Antitrust, Vol. 31, No. 3, Summer 2017.

The Future Is Now: Biometric Information and Data Privacy

BY SHARON ROBERG-PEREZ

SCIENCE FICTION ENTHUSIASTS MIGHT remember 2002's *Minority Report*, in which facial recognition technology was used to identify people as they moved about a city. The purpose? Targeted advertising. Fans may also remember 1997's *Gattaca*, in which biometric data was used to secure access to an aerospace corporation's campus, as well as to "sort" individuals into their appropriate professions, akin to the way that young wizards are sorted into appropriate houses in J.K. Rowling's Hogwarts. In the *Gattaca* world, though, sorting was based on a dystopic genetic determinism, where blood, urine, and hair samples served to keep people in their places.

Once limited to the realm of science fiction, we are increasingly encountering biometric systems in the real world, whether or not we are ready to navigate them. Apple, for instance, released the iPhone 5S with a fingerprint scanner, and is reportedly working to replace it with a 3D scanner for facial recognition.[1] Federal and state law enforcement agencies have turned to biometrics to prevent fraud, but also for routine surveillance.[2] A billion-dollar Chinese startup company called Face++ offers facial recognition technology that is already used by over 120 million people in connection with a mobile money transfer app.[3] And other startup companies look to monetize the biometric data sets themselves.[4]

Industry analysts predict both widespread consumer acceptance of biometrics—estimating the number of mobile devices equipped with a fingerprint scanner to hit one billion by early this year—as well as the emergence of new technologies based on everything from voice recognition to ocular blood vessel pattern, ear shape, gait, heart rhythm, and online behavior.[5] What could possibly go awry?

Turns out there is quite a lot that can go wrong from a privacy standpoint. And we are just beginning to determine whether our current legal framework can adequately address the use and misuse of information about unique identifying characteristics that are largely unalterable. We can always reset a password. But once biometric data is compromised, the horse is out of the barn.

Sharon Roberg-Perez is a Principal at Robins Kaplan LLP in the Intellectual Property and Technology Litigation Group. Her practice is focused on biotechnology and medical device disputes.

Bio What?

"Biometrics" or "biometric authentication" typically refers to automated methods for identifying or recognizing an individual based on one or more unique characteristics. Ideally, the measured characteristic has the following properties:

- It is robust: Within any given individual, the trait is invariant over time.
- It is distinctive: The characteristic shows great variability within the population.
- It is "available": The entire population has it, and it can be measured over and over again, for any given individual.
- It is accessible: It can be measured electronically.
- It is acceptable: Most people do not object to the measurement being taken.[6]

Characteristics may be innate and generally immutable, including physiological characteristics, such as anatomical features or genomic sequences. Or, characteristics may be behavioral, reflecting an individual's interactions with her environment. These traits are difficult (but not impossible) to modify, and include the way one walks, speaks, writes, or interacts with a computer.[7] Characteristics may even include both physiological and behavioral components. Consider a wearable authentication device that analyzes one's heartbeat, and the way that a heartbeat changes depending on one's activities.[8]

As an initial matter, biometric systems fall into one of two broad categories—positive and negative identification systems.

Positive identification systems are designed to prove that an individual is known to the system. They compare a submitted sample to a single template. They are typically voluntary. They may often include alternative authentication mechanisms (i.e., you may or may not choose to lock your iPhone with your fingerprint). Anyone desiring to circumvent this type of authentication must create a false match, for example, by copying a fingerprint with a printer.[9]

Negative identification systems are designed to prove that an individual is *not* known to a system. Submitted samples are compared to a database of samples. Participation is mandatory, and these systems do not include alternative authentication mechanisms. To get around these systems, it is necessary to trick the system in one of two ways. Either the system must erroneously believe that you submitted a sam-

ple, when you have not. Or the system must receive your sample, and respond as if the sample is completely novel (even if it is not). These systems may be used to avoid fraud, by preventing double dipping in connection with the collection of government benefits.[10]

Biometric systems of all types must be configured to make the desired comparison and arrive at a probabilistic answer—the submitted sample is (or is not) a match.[11]

Regardless of how a system is designed, it must include sensors appropriate for collecting an individual's sample. It must correlate each sample with other, personally identifiable information. And it must store—and often transmit—individualized data. Consequently, there are multiple ways in which a biometric system may be vulnerable to being hacked: during data collection, while data is stored, or when data is transmitted.

