

Biometrics, Genetics, and Insurance Coverage

By Timothy M. Thornton

Timothy M. Thornton is a partner with Gray Duffy LLP in Encino, California. He has more than 30 years' experience providing legal counsel on insurance-related matters, including insurance coverage issues in advertising and personal injury coverage, environmental contamination and toxic torts, insurance coverage of intellectual property claims and entertainment claims, and cyber liability claims. He can be reached at tthornton@grayduffylaw.com.

In December 2017, a court approved a \$1.5 million settlement in *Sekura v. L.A. Tan*. A class of tanning salon customers sued L.A. Tan under Illinois' Biometric Information Privacy Act (BIPA). L.A. Tan used customer fingerprint data for membership identification purposes, without notice or consent. *Sekura v. L.A. Tan Enterprises Inc.*, Case No. 2015 CH 16694, Cir. Ct. of Cook Cty., Ill., Cty. Dep't, Chancery Div. (Dec. 2017).

Biometric Information Privacy Laws

Illinois, Texas, and Washington have passed biometric information privacy acts. See 740 ILCS 14/10 *et seq.*; Tex. Bus. & Com. Code 503.001; RCWA 19.375.010 *et seq.* Laws have been proposed in other states.

Biometric information privacy laws require written policies for collection, retention, and destruction of such data; time limits on retention of such data; consent before such data can be collected; prohibition of sale of or profit on such data; limited circumstances for use; and safeguarding of such data.

The Illinois Biometric Information Privacy Act (BIPA) establishes a private right of action. BIPA allows plaintiffs to recover the greater of actual damages or per violation statutory damages—\$1,000 for a negligent violation and \$5,000 for a reckless or willful violation.

This scheme recalls the Telephone Consumer Protection Act (TCPA), 47 U.S.C. section 227, which led to many lawsuits and related coverage litigation. BIPA may do the same. (Texas and Washington do not provide a private right of action.)

Genetic Information Privacy Laws

Many states have passed genetic information privacy acts as well. Congress passed the Genetic Information Non-Discrimination Act (GINA) in 2008 (42 U.S.C. § 2000ff (4)).

Genetic information is defined by regulation under HIPAA. 45 C.F.R. 160.103. Many state statutes use this definition, e.g., 410 ILCS 513/10.

The Illinois Genetic Information Privacy Act, 410 ILCS 513/1 *et seq.*, makes genetic testing and information derived from genetic testing confidential and privileged, except as otherwise provided in the Act. It may only be released to the individual tested and to persons specifically authorized in writing by that individual to receive the information. The law provides a right of action. An aggrieved person can recover the greater of actual damages or liquidated damages, reasonable attorney's fees and costs, and other appropriate relief including injunctive relief.

Litigation under These Laws

Many more businesses can and do use biometric information, which can be readily captured in real time. Collection of genetic information is more limited, primarily in the medical field. Lawsuits have focused on business practices involving biometric data and have not alleged security breaches resulting in the taking of biometric data.

The cases have explored several issues. First, do online photo services' use of facial recognition come within the statute, which covers face scans but excludes photos and information derived from photos? *See In re Facebook Biometric Info. Privacy Litig.*, 185 F. Supp. 3d 1155 (N.D. Cal. 2016) (yes, it applies).

Second, is there adequate notice and consent? *See Vigil v. Take-Two Interactive Software, Inc.*, 235 F. Supp. 3d 499, 513 (S.D.N.Y. 2017) (yes; personalized "avatars" in a basketball video game), *aff'd in part, vacated in part and remanded, Santana v. Take-Two Interactive Software, Inc.*, 717 Fed. App'x 12 (2d Cir. 2017); *McCullough v. Smarte Carte, Inc.*, No. 1:2016cv03777, 2016 WL 4077108, at *3 (N.D. Ill. Aug. 1, 2016) (yes; fingerprint scans to access rented locker).

Third, is there actual injury that satisfies Article III? *See Vigil, supra* (no); *but see Patel v. Facebook Inc.*, 290 F. Supp. 3d 948, 954 (N.D. Cal. 2018) (yes).

