

5 CMET (2018) 72

Scanning Your Way In: An Analysis of Legal Framework Around Collection and Treatment of Biometric Data

by

Arushi Gupta and Sanchit

ABSTRACT—*Imagine walking into a bank and having your account details flash onto the teller's computer screen before you even say a word. Or consider what it would be like to call your institution's customer service line and not have to bother going through the laundry list of your name, birth date, PIN and security questions. All of this started with a fingerprint sensor. Using a person's biological characteristics to verify identity is known as biometric authentication. In a variety of government and private domains, biometric recognition is being promoted as a technology that can help provide better control of access to physical facilities and financial accounts help identify criminal elements, and increase the efficiency of access to services. Biometric recognition has been applied to identification of criminals, patient tracking in medical informatics, and the personalization of social services, among other things. Despite substantial effort, however, there remain unresolved questions about the effectiveness and management of systems for biometric recognition, as well as the appropriateness and societal impact of their use. Like any new technology, this one has also come under the scanner of security and legal regulation. This article aspires to present a comparative analysis of the approaches taken to protect biometric data by various jurisdictions across the globe while fleshing out their shortcomings. By engaging in a scrutiny of the case law material available on the subject, the authors will also try to lay down a few guidelines for both data subjects and organizations dealing with biometric data.*



Page: 73

INTRODUCTION

The use of biometric data in our everyday life has increased tremendously over the past few years. Gone are the days when use of biometric data was limited to investigating crimes and authenticating financial documents. From unlocking your smartphone with your fingerprint to logging your attendance at work, biometric data has engulfed our world like a giant whale. The science of analysing physical or behavioural characteristics specific to each individual in order to be able to authenticate his or her identity is the new world order now.¹ Once the bread and butter for sci-fi movies, biometric technology has now become a quintessential part of everyday life with its pervasive usage in online and mobile services - social networking websites and smartphone manufacturers.

In non-professional terms, a *biometric* is a unique, measurable, biological characteristic or trait for automatically recognizing or verifying the identity of a human being. As per the Indian Aadhaar Act, biometric information means photograph, fingerprint, iris scan, or such other biological attributes of an individual as may be specified by regulations.²

The use of biometric characteristics as a means of identification is not a new

concept. By 1926, law enforcement officials in several United States (hereinafter US) cities had begun submitting fingerprint cards to the Federal Bureau of Investigation (hereinafter FBI) in an effort to create a database of fingerprints from known criminals. Human experts in the law enforcement field were subsequently able to manually match fingerprint samples collected at a crime scene against the prints in this criminal database.³ Years of research by pioneers (such as Lee and Gaensslen⁴) in developing accurate and distinctive fingerprint classification schemes made these manual matching processes feasible by drastically reducing the required database search space. This led to law enforcement agencies such as the FBI investing capital and effort into development of automated fingerprint identification systems. These systems are now exceedingly commonplace, from protecting banks to securing your Instagram profile.⁵ A system to scan the geometry of a human hand was devised as an access control measure in the 1970s. Interest in biometric identification eventually moved, in the mid-1980s, from measuring characteristics of the hand to mapping characteristics of the eye. A few new, innovative



Page: 74

approaches are also being examined for biometric analysis - for instance, ear shape, DNA, keystroke (typing rhythm), and body odour.

One need not be a technological savant to understand the ramifications of this advancement. Terabytes of personal data in the form of facial geometry, fingerprints, voice samples et al. now reside in data centres owned by private enterprises like Google and Facebook. To add insult to injury, the business practices of these providers tend to exhibit a certain degree of insensitivity for transparency especially when it comes to collection and manipulation of personal data. This has led to the enactment of stringent regulatory measures in many jurisdictions across the globe. This article is an attempt to examine the laws regulating biometric data and judicial developments thereon with central focus on one of the first laws in the United States to tackle with the subject of biometric data privacy, the Illinois Biometric Data Privacy Act of 2008 (hereinafter BIPA).⁶ Through an analysis of the recent uptick in litigation against Big Data, we will try to establish the strengths and weaknesses of BIPA while drawing parallels with the European Union data protection law and the recent developments in Asia Pacific and India. Finally, the authors would highlight the risks of utilization of biometric data and suggest practices to be adopted by organisation to ensure compliances and escape litigations on the subject matter.


