# Facial Recognition Technology: Boon or Bane

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

**Saahil Dutta**

Spring 2023

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor
Kent Wayland, Department of Engineering and Society

## Introduction

In this age of technology, society is becoming reliant on data-driven software as these applications in information technology continue to grow, with the emergence of artificial intelligence, the Internet of Things, fifth generation communication devices (5G) and advanced data analytics applications. With these advancements, much more data can be collected, stored and analyzed. This encourages more organizations and businesses to start collecting data from websites, e-commerce platforms, social media, electronic devices and surveillance cameras. Naturally, this development is causing concerns at the individual level regarding personal privacy and secrecy, leading to demands of laws and regulations to govern this space. Academic research on information privacy has been a growing field and there is an increasing interest in this area of research. (Dinev and Hart 2006; Hui, Teo and Lee 2007). Information privacy is inherently the right to control information by deciding the level of information to provide, when and how such information is provided and used, and who can access this information (Van Zoonen 2016). The right to information privacy is the right of individuals to make decisions regarding their personal information.

These concerns are accentuated with the advent of Facial Recognition Technology (FRT) and its many practical uses. The question remains: what are the potential benefits of FRT and where is the line drawn before it becomes an abusive technology to societal standards of privacy? Since the governments and law enforcement proponents promote the beneficial aspects of FRT, individuals and societies may be tempted to invite the growth and universal acceptance of FRT into their private lives and neighborhoods. However, it is also important to analyze the potential of harm or disruption of personal privacy as a result of FRT and evaluate the trade-offs.

In this paper I review relevant literature on this topic, starting with Bentham's theory on Panopticon, the SCOT theory and theories on internet privacy concerns (IPC). I then summarize the uses of this technology all over the world. FRT has been abused by some repressive governments for racial profiling as well as spying on the dissidents. I then provide a critical evaluation of this technology and link it to the theoretical construction. I conclude with a brief summary and a caveat on the unchecked development and application of this technology.

**Theory on Internet Privacy**

The concerns related to internet privacy have been discussed only over the last fifteen to twenty years. However, the underpinnings on privacy discussion dates back to the 18th century in the work of the renowned philosopher Jeremy Bentham. In the computer age, in the late 20th century, early socio-technological scholars discussed the ramification of technological development on society and proposed a theory based on the idea that technology is what shapes human behavior and not the other way around (Social Construction of Technology). With the rise of the internet and its assimilation in the daily lives of ordinary people, researchers explored issues of privacy concerns on the internet. There are two competing theories in this domain (privacy calculus theory and privacy paradox theory). Since FRT is new and still developing there is little academic research that focuses on privacy with respect to this technology.

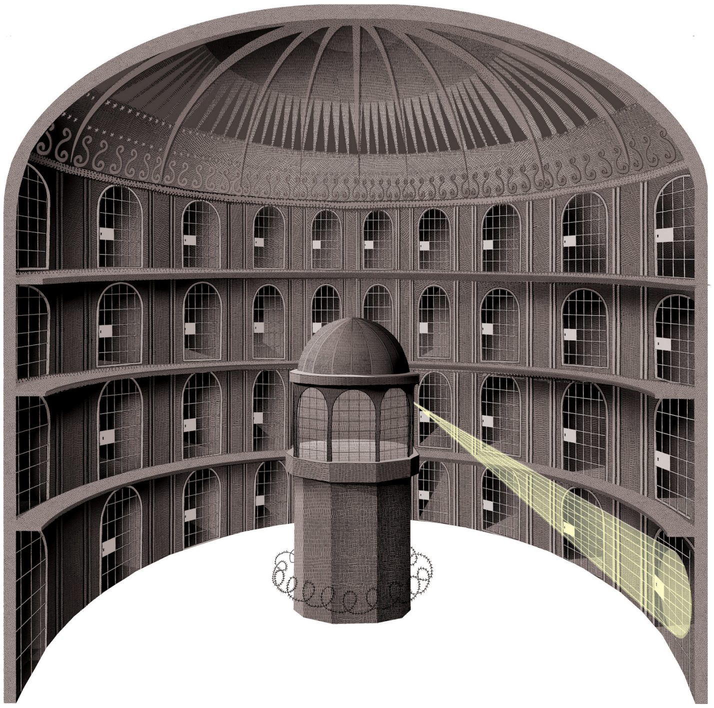


Figure 1: Bentham's Panopticon

The 18th century social reformist and creator of the definition of utilitarianism, Jeremy Bentham proposed the idea of a “Panopticon” (Figure 1) and had a brother who generated the idea that if he sat in the middle of a circle of workers at their stations, he would be able to monitor all of their actions at all times. Jeremy Bentham then began to ponder if he could apply his brother’s system of observing workers to observing prisoners as well. The design can be seen in Figure 1, whereas all the prison cells have one open side facing inwards towards the guard tower such that there can be constant observation of the inmates. This “inspection principle” was not only to observe the behavior of the prison inmates, but the prison manager’s behavior as well. Since there is always the question of who is holding the manager of the prison accountable for their position of authority and responsibility over the inmates. However, the inmates are under the guise that there is always an observer in the guard tower, when that may not be the case, giving the illusion that they are always being watched.

