US-China Law Review, June 2022, Vol. 19, No. 6, 259-266
doi:10.17265/1548-6605/2022.06.002

Legal Regulation of Government Applications of Facial Recognition Technology: A Comparison of Two Approaches

WANG Geng
University of International Business and Economics, Beijing, China
ZHANG Chaolin
Nankai University, Tianjin, China

Facial recognition technology is widely used due to its irreplaceable advantages, providing technical support for the intelligent transformation of government social governance. However, in recent years, the complaints about facial recognition technology have been getting louder. In addition to some shortcomings of the technology itself, people are more concerned about the threats and challenges to personal privacy and personal information security brought about by the application of facial recognition technology. In particular, the unrestricted use of facial recognition technology by government agencies will expand public power, breaking the balance between public power and private rights. At the moment, two approaches have been developed to address this challenge: one is the technology restriction approach used by countries represented by the United States, which explicitly states that facial recognition technology should not be used in general and should only be used in a small number of licensed or special cases; the other is the data protection approach used by China and the European Union, which is based on the theory of technology neutrality but requires that technology be used in accordance with personal information and data processing rules. Although the approaches used by different countries differ, they all reflect the same attitude and position, namely, that the exercise of public power is not disorderly, and that the use of facial recognition technology by government agencies must adhere to corresponding norms.

Keywords: facial recognition technology, privacy, personal data protection, technological neutrality

Introduction

George Orwell (2021) once wrote in his famous novel, *1984*, that

> Any sound that Winston made, above the level of a very low whisper, would be picked up by it, moreover, so long as he remained within the field of vision which the metal plaque commanded, he could be seen as well as heard. (p. 5)

Today, with the widespread use of facial recognition technology, this seems to have actually happened.

Facial recognition technology is a biometric technology that identifies individuals based on their facial features. This technology is more secure and acceptable than other forms of identification. This technology is preferred because it is more secure and acceptable than other identification technologies (Kaur, Krishan,

WANG Geng, Ph.D. student, Law School, University of International Business and Economics, Beijing, China.
ZHANG Chaolin, Ph.D. student, Law School, Nankai University, Tianjin, China.

Sharma, & Kanchan, 2020, pp. 131-132), and it can interact with other technologies for a wide range of applications (Schwartz, Guo, & Davis, 2010, pp. 476-477). Some websites will use facial recognition technology to verify user identities, and some shopping malls will use it for safety prevention and control, as well as passenger flow analysis. Aside from commercial applications, government agencies frequently use it for social security management, such as investigating and arresting suspects, managing the entry and exit of key units such as prisons, and even traffic police departments use it to manage pedestrians who run red lights.

However, the overuse of facial recognition technology has sparked widespread concern among the public. They believe that government agencies' misuse of facial recognition technology endangers personal privacy and information security. In the United Kingdom, a citizen named Edward Bridges has filed a lawsuit against South Wales Police, which deployed the facial recognition cameras.[1] Bridges claimed that two facial recognition cameras in the commercial shopping street and the exhibition hall filmed him without his permission, infringing on his personal rights. In Sweden, a similar situation occurred. The Skelleftea municipality was fined by the Swedish Data Protection Authority because Anderstorp's High School in Skelleftea used facial recognition technology to track students' attendance and absence (BBC News, 2022). In China, the use of facial recognition technology by traffic police to expose red-light runners has also been hotly debated (Liu, 2017). The US Government Accountability Office even released a 90-page report detailing the use of facial recognition technology by federal agencies in response to public inquiries (Ryan-Mosley, 2021). Thus, these countries have enacted legislation to govern the use of facial recognition technology and to coordinate the relationship between the exercise of public power and the protection of individual private rights. However, the methods of regulation differ from one country to the next. This article proceeds in three parts. Part II describes how government agencies' use of facial recognition technology affects individual rights and freedoms, Part III compares regulatory approaches in the United States, the European Union, and China, and Part IV concludes.

