Liisa Thomas Partner
LMThomas@sheppardmullin.com

Shanna Pearce Senior Associate
SPearce@sheppardmullin.com

Eric Dilulio Associate
EDiiulio@sheppardmullin.com

Sheppard Mullin Richter & Hampton LLP, Chicago

Dealing with US biometric laws and litigation

US states have begun to pass legislation that regulates how companies can collect biometric data, whether they can share this information, and how the information should be protected. Even for companies that operate outside of these states, there are risks to companies who fail to protect biometric data, in the form of state data breach notification laws. Liisa Thomas, Shanna Pearce, and Eric Dilulio, Partner, Senior Associate and Associate respectively at Sheppard Mullin Richter & Hampton LLP, examine the requirements and steps companies can take to address their obligations and the risks.

Biometrics in context

Biometric identification is not new. Businesses like biometrics because they can be harder to steal than more traditional identifiers. They may also be easier to use for individuals, since they can't be forgotten like a traditional password. Fingerprint recognition is being used to let people access their smartphones or conduct online banking. Employers might find fingerprint tracking harder to tamper with than more traditional time-keeping systems. Facial recognition technology is starting to be used as well, for instance, advertisers might use facial recognition on a billboard to serve targeted ads.

In the age of data breaches and litigation, these benefits come with risks. Prime among these is the irreplaceable nature of biometric data. We cannot get new fingerprints, or a new face. Regulators are concerned about risks to consumers and are introducing biometric privacy laws. Many have also added biometric data to breach notification laws. With these laws in mind, companies considering collecting biometric data should think about notice and consent, as well as the possibility of subsequent sharing. Companies also need to keep in mind how to protect that information and the consequences if the data is not protected.

Collecting biometric information: do you need consent?

Illinois, Texas, and Washington are the only US states with biometric-specific privacy laws. These laws regulate how and when companies can collect biometric information[1]. All three laws require companies to give notice to individuals about collection and use of biometrics. Illinois and Texas also require companies to get consent. BIPA is the most specific and has resulted in the most litigation.

Obtaining consent

For consent to be sufficient in Illinois, a company that collects or receives biometrics must (Section 15(b) of BIPA): tell people in writing that it is collecting biometrics; tell the individual why biometrics are being collected, and how long they will be stored or used; and get signed consent. In Texas, companies must 'inform the individual' before collecting the biometric information and get consent (Section 503.001(b) of the Texas Law). In Washington, companies must either give notice, get consent, or 'prevent the subsequent use of a biometric identifier for a commercial purpose' (Section 19.375.020(1) of the Washington Law). For notice to be sufficient, it has to be readily available to people, but can be context-specific (Section 19.375.020(2) of the Washington Law). Companies which comply with the Illinois law would thus presumably be in compliance with the less specific Texas and Washington statutes.

BIPA is the only of the three that provides for a private right of action, and dozens of class action complaints have been filed. Most have been against employers over use of fingerprint timeclocks[2]. These timeclocks are popular because they stop employees from marking absent co-workers present[3]. The lawsuits accuse employers of collecting and using employees' fingerprints without the employees' written consent and/or without properly informing the employees about the company's policy of use, storage, and ultimate destruction of the fingerprint data. However, at least one court has concluded that substantial compliance with the notice and consent provisions is sufficient[4].

Consumers have also sued alleging violations of notice and consent requirements. Website users have filed complaints challenging companies' use of facial recognition to identify individuals in photos uploaded by users to social media and photo storage sites[5]. Customers have also filed suits concerning the use

Companies will increasingly use systems that rely on biometric identifiers. When used appropriately they can be more secure and easier for the individual to use.

continued

of their fingerprints to access lockers and tanning booths, and use of facial recognition to verify purchases at self-service kiosks[6]. Some of these lawsuits have resulted in settlements for amounts well over $1 million[7]. It is thus clearly in companies' best interests, if using biometrics in Illinois, to be familiar with the requirements of the Illinois statute.

Companies outside of Illinois (and Texas and Washington) are not off the hook, however. The Federal Trade Commission ('FTC') has also been active in the biometrics space. The FTC enforces privacy violations under Section 5 of the FTC Act of 1914, which prohibits unfair and deceptive commercial practices. To help companies understand what might be considered an unfair or deceptive practice, the FTC regularly issues reports and guidance. It did so for facial recognition technologies in 2012[8]. In its report, the FTC indicated that companies using facial recognition should give notice of the purpose of the technology and tell consumers how to get more information[9]. Companies should, according to the FTC, also get consent before using facial recognition in a way that differs from the original notice or to identify anonymous people[10].

Sharing biometric information

BIPA prohibits companies from selling biometric data, and from sharing such data unless the individual has consented (Section 15(c) and (d)(1) of BIPA). Sharing can also occur if it is needed to complete a financial transaction the person asked for or it is required by law (Section 15(d)(2) and (3) of BIPA). In Texas, companies can both share and sell biometric data with an individual's consent, if it will be used to identify the person in case the person disappears or dies (Section 503.001(c)(1) of Texas Law). The information can also be shared or sold under Texas law, without consent, if it completes a financial transaction the person has requested.