Privacy and Individually Identifiable Information

Digital data is difficult to protect, and digitized biometric data is no different.[12] Consider that the fingerprints of over 5.6 million government employees were stolen from the federal government's Office of Personnel Management.[13] It was likely of little comfort to the victims to know that the government retained an "identity theft protection service" to monitor whether their biometric data was misused.

What recourse is there when individualized information gets into unauthorized hands? Or when personal information that is provided for one purpose is handled or used in a manner that its owner/originator never intended?

Given the spate of well-publicized data breaches over the last several years,[14] it is no surprise that, for many people the answer is to litigate. But what causes of action are available?[15] Moreover, what must a plaintiff allege to demonstrate that she has standing to bring a case?[16]

In federal district courts, a plaintiff must be able to establish that (1) there has been an invasion of a legally protected interest; and (2) she has suffered a "concrete and particularized" harm that is "actual or imminent," not "conjectural or hypothetical."[17] An injury sufficient to confer standing does not necessarily have to be a tangible injury, but it must be more than a mere statutory violation.[18] Since the Supreme Court's decision in *Spokeo v. Robins* last year, several courts have had an opportunity to consider what types of injuries are sufficiently "concrete and particularized," reflecting actual or imminent harm.

In the Second and Seventh Circuits, plaintiffs have made unsuccessful attempts to bring claims for violation of the Fair and Accurate Credit Transaction Act (FACTA), which is intended to prevent identity theft by restricting the amount of information that is printed on credit card receipts.[19] Plaintiffs in these cases alleged that retailers wrongfully printed credit card expiration dates on their receipts, but they had not alleged that any third party had ever seen the receipts. Similarly, in the Eighth Circuit, a plaintiff unsuccessfully filed suit against his former cable company, alleging a violation of the Cable Act, because the company retained his personally identifiable information for some three years after he had canceled his subscription.[20] Plaintiff had not alleged, however, that his information had been disclosed to, or accessed by, a third party, or even that the defendant had used the information in any way. In these cases, any threat to plaintiffs' identities was purely hypothetical, and plaintiffs had no standing to sue.

Plaintiffs have fared better—at least for standing purposes—when they have alleged that their information was disclosed to a third party (Facebook),[21] or used in a way that violated their right to be free of intrusive phone calls or texts under the Telephone Consumer Protection Act (TCPA).[22] But credit card data, phone numbers, social media activity, and browsing history are distinctly different from biometric data, which presents different risks. Credit cards and phone numbers can be changed. In theory, people can "unplug." They cannot, however, generate new and different fingerprints or alter the pattern of blood vessels in their eyes.

Certain cases involving claims under the Fair Credit Reporting Act (FCRA) or the Privacy Act (5 U.S.C. Section 552a) are instructive regarding how courts may view biometric data privacy claims. In the Sixth Circuit, plaintiffs brought FCRA claims based on the theft of over one million insurance customers' personal identifying information, including their names, birthdates, genders, occupations, and employers.[23] The plaintiffs had standing because their personal information had been specifically targeted, and a reasonable inference could be drawn that the victims' data would be used fraudulently.

The plaintiffs also had standing in an FCRA case brought in the Third Circuit based on stolen laptops.[24] The laptops contained names, birthdates, medical histories, and laboratory test results, and the plaintiffs had alleged an "unauthorized dissemination of their own private information," which was exactly the reason the FCRA was enacted.

By contrast, the plaintiffs lacked standing in a case in the Fourth Circuit against the Secretary of Veterans Affairs for violation of the Privacy Act.[25] A laptop with patient names, birthdates, physical descriptions, and testing results had been stolen. But while the plaintiffs alleged an increased risk of future identity theft and costs to guard against the same, they had not articulated a harm that was "certainly impending."[26] Indeed, having relied on a statistical likelihood that 33 percent of health data breaches would result in identity theft, the plaintiffs were faced with the 66 percent likelihood that there would be no identity theft at all.