The Impact of Facial Recognition Technology on Personal Information and Privacy

Modern privacy scholarship began in 1890 (McClurg, 2007, p. 1875), and Samuel Warren and Louis Brandeis (1890) defined privacy as the "right to be let alone" (p. 193). According to them, this right is not absolute, and if a person exposes his privacy to the general public, or if the privacy involves the public or general interest, he will lose this right. However, as surveillance and camera technology became more widely available, this viewpoint was challenged (Rothenberg, 2000, p. 1158). In *Daily Times Democrat v. Graham*[2], the court in the US recognized the existence of privacy in public places. The plaintiff in the case, a housewife, had her dress blown up by a gust of air while exiting a fun house at a county fair. A cameraman captured the scene and photographed it, which was then published in a local newspaper. Even though the photograph was taken in a public place, the court determined that it violated the plaintiff's right to privacy. The idea that privacy exists in public places forms the theoretical basis for protecting the privacy of individuals under the applications of facial recognition technology. Although the face is exposed, it is a central and prominent place

[1] The Queen (on application of Edward Bridges) v. The Chief Constable of South Wales Police, Secretary of State for the Home Department, Information Commissioner, Surveillance Camera Commissioner [2019] EWHC 2341 (Admin).
[2] Daily Times Democrat v. Graham, 276 Ala. 380, 162 So. 2d 474, 1964 Ala. LEXIS 351 (Ala. Sup. Ct. 1964).

for identity, an image of the person, and "the window to the soul" in cultural conceptions (Wright, 2018, pp. 619-620). Others can probe individuals' inner worlds through human faces, which people do not want outsiders to see.

Personal data protection is closely related to the right to privacy. It has been debated whether personal data protection can become an independent right. Personal data protection is a product of the development of the information society. Telecommunications, advanced transportation systems, and the evolution of the Internet have accelerated the rate of information generation and the proliferation of technologies capable of collecting, analyzing, and disseminating personal information, posing challenges to traditional privacy protection (Banisar & Davies, 1999, p. 4). In some countries, such as the United States, the concept of "privacy" has been expanded to include the protection of personal information and data as part of the right to privacy. The *Privacy Act of 1974* provides for the protection of records maintained on individuals. The term "record" means any item, collection or grouping of information about an individual that is maintained by the departments, which includes personally identifiable information such as fingerprints, voice prints, or photographs. In the European Union, on the other hand, a new right has been created directly. *The Charter of Fundamental Rights of the European Union* (hereinafter referred to as *The Charter*), which entered into force in 2009, sets out the right to privacy and the protection of personal data in Articles 7 and 8 respectively.[3] In *Tele2 Sverige AB v. Post-och Telestyrelsen*[4], the Court of Justice of the European Union made it clear that Article 8 of *the Charter* relates to a fundamental right which is distinct from the rights set out in Article 7 of *The Charter* and which has no equivalent in *The European Convention on Human Rights*. The rules of the *Chinese Civil Code* are similar, with separate articles addressing the right to privacy and the protection of personal information and data.[5] From a normative standpoint, the European Union and China generally regard the right to privacy and the right to personal information and data protection as two different rights. The former is more "classical", while the latter is more "modern" (European Union Agency for Fundamental Rights, 2019). Privacy and personal information are intertwined, with overlaps and differences (Zhang, 2015, p. 39). The two rights are inextricably linked in that they strive to protect similar values, human dignity, and personal autonomy, by providing each person with an independent personal sphere in which to develop their personalities, think, and shape their own opinions (European Union Agency for Fundamental Rights, 2019).

With the widespread use of facial recognition technology, the boundaries between the personal and public spheres are easily breached. Face information can be collected easily because the technology used to capture faces is undetectable when users are recognized, and the results are highly accurate. Furthermore, facial recognition technology's high scalability accelerates the flow of face information and the re-mining of its value. While a single face can be used to identify and locate a person, hundreds or thousands of such faces can be used to map the person's trajectory and behavioral preferences, as well as predict his or her next steps. As a result,

[3] Article 7 of *The Charter* stipulates that: "Everyone has the right to respect for his or her private and family life, home and communications." Article 8 (1) of *The Charter* stipulates that: "Everyone has the right to the protection of personal data concerning him or her."

[4] Tele2 Sverige AB v. Post-och Telestyrelsen, Case C-203/15, ECLI:EU:C:2016:970, (CJEU 2016). Judgement of 21 Dec. 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62015CJ0203.

[5] Chapter VI of the *Chinese Civil Code* is titled "Right to privacy and protection of personal information", and in this chapter Article 1032 stipulates that natural persons have the right to privacy, while Article 1034 stipulates that natural persons' personal information is protected by law.

unauthorized use of facial recognition technology may violate both the right to privacy and the protection of personal information and data.

Two Approaches: Technical Restriction Approach and Data Protection Approach

At the moment, there are two approaches for balancing the relationship between public power and private rights and addressing the impact of facial recognition technology on privacy as well as personal information and data: the first is to directly restrict the use of facial recognition technology, and the second is to strengthen the supervision of face information and, thus, indirectly reduce the abuse of facial recognition technology.