This theory of Panopticon can be applied to modern day surveillance of the general public, which can “assure the automatic functioning of power,” by rendering its actual exercise unnecessary.” (Sheridan, et al. 1995) With the increasing number of entities, both public and private, investing more resources into surveillance and monitoring methods as well as the systems that allow for a deep network for this purpose, ordinary people who are exposed to this knowledge will feel evermounting pressure to adhere to the societal normalities that the observers in charge want to promote. Although this notion was developed 200 years ago, it remains relevant in the current age with the rapid rise of AI technology and the increased efficiency of how data is collected, stored and analyzed.

With the emergence of computer technology and its increased adoption in daily lives, researchers Wiebe Bijker and Trevor Pinch in the late 20th century developed a theoretical framework. This is referred to as the Social Construction of Technology (SCOT). This framework argues that the development of new technology does not shape human action, but rather human action shapes the course that technology takes over time. They argued their concept in the context of weapons and warfare. Conflicts between different groups based on religion, political ideals, and possessions have dominated human history. These conflicts drove the advancement of weapons from swords and spears to flamethrowers and the atomic bomb. This altered technology can be explained through human behavior such as creating laws and policies, dictating wars and expansion, or even adopting religious beliefs for their people. All of these have led to an advancement in technology, such as the creation of bridges and roads in the Roman Empire after decrees by the emperors to connect the territories. Even dating back to the start of the Paleolithic Age, human behavior and the need to survive as a species led to the development of the earliest stone tools. Likewise, in the domain of computer technology, the need to solve a problem or gain competitive advantage drives the development, and not the other way around.

With the growth of the internet's popularity and its adoption in daily lives, in the early 21st century, academic research was conducted on information privacy concerns (IPC). IPC is defined as individual perception related to viewing the leakage of sensitive information as a threat (Dinev and Hart 2006). Campbell (1997) found that IPC differs among individuals according to their age, personal experiences, educational attainment and social status. Additionally, environmental factors, laws and social regulations can affect the level of IPC (Chen et. al. 2008) and societal factors such as power distance and uncertainty avoidance have an effect on IPC (Milberg et. al. 2000). Furthermore, individuals are sensitive to sharing certain types of personal data. Cormode et. al (2018) posit that people are most sensitive to sharing medical history, personal interests and opinions. Hence, it is not feasible to gather this information without providing strong assurances of privacy to the users. They propose that a model of differential privacy (or local differential privacy) can provide such a guarantee. LDP has been implemented by leading technology companies including Google, Apple and Microsoft.

There are two contrasting theories regarding IPC: the privacy calculus theory and the privacy paradox theory. The privacy calculus theory (Smith, Dinev and Xu 2011) states that individuals make decisions about sharing information based on rational trade-offs between profits gained by providing the information and potential threat to their privacy. The privacy paradox theory (Norberg, Horne and Horne 2007), in contrast, argues that individuals ignore privacy concerns even when the information provided is sensitive and there are limited gains from doing so.

In summary, people's concerns often vary on a wide spectrum that often shift based on various events both on a national and global scale. As a society, we should consider whether it's even possible to retain privacy in our daily lives in this era of technology where our daily activities can be constantly monitored. This question arises through the advancements of new technologies and social media platforms as they provide new avenues for authoritarian organizations to track the everyday movements of people who may be caught in others' content they wish to share with the world. Since FRT is still developing, there is limited academic research that explores privacy concerns with respect to this technology, hence we anchor our theory development based on the thoughts and recommendation in other domains.