Biometric Data Privacy Laws Vary Across Jurisdictions

A number of states have statutes, or pending legislation, that explicitly protect the privacy of biometric data.

Illinois. Illinois was at the forefront, having passed its Biometric Information Privacy Act (BIPA) in 2008.[27] A right of action was created for aggrieved parties to bring claims

against private entities that violate BIPA and seek damages or an injunction.

Under Illinois law, a "biometric identifier" is limited to "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry," and expressly excludes biological samples (including genetic samples) as well as physical descriptors (i.e., height, weight, eye color, hair color), medical images, and photographs. "Biometric information" is defined broadly to mean "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual." It expressly excludes "information derived from items or procedures excluded under the definition of biometric identifiers."

BIPA provides the following safeguards to consumers:

- Any private entity that possesses biometric identifiers or information must have a written policy that is publicly available and establishes a retention schedule and guidelines for permanently destroying biometric information when the reason for its collection has been satisfied, or when the individual has not interacted with the private entity in three years (whichever occurs first).
- Private entities are to adhere to their guidelines, absent a court order to the contrary.
- Private entities may not collect, capture, buy, or otherwise obtain any customer's biometric identifiers or information without first informing the customer in writing about the data that is being collected or stored. Customers must be informed as to the specific reason for the collection, and the length of time that the information will be retained. Customers also must provide a written release.
- Private entities may not profit from their customers' biometric identifiers or information. Nor may they distribute or disclose this data absent (1) consent; (2) the disclosure being required to complete a financial transaction that the customer initiated; or (3) the disclosure being mandated by state or federal law, or court order.
- Private entities are to use "the reasonable standard of care" within their industries to store, transmit, and protect biometric identifiers or information, which must be at least as protective as the manner in which they protect other confidential and sensitive information.

Two companies, L.A. Tan and Shutterfly, settled cases involving BIPA claims in 2016.[28] Shutterfly faced allegations that its facial recognition technology scanned every uploaded photograph to collect facial geometries of anyone in each photo, including third parties who had never agreed to use Shutterfly's services. And plaintiffs in the *L.A. Tan* case took issue with the tanning salon's failure to get consent to collect, store, and use their fingerprint data.

Plaintiffs seeking to recover under BIPA should anticipate standing challenges. A case against a video game manufacturer, Take-Two, was dismissed earlier this year because the plaintiffs had not articulated actual or imminent harm.[29] At issue was the game manufacturer's "MyPlayer" feature, which allows gamers to create an avatar based upon a three-dimensional facial scan. The plaintiffs argued that Take-Two had violated BIPA's provisions regarding notice and consent, and data storage and dissemination. But the plaintiffs had consented to Take-Two's Terms of Use and were fully aware that avatars would be created. They could not allege that Take-Two had used their avatars for profit. Nor could they identify an actual misappropriation of their biometric data, at best stating only an "enhanced" risk that their data may fall into the wrong hands. "Technical violations" of BIPA were insufficient, in this instance, to support standing.

Perhaps predictably, Facebook has also faced challenges under BIPA based on its facial recognition technology. The *In re Facebook Biometric Information Privacy* case is currently stayed pending a decision in the *Spokeo* case, which was remanded by the Supreme Court last summer. Should the case go forward, one of Facebook's defenses is that the Illinois statute is unconstitutional. According to Facebook, the statute—as plaintiffs have applied it—violates the dormant Commerce Clause and restricts interstate commerce.[30]

Apart from challenges to standing or constitutionality, BIPA defendants have also challenged whether or not accused data qualifies as biometric information.

