# A Comparative Study on the Sociopolitical Aspects of Facial Recognition in Different Societies

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

Thinh Tu
Spring, 2021

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

Signature ______Thinh Tu _______________________________ Date _5/12/21__
Thinh Tu

Approved ______Tsai-Hsuan Ku__________________________ Date _5/11/21___
Tsai-Hsuan Ku, Department of Engineering and Society

## Introduction

This project seeks to examine how different cultures respond to the use of facial recognition technology and similar technologies, which many consider a threat to privacy, for the purpose of safety or national security. Facial recognition software's capabilities have expanded greatly in recent years, bringing with it many controversies in terms of its applications. The growth of this technology is already impacting billions of people around the world. Stakeholders involve governments and people in countries with access to such technology, as well as developing countries that haven't taken a stance on the use of facial recognition. As such, I would like to perform a comparative study of the various responses to facial recognition technology as well as the difference in design, arrangement, and deployment of the technology under different social, political, and cultural conditions. Countries that would be suited for this comparison would be the United States, the European Union, and China, which are the farthest ahead in terms of research and development of this technology. Preliminary examination also highlights the very different responses each of these countries have towards the use of this technology, perhaps due to underlying political or cultural norms. With the advancements in this technology, the use of facial recognition is escalating rapidly in the U.S., the EU and China. In terms of influence, each of these groups have demonstrated influence on the laws of neighboring countries, whether directly or indirectly, so the decisions made by these influential nations could cause a ripple effect across their indirect spheres of influence.

In the United States, over 26 states allow law enforcement to run researches against their databases of driver's license and ID photos, while the FBI has access to all driver's license photos in 18 states (Thales group, 2020).  From a commercial standpoint, facial recognition software supplemented with artificial intelligence is also experiencing widespread growth across social media platforms and common devices used in everyday life, for various purposes such as login and verification, personalized ads, health tracking, and more. This is also true in the European Union, where facial recognition is used at border checks and police checks, and CCTV systems are continuously expanded. In China, a video surveillance network is being deployed nationwide, with over 200 million surveillance cameras in use by the end of 2018, with an estimated 626 million by the end of 2020 (Thales group, 2020).  These cameras are deployed in banks, airports and on the streets. This extensive facial recognition application is also linked with the developing Social Credit System in order to maintain public order and safety.

This is a study that could be benefitted from the STS investigation to systematically address sociopolitical and cultural conditions that enable or disable the use of this technology in these nations because stakeholders on different sides of the fence have very strong conflicting ideals, both with their own justifications. In countries like the United States, the general mindset seems to be against the use of facial recognition technology due to privacy concerns and worries about the technology being abused for political reasons.  In countries like China, facial recognition is more accepted as a way of maintaining public order. Police and governments argue that facial recognition technology could prevent tragedies and loss of lives and that the privacy tradeoff is worth it.  In the U.S., opposition has cited instances where facial recognition technology has seemingly been abused, such as to identify protestors during the Freddie Gray protests to be targeted for arrests, as well as concerns that facial recognition was used to identify protestors during recent events (Garvie, Bedoya & Frankle, 2016). These countries also have very different approaches towards the implementation and breadth of this technology. In the European Union, privacy and personal information is considered a fundamental right, with the Charter of Fundamental Rights in the European Union stating that everyone has the right to the protection of personal data (Pernot-Leplay, 2020). The United States, on the other hand, has a very minimalist approach in terms of data protection and privacy laws, leaving many areas fairly vague, leading to controversies and protests during significant social and political events as a result of the use of the technology (Pernot-Leplay, 2020). China on the other hand, provides strong biometric data protection against private entities, but increases the government's access to personal information, while public attitude is less opposed to the idea (Thales group, 2020). The research questions that this study seeks to address are as follows:

1. What is the social, political, or cultural basis for the differences regarding the politics, design, arrangement, and deployment of facial recognition technology in the U.S., the EU, and China?
2. How do different societies define and draw the boundary between public safety and individual privacy, and what factors influence this boundary drawing process in regulating the use of facial recognition?
3. What power relationships are evident during this boundary drawing process? What groups or parties have the influence or authority to influence the design and use of facial recognition? Who are the key stakeholders and what is the power relationship among these stakeholders in designing and promoting facial recognition technology?
4. What are the differences in public perception and government perception regarding facial recognition technology and what does this tell us in terms of trust in technology and trust in government in each of these areas?