With respect to sharing, Washington is the most liberal. It allows sharing and sale if the individual consents (Section 19.375.020(3) of Washington Law). A company can also share or sell biometric information if it is needed to provide a product or service or complete a financial transaction the person requested. It can also be shared or sold to a third party who promises that it will be used in a way consistent with the original notice and not further shared (Section 19.375.020(3)(e) of Washington Law). It can also be shared if required by law, 'to prepare for litigation,' or otherwise 'participate in the judicial process' (Section 19.375.020(3)(d) and (f) of Washington Law).

Protecting biometric information

Companies must reasonably protect biometric data under the Illinois, Texas and Washington laws. In Illinois and Texas, that means it must be protected to the same degree as other confidential and secret information (Section 15(e) of BIPA and Section 503.001(c)(2) of Texas Law). The laws also require destruction of the data within a fixed amount of time (Section 15(a) and (c) of BIPA and Section 503.001(c) of Texas Law).

What happens if biometric data is not protected?

The breach notification laws of Delaware, Illinois, Iowa, Maryland, Nebraska, New Mexico, North Carolina, Wisconsin, and Wyoming define biometric data as 'personal.' In other words, if biometric data is breached, companies must notify impacted individuals. Moreover, in Delaware, Iowa, Maryland, Nebraska, New Mexico, and North Carolina, companies also need to notify government authorities. Once a company raises its hand to say it had a breach, lawsuits often follow. In addition, there may also be investigations by regulatory entities. The basis of these suits is typically not that the company notified impacted individuals incorrectly. Instead, the suits allege that the company 'caused' the problem by failing to provide adequate protection, and as a result, engaged in an unfair act. The lawsuits might also allege that the company promised protection (in a privacy policy for example) but did not give protection, and this constitutes a deceptive act[11]. Where a company is viewed to have failed to take reasonable measures to protect the compromised information, or where it has failed to protect information as it stated it would, regulatory enforcement action and/or private lawsuits under state unfair and deceptive trade practices laws may ensue[12].

What can businesses do to minimise risk?

Companies will increasingly use systems that rely on biometric identifiers. When used appropriately they can be more secure and easier for the individual to use. There are however inherent risks. Many of the risks are practical. Has the company implemented sufficient security within the system? But other risks are legal. What happens if people don't know how their information will be used? What if companies have not provided notice? What if individuals have not given consent? To manage the legal risks when creating these systems, companies should look at the notice they give when they collect biometric information and what type of consent they obtain. They should also look at their sharing practices. Finally, companies should assess the sensitivity of their biometric data and tailor their data protection plans accordingly.