In a case brought against Snapchat, the plaintiffs alleged that the company violated BIPA through implementation of its "Lenses" technology, which allows users to track "facial shapes and expressions" to modify or transform their looks in real time.[31] Although the suit was voluntarily dismissed before Snapchat filed an answer to the complaint, the company was likely to argue that its technology relies not on facial recognition, but on object recognition.[32] While the technology might allow recognition of "a" nose, "an" eye, or "a" face, generally, it does not allow recognition of *specific* faces. And BIPA is intended to protect biometric data that uniquely identifies an individual.

Google has been similarly challenged with BIPA claims, in a case in which the plaintiffs allege that photographs taken on Google Droid devices are automatically uploaded to Google's cloud-based photo service.[33] The plaintiffs also allege that Google immediately scanned each uploaded photograph to create face templates. Google argued, to no avail, that because photographs are not "biometric identifiers" under BIPA, information "derived from" them is similarly outside of BIPA's protection. Face templates, however, *are* within the definition of biometric identifiers, which explicitly includes scans of face geometries.

This year a bill has been introduced to amend BIPA so that—with limited exceptions—private entities may not collect biometric data as a condition to providing goods or services.[34] The amendment makes an exception for companies providing medical services.

Other states have also taken steps to address biometric data privacy, and many are looking to protect broader categories of information than may be protected under BIPA.

Alaska. A bill introduced in January proposes notice and consent requirements before biometric information is col-

lected.[35] It would also restrict the disclosure and/or sale of biometric information and establish a 120-day window in which data must be erased after it has served its purpose.

"Biometric" data is defined a bit more broadly than it is under Illinois law, to mean "fingerprints, handprints, voices, iris images, retinal images, vein scans, hand geometry, finger geometry, or other physical characteristics of an individual." Unlike BIPA, the Alaskan bill includes photographs as biometric data under certain circumstances.

Connecticut. State agencies are required to ensure that contractors implement and maintain certain data security measures when handling confidential information, the definition of which includes "unique biometric data such as fingerprint, voice print, retina or iris image, or other unique physical representation[s]."[36] This year, legislators are considering a proposed bill that would prohibit retailers from using facial recognition software for marketing purposes.[37] Unlike BIPA, the Connecticut legislation does not provide for a private right of action.

Massachusetts. State data security laws already require entities that maintain or store personal information (but do not "own or license" the data) to provide notice of data breaches.[38] Pending legislation proposes to include biometric data within the scope of the existing law, defining it to mean "any unique biological attribute or measurement that can be used to authenticate the identity of an individual, including but not limited to fingerprints, genetic information, iris or retina patterns, facial characteristics, or hand geometry."[39] Unlike BIPA, the Massachusetts law would explicitly include genetic material. And, unlike BIPA (but similar to the pending Connecticut legislation), no private rights of action are contemplated.

Montana. A proposed bill is similar to BIPA in many respects, but applies to any "biologic or behavioral characteristic that uniquely identifies and enables automated recognition of an individual, including but not limited to retina or iris scan, finger or palm print, voice recognition, hand or face geometry, facial imaging, facial recognition, gait recognition, vein recognition, or other biologic or behavioral identifiers."[40] The plain language of the bill suggests that the intent is to provide, in some respects, more protection than BIPA provides. In doing so, however, legislators may have unintentionally introduced a source of confusion. While BIPA covers facial geometry, the pending Montana law applies to facial geometry, facial imaging, *and* facial recognition. Query whether (and what) the distinction is between these forms of biometric data.

New Hampshire. Pending legislation proposes to regulate the collection, retention, and use of biometric information.[41] The proposal is similar to BIPA in that the biometric data that is protected is narrowly defined to include "a retina or iris scan, fingerprint, voiceprint, or record of facial or hand geometry."

Texas. Existing state law regulates the collection, retention, and use of biometric information, which is defined to include "a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry."[42] Similar to the proposed legislation in Connecticut and Massachusetts, there is no private right of action, as there is under BIPA. But civil penalties for violations may be imposed in actions initiated by the state attorney general.

