3-27-2023

Facial Recognition Law: Why Should We Care?

Xueyang Peng
Cardozo International & Comparative Law Review, xpeng@law.cardozo.yu.edu

CICLR Mar 27 5 min read

Facial Recognition Law: Why Should We Care?

By: Xueyang Peng

What if you are a lawyer and you would like to spend an evening enjoying your favorite artist's concert at the Radio City Music Hall? Or a Knicks game at Madison Square Garden? The first thing you should check is not the ticket price, but rather whether you, or your law firm, has made the MSG blacklist. Even though for years, the owner of MSG has been using the blacklist to exclude its enemies (and their associates) from setting foot in any MSG-owned venue, the facial recognition technology ("FRT") just brought this practice to a new level.[1]

The FRT generally works in three steps: detection, analysis, and recognition.[2] Surveillance camera uses computer vision to detect people in images with much greater speed, accuracy, and efficiency than human levels. Then, artificial intelligence analyzes the image by mapping face geometry and facial landmarks, which are key to distinguishing a face from other objects. Finally, the FRT identifies a person by comparing the faces in more images and assessing the likelihood of a face match.[3] Therefore, MSG's use of the FRT is extremely effective in enforcing the blacklist to keep its enemies at bay.

While it is difficult to be sympathetic when lawyers are being bullied by a corporation, the chilling effects of the FRT's invasiveness are alarming. Lawmakers around the world are struggling to match the widespread use of the FRT. This article will examine the current facial recognition-related biometric legal frameworks in China and the US, and the implications on their respective societies.

China's Approach

China's facial recognition law based its source on a few authorities, including the Civil Code, Cybersecurity Law, Court Opinion, etc. In 2021, China's Supreme People's Court published the "Provisions on Relevant Issues on the Application of Laws in Hearing Civil Cases Related to the Application of Facial Recognition Technology in Processing Personal Information" ("Provisions").[4] The Provisions clarify that "facial information" is "biometric information,"[5] which is "sensitive personal information" for the purpose of the Personal Information Protection Law.[6]

The Provisions apply to civil cases arising from information handlers' use of FRT to process biometric information generated based on the FRT in violation of laws.[7] However, since the Provisions do not define "handlers," the collective regulations seem to only regulate private businesses but leave out law enforcement and other governmental entities. As a result, China uses FRT extensively, from accessing the Health Code during the zero-Covid policy era to the pervasive surveillance networks – SkyNet.[8] This ambiguity led some scholars to go so far in suggesting that China does not have a facial recognition law.[9]

This article does not purport to settle the debate over China's controversial use of FRT. However, this article highlights that in the absence of strict and clear regulations, the use of FRT will be abused.

The US Approach

While numerous bills have been proposed, there is currently no federal law regulating the FRT in the US.[10] Moreover, only two states passed laws to effectively protect people's biometric information being collected through the FRT – Illinois and Texas.[11]

In 2008, Illinois enacted Biometric Information Privacy Act (BIPA), which restricts how private entities collect, retain, disclose, and destroy biometric identifiers.[12] BIPA defines biometric identifiers to include retina or iris scans, fingerprints, voiceprints, and hand/face geometry scans.[13] BIPA requires informed consent and notice prior to collection, permits a limited right to disclosure, and mandates protection obligations and retention guidelines.[14] Illinois is the only state that allows a private cause of action for individuals harmed by BIPA violations.[15]

In 2009, Texas enacted the Capture or Use of Biometric Identifier Act (CUBI) to regulate the capture, possession, sharing and retention of biometric identifiers.[16] For the purpose of regulating the FRT, CUBI is similar to BIPA in many aspects: CUBI defines biometric identifiers to include record of hand or face geometry;[17] CUBI prohibits organizations from capturing biometric identifiers for a commercial purpose unless they provide notice and obtain consent from the affected individual.[18] The most significant difference is that CUBI does not create a private cause of action for the violation.