## STS Research

The data collected for this study consisted of legal documents on privacy and individual data protection from each of the three regions of interest, namely, the United States, the European Union, and China. Documents gathered and analyzed include the Privacy Act of 1974, passed in the United States, Council of Europe Convention 108, the European Union’s General Data Protection Regulation (GDPR), as well as China’s Cybersecurity Law. Due to the existence of a language barrier in analyzing China’s Cybersecurity Law (passed in 2016), an English translation by Rogier Creemers, Paul Triolo, and Graham Webster was analyzed instead, which may not perfectly represent the original document. Secondary data in the form of news articles and public opinion surveys was originally intended to be analyzed to provide further insights, but due to various limitations, a large enough sample from a variety of different news sources to accurately represent the people in each region could not be viably analyzed. These limitations include the vetting of particular news sources, as well as how organizations or governments might have influenced such news. Particularly in the case of news articles on the topic of data privacy in China, due to lack of information and a language barrier, assessment of how reliable and representative of the general population a particular news article is could not be reasonably done during the process of this research. As such, this analysis will focus mainly on the legal documents mentioned above, which was ratified by the respective governmental organizations in each region of interest, while considering secondary sources as supplementary information to provide a clearer context.

When comparing these documents, an important detail to notice is the time period in which each respective regulation was passed. Privacy laws in the United States and the European Union were first introduced around the late 1970s and early 1980s, while laws on data privacy in

China were created several decades later, in the 21st century. It could be argued that China's process towards creating privacy and data protection rights began in 1982, since the right to freedom and privacy of correspondence is protected under Article 40 of the Constitution. However, because of the fact that this Constitution cannot server as the legal ground for a judicial decision or interpretation in China, these provisions had essentially no effect, and a true data privacy protection act was not enacted until much later on. While the United States and European Union's approaches to data privacy were similar at first, with the Data Privacy Act of 1974 and the OECD Privacy Guidelines, the European Union began to lean towards more comprehensive data privacy laws with the ratification of European Commission Convention 108. The stricter regulations imposed in the European Union may have enacted as a response to abuses on privacy and personal information during and after World War II, as proposed by Pernot-Leplay. The United States, on the other hand, did not experience any notable events which could have led to the development of stricter privacy laws. As such, in the U.S., privacy rights and personal information protection are considered alongside several other interests, from commercial purposes to national security purposes. Another notable barrier to data privacy in the U.S. is the right to free speech protected by the First Amendment, which could be used to argue for the use of collected data. In China, the lack of data privacy laws until recent times might be attributed to traditional Chinese culture; However, Taiwan has stricter data protection laws compared to the standards in the United States, so this might not necessarily be the case.

Over time, data protection laws in the European Union have continued to evolve, growing in comprehensiveness, with the most current effective law being the General Data Protection Regulation (GDPR). In the United States, on the other hand, there is no single principal data protection legislation. Instead, there are hundreds of laws at both the state and federal level, which can broadly differ based on region in the United States. This phenomenon indicates the influences the different stakeholders have at each level of government. Companies and corporations have vested interests that differ from the individual, and these interests may be reflected in legislation at the state and regional levels, as acknowledged earlier. The GDPR details many categories of data protection for the individual, including lawfulness of processing, conditions for consent, processing of various special categories of personal data. It also provides rights of the data subject, most notably access to transparent information, communication and modalities for the exercise of the rights of the data subject and gives subject the right to rectification and erasure of data, as well as the right to restriction of processing of data. In addition to rights of individuals, obligations of the controller and processor of information are also clearly stated, including responsibility of the controller, data protection by design and by default, security of processing, which includes notification of a personal data breach to the supervisory authority and the data subject. Various regulations for the transfer of personal data to different countries and international organizations were also included, along with the establishment of independent supervisory authorities. These strict guidelines leave very little room for different interpretation of the law, as opposed to the U.S. Privacy Act of 1974, which is very general and had no specific guidelines to be followed.

Although the level of strictness is different in the legislation regarding data privacy and data protection in the U.S. and the E.U., generally speaking, these laws apply to all vested stakeholders equally. This is different from China's Cybersecurity Law, which regulates different privacy from the state and privacy from private actors. China's Cybersecurity Laws provide extensive protections to the individual consumer, that can be even stricter than regulations imposed in the U.S. and the E.U. In the Cybersecurity Law, there seems to be a distinct separation between the State and various other organizations and individuals. Article 1 of the GDPR states, “This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.” Meanwhile, Article 4 of the Cybersecurity Law states, “The State formulates and continuously improves cybersecurity strategy, clarifies the fundamental requirements and primary goals of ensuring cybersecurity, and puts forward cybersecurity policies, work tasks, and procedures for key sectors,” which could indicate a distinction on which parties are under the jurisdiction of the regulations. However, without this detail, the Cybersecurity Law provides very extensive consumer privacy from corporations and organizations utilizing data for commercial purposes. The draft of the Personal Information Protection Law in China further expands regulations, with its 70 articles containing large fines for violation of personal data. In terms of breadth of coverage, this legislation resembles the E.U.’s GDPR, indicating that perhaps privacy laws are considered in similar ways across different regions, with differences in culture having a smaller effect. Rather, the main differences in the wording and restrictions may have more to do with the systems of government in each region instead. However, this doesn’t necessarily mean that cultural differences have no effect at all, as seen in the differences between U.S. legislation compared to the E.U.’s despite having similar systems of government. From these documents, we can see the impact of socio-political and cultural factors on the purpose and targets of each legislation in their respective regions.