Washington. Legislation in Washington that amends the state's consumer protection and "disposal of personal information" laws to protect biometric identifiers recently passed.[43] The law defines "biometric identifier" to mean "data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual," but excludes physical or digital photographs, as well as video or audio recordings or data generated therefrom.[44]

We might expect to see litigation regarding what does—and does not—qualify as a biometric identifier under Washington state law. For example, voiceprints qualify. But a voice may be captured in an audio recording, which can then be used to generate a voice print.[45] Would a voiceprint generated from an audio recording fall within the scope of the act, or not?

Wisconsin. Like Massachusetts, Wisconsin law requires notification in the event of a data breach.[46] Biometric data, defined to include "fingerprint, voice print, retina or iris image, or any other unique physical representation" is protected, as is an individual's genetic information.

Federal Law. In addition to state data privacy laws, some federal laws may also be implicated depending on the nature of the biometric data, and the context in which the data is collected, used and stored:

- Individually identifiable health information is protected by the Health Insurance Portability and Accountability Act (HIPAA), but HIPAA's privacy rules apply only to certain entities handling health data, including providers and health plans.
- The Genetic Information Nondiscrimination Act (GINA) prohibits discrimination in insurance and employment based on genetic information.
- The Federal Privacy Act restricts access to—and disclosure of—any individual biometric data that is contained within federal records.
- Under Title 18 of the federal code, state motor vehicle departments are restricted in their abilities to disclose information they have obtained when licensing drivers.[47]
- Various federal regulatory agencies have guidance regarding handling biometric data, such as in the context of mobile medial apps, or when facial recognition software is utilized.[48]

The patchwork of applicable laws in the United States should be cause for concern. Once biometric data is digitized, it can very quickly be disseminated. By way of illustration, data transmission over the Internet is predicted to exceed 2.3 zettabytes annually within just the next three years. Fur-

thermore, the majority of that traffic will be through mobile devices.[49] As a result, it will progressively be easier and easier to send digital data (including biometric digital data) anywhere at all at the drop of a hat.

The lack of a uniform approach to protecting biometric data is problematic for all of the same reasons the lack of a uniform data security standard is problematic. Any individual who finds that his or her biometric data is compromised must determine which minimal protections are available.[50] A high degree of protection in one jurisdiction is of limited use if—in other jurisdictions—there is no protection for the same data. A private lawsuit may or may not be an available option. And, even if it is, current biometric statutes provide for limited damages. Under BIPA, a prevailing aggrieved party may recover up to $5,000 in liquidated damages or "actual damages," to the extent they are greater.[51]

Given that plaintiffs in privacy cases have had a difficult time proving injuries in fact (sufficient to confer standing in federal court), litigants should also expect there to be difficulty in proving up the value of hacked biometric data. Qualitatively, individuals are likely to view targeted marketing on Facebook differently than they view having their fingerprints or retina scans stolen. But whether this qualitative difference is translatable into a sufficiently concrete injury, so as to meet the burden of proving damages, remains to be seen.

Similarly, entities involved in collecting, storing and transmitting biometric data are also at a disadvantage because they must contend with requirements that differ among states, as well as between state and federal law. It is difficult for them to assess what liabilities they may have, and what their obligations are in the event of a breach. Moreover, any entity with an international presence must be mindful of additional protections that may be available overseas, in particular in Europe. The European Union approved a General Data Protection Regulation (GDPR) that is set to come on line in 2018.[52] The GDPR applies not only to organizations that are established in the EU, but also to any entities that sell goods or services within the EU. Biometric data is defined broadly and encompasses any personal data resulting from the technical processing of physical, psychological, or behavioral characteristics of an individual. Genetic and biometric data that is processed to uniquely identify an individual should be handled with enhanced protections, and the new law will allow national data protection authorities to impose significant fines for violations.

Companies looking to rely on biometric information for any purpose would do well to ensure that they are well informed regarding current jurisdictional differences in regulations, and that they watch closely to see how the law in this area develops. As rapidly as biometric technology is evolving, things are bound to get more and more interesting. ■

---

1 Anita Balakrishnan, *Next iPhone May Have Facial Recognition Instead of a Fingerprint Reader, Says Jpmorgan*, CNBC.com (Feb. 15, 2017), http://www.cnbc.com/2017/02/15/apple-new-iphone-biometric-scanners-faces-fingerprints.html.