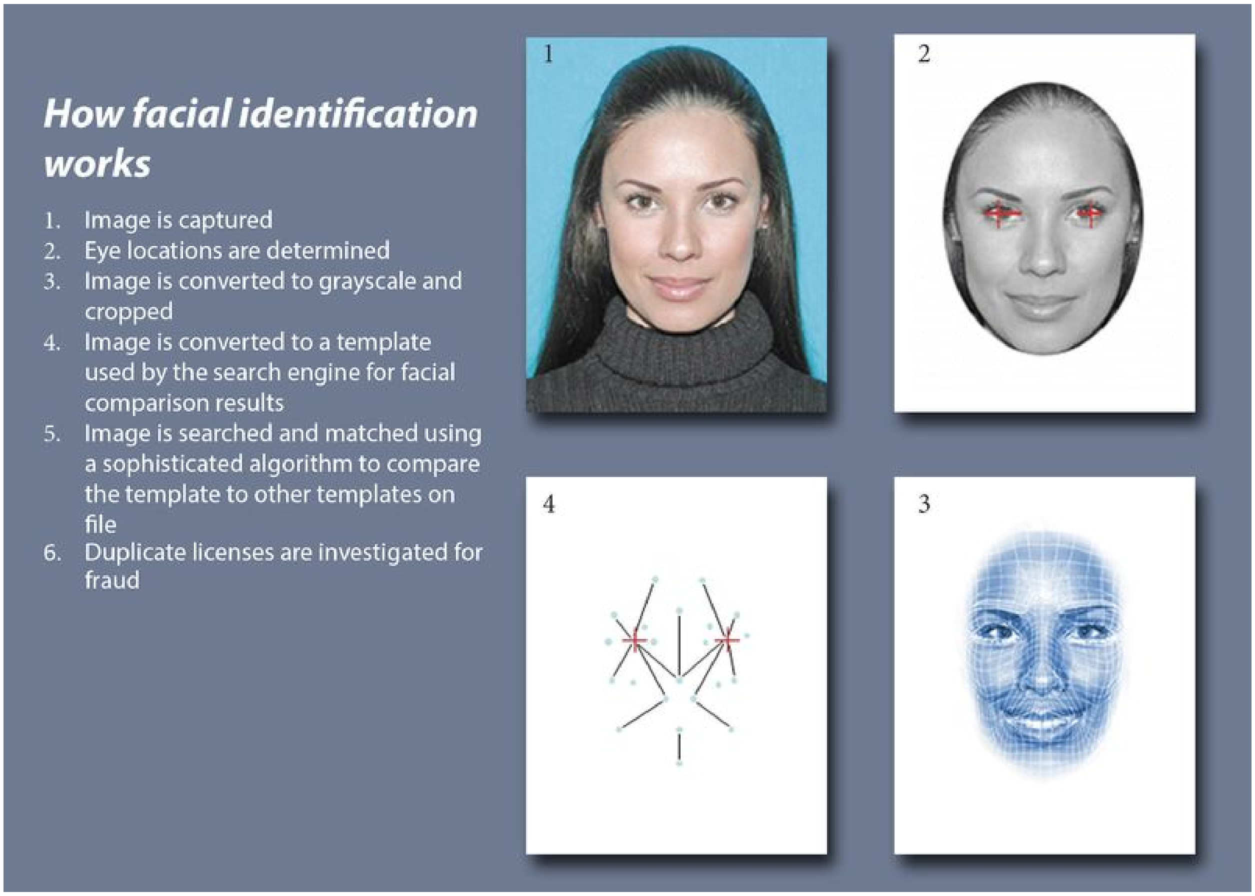
**Background on the development of FRT**

FRT is the latest innovation in the area of biometric systems. One of the first biometric systems to gain universal recognition was fingerprinting. While at inception, this was met with skepticism and incredulity, it is now a widely accepted form of evidence in forensics and criminal investigation. Subsequently, iris scan and voice recognition systems are being incorporated as security measures in highly sensitive venues, such as the CIA and MI-5 (CIA 1982).

Facial recognition is a non-intrusive biometric technology, meaning that it can be collected without the knowledge or explicit consent of the people it tracks. The information is captured on the network of surveillance cameras that are present in most major cities. Widespread use of FRT allows law enforcement to instantly screen millions of people each day, but without unnecessarily intruding on regular people's personal belongings.

The first development of Facial Recognition Technology occurred in the 1960s, when Woodrow W. Bledsoe created the idea of the first face recognition system (Bledsoe 1966). The system relied on facial features such as the eyes, ears, mouth, and nose and computed metrics such as lengths and ratios across facial features. FRT takes the previous development one step further by comparing these metrics across a large database of facial characteristics to identify individuals.

The popularity of FRT has been led by the reduction in cost and improvement of the quality of video cameras. More recently, these features have been integrated into other newer technologies like smartphones and laptops, making an increasing number of people accustomed to the implementation of these new technologies in their daily lives. With the advent of digital technology, video-recorders no longer have bulky tapes or discs, instead the pictures and sound are stored in data-files for easier storage and transmission.



