BRYAN CAVE

What to Consider When Using Fingerprint Identification Technology

February 14, 2016

Authors/Presenters

David A. Zetoony

Partner
Boulder, Colorado
david.zetoony@bryancave.com

Fingerprint identification technology uses fingerprints to uniquely identify individuals. The technology has been used by law enforcement agencies for decades, and dozens of statutes regulate when government agencies may collect fingerprints, how they are permitted to use them, and with whom they can be shared.

Advances in fingerprint recognition software have led some private entities to begin using the technology to authenticate consumers. For example, some mobile devices have integrated fingerprint recognition technology to replace, or supplement, passwords or passcodes. Some employers are also using fingerprint recognition technology to increase the accuracy and efficiency of employee timekeeping systems.

There is currently no federal statute that expressly regulates private-sector use of fingerprint recognition software. Nonetheless, the FTC, which has authority to prevent unfair and deceptive practices, may proceed against companies that misrepresent the function of the technology, or how they use, secure, or disclose captured fingerprints or fingerprint geometry.

At least two states have also enacted statutes that govern the technology. Those statutes generally require that if an organization “captures” a fingerprint, it must provide the consumer with notice and obtain their consent. In addition, if an organization stores or “possesses” a fingerprint, then it must limit its disclosure to third parties, enact measures to secure the fingerprint from unauthorized access, and limit its retention of the fingerprint after it is no longer needed. A number of additional states require that if a company collects fingerprints, it take steps to prevent the fingerprint from being acquired when in the process of being destroyed.

Consider the following when using fingerprint identification technology:

1. Data Inventory. If your organization keeps a data inventory or a data map, you should include fingerprints and/or fingerprint geometry in that inventory.

2. Security. Assess the risk that fingerprints and/or fingerprint geometry may be compromised and consider what steps can be reasonably taken to attempt to keep the information secure.

3. Retention and Disposal. Review your retention and disposal practices to see if they specify how long such information should be kept, and how it should be disposed.

4. Notice. Consider providing clear notice to consumers or employees before capturing their fingerprints.

5. Consent. Consider obtaining opt-in consent before capturing or using fingerprints.

6. Sharing. Consider obtaining opt-in consent before sharing fingerprints or fingerprint geometry with any third parties.

The following provides snapshot information concerning fingerprint identification technology.

2,941,036 Number of fingerprints processed by one government agency in a year.[1]	1 in 50,000 Probability of a false match claimed by one mobile device in conjunction with fingerprint recognition software.[2]	$5,000 - $25,000 The range of possible fines and damages that could be assessed under state law for each violation of a fingerprint identification statute.[3]

[1] FBI, Next Generation Identification (NGI) Monthly Fact Sheet (Sept. 2015) available at https://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi/next-generation-identification-monthly-fact-sheet (viewed Dec. 2015).

[2] https://support.apple.com/en-us/HT204587 (last viewed Dec. 2015).

[3] See, 740 ILCS 14/20 (1)-(4); Tex. Bus. & Com. Code § 503.001(d).

RELATED PRACTICES

Antitrust and Competition

Data Privacy and Security Team