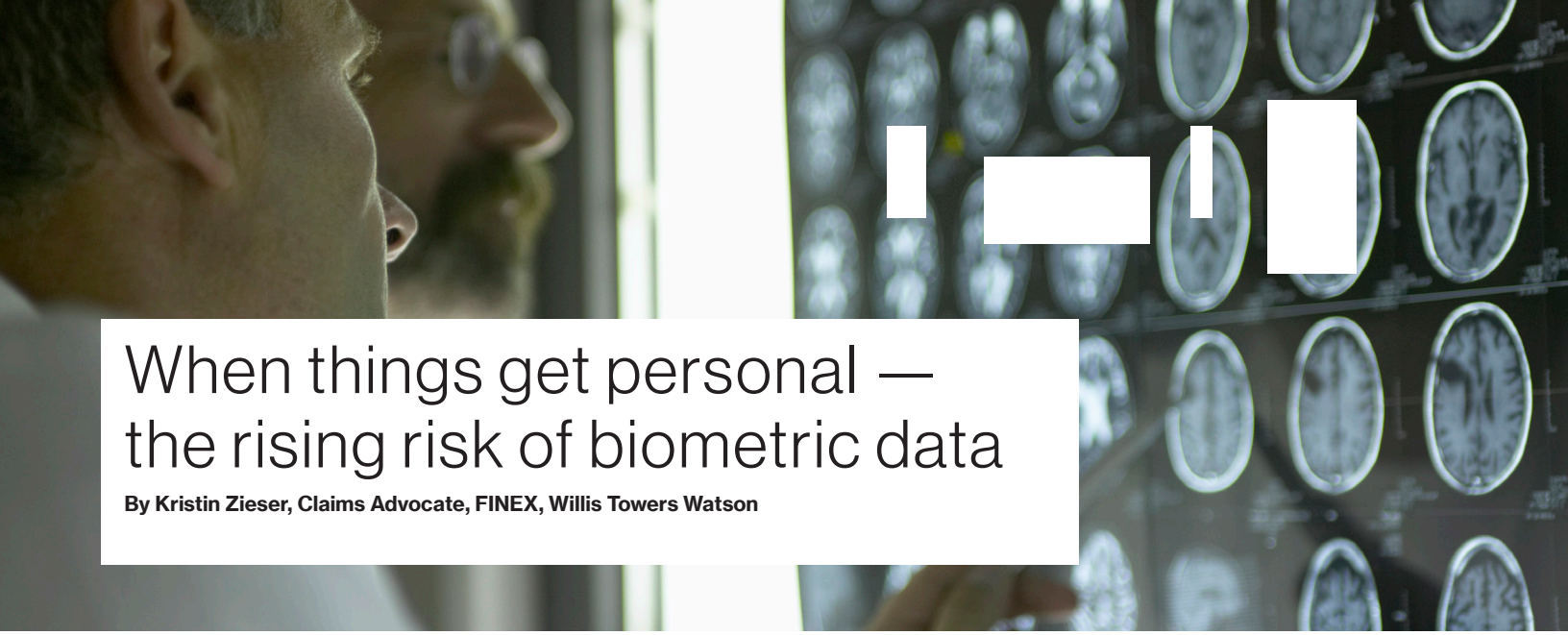

When things get personal — the rising risk of biometric data

By Kristin Zieser, Claims Advocate, FINEX, Willis Towers Watson

In today's world of new technology and automated systems, biometric data has become a popular option for businesses managing employees and clients/customers. While more and more companies are adopting this form of data keeping, which is effective in identifying employees and/or customers based on their physical characteristics, it does not come without risks associated with the collection, distribution and storage of this personal information. Over the past decade, policies have been established to protect this information. While only three states have policies in place directly related to biometric data, more states are expected to follow suit. Federal regulations are also expected to be implemented in response to the increased usage of biometrics. In order to decrease the risk of litigation relative to biometrics, it is in the best interest of every company that uses or interacts with this type of data to know which policies protect employees and customers.

What is biometrics?

Biometrics is the measurement and statistical analysis of people's unique physical and behavioral characteristics, such as fingerprints or voice patterns, as a means of determining personal identity. Unlike a credit card or social security number, which can be changed if exposed or stolen, biometric data, when compromised, cannot be changed or replaced. Given the serious consequences of compromised biometric data, a number of states have proposed or passed legislation regulating the collection and storage of such data. Currently three states have statutes regulating the collection and storage of biometric data: Illinois, Texas and Washington.