When examining these documents through the lenses of Langdon Winner’s theory of technological politics, we can see the differences in political power between the different groups in each of the regions explored above. While there may be similarities in terms of what the respective laws of each region covers, the differences in the party dominating the regulation and development of the technology and the structure of the power hierarchy can be clearly seen. While there are certain complexities and nuances within the power hierarchy in each region of the study, this hierarchy can be generally divided into three groups: the individual, the governmental authority, and the capitalist in the form of large corporations. In China, the central government lies at the top of the power hierarchy, as seen through the way the laws and regulations were implemented, followed by the individual and finally corporations. We can see the broader impact of this power structure on the organization and deployment of the technology, and the impact of this deployment as forms of life. In China, a video surveillance network is being deployed nationwide, with over 200 million surveillance cameras in use by the end of 2018, with an estimated 626 million by the end of 2020 (Thales group, 2020).  These cameras are deployed in banks, airports and on the streets. This extensive facial recognition application is also linked with the developing Social Credit System, demonstrating the power and authority available to the central government. In the E.U. and the U.S., the way in which regulations are created and deployed indicate more power towards the individual, who have the ability to strongly influence regulations through their representatives in government. In the U.S., however, corporations have a significant impact, arguably higher than that of the individual, on regulations regarding facial recognition technology. Large corporations like Amazon and Microsoft spend large amounts of money to lobby officials for more beneficial regulations regarding the development and application of facial recognition technology. With the announcement of Joe Biden as president-elect, these companies and others sent public congratulatory messages expressing hope that his administration would ease the nation’s political divisions, and suggested it consider crafting the first federal rules governing face recognition. These corporations also took a stance against the use of the technology for “mass surveillance, racial profiling, or violations of basic human rights and freedoms," but implicitly support its use for commercial applications (Simonite, 2020). This indicates the balance of power between the government and corporations, as neither parties are willing to publicly take a stance purely support the technology's application for commercial and security purposes and take in mind the individual's concerns.

Although there is a significant number of concerns and backlash against facial recognition technology in both the United States, the EU, and China, the primary issues of concern are different. For example, in China, a survey released in 2019 by the Nandu Personal Information Protection Research Center found that 74% of respondents said they wanted the option to be able to use traditional ID methods over the tech to verify their identity (Shead, 2019). Respondents were also concerned about biometric data being hacked or otherwise leaked, and approximately 80% of respondents were worried that facial recognition operators had lax security measures. This shows a lack of faith in corporations and concern towards the application of technology for commercial purposes, but there is significantly less backlash against the government itself, which had already implemented widespread facial recognition systems. In the United States and the EU, on the other hand, backlash towards facial recognition comes in the form of accuracy concerns. A December 2019 National Institute of Standards and Technology (NIST) study evaluated the effects of factors such as race and sex on facial recognition software. The study analyzed 189 facial recognition algorithms from 99 developers, using collections of photographs with approximately 18 million images of eight million people pulled from databases provided by the US Department of State, the Department of Homeland Security and the Federal Bureau of Investigation. The study found disproportionately higher false positive rates for African American, Asian and Native American faces for one-to-one matching, and higher rates of false positives for African American females for one-to-many matching (Jehl and Prochaska, 2019). There is also concern about abuse of facial recognition by law enforcement agencies, leading to increased regulatory scrutiny. One example of abuse that was fairly significant was reports about Clearview AI, which counts many law enforcement agencies as clients, was found to have amassed more than three billion images scraped from publicly available social media websites. The company was allegedly collecting data without notice or consent. A study conducted in the United Kingdom, found that there was an almost 50/50 split between acceptance and rejection of facial recognition for police use (Bradford, Yesberg, Jackson and Dawson, 2020). These concerns raised indicate a lack of faith in governmental and law enforcement organizations as well as corporations, and demonstrate how the individuals have the largest influence in the power hierarchy in these regions.

