What Employers Should Consider Before Switching to Fingerprint-based Time Clocks, Padlocks and Access Points

February 18, 2016

Several companies now offer time and attendance solutions that incorporate the use of fingerprint identification technology and purport to eliminate “buddy punching” for hourly employees. In addition to time and attendance devices, companies are increasingly considering fingerprint identification technology as part of their physical security program to replace badges, access cards, or access codes when entering into sensitive areas, or to replace (or supplement) passwords when logging into workstations. The increasing use of fingerprint identification raises data privacy and data security questions for many employers.

Authors/Presenters

David A. Zetoony

Partner
Boulder, Colorado
david.zetoony@bryancave.com

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; the FTC can also proceed against a company that misrepresents their data privacy and security practices including how they use, secure, or disclose captured fingerprints or fingerprint geometry.

At least two states have also enacted statutes that govern the data privacy and security implications of 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.

You should consider the following when deciding whether to implement fingerprint identification-based timekeepers, physical access controls, or hardware access controls:

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. Among other things, you should consider how the device that captures fingerprints stores and transmits that data.

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.

10% Reduction in payroll costs claimed by one fingerprint time clock provider.[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] http://www.bioelectronix.com/specifications/x180/x180_usb_brochure.pdf (pg. 2)

[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