Republic of the Philippines
House of Representatives
Quezon City

EIGHTEENTH CONGRESS
Second Regular Session

House Bill No. 9231

Introduced by REPRESENTATIVE ERIC L. OLIVAREZ

EXPLANATORY NOTE

Facial recognition technology is becoming ubiquitous in society today. This technology uses an image or video of a person to measure the unique features of their face to identify and/or track them. Through this technology, a unique marker can be made for each person which can then identify or determine various information about him or her including his or her behavioral patterns, personal inclinations, location and the time he or she was there. With enough cameras, the majority of a person's day can be recoded without his or her knowledge or consent.

Facial recognition technology allows a person, entity, or device to learn to identify large amounts of people for various intentions, but oftentimes this is used for commercial purposes. The facial recognition technology may be applied to a video footage from everyday security cameras while observing the general public and even to mobile phones to scan for faces when taking a picture. Facial recognition technology is also extensively utilized by the apps that we open and use every day.

The data obtained from the said technology is widely used by commercial entities particularly big corporation to track a consumer's shopping and spending habits, among other things, and it can in turn be sold to other entities for a variety of profit-driven purposes such as targeted marketing and advertising without the knowledge and consent of the consumer.

Worse, the utilization of facial recognition technology and other biometric markers, if left unregulated, can also be used for nefarious purposes. For instance, if the data obtained from such facial recognition technology and other biometric markers were to fall into the wrong hands - whether it is intentional or due to negligence in the storing or handling of data, it could empower a criminal mind to track and spy on persons of interest including high-ranking officials, politicians, and other important public figures.

Having said this, it cannot be refuted that consumers should always have the choice and the right to say “No!” to being subjected to a facial recognition technology and other biometric markers without suffering a denial of service from and/or by a commercial entity, or be penalized or discriminated for their respective choices. It is for this reason that this bill is being proposed. This bill aims to protect, promote, and uphold the right to privacy of the Filipino consumers in the growing world of digital corporatocracy.

ERIC OLIVAREZ

Republic of the Philippines
House of Representatives
Quezon City

EIGHTEENTH CONGRESS
Second Regular Session

House Bill No. 9231

Introduced by REPRESENTATIVE ERIC L. OLIVAREZ

"AN ACT PROHIBITING COMMERCIAL ENTITIES FROM TRACKING OR IDENTIFYING CONSUMERS VIA FACIAL RECOGNITION TECHNOLOGY AND OTHER BIOMETRIC MARKERS WITHOUT THEIR FULL KNOWLEDGE AND EXPRESS CONSENT"

Be it enacted in the Senate and the House of Representatives of the Republic of the Philippines in Congress assembled:

Section 1. *Short Title.* This Act shall be known as the *"Consumers' Protection on Facial Recognition and other Biometric Forms of Tracking Act of 2021"*.

Section 2. *Policy of the State.* It is hereby declared as a policy of the State to protect consumers in the Philippines from unwanted, undisclosed, and unnecessary forms of tracking by use of biometrics by commercial entities.

Section. 3. *Definition of Terms.* For purposes of this Act, the following terms shall mean:

Facial Recognition Technology – Technology used to identify and/or assign an identity to a person through the use of artificial intelligence or machine-learning assisted software that measures facial features from an image or video frame.

Biometric Markers – Data created with the use of artificial intelligence or machine-learning software that is used to identify and/or assign an identity to a person through the measurement of a consumer's physical and physiological traits. For purposes of this Act, this term is used interchangeably with the term "biometrics recognition technology".

Commercial Entities – any corporation, partnership, limited partnership, proprietorship, sole proprietorship, firm, enterprise, franchise, or association that performs a commercial activity, whether for profit or non-profit.

Server – A computer or computer program which manages access to a centralized resource or service in a network

Express Consent – permission granted in explicit and overt form by the consumer after he or she has been fully informed of the existence of a facial recognition system and other forms of biometric markers and the desire of the commercial entity to capture the consumer's biometrics to obtain data, insights, and information for whatever legally permissible purpose.

Encryption – the process of converting information or data into a code not readily readable or comprehensible primarily to prevent unauthorized access.

Unencrypted Format – Data that is readily readable without the use of passwords, keys, codes, or other special protections through the use of software.

Data Breach – A security incident in which information is intentionally or unintentionally released without authorization.

Section. 4. *Prohibition on Facial Recognition and other Forms of Biometric Tracking and Identification without the Consumer's Full Knowledge and Express Consent.* It shall be unlawful for commercial entities to track users by the use of facial recognition or any other forms of biometric markers without the latter's knowledge and express consent.

Section. 5. *Prohibition on Denying Service, or Punishing or Rewarding Consumers Based on their Willingness to be Tracked or Identified via Facial Recognition and Other Biometric Markers.* It shall be unlawful for commercial entities to deny service, or penalize any person who does not consent to the use of facial recognition technology or any other forms of biometric markers, such as de-prioritization in terms of access to service, offering of higher prices, and exclusion

from sale and other promotional events, among other forms of consumer discrimination.

Furthermore, it shall be unlawful for commercial entities to offer any kind of reward or incentive to any person who consents to the use of facial recognition or any other forms of biometric recognition, such as discounts, early access, accumulated points system, among other schemes, devices, strategies or tactics.

Section. 6. *Regulation on Data Generated by Facial Recognition and other Biometric Markers Obtained with the Express Consent of the Consumer.* It shall nonetheless be unlawful for commercial entities to do the following activities on data that they have obtained from the consumer even though said data was obtained with the latter's full knowledge and express consent:

a) Sell, trade, or give another commercial entity the data generated by the use of facial recognition or any other forms of biometric recognition technology.

b) Store data generated by the use of facial recognition or any other forms of biometric recognition technology outside of the Philippines.

c) Store data generated by the use of facial recognition or any other forms of biometric recognition technology in an unencrypted format.

Section. 7. In the event that there is a data breach on a server where a consumer's facial recognition or other forms of biometric recognition data are stored upon their express consent, it shall be the duty of commercial entities to publicly disclose such breach and attempt to contact consumers whose data were potentially compromised.

Section. 8. *Penalty.* Any commercial entity found to be in violation of any provisions of this Act shall be meted out with the following penalties:

1. For the first offense, a fine commensurate to the size and financial standing of the business enterprise and the severity of the violation as determined by the National Privacy Commission.

2. For the second offense, a fine commensurate to the size and financial standing of the business enterprise and the severity of the violation as determined by the National Privacy Commission and two (2) months suspension of business permit or license to operate.

3. For the third and succeeding offenses, revocation of the commercial entity's business permit or license to operate.

Section. 9. *Implementing Rules and Regulations.* The National Privacy Commission (NPC) in consultation with the Department of Information and Communications Technology (DICT) shall, within sixty (60) days from the effectivity of this Act, promulgate the implementing rules and regulations to effectively carry out the provisions of this Act.

Section. 10. *Separability Clause.* If, for any reason, any part, section or provision of this Act is held invalid or unconstitutional, the remaining provisions not affected thereby shall continue to be in force and effect.

Section. 11. *Repealing Clause.* All laws, decrees, executive orders, proclamations, rules and regulations, and other issuances, or part or parts thereof, which are inconsistent with the provisions of this Act are hereby repealed, amended or modified accordingly.

Section. 12. *Effectivity Clause.* This Act shall take effect fifteen (15) days after its publication in the Official Gazette or at least two (2) newspapers of general circulation, whichever comes earlier.

Approved.