Technical Restriction Approach

Many states in the United States have taken the first approach, enacting legislation to limit the scope of facial recognition technology. According to Maine revised statutes, facial recognition technology may only be used in the investigation of serious crimes, to assist in the identification of people who are deceased or believed to be deceased, as well as missing or endangered people, for prison management, or for some user authentication.[6] Virginia Code indicates that local law enforcement agencies are not permitted to purchase or deploy facial recognition technology unless expressly authorized by law.[7] Similar laws exist in Washington, D.C. and Utah. In Washington, D.C., state or local government agencies are generally prohibited from using facial recognition services to engage in ongoing surveillance, conduct real-time or near real-time identification, or start persistent tracking unless authorized by administrative or court order or in an emergency.[8] Utah strictly restricts the subjects who use facial recognition technology and process face information.[9] Utah has established the state's only department authorized to use a facial recognition system to conduct a facial recognition comparison on an image database. According to Utah Code, only law enforcement agencies that exist to prevent, detect, or prosecute crime, as well as to enforce criminal statutes or ordinances may make a request for this government. In some parts of the United States, facial recognition technology is outright prohibited. In 2019, California, for example, enacted a three-year ban on law enforcement agencies using facial recognition technology in officer cameras.[10] The ban will be lifted on January 1, 2023.

In the United States, government agencies' unreasonable use of facial recognition technology may violate *The Fourth Amendment to the United States Constitution*. The fundamental purpose of *The Fourth Amendment* is to protect the privacy and security of individuals from arbitrary intrusion by government agencies[11], and technological advances may increase the possibility of unreasonable intrusion into individual privacy[12]. In *United States v. Jones* (2012)[13], a majority of the Supreme Court held that the placement of a GPS device on a

---

[6] Section 6001, Facial surveillance, https://legislature.maine.gov/statutes//25/title25sec6001.html.
[7] Section 15.2-1723.2 and Section 23.1-815.1 of Virginia Code, https://lis.virginia.gov/cgi-bin/legp604.exe?212+ful+HB2031ER+hil.
[8] Washington Code 43.386.080, Use for surveillance, real-time identification, or persistent tracking—When permitted—Restrictions on law enforcement use, https://app.leg.wa.gov/RCW/default.aspx?cite=43.386.080.
[9] Chapter 23e of Utah Code, Government Use of Facial Recognition Technology, https://le.utah.gov/xcode/Title77/Chapter23E/C77-23e_2021050520210505.pdf.
[10] AB-1215 law enforcement: Facial recognition and other biometric surveillance, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB1215.
[11] Michigan v. Tyler, 436 U.S. 499, 98 S. Ct. 1942, 56 L. Ed. 2d 486, 1978 U.S. LEXIS 97 (1978).
[12] Patel v. Facebook, Inc., 932 F.3d 1264 (9th Cir. 2019).
[13] United States v. Jones, 565 U.S. 400 (2012).

suspect's vehicle to monitor the vehicle's movements constituted a search under *the Fourth Amendment*. In this case, justice Sotomayor, in particular, emphasized the potential risks of government access to personal information, arguing that the government's unrestrained power to assemble data revealing the privacy of identities could be easily abused (United States v. Jones, 2012). Government uses of facial recognition technology are considered more coercive and surreptitious than commercial ones, and may have more serious consequences (Barrett, 2020, p. 236). Moreover, the government's widespread use of facial recognition technology is seen as potentially upending the existing power relationship between the government and the people (Ferguson, 2020, p. 1107). Thanks to sensitive technology, the government has gained greater authority to conduct surveillance.

Overall, the United States is more concerned about the dangers posed by government agencies' use of facial recognition technology, believing that not only is the information generated by the technology sensitive, but that the technology itself will pose significant risks, and thus tends to regulate the technology directly in order to adequately curb the damage caused by this particular technology.

Data Protection Approach

The second approach, which is primarily used by China and the European Union, is based on an implicit belief in technological neutrality. The term, technology neutrality, is used in a variety of contexts, resulting in multiple layers of meaning. In the field of intellectual property law and international trade, for example, technology neutrality is used to address the challenge posed by new technologies to the old regime, with the technology-neutral view that the application of new technologies has no effect on the application of the old regime (Kwak, 2022, p. 3; Siu, 2013, p. 80). Technology neutrality gives courts the flexibility to apply existing laws to new technologies while avoiding discrimination against new technologies and preventing technologies unrelated to the law's purpose from interfering with the law (Siu, 2013, p. 80). In addition, the concept of "net neutrality" is derived from technology neutrality. Net neutrality requires broadband providers to not treat different users differently when it comes to broadband usage (Wu, 2003, p. 168). The concept of technology neutrality we use is slightly different from the previous ones. We consider how laws that have a direct impact on technology should be designed. Roughly speaking, technology neutrality in law is the idea that the law should not determine the winners and losers of technology, that the law should neither help nor hinder specific types of technology and their applications, and that the law should be framed in terms of function and values rather than the technology itself (Thompson, 2012, pp. 303, 307). Therefore, from a technology-neutral standpoint, it is not reasonable to introduce laws that specifically prohibit or restrict facial recognition technology.