Fourth, is plaintiff an "aggrieved person" under BIPA? Does this require actual injury and must there be actual damages before statutory damages are awarded? *See Vigil, supra*, 235 F. Supp. 3d at 519 (actual injury required to state a claim under BIPA) (no); *but see Monroy v. Shutterfly, Inc.*, 2017 WL 4099846, at *9 (N.D. Ill. Sept. 15, 2017) (showing of actual damages not necessary to state a claim under BIPA).

Fifth, do the lawsuits seek to apply the statute extraterritorially? And, relatedly, sixth, does BIPA as applied violate the dormant Commerce Clause? *Monroy, supra*, held there was insufficient information to resolve these issues on a motion to dismiss.

Insurance Coverage Issues

Cyber insurance typically applies to defined wrongful acts. The current lawsuits do not allege breach but instead focus on business practices. If the coverage applies to a "data breach," then it may not apply if there has been no breach. But if a covered wrongful act includes "failure to prevent unauthorized access to or use of data containing identity information," the coverage arguably may apply.

If there is a breach of biometric and genetic information, these policies may provide coverage. Analytically, these suits would seem to be much like other data breach lawsuits.

Commercial general liability and excess umbrella liability policies cover personal and advertising injury, including "oral or written publication, in any manner, of material that violates a person's right of privacy." Another possible "offense" found in some policies would be "discrimination" if the claim was genetic discrimination.

As to invasion of privacy, courts split on the "publication to third parties" issue. *See State Farm General Ins. Co. v. JT's Frames, Inc.* 104 Cal. Rptr. 3d 573 (2010) (TCPA violation was not covered); *but see Valley Forge Ins. Co. v. Swiderski*, 860 N.E.2d 307, 317 (2006) (material that violates a person's seclusion could include unsolicited fax advertisements).

The question has two aspects for claims involving biometric and genetic information privacy. First, if

Published in *TortSource*: Volume 20, Number 3, ©2018 by the American Bar Association. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

the issue is business practices, there is not an unsolicited fax or text publication as in TCPA cases. Is the internal use, or the generation of biometric information from a biometric identifier, going to be argued to be a “publication”? As to network breach claims, the parties will argue whether disclosure by hackers is sufficient to trigger coverage.

The 2013 ISO standard commercial general liability form contains a Recording and Distribution of Material or Information in Violation of Law exclusion. It excludes injury or damage arising out of any action or omission that violates any statute, ordinance, or regulation—other than the TCPA, CAN-SPAM, or FCRA—that addresses, prohibits, or limits the printing, dissemination, disposal, collecting, recording, sending, transmitting, communicating, or distribution of material or information.

ISO has issued policy forms that contain exclusions relating to access or disclosure of confidential personal information, e.g., CG 21 06 05 14. These exclusions preclude coverage for injury or damage arising out of any access to or disclosure of any person’s or organization’s confidential or personal information, including health information or any other type of nonpublic information.

Always consider the exact language of the policy.

Employment practices liability insurance is typically provided for defined wrongful acts. This may cover alleged wrongful acts involving collection or use of biometric or genetic data of employees. Some of the laws specifically refer to biometric and genetic data of employees. GINA seeks to avoid discrimination in hiring decisions based on genetic data. It prohibits employers from discriminating against employees on the basis of genetic information. GINA prohibits collecting genetic information from employees, except in limited circumstances.

The ISO EPL Form, EP 00 01 11 09, “wrongful acts” include “invasion of privacy.” If an employee is denied training or promotion or career opportunity or given a negative evaluation because of genetic profile, this may be wrongful under GINA and state laws.

The ISO Violation of Laws Applicable to Employers exclusion precludes coverage for violation of an employer’s responsibilities required by any other federal, state or local law, but the exceptions include GINA.

Use of biometric information is much more widespread than genetic information at this time. It offers the potential for relatively secure and easy authentication of identity. We can expect more litigation under BIPA. If the Article III “actual injury” and BIPA “aggrieved party” issues are resolved in favor of the defendants, this will stop the business practices litigation. Even then, if there is a breach disclosing such information, the “actual injury” and “aggrieved party” requirements may be satisfied, and litigation may proceed. Counsel for those defendants will want to review their coverage in all of these circumstances for possible defense and indemnity.