## Ethical Framework

The development of facial recognition technology in recent years has enabled many other technologies and industries to develop through its usage, from new methods of identification for personal electronic devices to targeted commercial applications, and national security applications. However, the growth and development of this technology is definitely not without ethical concerns.  Facial recognition software's capabilities have expanded greatly in recent years, bringing with it many controversies in terms of its applications. Due to the fact that this technology has the ability to influence the lives of billions of individuals around the word, an ethical analysis of the technology's development, distribution, and application would help us see the nuances and intricacies behind this technology.

An ethical framework that could be used to analyze the aspects of facial recognition technology would be the technological mediation framework. While at first glance it may seem that the ethical issues surrounding facial recognition technology have more to do with the individuals, corporations, and governmental organizations that utilize this technology, it could be argued that there is no pure autonomy, and that facial recognition technology is not a neutral intermediary between different stakeholders, but can act as active mediators that can shape the relationship between these different groups. In fact, development of facial recognition technology can be considered as a feedback loop influenced by similar technologies, designers, and users. The designers of the technology might have a different purpose from the user of the technology, or the technology itself, so different interpretations and actions regarding the technology may raise different forms of moral engagement and responsibility. Interpretations include the government's duty in using of the technology to provide safety and security for individuals while not jeopardizing the privacy of said individuals. In the case of facial recognition technology, the values of privacy in terms of trust, control, and security are mediated by the system among users, designers, and technology. In the U.S. and the E.U., the reality about privacy and security is interpreted as a constantly changing boundary between privacy, day-to-day convenience, and even national security, causing changes in the development and actions using the technology. This idea of privacy can be thought of as a mediated reality constructed by the different groups with a vested interest in the technology, where each participating group has their share of responsibility in how the technology is shaped. Individuals in the U.S. and the E.U. mediate the technology through voicing their opinions by selecting the representatives with similar ideas and beliefs, as well as through outright protests against certain regulations or applications of facial recognition technology that poses ethical concerns, such as issues with the algorithms themselves or the application of the technology without consent (Jehl and Prochaska, 2019).

With this technology, designers have the ability build moral values and more commitment into the technology itself to prevent misuse and abuse of facial recognition that could jeopardize the safety and freedom of many individuals. However, these designers are also constrained by parties that provide funding to enable the technology's development, such as corporations and governments. This influence can be seen from the very first emergence of the technology, as the very first facial recognition project initiated in 1964 was funded by an undisclosed intelligence agency for the purposes of surveillance. In recent times, funding for further development of facial recognition algorithms come from corporations for the purposes of streamlining daily human machine-interactions in order to increase commercial revenue. These corporations and governments can then be influenced by the people onto which the technology is applied, so all three parties have a share of responsibility in the moral development of the technology.

Another ethical framework that could be applied in the analysis of facial recognition technology would be political-social-cultural roots of engineering ethics. In different regions around the world with different socio-political and cultural backgrounds, facial recognition technology's applications and developments, as well as regulations or public perception regarding the technology can be drastically different. In the United States, where individualism and private interest are prized concepts, various applications of facial recognition technologies by governments and commercial corporations have received several knockbacks by the individuals affected by the technology. Various privacy concerns have been raised, and the amount of public trust in the government's moral responsibility to utilize the technology properly is constantly fluctuating. Skepticism of various new technologies is widespread, with some individuals valuing the convenience, through facilitation of daily activities, and safety provided by the technology while others state the possible consequences of unregulated or underregulating of the technology, which could lead to abuse. Meanwhile, in countries like China, where collectivism is more prominent, widespread implementation of the technology is more possible, and by recent times, the technology has already become a prominent part of society and people's daily lives. With public benefit more valued over private interests, application of facial recognition for identification and national security influences the entire population, allowing for more effective leveraging of the technology, as demonstrated by China's efficient countrywide comprehensive facial recognition system (Thales Group, 2020).

## Conclusion

The propagation of facial recognition software in recent times has led to many sociopolitical changes in regards to its organization and decision making everywhere around the world. In regions like the U.S. and the E.U., decision making power on the development and usage of the technology has shifted from governments to now incorporate a large number of stakeholders, including companies as well as individuals. With the technology being commonly seen and utilized in daily life, many individuals have become aware of the possible risks and implications of the development of such a technology. One party no longer has absolute authority over deployment of such software, and many concerns have been raised towards current applications of the technology. The ethics of facial recognition technology have been considered in a diverse variety of different fields and professions. Ethical issues posed in the context of facial recognition for national security mainly revolve around violation of privacy, or the lack of detailed legal guidelines regarding implementation of the technology. Ethical concerns regarding the burgeoning integration of facial recognition and facial detection into compulsory schooling include issues of diminished accountability, compromised civil rights, and limitations on the concentration of power, foregrounding of gender and race, dehumanization of schooling, increased authoritarian nature of schooling, and possible oppression of marginalized groups (Andrejevic and Selwyn, 2019). In fields such as healthcare, the use of facial recognition suggests the importance of informed consent, data input and analysis quality, effective communication about incidental findings, and potential influence on patient-clinician relationships, privacy and data protection (Martinez-Martin, 2019).