**How facial identification works**

1. Image is captured
2. Eye locations are determined
3. Image is converted to grayscale and cropped
4. Image is converted to a template used by the search engine for facial comparison results
5. Image is searched and matched using a sophisticated algorithm to compare the template to other templates on file
6. Duplicate licenses are investigated for fraud

**Figure 2: The inner workings of FRT (Electronic Frontier Foundation 2017)**

The process that FRT follows involves intake and analysis of unique characteristics and referencing them to a database of images to detect and confirm the identity of an individual. As seen in Figure 2, the process starts with taking a picture of an individual with a high definition digital camera, identifying their unique features, and storing the collection of those features in an easily accessible database. There has been exponential growth in the field of FRT, mostly due to the advancement of the other technology crucial to the implementation of the larger framework. For example, the quality of picture and video has improved significantly in recent years, with newer models capturing even the slightest of details such as a wrinkle or dimple. Furthermore, as the use of these technologies have become widespread, the need for vast amounts of data storage has also grown. With these advancements in storage capabilities, such as pushing information into “the cloud,” there have been many more possibilities to advance FRT and the databases required to uphold a wide-scale organization of individuals under separate nations.

Modern FRT systems can also be trained to identify an individual with a wide variety of facial expressions. (Deshmukh et. al. 2016). In addition, software companies integrate mobile applications that are used frequently to synchronize with FRT software and collect even more data on individual characteristics (Biometrics 2016). This can be utilized in our daily lives with various third-party applications to track our emotions throughout the course of the day and advertise to us accordingly.

In some parts of the world, machine learning techniques that recognize patterns are being used to quickly sift through large data sets of pictures and develop patterns that identify racial and ethnic facial characteristics. While this is an interesting application of this technology and nonetheless impressive, one should consider the potential ethical consequences.

## Methods

In order to gather information for this paper, I conducted a literature review of scholarly articles as well as news items on the use and abuse of FRT. I conducted a survey of existing and developing government and regulatory guidelines and policies on this subject. Subsequently, I explored literature in philosophy dealing with abstract concepts of privacy, surveillance and human behavior. Furthermore, I studied the Social Construction of Technology and applied its definition of how humanity shapes technology to this specific point of societal contention.

## Benefits of FRT and how they can be used to benefit society

The material in this section is based on news articles and studies conducted by research organizations such as Pew Research (Nadeem 2023) and Brookings Institute (Lee & Chin, 2022).

As FRT is relatively new, academic research is sparse on the benefits and risks of FRT. Law enforcement began using real-time FRT for extremely large events, and eventually expanded its use at demonstrations and transportation systems. The first instance of this in the United States occurred during the Super Bowl in 2001; where law enforcement screened and profiled 100,000 people using this new technology – among this large number, 19 people were arrested due to the existence of active warrants in their name (Cavadini 2008). Another example of the use of FRT was by the Metropolitan Police in London to scan the crowds at a remembrance ceremony (Townsend 2017).

Instant identifications using an organized database of individuals have the potential positive influences to locate missing persons, allow quick arrests of those wanted for serious crimes and even make the airline industry safer. In a more niche area of police work, FRT instantly informs officers of potential special needs or medical conditions for an individual they are dealing with. In California, the San Diego Sheriff's Department employs FRT to aid citizens with disabilities (San Diego County Sheriff's Department). Government funded organizations such as the Take Me Home Program allows access of personal information to first responders which could communicate important information in a life-threatening situation.

In the sphere of law enforcement, officers could benefit from the use of real-time FRT if pictures of missing persons were included in the database. In the United States, for example, there are more than half a million missing person cases. Another use of FRT would be an easy to use "scan to pay" implementation on subways and other public transportation. This could help specifically in areas of the world that require fast moving lines during busy hours such as in the morning commute or the rush hour to get home (Perez 2017). The implementation of this facial recognition technology, which can be compared to EZ-pass will eradicate the need for long wait times and will make the vast majority of workers daily commutes more efficient and enjoyable.

As the technology is further developed with each new addition to the usability of the FRT systems, this technology is frequently used as a real-time application to identify criminals and suspects. This has the potential to not only help law enforcement bring existing criminals to justice, but as soon as the public becomes generally aware of this, there will likely be a decrease in petty crimes such as shoplifting and vandalism.