LEGISLATIVE STRUCTURE IN DIFFERENT GEOGRAPHIES

The United States of America

When 'Pay by Touch' first introduced the payment system that made use of an individual's fingerprints in 2007 to authenticate payments, it completely revolutionized the market. The idea of getting rid of complex alphanumeric passwords and the heightened sense of security that it brought, made the public lap it up rapidly. However, with the advent of new technology the need for legal framework to govern it arose and gave rise to enactment of legislations across the globe.

There is a stark contrast in the manner in which personal data (including biometric data) is protected by different States. With the European Union preparing itself for a full pledged compliance with the General Data Protection Regulation (hereinafter GDPR) by May, 25th 2018, all States are (and ideally should be) in a rush to bring their laws at par with GDPR or at least as close to it as possible to ensure seamless commercial transactions. It is pertinent to examine the different state legislations

revolving around biometric data of an individual, the kind of protection afforded to it and the remedies available in case of violations.

 Page: 75

Illinois was the first US state to come up with an exclusive legislation on biometric data. BIPA came into force with the objective of governing the manner in which biometric data is 'collected, stored and disseminated by private entities'. It is worth noting that BIPA does not restrict the use or the purpose for which the data is being collected. It is applicable to private entities, they being defined as "*any individual, partnership, corporation, limited liability company, association, or any other group, however organized.*"⁷


Section 15 of BIPA captures the spirit of privacy rights of an individual. It requires a private entity to create a policy on retention and destruction of data and making the same publicly available thereafter. It caps the retention of data to a period of 3 years after the last interaction with the individual.⁸ While Section 15(b) defines strict information and consent parameters, section 15(d) puts down the guidelines for disclosure, re-disclosure or otherwise dissemination of biometric identifiers.

The damages under BIPA are classified in relation to the manner in which the breach has occurred. For negligent violations the penalty is \$1,000 per violation in liquidated damages or the amount of actual damages, whichever is greater.⁹ For intentional or reckless violations, liquidated damages hike up to the greater of \$5,000 per violation or actual damages.¹⁰

The Texan Capture or Use of Biometric Identifier Act, 2009 (hereinafter CUBI), unlike its Illinois counterpart provides a much more concise definition of 'biometric identifier', which has been defined to mean a retina or iris scan, fingerprint, voiceprint, record of hand or face geometry.¹¹

CUBI while maintaining strict information and consent requirements for the organizations collecting biometric data¹², also provides that in the event biometric data of an individual is being processed by an organization for commercial purposes, the concerned organization cannot sell, lease or otherwise disclose the information unless one of the following three conditions are met:

- I *The individual consents to the disclosure for purposes of identifying him in the event of his disappearance or death;*
- II *The disclosure completes an authorized financial transaction;*
- III *The disclosure is required or permitted under a state or federal statute, or responds to a warrant from law enforcement.*¹³

 Page: 76

The data collected cannot be perpetually retained and must be destroyed no later than a year from the time the purpose for which it was collected is accomplished.¹⁴ Where the employer for security purposes has collected such data from its employee, the purpose expires on determination of employment.¹⁵ Unlike BIPA, CUBI does not provide for a private right of action and action for civil penalties in the event of statutory violation may be taken only by the Texas Attorney General. The penalty

imposed may go as high up as \$25,000 for each violation.¹⁶

In 2017, Washington became the third US state to have a comprehensive legislation on Biometrics by enacting House Bill 1493 (hereinafter HB 1493). The HB 1493 defines "biometric identifier" as 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 are used to identify a specific individual.¹⁷ This law projects some major deviations from the other two. Firstly, facial recognition data has not been included in the definition. Secondly, the statute leaves out the capturing and processing of data expressly and regulates enrolment of biometric identifier in a database for commercial purposes. Thirdly, the consent and information requirements have been made contextual.¹⁸ Similar to the Texas legislation, it does not provide a right of action to private individuals rather the Washington Attorney General has been empowered to enforce the legislation.

