ISSN 2616-5783 Vol.4, Issue 1: 19-23, DOI: 10.25236/AJHSS.2021.040104

Biometric Information Privacy Act: Statutes, Litigation, and Future

Yang Dong

School of Law, Southwest Minzu University, Chengdu 610041, China
1809152977@qq.com

Abstract: *The widespread use of biometric information has motivated more litigations under BIPA, especially after the case of Rosenbach v. Six Flags Entertainment. To give more specific protection of the citizens, the state should not just rely on the federal judgment decisions to give their opinionsm and make independent and concrete interpretations of the term "aggrieved". The infringed party can get more substantial protection from the state justice while the legislation still seems to have a long way to go.*

Keywords: *BIPA, Rosenbach v. Six Flags Entertainment, biometric information*

1. Introduction

Biometric information is the technical terms to describe human characteristics. It refers to but is not limited to fingerprint, facial features, palm veins, DNA, iris. Behavioral characteristics are also a kind of biometric information, related to the pattern of behavior of a person, including but not limited to typing rhythm, gait, and voice.

To solve the problem that password is too easy to be cracked, technology companies developed biometric information authorization. Unlike other unique identifiers, it's not readily accessible to other people. And gradually it replaces traditional protection ways with the trend that more and more people have more than one electronic device and internet accounts. A perfect example is that we used our password to unlock iPhone 5s but now iPhone X asks us for face ID. A paragraph in BIPA also clearly explain the reason:

Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual;

However, the more popular it is, the more risks it faces. "once compromised, the individual has no recourse, [and] is at heightened risk for identity theft." In China, Alipay, the largest third-party mobile and online payment platform, in 2014, discovered an employee plotting to steal and sell more than 20 Gigabyte user data including fingerprint. In India, people sold access to Aadhaar data, which is the official collection of 1.13 billion citizens' fingerprints, faces, and irises on WhatsApp, for alarmingly low prices. In USA, Equifax reported that the names, Social Security numbers, and dates of birth of 143 million consumers had been exposed. Also recently, 50 million user's data is at risk because breached Facebook network.

To conclude, data thieves are adding biometric database to their potential preys and a strong regulation is emergently needed.

2. Comparison among statutes in Illinois, Texas, and Washington.

Till now, three states have released act on biometric information protection. Illinois is the first state to regulate tech firms on biometric info leak. It passed Biometric Information Privacy Act ("BIPA") in 2008. Then Texas codified the rules in 2009. In 2017, Washington State signed into law House Bill 1493, which establishes requirements of collecting and using biometric identifiers for commercial purposes. And more biometrics bills remain pending. In Massachusetts, the legislature is considering a bill including regulatory framework on biometric indicators. In New Hampshire, more restrictions on biometric identifiers or information will be valid if the bill successful earns most of representatives'

ISSN 2616-5783 Vol.4, Issue 1: 19-23, DOI: 10.25236/AJHSS.2021.040104

heats. In Alaska, a bill about full consent of using biometric data and private right of damage is being considered. Similarly, Connecticut, Montana, California, and New York, have proposed or are proposing bills regarding biometric information from 2014 to now. But among all these states, acts in Texas, Illinois and Washington are most representative. Each of these laws is similar in general concept: notice and consent for collection are required, restrictive use of individual biometric identifiers, recovery of violations. But distinctions are also apparent.

2.1 Definition of "Biometric Identifier"

The definitions given by three states are similar but obviously different. Texas and Illinois both define it as "a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry." But Illinois gives more detailed explanation. It excludes physical descriptions, body parts, biological materials, patient information captured for treatment, human anatomy used materials.

Washington's definition looks broader. A "biometric identifier" is "data generated by automatic measurements of an individual's biological characteristics" without a "scan of hand or face geometry" in flowing examples, which means the statute will have limited affection in the context of facial recognition scenarios. It also excludes "physical or digital photograph, video or audio recording or data generated therefrom, or information collected, used, or stored for health care treatment, payment, or operations under the federal health insurance portability and accountability act of 1996."

2.2 Enforcement & Recovery

Significantly, Illinois is the only state with a biometric statute that includes a private right of action, in which ambiguous words garners substantial recent attention today. Texas narrows the party who can "bring an action to recover the civil penalty" to only the attorney general. Washington not only limits the party to the attorney general but also requires that "this chapter…be forced…under the consumer protection act" because of "practices…vitally affecting the public interest" and "a violation…deceptive act in trade…unfair method of competition." In a word, Illinois Act entitles person who suffers damage to direct file a lawsuit without any strict limitation but Texas and Washington are more cautious about the "party."

2.3 Notice & Consent

The third difference between these acts is notice & consent requirement. Illinois has the most detailed standards, then Washington, Texas the last. In Illinois statutory, a "written policy" and the receipt of written authorization are mandatory. But these provisions do not appear in Washington and Texas's statutes. Washington also require "notice…is not affirmative consent." And it provides that "the exact notice and type of consent required to achieve compliance . . . is context-dependent" and requires that notice only be "given through a procedure reasonably designed to be readily available to affected individuals." But Texas only simply requires "inform…before capture" and "receive…consent." All these three statutes have limitations on sell, lease, trade or other kinds of disclosures and retentions but Washington is notable for its longest enumerated list of exceptions. Also, retention and disposal of biometric identifiers are all regulated under three acts. What's more, Washington also sets rules about third party disclose. It provides "a third party…promises the biometric identifier will not be further disclosed...and…not be enrolled in a database for a commercial purpose."