Thus, the innovation of FRT has the potential to aid society in all facets of life, particularly ones that revolve around the safety and security of our individual selves. Proponents of law enforcement laud developments in FRT and wish to incorporate the new technology to apprehend culprits and more importantly to preemptively stop a crime from occurring through real-time surveillance mechanisms (Nadeem 2023).

### Risks of FRT and how they infringe on personal privacy

Although there are countless beneficial applications of FRT in the public sphere and our private lives, there are aspects of the technology that may be unsettling to an individual concerned about personal privacy, since FRT operates clandestinely it can capture significant amounts of information on individuals without them ever even realizing it. This is quite an unnerving concept, as it would hypothetically be possible for each individual to be tracked by their movements in public through the network of security cameras that already exist in major cities. If this footage were to be followed by a machine learning algorithm for each individual, it would be possible to track everyone’s daily schedule based on where they are and what establishments they visit.

Through the use of FRT, individual freedom could be restricted to levels that have never been seen before in the United States. For example, if there were to be some sort of curfew imposed on people of a certain age, this would be easy to implement with FRT. Although there is some reason to employ such systems in the general public, it is unfair to put normal citizens under such a level of scrutiny. This is due to the right of every citizen to have privacy when conducting business or personal affairs. Once that right to privacy is removed, people may begin to feel pressured to limit the amount of activities they enjoy or need to do in public. Hobbies such as playing sports in public fields or social interactions such as getting a drink with friends could become infrequent and perhaps even taboo. This would lead to an almost voluntary decline of societal norms as people could be worried about being tracked when engaging in their normal activities.

Some people and organizations, such as the ACLU, contend that ordinary and law-abiding citizens should not be subject to constant surveillance of their daily activities by law enforcement or the government. They are wary that it infringes on personal freedom and people's inherent right to privacy, the idea of the 'right to remain anonymous.' While people visit public places knowing fully well that they will be seen by others, they do not expect constant monitoring, or eavesdropping by authorities. There is a risk that this would lead to racial profiling and prosecution of individuals for petty crimes, such as loitering, jaywalking or littering (Brookings Institute 2022).

Through FRT it is conceivable that an individual's personal network could be traced and mined. For example, with FRT it will be relatively easy to track who an individual meets and who they spend time with. This kind of data, while not secret, is not expected to be recorded or retained in a database. Such information could be used to determine someone's interests, political affiliation and involvement in sensitive matters. This could be deemed as a violation of personal privacy and the information could be used, with the aid of other computing tools, to target individuals, such as disenfranchising them from voting and other democratic processes.

In more authoritative regimes, like Russia and China, the above issues are even more dire. The government keen on holding on to power tends to prosecute any form of dissent. In such societies, FRT imposes greater risks and fear of criminal prosecution to its citizens for simply associating with known detractors of the ruling government. Public skepticism and concern about misuse of FRT in China is not unfounded. An U.S. State Department report dedicated to Uyghurs validate that Chinese authorities are using an extensive, confidential network of FRT to track and corral the Uyghurs, a largely Muslim minority. It is the first instance of an authoritative regime using artificial intelligence combined with machine learning for profiling racial groups. This technology is being employed to keep tabs on China's 11 million Uyghurs (U.S. Department of State 2020).

FRT, which is an integral part of China's perpetually growing network of surveillance cameras, searches for Uyghurs primarily based on their distinctive facial characteristics which differentiate them from the majority Han. The surveillance tracking systems keep a log of the movement of the Uyghur individuals for further search and review. This allows the Chinese government to effectively profile the minority, arrest them and send them to "re-education" camps with utmost efficiency. The use of FRT has automated the identification of Uyghurs in the nation's most populous cities (Human Rights Watch 2023).

The abuse of this powerful technology by the repressive governments imposes a greater risk to humanity and outweighs the benefits outlined in the previous section. We expand on this trade-off in the next section. Early availability of this technology could have altered the course of recent history. Imagine whether the *Arab Spring* would occur if FRT was available to the rulers of Egypt, Libya and other North African countries, whereby dissent and rebellions could have been effectively quashed in the bud and never allowed to materialize into a large civic demonstration.

**Analysis and results of research use Panoptic surveillance and maybe IPC but can get rid of IPC**

In this section we provide our views and analysis of the ramifications of wide adoption of FRT, particularly by law enforcement agencies and governments. FRT is an invasive technology that infringes upon personal freedom of ordinary citizens. Law abiding citizens are entitled to their privacy and personal information on them cannot be collected without their explicit consent. FRT, by design, collects data through strategically placed video technology often without the knowledge of individuals whose movement is being tracked. This violates an individual's 'right to anonymity.' The 1960's philosopher Alan Westin had defined anonymity as a certain "state of privacy" that is perpetually upheld when an individual is in public spaces or performing acts in public but still maintains freedom from surveillance by governmental systems and identification by law enforcement (Westin 1969).