All previously mentioned legislations fail inconclusively stating if the information derived from a photograph or image qualifies as a biometric identifier thus giving rise to multiple litigations that are analysed hereinafter. The other US states are in the process of enacting their biometric data protection legislation and it is expected that they would duly remedy this.

European Union

GDPR defines biometric data as, personal data resulting from specific technical processing related to "the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data".¹⁹

A plethora of rights is bestowed upon the data subjects under Articles 12 to 23, including but not limited to right to rectification, erasure, access, portability, and restriction of processing. Chapter 8 of the GDPR delineates enforcement mechanisms for these rights. GDPR provides that every data subject has the right to lodge a complaint with a supervisory authority.²⁰



The jurisdiction of GDPR is extensive enough to include the subject's place of habitual residence, place of work, as well as the place of alleged violation.²¹ Further, it allows compensation for infringement of the regulations from controller or processor for material and non-material damages suffered; but has left the question of determining the quantum of compensation to the judgment of the member states.²² The states in addition also have to enact rules to govern administrative fines and other penalties for infringement of the regulations.²³

Asia Pacific Nations - Australia and Japan

Taking cue from its western counterparts, Asia Pacific nations has started taking cognizance of the importance of affording adequate protection to biometric data of an individual. Although the legislative developments are still unfortunately minimal, the progress in Japan and Australia is noteworthy.

Japan's data privacy law has been consolidated under the Act on the Protection of Personal Information. The Act as it originally stood did not expressly include biometric data in the definition of personal information; however, the Amended Act on the Protection of Personal Information has remedied the same.²⁴


Australia's Federal Privacy Act, 1988 does not expressly call out biometric data, however, various state legislation of Australian Capital Territory classify biometric

information about an individual as sensitive information.²⁵

India

Looking closer to home, India still has miles to go to catch up with its counterparts in ensuring protection to personal data of its citizens. The first attempt to enact a legislative framework referring to biometric data was made in 2006 as the Personal Data Protection Bill. The bill unfortunately never saw the light of day. In 2013, the Parliament tried once more to resuscitate the issue by introducing the Personal Data (Protection) Bill, 2013 (hereinafter Bill).

The Bill has introduced the concept of biometric identifier into our legal regime by defining it as "any data relating to the physical, physiological or behavioural characteristics of a person which allow their unique identification including, but not restricted to, facial images, finger prints, hand prints, foot prints, iris recognition, hand writing, typing dynamics, gait analysis and

 Page: 78


speech recognition".²⁶ Biometric data has been expressly classified as sensitive personal data.²⁷

The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (hereinafter Aadhaar Act) is a first-of-its-kind Indian legislation dealing with the collection, storage and processing of biometric data. Enacted with the objective of providing for efficient, transparent, and targeted delivery of subsidies, benefits and services, the Aadhaar Act was touted as a positive step in good governance. Through the assignment of unique identification numbers to individuals residing in India, the Aadhaar Act sought to emulate the much-acclaimed US Social Security Number (SSN) system.²⁸ The Unique Identification Number (UID or Aadhaar Number) for each individual is formulated in an amalgamation of factors. The data collected, as part of the Aadhaar scheme is stored with Central Identities Data Repository, which is the central and unified database created under the Act.²⁹ The Act defines biometric information, which also constitutes identity information³⁰, to mean photograph, fingerprint, iris scan, or such other biological attributes of an individual as specified by regulations,³¹ and distinguishes it from core biometric information by excluding photographs from its scope.³² It goes on to classify biometric information as 'sensitive personal data or information' as defined under the Information Technology Act, 2000 (hereinafter IT Act).