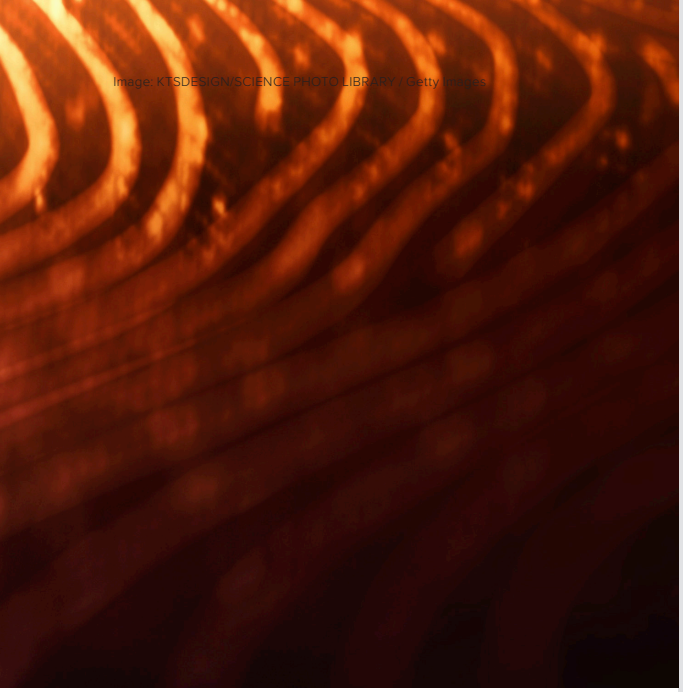

Image: KTSDESIGN/SCIENCE PHOTO LIBRARY / Getty Images

1. Texas Law on the Capture or Use of Biometric Identifiers (11 Business and Commerce Code §503.001) ('the Texas Law'); Biometric Information Privacy Act 2008 (740 Illinois Compiled Statutes 14) ('BIPA'); Washington Law on Biometric Identifiers (19 Revised Code of Washington §375) ('the Washington Law').
2. *Freeman-McKee v. Alliance Ground International LLC*, No. 2017-CH-13636 (Ill. Cir. Ct., Cook County 2017); *Baron v. Roundy's Supermarkets Inc., et al.*, No. 1:17-cv-03588 (N.D. Ill. 2017); *Howe v. Speedway LLC, et al.*, No. 2017-CV-11992 (Ill. Cir. Ct., Cook County 2017); *Diaz v. Greencore USA - CPG Partners LLC*, No. 2017-CH-13198 (Ill. Cir. Ct., Cook County 2017). While the Texas and Washington Laws also require notice and consent, the laws may only be enforced by the States' Attorneys General and not via private lawsuits.
3. Janofsy, Adam, Fingerprint-Scanning Time Clocks Spark Privacy Lawsuits, The Wall Street Journal, 11 January 2018.
4. *Santana v. Take-Two Interactive Software, Inc.*, 2017 WL 5592589, at 3 (2d Cir. 21 November 2017) (notice that video game feature required a 'face scan' was 'sufficient to meet BIPA's mandates under the circumstances here' even though BIPA defines a 'biometric identifier' as a 'scan of [...] face geometry.')
5. See, e.g., *Monroy v. Shutterfly Inc.*, No. 16-cv-10984 (N.D. Ill. 2016).
6. See, e.g., *Sekura v. L.A. Tan Enterprises*, No. 2015-CH-16694 (Ill. Cir. Ct., Cook County Chancery Division 2015); *McCollough v. Smarte Carte Inc.*, No. 1:16-cv-03777 (N.D. Ill. 2016).
7. See, e.g., *Sekura v. L.A. Tan Enterprises*, No. 2015-CH-16694 (Ill. Cir. Ct. Cook County Chancery Division, order dated 1 December 2017).
8. FTC, Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies, October 2012.
9. Ibid. pg. 15.
10. Ibid. at iii.
11. Thomas, Liisa M., Thomas on Data Breach: A Practical Guide to Handling Data Breach Notifications Worldwide, Thomson Reuters, 2018.
12. While the inclusion of biometric information in these statutes and rules may be recent, regulatory action and lawsuits under unfair and deceptive trade practices laws arising from data breaches involving personal information are commonplace. See, e.g., *United States v. Vtech Electronics Ltd. et al.*, No. 1:18-cv-114 (N.D. Ill. 2018); *In re: Barnes & Noble Pin Pad Litigation*, No. 1:12-cv-08617 (N.D. Ill. 2012); *Walters v. Kimpton Hotel & Restaurant Group LLC*, No. 3:16-cv-05387 (N.D. Cal. 2016); *Stevens v. Zappos.com, Inc.*, No. 16-16860 (9th Cir. 2016).

Council of Europe modernises Convention 108

The Council of Europe ('CoE') adopted, on 18 May 2018, the Protocol (CETS No. 223) to amend the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data ('Convention 108') ('the Protocol'), following a seven year process, and issued an explanatory report ('the Report') on the same. The Protocol seeks to modernise Convention 108 in light of new information and communication technologies, as well as strengthen its effective implementation.

The Report states, '[Convention 108] has served as the foundation for international data protection law in over 40 European countries. It has also influenced policy and legislation far beyond Europe's shores. With new challenges to human rights and fundamental freedoms, notably to the right to private life, arising every day, it appeared clear that [it] should be modernised in order to better address emerging privacy challenges [...] and, at the same time, to strengthen [its] evaluation and follow-up mechanism [...] The general and technologically neutral nature of Convention 108's provisions must be maintained; [its] coherence and compatibility with other legal frameworks must be preserved; and [its] open character, which gives it a unique potential as a universal standard, must be reaffirmed.'

The amendments introduced by the Protocol include the replacement of the term 'automatic processing' with 'data processing,' which encompasses automated and non-automated processing, and the introduction of the terms 'recipient' and 'processor.' Moreover, the conditions for the legitimacy of data processing and quality of data have been expanded to include the data subject's consent or any other legitimate basis laid down by law, such as the fulfilment of a contract, the vital interest of the data subject or a legal obligation of the controller, as well as the scope of sensitive data to include genetic and biometric data. The Protocol also introduces a data breach notification requirement in cases where the fundamental rights and freedoms of the individual may be seriously affected.

The Report explains, 'Where such a data breach has occurred, the controller is required to notify the relevant supervisory authorities of the incident, subject to the exception permitted under Article 11 paragraph 1. This is the minimum requirement. The controller should also notify the supervisory authorities of any measures taken and/or proposed to address the breach and its potential consequences.'

Moreover, the Protocol provides for a right to obtain knowledge of the reasoning behind the processing of data of an individual, and establishes the right to object to the processing of data unless the controller demonstrates compelling legitimate grounds for the processing which override those of the data subject's. Furthermore, the facilitation of transborder data flows is established by two means: either by law, or by ad hoc or approved standardised safeguards. The Protocol will be open for signature on 25 June 2018 in Strasbourg during the third part-session of the Parliamentary Assembly.