As we move closer to the apex of technological innovation with the recent developments in ChatGPT, FRT, AI generated art and other Artificial Intelligence, these technologies can be combined and lead to previously unconceived consequences. These technologies, when merged, could further infringe on personal privacy and the right to anonymity. That is, the right of a law-abiding citizen to remain 'nameless.' The underlying right to public anonymity guarantees that when venturing out in the public domain, any given individual will remain nameless, unmarked, and undifferentiated from the rest of a crowd under a government's watchful eye.

This right is only conceded when one commits an act that is unlawful under the generally accepted rules of society. For example, there could be instances where a group of individuals go to a bar, which is still a public space, but oftentimes patrons still want to maintain anonymity as they are there to discuss personal matters or maintain private relationships. It is likely that a majority of people would like to avoid their frequency of bar attendance being recorded, stored in a database and analyzed without being informed that this is occurring.

On the other hand, it would be a different scenario if people were being told that their actions in public were being monitored and stored for later analysis. As discussed in the theory section, Jeremy Bentham had speculated that when people are aware they are under surveillance, they tend to behave differently, or more obediently. This theory of Panopticon can be applied to modern day surveillance of the general public, which can "assure the automatic functioning of power," by "rendering its actual exercise unnecessary" (Sheridan, et al. 1995). People will become more cautious in their interactions and associations with others, if they know that those interactions are being observed, recorded and stored for later analysis. With the increasing number of entities, both public and private, investing more resources into surveillance and monitoring methods as well as the systems that allow for a deep network for this purpose, ordinary people who are exposed to this knowledge will feel evermounting pressure to adhere to the societal normalities that the observers in charge want to promote. This will implicitly restrict freedom even for law abiding citizens.

Likewise, the emergence of new FRT technologies and the manner in which they are used can be attributed to the theoretical framework of the Social Construction of Technology (SCOT). This framework argues that the development of new technology does not shape human action, but rather human action shapes the course that technology takes over time. This can be seen with the case of how FRT is being used in the public domain, as those who control these technologies are able to realize the benefits of implementing new systems and also are able to exercise a certain amount of control over those who are unaware of the creation of these innovations. Further, it can be seen through public action and use of these technologies that people behave differently when introduced to new technology, not that they shape the technology itself.

Even more recently, there have been theories on Information Privacy Concern (IPC) which are directly applicable to the development of FRT. Firstly, the privacy calculus theory can be stated as people make rational decisions on the trade-off regarding the benefits of sharing personal data relative to the threat to their information safety. On the other hand, the privacy paradox theory argues that individuals will provide their personal information with no regard for their safety even if there are any limited benefits. With the development of FRT, it can be seen that law enforcement and governments seem to extol the virtues of use of FRT in crime prevention and enforcement without adequately cautioning the society on its potential risks. In other words, there is an exaggeration of benefits with no mention of potential threat. This can be viewed as a concerted effort to entice the general public to support the broad deployment of this technology.

If the general public were aware that this system of surveillance were being implemented, they may be willing to concede some of their rights to privacy and anonymity for the well-being of their community. For example, if there were some guarantee to public safety from threats of death or mass destruction through acts of terrorism, then the public may agree to be put under constant surveillance to prevent harm for themselves and their loved ones. This is the argument that law enforcement has made, as outlined in the *Benefits* section. In recent years as they have employed FRT in large gatherings and demonstrations, however, they have failed to inform the public beforehand regarding their use of this technology.

Furthermore, recent use of this technology and the data it has produced seem to suggest the exact opposite of what law enforcement claims. For example, in the UK, the criminal offenses that are typically prosecuted the most through the use of CCTV data have been mostly minor offenses. These include non-violent crimes such as littering, public urination, and disobeying traffic laws. While these acts are against the law, they are generally regarded as commonplace nuisance rather than a crime with victims. These occurrences very rarely actually affect the safety of those surrounding the "criminals" and are simply not the crimes that the new FRT should be geared towards solving, given the power of the technology to identify nearly anyone on the planet. It seems as though this technology is being used to enforce social conformity rather than solving actual crimes. Thus, while law enforcement officials utilize this technology with the promise of preventing major crime through the use of 'scare tactics,' the reality in practice is the intrusion of relatively normal citizens who happen to bend the law on occasion, such as running a red light, speeding or throwing a banana peel out of a car window.