The Aadhaar scheme permits a requesting entity (whether an individual or agency)³³, to seek authentication of the UID of an individual in relation to his/her biometric information.³⁴ It is interesting to note that the Aadhaar Act has tried to incorporate some of the GDPR principles:

- I requirement of consent from the individual from whom the data is being collected³⁵;
- II informing the individuals on the nature of information, uses to which the information obtained during authentication shall be put to use, alternatives to providing the said information³⁶; and
- III provision for one's own information³⁷.

However, the Aadhaar Act fails to capture the essence of these requirements being in the nature of rights of the data subjects. The legislation leaves

 Page: 79

an overabundance of issues to be determined by way of regulations that gives excessive scope for politically inclined interpretations and easy violations. The violations of the Aadhaar Act may result in imprisonment that may extend to 3 years in some cases and a penalty with a maximum cap ranging from ten thousand rupees to one-lakh rupees or both.

In the event of violation, recourse can be taken to section 43A of the IT Act, which states that:

"a 'body corporate' possessing, dealing or handling any "sensitive personal data or information" in a computer resource which it owns, controls or operates is negligent in implementing and maintaining "reasonable security practices and procedures", and thereby causes wrongful loss or wrongful gain to any person, this body corporate will become liable to pay damages as compensation to the affected person."

The Apex Court's verdict confirming the right to privacy as a fundamental right³⁸ and determination of the constitutional validity of the UID pending with the court³⁹, indicate movement in the direction of increased emphasis on providing protection to an individual's personal data, including biometric data. Certain issues arising out of the Aadhaar Act, challenging its constitutional validity are however currently *sub-judice* and it would be interesting to note the direction in which the Supreme Court of India gets swayed on it.

Further, the lack of a legislation governing treatment of biometric data by private entities leaves much room for foul play.

AN ANALYSIS OF THE LITIGATIONS UNDER BIPA AND RELATED JUDICIAL DEVELOPMENT

Facial Scan Via Photographs Vis-À-Vis In-Person Facial Scan

In a catena of recent BIPA litigation against social media providers, claimants have strongly maligned their 'photo tagging' features and associated biometric data collection and storage practices. Plaintiffs have focused on the practice of collection of biometric information without adequate notice and consent, failing to provide a retention schedule, and guidelines for permanent deletion after the purpose of collection is served. A few such suits were dismissed for Article III⁴⁰ standing; however, a recurring issue has been whether data collected by mapping the facial geometry from an actual photograph

could be construed as 'biometric identifier' and/or 'biometric information' under BIPA.

Sometime in March 2016, Lindabeth Rivera and Joseph Weiss discovered that through the Google Photos application on an Android smartphone, Google was scanning the user's facial features to create a unique 'face-template' for each user. Both Rivera and Weiss brought a class action suit against Google claiming this as an egregious violation of one of the fundamental tenets of BIPA i.e. the obligation to notify users and seek their prior consent before collection of biometric information. Significantly though the app was not designed to distinguish between the user and non-user (e.g. people apart from the smartphone user who may appear in a group photo), but more on that later.⁴¹

Google attempted to exploit a seemingly apparent ambiguity in the definitions of 'biometric identifier' and 'biometric information' to seek a dismissal of the suit. Their

primary argument was that Rivera and Weiss were in fact aggrieved by Google's usage of their pictures, but BIPA does not cover photographs under the definition of 'biometric information' or any information derived from photographs.

Justice Chang of the Northern Illinois District Court, while dismissing Google's argument, attempted to interpret the definitions of 'biometric identifier' and 'biometric information' under BIPA. In simple terms, according to the judge, a 'biometric identifier' is any biology-based information that can be used to identify a person.⁴² BIPA defines "biometric identifier" in the form of a positive, exhaustive list - retina or iris scan, fingerprint, voiceprint, or scan of the hand or face geometry.⁴³ This contrasts with the myriad of statutory definitions that use generic words like 'record, document, or tangible object'⁴⁴, or the statutes that list out a set of specific items and then add a broader general word, like 'moneys, funds, credits, securities or other things of value'.⁴⁵

