Don't You Look Familiar?: Company's Use of Facial Recognition Technology At A Glance

Facial recognition technology uses algorithms that map facial features – such as the distance between a person's eyes, or the width of a person's nose) and compares those features to a database of known individuals. For companies the technology may be used for security (*e.g.*, cameras that "ID" employees or criminals), to market to consumers (*e.g.*, cameras that "ID" particular customers), or to design products that quickly categorize digital media (*e.g.*, photograph sorting).

There is currently no federal statute that expressly regulates private-sector use of facial recognition technology. Nonetheless, the Federal Trade Commission ("FTC"), which has authority to prevent unfair and deceptive practices, has expressed interest in the privacy implications of facial recognition technology, has issued a set of best practices concerning its use, and has investigated companies that it believes violated those recommendations.

Two states have also enacted statutes that govern the technology. Those statutes require that a company (1) notify state residents that the technology is in use, and (2) obtain the consent of those subject to the technology.

The number of years that a company is allowed to keep biometric data under state law after the purpose for which it was collected has expired.*

1

Percentage increase in accuracy of facial recognition algorithms over a three year period.†

30%

Number of public comments received following FTC workshop on facial recognition technology.‡

80

Number of state data breach notification laws that may apply to facial recognition telemetry if lost or stolen.§

5

$5,000 - $25,000

The range of possible fines and damages that could be assessed under state law for each violation of a facial recognition statute.**

* Tex. Bus. & Com. Code § 503.001(b)(3).
† NISTk, Article: Performance of Facial Recognition Software Continues to Improve (June 3, 2014).
‡ See Public Comments, FTC Matter No. P115406.
§ Bryan Cave, Data Breach Notification Survey (2015).
** *See* 740 ILCS 14/20 (1)-(4); Tex. Bus. & Com. Code § 503.001(d).

Global Data Privacy and Security Team

Bryan Cave's Global Data Privacy and Security Team helps clients safely collect, utilize, transfer, and monetize data.

For more Information Contact:

David A. Zetoony
Partner
david.zetoony@bryancave.com
1155 F Street, N.W.
Washington, D.C. 20004
T: 202 508 6000

One Boulder Plaza
1801 13th Street, Suite 300
Boulder, CO 80302-5386
T: 1 303 444 5955

BRYAN CAVE

Practices recommended by the FTC when deploying facial recognition technology:

- ✓ **Security.** Companies should maintain reasonable data security for consumers’ images and facial geometry.
- ✓ **Retention and Disposal.** Companies should establish and maintain appropriate retention and disposal practices for consumers’ images and facial geometry.
- ✓ **Sensitivity of Video-Feed.** Companies should consider the sensitivity of the data that they capture including, specifically, not placing cameras in areas in which consumers would not expect them (e.g., locker rooms, bathrooms, health care facilities, etc.).
- ✓ **Notice.** Companies should provide “clear notice” when facial recognition technology is being utilized.
- ✓ **Opt-in Consent For Materially Different Use**. Companies should obtain consumers’ affirmative express consent if they use an image in a “materially different manner than they represented when they collected the data.
- ✓ **Opt-in Consent For Sharing.** Companies should obtain consumers’ affirmative express consent if they identify anonymous images of a consumer to someone who could not otherwise identify the consumer.