Technology neutrality does not preclude the law from regulating technology. Indeed, given that facial recognition technology is a double-edged sword, China and the European Union have imposed restrictions on the flow of information and data in order to mitigate the risks it poses.

The use of technology to collect information and data by Chinese government agencies is governed by a number of laws, including *The Chinese Civil Code*, *The Cyber Security Law*, *The Anti-Terrorism Law*, *The Data Security Law*, and *The Personal Information Protection Law*. The basis for the protection of personal rights is provided by Chapter VI of *The Chinese Civil Code*, titled "Right to privacy and protection of personal information". *The Personal Information Protection Law*, which goes into effect in 2021, expands on the rules

of personal information protection by laying out the principles and specific norms that information processors must follow when processing personal information. According to this law, government agencies must follow the authority and procedures outlined in laws and administrative regulations, and they must not go beyond the scope and limits required to carry out their legal responsibilities. Unless there are special circumstances provided for by law, the use of facial recognition technology to process such sensitive personal information requires the data subject's separate consent or written consent.

Similar provisions have been made in the European Union regarding the processing of facial information in the context of criminal law enforcement. In 2016, the European Parliament and the Council of the European Union enacted *Direct (EU) 2016/680*[14] to protect natural persons' rights and ensure the free movement of data when personal data are processed by competent authorities for the purposes of preventing, investigating, detecting, or prosecuting criminal offences or enforcing criminal penalties. According to this rule, processing of face information as biometric data that uniquely identifies a natural person is only permitted when absolutely necessary, such as when authorized by European Union or Member State law, to protect the data subject's or other natural persons' vital interests, or to process data that are clearly publicly available to the data subject[15]. Besides, in May of this year, the European Data Protection Board (hereinafter referred to as "EDPB") issued *Guidelines 05/2022 on the Use of Facial Recognition Technology in the Area of Law Enforcement*[16]. EDPB Chair, Andrea Jelinek said that while modern technology is beneficial to law enforcement, the use of facial recognition technology must satisfy the requirements of necessity and proportionality (European Data Protection Board, 2022).

Commonalities and Differences

In contrast to commercial applications, the use of facial recognition technology in government social administration is likely to pose a greater threat to individual rights and freedoms. With these considerations in mind, the United States, China, and the European Union have all chosen to tighten government regulation on the use of facial recognition technology. However, the United States' attitude toward facial recognition technology differs to that of China and the European Union, which has a direct impact on the regulatory approaches chosen by these countries.

In the United States, facial recognition technology is viewed as a potentially dangerous artificial intelligence technology, with a number of state laws stating that special permission is required for its use, whereas in China and Europe, despite the heated debate over facial recognition technology, legislation is not required to impose special restrictions on this technology, given that it is a double-edged sword. However, China and Europe have not abandoned legal regulation of government agencies' use of facial recognition technology, but instead have taken an indirect approach by requiring government agencies to follow certain procedures when processing sensitive information such as face information. Furthermore, the focus of the two

[14] The European Parliament and the Council of the European Union, *Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680#d1e937-89-1.

[15] Article 10 of *Direct (EU) 2016/680*.

[16] The European Data Protection Board, *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement*, https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-052022-use-facial-recognition_en.

approaches differs in terms of the rights protected by legislation. The approach taken in China and the European Union is based on the protection of personal information, whereas the emphasis in the United States is on protecting individuals' privacy.

Conclusion

The new round of technological revolution is accelerating humanity's transition from an industrialized society to an information-based society, and new generations of information technology such as artificial intelligence and deep learning are having a significant impact on human production and living. Facial recognition technology, a new artificial intelligence technology, is widely used by government agencies and has sparked debate. While technology is neither good nor bad in and of itself, its misuse may exacerbate the threat to individual rights. If the use of this technology is not properly regulated in the early stages, the Collingridge dilemma may occur.