To further ensure specificity, the draftsmen go on to provide a negative list i.e. the items, which would not constitute 'biometric identifier':

"Biometric identifiers do not include writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color. Biometric identifiers do not include donated organs, tissues, or parts as defined in the Illinois Anatomical Gift Act or blood or serum stored




on behalf of recipients or potential recipients of living or cadaveric transplants and obtained or stored by a federally designated organ procurement agency. Biometric identifiers do not include biological materials regulated under the Genetic Information Privacy Act. Biometric identifiers do not include information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996. Biometric identifiers do not include an X-ray, roentgen process, computed tomography, MRI, PET scan, mammography, or other image or film of the human anatomy used to diagnose, prognose, or treat an illness or other medical condition or to further validate scientific testing or screening."⁴⁶

The court observed that not all of the above can be treated as true 'exceptions' to the affirmative list of biometric identifiers. To be an exception to the definition, the item must be such that it would automatically form part of the definition but for the legislative rider. Only a few of the above are exceptions; for instance, an X-ray taken of a person undergoing facial reconstruction surgery would not qualify as a biometric identifier, even though it entails a face geometry scan of the patient. The first sentence simply puts out a list of disqualifiers because, according to the court, it would seem dubious to classify someone's signatures as a biometric identifier (because it is not derived from the biology of the person).⁴⁷

Going on to the definition of 'biometric information'⁴⁸, the court observed that the law uses an affirmative method to define this so that private entities cannot evade (or try to evade) BIPA's restrictions by converting a person's biometric information into some other form, such as a unique numeric representation. Therefore, notwithstanding any form of manipulation by the entity, information from a biometric identifier would fall under this definition if said information can be used to identify the person.

Google argued that a reading of the two definitions together suggests that the

legislature only aimed to cover 'biometric identifiers' if they were derived from the person of the subject i.e. only if the subject's face were scanned by a device on the spot the resultant mapping would qualify under the definitions. Whereas a scan of the subject's face from a photograph would be directly excluded by the negative list. Furthermore, Google stated that since the negative list expressly carves out photographs from the definition of 'biometric identifier' a collective reading with the definition of 'biometric information' would suggest that biometric information does not include information derived

 Page: 82


from photographs. In deciding for the plaintiffs Google contended that the statute's 'careful structure' distinguishing the two would collapse⁴⁹, thereby rendering the definitions meaningless.

The court proceeded to knock these arguments off the board by relying on the textual structure of the definitions. A reading of the definition of 'biometric identifier' clearly indicates that it is source-agnostic i.e. it was immaterial how the biometric measurements are obtained as long as they coincided with the positive list.⁵⁰ The court acknowledged that technological advancements may lead to different modes of collecting biometric identifiers and that Illinois legislature would therefore not want to curtail the scope of BIPA by limiting it to identifiers collected by some processes. The court cites fingerprints as a valid example - the definition does not discriminate between fingerprints inked on paper and a digital image thereof. Thus, to say that a scan of face geometry must be only in person would be antithetical to legislative intent.

As for Google's secondary argument, the court noted that the plaintiffs never alleged that the photographs themselves were subject to BIPA's restrictions. Their challenge was only directed to the facial geometry scans derived therefrom. If Google simply captured and stored the photographs and did not measure and generate scans of face geometry, then there would be no violation of BIPA. As noted previously the definition of 'biometric identifier' does not use words like 'derived from a person', 'derived in person', or 'based on an in-person scan', whereas the definition of 'biometric information' does say that it is information 'based on' a biometric identifier to avoid backdoors of format conversion. Hence, there is no parallel structure to rely upon. While the former is set of biological measurements, the latter deals with conversion of those measurements to a usable version.

Google went on to contend that such a sweeping interpretation would lead to any individual using common photo-organizing software being subjected to the BIPA's procedural rigors, relying on its legislative history.⁵¹ The court refused to accept this line of reasoning as well, however, without providing a clear opinion on whether the legislation could actually extend to such length.⁵² The court did albeit state that simply because this scenario is not considered in the legislative history of the legislation, it could not be deemed included (or even excluded) therefrom.