2 Kaveh Wadell, *Half of American Adults Are in Police Facial-Recognition Databases*, Atlantic (Oct. 19, 2016), https://www.theatlantic.com/technology/archive/2016/10/half-of-american-adults-are-in-police-facial-recognition-databases/504560/; Jeff John Roberts, *Homeland Security Plans to Expand Fingerprint and Eye Scanning at Borders*, Fortune (Sept. 12, 2016), http://fortune.com/2016/09/12/border-security-biometrics/; Press Release, New York State, Governor Cuomo Announces More than 100 Arrests Since Major Enhancement to DMV's Facial Recognition Technology (Aug. 24, 2016), https://www.governor.ny.gov/news/governor-cuomo-announces-more-100-arrests-major-enhancement-dmvs-facial-recognition-technology. .

3 *Will Knight, Paying with Your Face. Face-Detecting Systems in China Now Authorize Payments, Provide Access to Facilities, and Track Down Criminals. Will Other Countries Follow?* MIT Tech. Rev. (Feb. 2017), https://www.technologyreview.com/s/603494/10-breakthrough-technologies-2017-paying-with-your-face/.

4 *See, e.g.*, Taylor Bloom, *Hypergolic Helps Ensure Athlete Biometric Data Privacy Is Properly Managed, Protected And Monetized*, SportTechie (Nov. 14, 2016), http://www.sporttechie.com/2016/11/14/industryinsights/start up-profile-series/hypergolic-helps-ensure-athlete-biometric-data-privacy-is-properly-managed-protected-and-monetized/.

5 Alan Goode, *Biometric Trends for 2017*, Veridium (Dec. 15, 2016), https://www.veridiumid.com/blog/biometric-trends-for-2017/; Luke Graham, *Biometrics: The Future of Digital Security*, CNBC.com (Apr. 5, 2016), http://www.cnbc.com/2016/04/05/biometrics-future-of-digital-cyber-security.html; April Glaser, *Biometrics Are Coming, Along with Serious Security Concerns*, Wired (Mar. 9, 2016), https://www.wired.com/2016/03/biometrics-coming-along-serious-security-concerns/.

6 Biometric Systems: Technology, Design and Performance Evaluation 1–3 (James Wayman et al. eds., 2005).

7 New Directions in Behavioral Biometrics 1–2 (Khalid Saeed et al. eds., 2017).

8 *Nymi Heartbeat Biometrics Authenticates Wearable Payment*, FindBiometrics (Aug. 11, 2015), http://findbiometrics.com/nymi-payment-28114/.

9 John Zorabedian, *Your Smartphone Fingerprint Reader Could Be Hacked Using Paper and Ink*, Sophos (Mar. 8, 2016), https://nakedsecurity.sophos.com/2016/03/08/your-smartphone-fingerprint-reader-could-be-hacked-using-paper-and-ink/.

10 Joseph N. Pato & Lynette I. Millett, *Introduction and Fundamental Concepts*, *in* Biometric Recognition: Challenges and Opportunities 45 (National Academies Press 2010).

11 Biometric Systems: Technology, Design and Performance Evaluation, *supra* note 6, at 8–14.

12 *Biometric Security Poses Huge Privacy Risks*, Sci. Am. (Jan. 1, 2014), https://www.scientificamerican.com/article/biometric-security-poses-huge-privacy-risks/.

13 Marina Koren, *About Those Fingerprints Stolen in the OPM Hack*, Atlantic (Sept. 23, 2015), https://www.theatlantic.com/technology/archive/2015/09/opm-hack-fingerprints/406900/.

14 Lazaro Gamio & Chris Alcantara, *How Data Breaches Grew to Massive Proportions in 11 Years*, Wash. Post (Dec. 14, 2016), https://www.washingtonpost.com/graphics/business/the-scale-of-large-hacks/; Robert Hackett, *Data Breaches Now Cost $4 Million on Average*, Fortune (June 15, 2016), http://fortune.com/2016/06/15/data-breach-cost-study-ibm/.