Nowadays, Government agencies in the United States, the European Union, and China have placed some restrictions on the use of facial recognition technology. The difference is that the United States is more cautious about the use of facial recognition technology by government agencies for law enforcement purposes and has a more negative attitude toward the technology itself, leading many states to outright ban or restrict the use of this technology, with only a few exceptions allowing it to be used by government agencies. China and the European Union, on the other hand, are neutral on facial recognition technology, acknowledging the convenience and efficiency it brings to government agencies' law enforcement activities while also being aware of the threat it poses to individuals' rights and freedoms. They do not impose limitations on technology, but rather seek to reduce the threats and challenges by safeguarding personal information and data. Although the choice of various approaches is determined by national circumstances, values, and legal systems, a technology-neutral attitude appears to be more appropriate from the standpoint of development. Technology should not elicit moral judgments of good or evil, and a preoccupation with preventing its development and spread is counterproductive to social progress. Concerns about the government, a powerful user, can be addressed more effectively through a variety of procedural settings. More smart technologies will emerge in the future, impacting modern society's institutions. It would be prudent to approach these technologies with a more open mind, identify the root causes of conflicts and challenges, and then prescribe the appropriate medicine.

References

Banisar, D., & Davies, S. (1999). Global trends in privacy protection: An international survey of privacy, data protection, and surveillance laws and developments. *John Marshall Journal of Information Law, 18*, 1-111.

Barrett, L. (2020). Ban facial recognition technologies for children—And for everyone else. *Boston University Journal of Science & Technology Law, 26*, 223-285.

BBC News. (2022). Facial recognition: School ID checks lead to GDPR fine. Retrieved from https://www.bbc.com/news/technology-49489154

European Data Protection Board. (2022). EDPB adopts guidelines on calculation of fines & guidelines on the use of facial recognition technology in the area of law enforcement. Retrieved from https://edpb.europa.eu/news/news/2022/edpb-adopts-guidelines-calculation-fines-guidelines-use-facial-recognition_en

European Union Agency for Fundamental Rights. (2019). Facial recognition technology: Fundamental rights considerations in the context of law enforcement. Retrieved from https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law

Ferguson, A. G. (2020). Facial recognition and the fourth amendment. *Minnesota Law Review, 105*, 1105-1210.

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. Retrieved from https://doi.org/10.1177/0025802419893168

Kwak, D. (2022). No more strategical neutrality on technological neutrality: Technological neutrality as a bridge between the analogue trading regime and digital trade. *World Trade Review, 21*(1), 18-32.

Liu, Y. (2017). How to solve the deadly knot of "Chinese style crossing". *People's Daily Online.* Retrieved from http://world.people.com.cn/n1/2017/0626/c1002-29362427.html

McClurg, A. J. (2007). In the face of danger: Facial recognition and the limits of privacy law. *Harvard Law Review, 120*(7), 1870-1891.

Orwell, G. (2021). *Nineteen eighty-four*. London: Penguin Classics.

Rothenberg, L. E. (2000). Re-thinking privacy: Peeping toms, video voyeurs, and the failure of criminal law to recognize reasonable expectation of privacy in the public space. *American University Law Review, 49*(5), 1127-1166.

Ryan-Mosley, T. (2021). US government agencies plan to increase their use of facial recognition technology. *MIT Technology Review.* Retrieved from https://www.technologyreview.com/2021/08/24/1032967/us-government-agencies-plan-to-increase-their-use-of-facial-recognition-technology/

Schwartz, W. R., Guo, H., & Davis, L. S. (2010). A robust and scalable approach to face identification. In K. Daniilidis, P. Maragos, and N. Paragios (Eds.), *Computer vision—ECCV 2010. ECCV 2010. Lecture notes in computer science* (Vol. 6316). Berlin, Heidelberg: Springer. Retrieved from https://doi.org/10.1007/978-3-642-15567-3_35

Siu, K. P. (2013). Technological neutrality: Toward copyright convergence in the digital age. *University of Toronto Faculty of Law Review, 71*, 76-112.

Thompson, M. (2012). The neutralization of harmony: The problem of technological neutrality, east and west. *Boston University Journal of Science & Technology Law, 18*, 303-342.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review, 4*, 193-220.

Wright, E. (2018). The future of facial recognition is not fully known: Developing privacy and security regulatory mechanisms for facial recognition in the retail sector. *Fordham Intellectual Property, Media and Entertainment Law Journal, 29*, 611-684.

Wu, T. (2003). Network neutrality, broadband discrimination. *Journal on Telecommunications and High Technology Law, 2*, 141-179.

Zhang, X. (2015). From privacy to personal information: The theory of interest remeasurement and institutional arrangement. *China Legal Science, 3*, 38-59. doi:10.14111/j.cnki.zgfx.2015.03.003