narrative reaches its peak in this function.



Functions 20 to 31: A. The hero returns and is rewarded for their actions. B. The false hero takes credit for the hero's actions, but is eventually exposed and punished. The hero is then rewarded for their deeds.

20. The hero returns. (Definition: return)
21. The hero is pursued. (Definition: pursuit, chase)
22. Rescue of the hero from pursuit. (Definition: rescue)
23. The hero, unrecognized, arrives home or in another country. (Definition: unrecognized arrival)
24. A false hero presents unfounded claims. (Definition: unfounded claims)
25. A difficult task is proposed to the hero. (Definition: difficult task)
26. The task is resolved. (Definition: solution)
27. The hero is recognized. (Definition: recognition)
28. The false hero or villain is exposed. (Definition: exposure)
29. The hero is given a new appearance. (Definition: transfiguration)
30. The villain is punished. (Definition: punishment)
31. The hero is married and ascends the throne. (Definition: wedding)



(Propp, pp. 879-83, 1968)