15 *See generally* Bradyn Fairclough, *Privacy Piracy: The Shortcomings of the United States' Data Privacy Regime and How to Fix It*, 42 Iowa J. Corp. L. 461, 474 (2016).

16 *See generally* Nicholas Green, *Standing in the Future: The Case for Sub-*

*stantial Risk Theory of "Injury in Fact" in Consumer Data Breach Class Action*s, 58 B.C. L. Rev. 287 (2017).

[17] Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1547–48 (2016).

[18] *Id.* at 1549, 1550.

[19] Meyers v. Nicolet Restaurant of De Pere, 843 F.3d 724 (7th Cir. 2016); Cruper-Weinmann v. Paris Baguette Am., Inc., No. 13-cv-7013, 2017 U.S. Dist. LEXIS 13660 (S.D.N.Y. Jan. 30, 2017).

[20] Braitberg v. Charter Commc'ns, Inc., 836 F.3d 925 (8th Cir. 2016).

[21] Carlsen v. GameStop, Inc., 833 F.3d 903 (8th Cir. 2016) (holding that plaintiffs had standing, but affirming dismissal based on plaintiffs' acceptance of defendant's terms of service).

[22] Van Patten v. Vertical Fitness Group, LLC, No. 14-55980, 2017 U.S. App. LEXIS 1591 (9th Cir. Jan. 30, 2017) (holding that plaintiffs had standing, but affirming a grant of summary judgment for defendants on the TCPA claims based on consent).

[23] Galaria v. Nationwide Mutual Ins. Co., Nos. 15-3386, 15-3387, 2016 U.S. App. LEXIS 16840 (6th Cir. Sept. 12, 2016).

[24] *In re* Horizon Healthcare Servs. Inc., 846 F.3d 625 (3d Cir. 2017).

[25] Beck v. McDonald, Nos. 15-1395, 15-1715, 2017 U.S. App. LEXIS 2095 (4th Cir. Feb. 6, 2017).

[26] *Id.* at *268.

[27] Biometric Information Privacy Act, 740 Ill. Comp. Stat. Ann. 14/1 through 14/20 (2016).

[28] Rebecca Campbell, S*hutterfly Settles Illinois Privacy Class Action over Facial Recognition Tech*, Cook County Record (May 9, 2016), http://cookcountyrecord.com/stories/510723060-shutterfly-settles-illinois-privacy-class-action-over-facial-recognition-tec; see generally Norberg v. Shutterfly, Inc., 15-cv-05351 (N.D. Ill. 2016); Gabe Friedman, *First Settlement Reached Under Illinois Biometric Law*, Bloomberg Law (Dec. 5, 2016), https://bol.bna.com/first-settlement-reached-under-illinois-biometric-law/.

[29] Opinion and Order Granting Motion to Dismiss Second Amended Complaint, Vigil v. Take-Two Interactive Software, Inc., 15-cv-8211 (S.D.N.Y. Jan. 30, 2017), D.I. 74.

[30] Amended Answer at 30, *In re* Facebook Biometric Privacy Litig., 3:15-cv-03747 (N.D. Cal.), D.I. 169; Justin Lee, *Facebook Says Illinois Biometrics Privacy Law Violates Constitution*, BiometricUpdate.com (Nov. 21, 2016), http://www.biometricupdate.com/201611/facebook-says-illinois-biometrics-privacy-law-violates-constitution.

[31] Complaint ¶ 27, Martinez v. Snapchat, Inc., 16-cv-05182 (C.D. Cal. July 14, 2016), D.I. 1.

[32] Will Yakowicz, *Snapchat Sued Under Illinois Biometric Information Usage Law*, INC (July 18, 2016), http://www.inc.com/will-yakowicz/snapchat-sued-illinois-biometrics-information-privacy-act.html.

[33] Rivera v. Google Inc., No. 16-cv-02714, 2017 U.S. Dist. LEXIS 27276 (N.D. Ill. Feb. 27, 2017).