2.4 Enrollment

Regulations of "enroll" in Washington statute also make these statutes distinguishable. In the law, "enroll" is defined as an activity "to capture a biometric identifier of an individual, convert it into a reference template that cannot be reconstructed into the original output image, and store it in a database that matches the biometric identifier to a specific individual." This definition is much wider that that in Illinois and Texas statutes, which only pay attention to single activity of "collecting or capturing biometric identifiers."

2.5 Destroy & Expiration requirement

The last thing to mention is destroy requirement after reasonable use with authorization in Texas statue. It places requirements on mandatory destroying, saying, "a person who possesses a biometric

ISSN 2616-5783 Vol.4, Issue 1: 19-23, DOI: 10.25236/AJHSS.2021.040104

identifier…for a commercial purpose shall destroy the biometric identifier within a reasonable time." Also, if a biometric identifier is captured for security purpose, the purpose "…is presumed to expire on termination of the employment relationship." Similarly, In Illinois statute, it requires a private entity "establishing…guidelines for permanently destroying biometric identifiers…when the initial purpose…satisfied" or "within 3 years of the individual's last interaction." But nothing related destroy appears in Washington statute.

To conclude, the widely use and serious leak of biometric information leak has successfully raised public's awareness of its importance. Some states have released statutes and posed regulation on giant firms by various recovery ways. Illinois, however, as the only state which allows private right of action, is facing a growing number of litigation and controversial interpretation of specific provisions.

3. The Analysis of the Lawsuits under BIPA in Recent Years

3.1 The Causes of Actions under the Statute

According to the above comparative analysis among several states, we find that citizens of Illinois are entitled to more robust protections under BIPA since Illinois is now the only state that allows a private cause of action for violation of BIPA, which is why there has been a multitude of new class action BIPA cases filed in Illinois with voracious Plaintiff's firms. Although the act is promulgated in 2008, the wave of litigations has not been provoked in Illinois until these years due to the increase in popularity of fingerprint timekeepers.

In these cases, to pursue the statutory damages, the plaintiffs have to evince the existence of the "aggrieved person" according to BIPA, which states that "any person aggrieved by a violation of this Act shall have a right of action in a State circuit court or as a supplemental claim in federal district court against an offending party". One interpretation refers being aggrieved to the only breach of the substantive privacy rights under the common law, like the dissemination of the personal biometric information during the business's use, storage and transformation which is written explicitly by legislation. The second opinion points out that being aggrieved can also means the deprivation of the procedural right of being informed, which is more complex than the breach of the substantive one. Recently with the development of the class BIPA-related litigation, whether the interpretation should be expanded to the procedural breach has become the main controversy.

More complexly, the federal and state courts always have diverse interpretations of the key word "aggrieved" under the common law and the BIPA. Theoretically the "standing to sue in Illinois state court is unaffected by [federal] decisions", but the state judges may still refer to the federal judgments in practice since the statute texts are so vague and ambiguous and the federal judgments can be more authoritative and convincing. Nevertheless, noting the pressure from the flood of litigations, both the federal and state judges are also adjusting their conclusions and views recently, which makes the BIPA-related judgments more unpredictable.

3.2 Reflecting on the Standing Clause: Can Mere Procedural Breach Constitute an Actual Injury?

Unlike Washington and Texas, in Illinois, citizens have private rights of action authorized by BIPA. So it is more convenient for citizens to file lawsuits but the businesses may in response easily slip into in the bog of lawsuits. Comparatively, despite growing public attention to the privacy and data security implications of collecting biometric information, the decade-old BIPA is the only biometrics privacy statute providing for a private right of action. Comparatively, other two states—Texas and Washington—presently have biometric statutes, nonetheless there only the state's attorney general can pursue enforcement and move the case to the court but the citizens can not. Nowadays, consumer-based business collection of the personal data from the consumers has become the main source of the BIPA-related actions. To avoid the high damages and long time cost, BIPA defendants thus are more willing to use litigation trickiness to "challenge the plaintiffs' standing or right to use" in either federal or state courts rather than focus solely on the substantive one.

BIPA has enforced businesses to provide notice to and obtain consent from the consumers before they use the biometric data collected from the individuals. The case analysis reveals that most federal courts concluded that "violation of BIPA's notice and consent requirement alone is not adequate injury to establish standing to sue in federal court under Article III of the U.S. Constitution". However, the judgments of the state courts are more variable and thus more unpredictable.