In many regions around the world, this is a critical time in terms of deciding how much should the technology be used for various purposes, as well as how to prevent abuse of the technology and balancing the potential benefits with potential harms. With this in mind, each of the regions examined in this study are determining this balance in their own way, based on sociopolitical and cultural factors and the power hierarchy between groups inherent in each region. In China, the central government has the largest influence on development and integration of facial recognition into different aspects of daily lives, while individuals are in that position of power in the U.S. and E.U. The decisions made as a result of the influence of these groups and various internal and external factors will have a significant impact and could majorly reconfigure social relationships and power between individuals, individuals, and corporations moving forward.

## References

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

Bowyer, K., 2004. Face recognition technology: security versus privacy. *IEEE Technology and Society Magazine*, [online] 23(1), pp.9-19. Available at: <https://ieeexplore.ieee.org/abstract/document/1273467> [Accessed 23 October 2020].

Bradford, B., Yesberg, J., Jackson, J. and Dawson, P., 2020. Live Facial Recognition: Trust and Legitimacy as Predictors of Public Support for Police Use of New Technology. *The British Journal of Criminology*, [online] 60(6), pp.1502-1522. Available at: <https://academic.oup.com/bjc/article-abstract/60/6/1502/5843315> [Accessed 25 October 2020].

Gates, K., 2011. *Our Biometric Future: Facial Recognition Technology And The Culture Of Surveillance*. New York: New York University Press.

Harwell, D., 2020. *Unproven Facial-Recognition Companies Target Schools, Promising An End To Shootings*.. [online] Washington Post. Available at: <https://www.washingtonpost.com/business/economy/unproven-facial-recognition-companies-target-schools-promising-an-end-to-shootings/2018/06/07/1e9e6d52-68db-11e8-9e38-24e693b38637_story.html> [Accessed 23 October 2020].

Introna, L., 2005. Disclosive Ethics and Information Technology: Disclosing Facial Recognition Systems. *Ethics and Information Technology*, [online] 7(2), pp.75-86. Available at: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.874.1450&rep=rep1&type=pdf> [Accessed 25 October 2020].

Jehl, L. and Prochaska, K., 2020. Public Backlash Calls Use Of Facial Recognition Systems Into Question. *The National Law Review*, [online] (299). Available at: <https://www.natlawreview.com/article/public-backlash-calls-use-facial-recognition-systems-question> [Accessed 23 October 2020].

Martinez-Martin, N., 2019. What Are Important Ethical Implications of Using Facial Recognition Technology in Health Care?. *AMA Journal of Ethics*, 21(2), pp.E180-187.

MIT Technology Review. 2017. *The EU Might Ban Facial Recognition In Public For Five Years*. [online] Available at: <https://www.technologyreview.com/2020/01/17/238092/facial-recognition-european-union-temporary-ban-privacy-ethics-regulation/> [Accessed 23 October 2020].

Pernot-Leplay, E., 2020. EU Influence on Data Privacy Laws: Is the U.S. Approach Converging with the EU Model?. *Colorado Technology Law Journal*, [online] 18(1). Available at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3542730#references-widget> [Accessed 23 October 2020].

Shead, S., 2019. *Chinese Residents Worry About Rise Of Facial Recognition*. [online] BBC News. Available at: <https://www.bbc.com/news/technology-50674909> [Accessed 23 October 2020].

Simonite, T. (2020, November 23). Congress Is Eyeing Face Recognition, and Companies Want a Say. Wired. https://www.wired.com/story/congress-eyeing-face-recognition-companies-want-say/.

Smith, A., 2019. *More Than Half Of U.S. Adults Trust Law Enforcement To Use Facial Recognition Responsibly*. [online] Pew Research Center: Internet, Science & Tech.

Available at: <https://www.pewresearch.org/internet/2019/09/05/more-than-half-of-u-s-adults-trust-law-enforcement-to-use-facial-recognition-responsibly/> [Accessed 23 October 2020].

Thalesgroup.com. 2020. *Facial Recognition In 2020 (7 Trends To Watch)*. [online] Available at: <https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/facial-recognition