Illinois Biometric Information Privacy Act (BIPA) and other statutes

Enacted in 2008, BIPA is the most stringent of any state. BIPA requires any private entity that collects, captures or obtains a person's biometric information to first obtain the individual's consent through a written release. The entity must provide notice about its purpose for collecting, storing and using information and must post a publicly available retention and destruction schedule. Furthermore, the biometric information must be destroyed when the purpose for obtaining such information has been satisfied, and the entity may not sell the data, though it can disclose the data with consent, as long as it does not profit from the disclosure. BIPA also creates a private right of action for any person whose rights under the statute have been violated, providing $5,000 per violation in liquidated damages, as well as the recovery of attorneys' fees. BIPA is the only statute thus far that allows a private right of action.

The Texas and Washington statutes are less stringent. Texas limits its scope to the collection and storage of "biometric identifiers," and does not include information that is based on those identifiers. Washington's statute does not explicitly include "hand or face geometry." Both Texas and Washington only apply to entities that collect the data for a commercial purpose. While they also require employers to provide notice and to obtain consent before collecting and storing biometric data, they do not specify that the consent must be in writing (unlike Illinois). The Texas statute only requires the employer to destroy the data "within a reasonable time," but no later than one year after the biometric data is no longer needed.

Washington requires employers to retain the information "no longer than reasonably necessary." Neither Texas nor Washington provides a private right of action – claims must be brought by the state's attorney general.

Litigation status

BIPA went largely unnoticed until 2015 when a series of class actions were filed against Facebook, alleging violations of BIPA in response to their suggested photo tagging feature which scans photographs and suggests other Facebook users "tag" themselves in photos. Facebook moved to dismiss the action, arguing plaintiffs lacked standing under Article III, because collection of biometric information without notice or consent did not result in "real world harms," such as adverse employment or even anxiety. The court denied Facebook's motion to dismiss, ruling that the plaintiffs do not need to show "'actual' injury beyond invasion of privacy rights afforded" by BIPA. (*In re: Facebook Biometric Information Privacy Litigation*, case number 3:15-cv-03747 (U.S. District Court for the Northern District of California))

Similarly, in *Dixon v. The Washington and Jane Smith Community, et al.,* 17-cv-08033, plaintiff, a former employee of Smith Senior Living (Smith) filed a class action against Smith and Kronos, Inc. (the time clock supplier) alleging that Smith violated BIPA by sharing her fingerprint data with Kronos without her consent. Like the Facebook cases, the defense moved to dismiss, arguing plaintiff did not assert an "actual injury." The District Court for the Northern District of Illinois, however, found that "obtaining or disclosing a person's biometric data without his or her consent or knowledge constitutes an actual and concrete injury because it infringes on the right to privacy in that data." (See id.) In contrast, the Illinois Court of Appeals for the Second District held in December 2017 that a plaintiff must allege an actual injury to be aggrieved under BIPA in order to seek statutory damages and injunctive relief (*Rosenbach v. Six Flags Entm't Corp.*) These conflicting decisions are problematic for employers as they create uncertainty in an otherwise untested statute and leave employers open to BIPA claims, regardless of whether the claimant was actually injured.

What does the future hold?

There was an uptick in BIPA litigation in 2017 hitting a variety of industries. The allegations have been strictly technical violations, such as no policy in place, no waiver provided to employees, no retention/destruction protocols, etc. As these matters involve invasions of privacy, claims by employees (including former employees) would trigger employment practices liability insurance policies. As such, it is important to be aware of the potential implications and consult with industry specialists to ensure you have the proper coverages in place.

Contact

Kristin Zieser
+1 212 915 7924
kristin.zieser@willistowerswatson.com

About Willis Towers Watson

Willis Towers Watson (NASDAQ: WLTW) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to 1828, Willis Towers Watson has over 40,000 employees serving more than 140 countries. We design and deliver solutions that manage risk, optimize benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals. Our unique perspective allows us to see the critical intersections between talent, assets and ideas – the dynamic formula that drives business performance. Together, we unlock potential. Learn more at willistowerswatson.com.

willistowerswatson.com/social-media

Willis Towers Watson