Other jurisdictions like New York also have laws regulating biometric identifiers, which include scans of face geometry.[19] However, these laws do not require private companies to obtain consent from affected individuals. Instead, a clear and conspicuous sign notifying people that their biometric identifier information is being collected, retained, and shared satisfies the requirement.[20]

Unsurprisingly, according to a report from the New York Times, MSG's FRT-Blacklist practice can be found anywhere in the US where MSG has a venue, except Illinois and Texas.[21]

Conclusion

From corporations' use of FRT to settle personal grudges to law enforcement's use of FRT to surveil the public, the lack of effective legal frameworks to match the ever-changing technology invites the abuse of power.

In proposing and adopting federal or state laws on facial recognition, the US policymaker should consider the relevant regulations in the EU. The EU has recognized that the use of FRT has impacts on human's fundamental rights and freedoms that may go beyond privacy and data protection.[22] While having strict regulations on FRT in place, the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) jointly proposed a categorical ban on the FRT for remote identification in public places.[23]

Xueyang Peng is a Staff Editor at CICLR.

[1] Kashmir Hill & Corey Kilgannon, *Madison Square Garden Uses Facial Recognition to Ban its Owner's Enemies*, N. Y. Times (Dec. 22, 2022), https://www.nytimes.com/2022/12/22/nyregion/madison-square-garden-facial-recognition.html [https://perma.cc/B528-V8KN].
[2] *What is Facial Recognition*?,Amazon Web Serv., https://aws.amazon.com/what-is/facial-recognition/ [https://perma.cc/DTN7-6L5V] (last visited Feb. 5, 2023).
[3] *Id.*
[4] Zuigao Renmin Fayuan Guanyu Shenli Shiyong Renllian Shibie Jishu Chuli Geren Xinxi Xiangguan Minshi Anjian Shiyong Falù Ruogan Wentide Guiding（最高人民法院关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定，法释【2021】15号）[Provisions on Relevant Issues on the Application of Laws in Hearing Civil Cases Related to the Application of Facial Recognition Technology in Processing Personal Information, No.15 [2021]] [hereinafter *Provisions*] (promulgated by the Judicial Comm. Sup. People's Ct., July 28, 2021) Sup. People's Ct. Gaz., July 28, 2021, https://www.court.gov.cn/fabu-xiangqing-315851.html (China).
[5] *Id.*
[6] Zhonghua Renmin Gongheguo Geren Xinxi Baohufa（中华人民共和国个人信息保护法）[Personal Information Protection Law of the People's Republic of China], Standing Comm. Nat'l People's Cong. Gaz.. Aug, 20, 2021, http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml.
[7] *Provisions*, supra note 4.
[8] *See generally* Dahlia Peterson, *China's "Sharp Eyes" Program Aims to Surveil 100% of Public Space*, CSET Georgetown Univ. (Mar. 2, 2021), https://cset.georgetown.edu/article/chinas-sharp-eyes-program-aims-to-surveil-100-of-public-space/.
[9] *See e.g.,* Zhaohui Su, Ali Cheshmehzangi, Dean McDonnell, Barry L. Bently, Claudima Pereira da Veiga, & Yu-Tao Xiang*, Facial Recognition Law in China*, Nat'l Libr. Med. (Apr. 5, 2022).
[10] E. B. Keener, *Facial Recognition: A New Trend in State Regulation*, Womble Bond Dickinson (Apr. 29, 2022), https://www.womblebonddickinson.com/us/insights/alerts/facial-recognition-new-trend-state-regulation.
[11] *Id.*
[12] Biometric Information Privacy Act, 740 ILCS 14.
[13] *Id*.
[14] *Id.*
[15] *Id.*
[16] Texas Capture or Use of Biometric Identifier Act, Bus & Com § 503.001.
[17] *Id.*
[18] *Id.*
[19] Biometric Identifier Information Law, NYC Admin. Code §§ 22-1201 – 1205.
[20] *Id.*
[21] *See* Hill & Killgannon, *supra* note 1.
[22] Frank Hersey, *Facial Recognition in Europe: What's Happening and How Can People Be Protected?* Biometric Update (May 17, 2022), https://www.biometricupdate.com/202205/facial-recognition-in-europe-whats-happening-and-how-can-people-be-protected.
[23] The Artificial Intelligence Act, 2021/0106 (COD).