ISSN 2616-5783 Vol.4, Issue 1: 19-23, DOI: 10.25236/AJHSS.2021.040104

In the federal level, the judges hold that the procedural breach of informing obligation is frivolous because the so-called breach is not concrete and precise enough to render a party "aggrieved" under the Act III. In *Robins v. Spokeo, Inc.*, the judges reiterate that the "concrete and particularized harm" can constitute the statutory violation. So just "a deprivation of a procedural right" like the right to be informed of the use and the risk is not adequate enough to "create Article III standing". In *Spokeo*, the federal courts support the defendant's claim that actual damages like "disseminat[ing] or [selling] the biometric data to third parties" should exist to constitute the actual injuries. That is to say, injuries stemming from violating the privacy right in the personal biometric data, rather than the procedural infringement of the BIPA-related notice and consent provisions alone, really count in judging the standing of an "aggrieved person". This rule has also been adopted and cited frequently by United States District Court for the Northern District of Illinois in dealing with the BIPA-related issue.

But recently, United States District Court for Northern District of California in *Patel v. Facebook, Inc.* states that mere disregarding BIPA's notice and consent requirements can also be interpreted to be a kind of concrete substantial injury. Northern District of Illinois in *Monroy v. Shutterfly Inc.* also holds that notice and consent rights are as equally important as the substantial right, which can constitute the actual substantial injury without alleging any harm or injury to a substantive privacy right under the common law. Thus, these recent decisions indicate the circuit split in how to interpret *Spokeo*.

The state court's jurisprudence comparatively remains more in flux with "subsequent rulings falling both ways". Some state courts hold the plaintiffs' claim can be justified by the Illinois legislature's intent. And the federal court's wrong interpretation of the BIPA would "lead to undesirable consequences for the vindication of substantive rights or the deterrence of socially undesirable conduct." The *Rosenbach*'s holding in the Illinois appellate court holds that a "person aggrieved by a violation of [the] Act" must allege some harm. On the contrary, in July 2018, The Center for Democracy &Technology filed an amicus brief on *Rosenbach v. Six Flags* with the Illinois Supreme Court, which alleges that the language, purpose and structure of BIPA all support that mere procedural violations of BIPA's consent requirements are actionable under the statute. Other lower courts followed *Rosenbach* also supported the plaintiffs' BIPA claims on this issue.

Factually, the federal court has wrongfully reckoned that the BIPA should share the same standing purposes with Article III. It is BIPA, not the common law, that defines the applicable standard of being aggrieved and getting damages in Illinois. The intention to specifically protect individuals' biometric data under BIPA requires that the consumers' procedural rights to be noticed and getting the consent is more than just a " technical" one, but itself can be interpreted to be important and concrete.

4. Conclusion

The widespread use of biometric information has motivated more litigations under BIPA, especially after the case of *Rosenbach v. Six Flags Entertainment* When actually injured by a violation of privacy right, the plaintiffs may better choose the federal court for the lawsuit to proceed since the common law is more concrete, developed and protective. But for the BIPA defendants who seek to remove the lawsuit to federal courts, "whether removal is the best strategy in each case" should be reconsidered because they need to prove the appropriate standing of the plaintiffs. Sometimes, however, the claim of inadequate standing under the Article III can also be defendant's tricky litigation strategy. The defendant may get benefits when the case is remanded back to state court for the lack of standing. Because the lower courts can easily be influenced by the federal judgments and opinion on the standing issue.

The tricky skills are based on the strategies of misinterpreting the word "aggrieved" in BIPA-related cases. More scholars are doubting that the insufficient interpretation is opposite to the state legislation purpose. Thus to give more specific protection of the citizens, the state should not just rely on the federal judgment decisions to give their opinions. Some scholars also strengthen that it's worth noting that standing to sue in Illinois state court should not be affected by these decisions. That is to say, the state courts should be really independent and make the final decision out of the citizens and the state's interests. Thus the state should make independent and concrete interpretations of the term "aggrieved". Under the background of ruling the businesses' behaviors stringently, the Illinois state courts should equal the procedural infringement with the actual injury and expand the means of "aggrieved" from the common law. In this way, the infringed party can get more substantial protection from the state justice while the legislation still seems to have a long way to go.

ISSN 2616-5783 Vol.4, Issue 1: 19-23, DOI: 10.25236/AJHSS.2021.040104

References

[1] Claudia Cuador, From Street Photography to Face Recognition: Distinguishing between the Right to Be Seen and the Right to Be Recognized, 41 Nova L. Rev. 237 (2017) (At common
[2] David J. Baldwin; Jennifer Penberthy Buckley; D. Ryan Slaugh, Insuring against Privacy Claims following a Data Breach, 122 Penn St. L. Rev. 683, 726 (2018).
[3] Daveante Jones, Protecting Biometric Information in Arkansas, 69 Ark. L. Rev. 117 (2016)
[4] J. Maria Glover, The Structural Role of Private Enforcement Mechanism in Public Law, 53 Wm. & Mary L. Rev. 1137, 1218 (2012).
[5] Daveante Jones, Protecting Biometric Information in Arkansas, 69 Ark. L. Rev. 117 (2016).
[6] Hannah Zimmerman, The Data of You: Regulating Private Industry's Collection of Biometric Information, 66 U. Kan. L. Rev. 637 (2018)