Repressive governments are not averse to using modern technological development for surveillance on its law-abiding citizens and as an effective tool to suppress political dissent. As noted in the Risks section, there have been severe human rights violations committed against the Uyghur Muslims in China. Through the use of FRT, Uyghurs have been identified by their unique facial characteristics and sent to concentration camps due to their religion. Unintended use of this technology for racial profiling is a very dangerous development that the public should be made aware of prior to their consenting to its deployment.

More broadly there have been even more outrageous invasions of privacy in countries such as Mexico. Though not in the domain of FRT it still has relevance to our discussion as evidence of overreach by the government in infringing upon liberty of law-abiding citizens. It has recently been revealed that the Mexican government used an advanced spyware called Pegasus to track the activity of individual cell phones (Kitroeff & Bergman 2023). This technology is extremely terrifying as it can track every single action taken on any phone within its radius. Every single email, photo, text message, and memo reminders can be viewed and extracted after the initial infection, and the spyware can essentially track your actions and location in real time. What started as a government program to track drug cartels and other criminals, slowly devolved into an invasive system to silence voices that opposed the government policies. While this program had great success with the capture of El Chapo and other major drug runners, there were also 'failures' where anti-corruption activists, human rights lawyers and journalists had their phones infiltrated in order to gather information on their daily lives and potentially blackmail or abduct them. This is evidence that even democratically elected governments are not averse to crossing the fine line of using the technology meant to prevent crime for silencing opposition.

Wide deployment of FRT can literally make the phrase "big brother is watching' a sad reality. In the renowned novel *1984* by renowned author George Orwell, supposed "thought crimes" were prosecuted in the fictional land of *Oceania*. This "unrealistic" world was populated by citizens who were wary of who they were associated with and what conversations they had, for even thinking of committing a crime was punishable by death. While this currently seems incredibly far-fetched, it is not at all impossible with the facial detection that is currently being used to prevent crime, or even isolate racial minorities (like in China) and if this technology is further developed, a scenario similar to Orwell's *1984* could become our reality.

## Conclusion

FRT has the potential of morphing our existence and activities into data that can be stored, shared and analyzed. The ubiquitous use of FRT can track each individual, the places they visited and others that they met, etc. If its full potential is realized, our descendants in about two generations would not know what it is like to be in public without being watched. They will become inured to being identified, profiled and potentially exploited, as they would grow up in a world where this will be the norm. In such a world, critics of the government and holders of alternative thoughts will be profiled and punished, and events like the *Arab Spring* will seem like fantasy.

While there are many benefits to implementing Facial Recognition Technology in our daily lives, we must be wary of the manner in which the entities that determine how it is used approach using these systems in the public domain which could potentially alter the course of our personal privacy rights moving forward. While the added convenience of not having to go through a turnstile while taking a subway, or not needing a boarding pass at the airport are welcome, the hidden costs of these conveniences are perhaps not. To sum up, the development of FRT can be viewed as a menace disguised as a blessing, similar to the Trojan horse–glittery and shiny on the outside while the true evil hides inside.

## References

Bledsoe, W. W. 1966. The model method in facial recognition. Panoramic Research Inc., Palo Alto, CA, Rep. PR1 15(47):2.

Casey, W. J. (1982, December 17). *IRIS Systems Development*. Central Intelligence Agency. Retrieved from https://www.cia.gov/readingroom/document/cia-rdp83m00914r002100120008-2

Chen, H. G., C. C. Chen, L. Lo and S.C. Yang. 2008. Online privacy control via anonymity and pseudonym: Cross cultural implications. *Behaviour and Information Technology.* 27 (3): 229-242. *SIGMOD* Houston, Tx June 10-18.

Chen, Long, Yadong Huang, Shumiao Ouyang, and Wei Xiong. "The Data Privacy Paradox and Digital Demand, by Long Chen; Yadong Huan." NBER Working Papers. National Bureau of Economic Research, Inc, February 2, 2021. https://ideas.repec.org/p/nbr/nberwo/28854.html.

Cormode, G., S. Jha, T. Kulkarni, N. Li, D. Srivastava and T. Wang. 2018. Privacy at scale: Local differential privacy in practice.

Department, S. (n.d.). *San Diego County Sheriff - Take Me Home Registry*. Take Me Home Registry. Retrieved April 23, 2023, from https://www.sdsheriff.gov/community/take-me-home-registry

Department of State, U. S. (2020, December 1). *2019 Report on International Religious Freedom: China - Xinjiang*. U.S. Department of State. Retrieved April 23, 2023, from https://www.state.gov/reports/2019-report-on-international-religious-freedom/china/xinjiang/

Dinev, T. and P. Hart. 2006. An extended privacy calculus model for e-commerce transactions. *Information Systems Research* 17 (1): 61-80.