[34] House Bill No. 2411, 740 ILCS 14/15 http://www.ilga.gov/legislation/100/HB/10000HB2411.htm

[35] House Bill No. 72, An Act Relating to Biometric Information (Jan. 20, 2017), http://www.legis.state.ak.us/basis/get_fulltext.asp?session=30&bill=HB72.

[36] Public Act No. 15-142, An Act Improving Data Security and Effectiveness (July 1, 2015), https://www.cga.ct.gov/2015/ACT/PA/2015PA-00142-R00SB-00949-PA.htm.

[37] Proposed House Bill No. 5522, An Act Prohibiting Retailers from Using Facial Recognition Software for Marketing Purposes (Jan. 2017), https://www.cga.ct.gov/2017/TOB/h/2017HB-05522-R00-HB.htm.

[38] Security Breaches, Mass. Gen. Laws Ann. 93H, §§ 1–6 (2016).

[39] Proposed House Bill No. 225, An Act Updating Chapter 93H Data Security Protections To Include Biometric Information (Jan. 2015), https://malegislature.gov/Bills/189/House/H225.

[40] Proposed House Bill 518, Act Establishing the Montana Biometric Information Privacy Act (2017), leg.mt.gov/bills/2017/BillPdf/HB0518.pdf.

[41] Proposed House Bill 523, An Act Relative to Limitations on the Use of Biometric Information (2017), https://legiscan.com/NH/text/HB523/id/1456913/New_Hampshire-2017-HB523-Introduced.html.

[42] Personal Identifying Information: Biometric Identifiers, Tex. Bus. & Com. Code § 503.001 (2016).

[43] J. Stang, *Washington State Passes Bill to Prevent Sale of Biometric Data Without Consent*, Geek Wire (Apr. 14, 2017), http://www.geekwire.com/2017/washington-state-passes-bill-prevent-sale-biometric-data-without-consent/.

[44] Proposed House Bill 1094, An Act Relating to Biometric Identifiers (Jan. 12, 2015), http://lawfilesext.leg.wa.gov/biennium/2015-16/Pdf/Bills/House%20Bills/1094-S.E2.pdf.

[45] S*ee, e.g.*, *Privacy International*, Biometrics, https://www.privacyinternational.org/node/70 (last accessed Apr. 20, 2017).

[46] Notice of Unauthorized Acquisition of Personal Information, Wis. Stat. § 134.98 (2017).

[47] S*ee generally* The HIPAA Privacy Rule, https://www.hhs.gov/hipaa/for-professionals/privacy/; EEOC's Final Rule on Employer Wellness Programs and the Genetic Information Nondiscrimination Act, https://www.eeoc.gov/laws/regulations/qanda-gina-wellness-final-rule.cfm; Privacy Act of 1974, https://www.justice.gov/opcl/privacy-act-1974; 18 U.S.C. § 2721.

[48] FDA, *Mobile Medical Application*s (Sept. 25, 2013), https://www.fda.gov/MedicalDevices/DigitalHealth/MobileMedicalApplications/ucm255978.htm; Press Release, Fed. Trade Comm'n, *FTC Recommends Best Practices for Companies That Use Facial Recognition Technologie*s (Oct. 22, 2012), https://www.ftc.gov/news-events/press-releases/2012/10/ftc-recommends-best-practices-companies-use-facial-recognition; *see generally* Timothy S. Hall, *The Quantified Self Movement: Legal Challenges and Benefits of Personal Biometric Data Tracking*, 7 Akron Intell. Prop. J. 27 (2014).

[49] *The Zettabyte Era—Trends and Analysis—Cisco*, Cisco (June 2, 2016), http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.html.

[50] *See, e.g.*, J.C. Pierce, *Note: Shifting Data Breach Liability: A Congressional Approach*, 57 Wm. & Mary L. Rev. 975, 985 (2016).

[51] 740 Ill. Comp. Stat. Ann. 14/20.

[52] Sam De Silva & Anthony Liu, *Europe's Tough New Laws on Biometrics*, Biometric Technology Today 5–7 (Feb. 2017).