Fan, J. M. Shao, Y. Li and X. Huang 2018. Understanding users'attitude toward mobile payment use: A comparative study between China and the USA. *Industrial Management and Data Systems.*

Frontier Foundation, E. (2017, October 24). *Face recognition*. Electronic Frontier Foundation. https://www.eff.org/pages/face-recognition

Gostin, L. O., S. F. Hababi and K. Wilson. 2018. Health data and privacy in the digital era. *JAMA.* 320 (3): 233-234

Hui, K. L, H. H. Teo and S. T. Lee. 2007. The value of privacy assurances: An exploratory field experiment. *MIS Quarterly.* 31 (1): 19-33.

Iyengar, A., A. Kundu and G. Pallis. 2018. Healthcare informatics and privacy. *IEEE Internet Computing* 22 (2): 29-31.

Kitroeff, N., & Bergman, R. (2023, April 18). *How Mexico became the biggest user of the world's most notorious Spy Tool*. The New York Times. Retrieved April 24, 2023, from https://www.nytimes.com/2023/04/18/world/americas/pegasus-spyware-mexico.html

Kozyreva, A., P. L. Spreen, R. Hertwig, S. Lewandowsky and S. M. Herzog. 2021. Public attitudes towards algorithmic personalization and use of personal data online: Evidence from Germany, Great Britain and the United States. *Humanities and Social Sciences Communications.* 8 (1): 1-11.

Lee, N. T., & Chin, C. (2022, April 14). *Police surveillance and facial recognition: Why data privacy is imperative for communities of color*. Brookings. Retrieved April 23, 2023, from https://www.brookings.edu/research/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/

Milberg, S. J., H. J. Smith and S. J. Burke. 2000. Information privacy: Corporate management and national regulation. *Organization Science.* 11 (1): 35-57.

Norberg, P. A., D. R. Horne and D. A. Horne. 2007. The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs,* 41 (1) 100-126.

Nadeem, R. (2023, March 1). *2. public more likely to see facial recognition use by police as good, rather than bad for Society*. Pew Research Center: Internet, Science & Tech. Retrieved April 23, 2023, from https://www.pewresearch.org/internet/2022/03/17/public-more-likely-to-see-facial-recognition-use-by-police-as-good-rather-than-bad-for-society/

Perez, B. (2017, December 6). *Shanghai subway to use Alibaba Voice and Facial Recognition Technologies*. South China Morning Post. Retrieved April 23, 2023, from https://www.scmp.com/tech/enterprises/article/2123014/shanghai-subway-use-alibaba-voice-and-facial-recognition-systems-ai

Reichart, L., S. Brack and B. Scheuermann. 2020. Privacy preserving contact tracing of COVID-19 patients. *Cryptology e-Print Archives.*

Rights Watch, H. (2023, March 28). *China's algorithms of repression*. Human Rights Watch. Retrieved April 23, 2023, from https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass

Reynolds, O. M. (1969). [Review of *PRIVACY AND FREEDOM*, by A. F. Westin]. *Administrative Law Review*, *22*(1), 101–106. http://www.jstor.org/stable/40708684

Sannon, S., N. N. Bazarova and D. Cosley. 2020. Privacy lies: Understanding how, when and why people lie to protect their privacy in multiple online contexts. CHI.

Smith, H. J., T. Dinev and H. Xu. 2011. Information privacy research: An interdisciplinary review. *MIS Quarterly* 35 (4): 989-2016.

Yang, F. and J. Xu. 2018. Privacy concerns in China's smart city campaign: The deficit of China's cybersecurity law. *Asia and the Pacific Policy Studies.* 5 (3): 533-543.

Yasaka, T. M., B. M. Lehrich and R. Sahyouni. 2020. Peer-to-peer contact tracing: Development of a privacy-preserving smartphone app. *JMIR mHealth and uHealth* 8 (4).

Xiong, Aiping, Tianhao Wang, Ninghui Li, and Somesh Jha. Towards Effective Differential Privacy Communication for Users' Data Sharing Decision and Comprehension. arXiv.org. IEEE Symposium for Security and Privacy, March 31, 2020. https://doi.org/10.48550/arXiv.2003.13922.

Xiong, A., T. Wang, N. Li and S. Jha. 2020. Towards effective differential privacy communication for users' data sharing decision and comprehension. *IEEE Symposium on Security and Privacy.*