A similar story had previously ensued with Facebook in May 2016. Adam Pezen, Carlo Licata and Nimesh Patel, all of the Chicago area, separately sued the social media giant in 2015, alleging Facebook's 'Tag Suggestion' feature was illegally collecting biometric data from people tagged in photos posted by

 Page: 83

other users. Licata filed his suit in Cook County Circuit Court in April 2015, and Pezen and Patel filed theirs in federal court in April and May 2015. All alleged that Facebook's use of facial recognition software violated the BIPA. The three complaints were combined and transferred to Judge Donato of the Northern District of California.⁵³

Ruling that the trio had in fact made a valid complaint and allowing trial, Judge Donato rejected Facebook's contention that BIPA categorically excluded all information involving or derived from photographs. Using the literal rule of statutory interpretation as expounded in previous cases⁵⁴, the court ruled that the statute was designed to focus on newer technology like scans of facial geometry, whose full ramifications are not known. The definitions of 'biometric identifier' and 'biometric information' indicate that the Illinois legislature enacted BIPA to address emerging biometric technology, such as Facebook's face recognition software, without including physical identifiers that are more qualitative and non-digital in nature. 'Photographs' as used under BIPA can be better understood to mean paper prints of photographs and not digitized pictures uploaded on the Internet.⁵⁵ Consequently, it would go against the grain to exclude data collection processes reliant on digitized images because the scanning of biometric identifiers is often based on an image or photograph.⁵⁶

Probably as a Hail Mary pass, Facebook attempted to use the same line of reasoning as Google - the only way to reconcile the statute's inclusion of 'scan' and exclusion of 'photographs' is to read the word "scan" to mean in-person scan. The court rejected this contention, stating that BIPA is an informed consent privacy law that addresses the collection, retention and use of personal biometric identifiers and information in an era where biometric technology is booming rapidly. Confining the Act's purpose within a specific in-person data collection technique finds no support in either its drafting or intent.

We agree with the court's reading of biometric data obtained from photographs being considered as biometric data for the purposes of BIPA as any interpretation otherwise would amount to bypassing the intent of the legislature to provide adequate protection to biometric data irrespective of its mode of collection.

Further, in *Alejandro Monroy v. Shutterfly Inc.*⁵⁷, the defendant's contention that 'scan of face geometry' implies only in-person scan and not the scan



derived from an image or photograph was denied because the statute does not limit the definition of biometric identifier to scans 'derived' from a person but included all information 'based on' biometric identifier. Therefore, the court in *Monroy* enlarged the scope of biometric data to not only include facial mapping done using images and but fingerprints and retina capture using such images but everything which has not been expressly excluded from the ambit of the legislation. Such a wide interpretation would, on hand would enable individuals to enforce their right to privacy and on the other it would massively restrict the data controllers and processors from any exercising any negligence without due consequences. Legislative clarity on the point shall help settle the deliberation more effectively. It is pertinent to note here that an amendment was proposed to exclude photographs, both digital and physical from the scope of biometric identifiers under BIPA in May 2016 by Illinois State Senator Terry Link. The said amendment however never got passed.

Procedural Breaches of Bipa- 'Person Aggrieved' and 'Actual Damages'

In *Vanessa Vigil v. Take-Two Interactive Software Inc.*⁵⁸, the defendant was a

developer, publisher and distributor of video games. They designed a video game, 'NBA 2K15' and 'NBA 2K16', wherein they introduced the feature of letting the player create a 3D avatar of himself/herself using face mapping technology, termed by them as 'My Player'. A game could be played online with multiple other players who in turn would be able to see the 3D rendition of the gamer's face. To access My Player, the gamer would have to agree to the following term of service:

"Your face scan will be visible to you and others you play with and may be recorded or screen captured during gameplay. By proceeding you agree and consent to such uses and other uses pursuant to the End User License Agreement."

The Plaintiffs bought NBA 2K15 and used the My Player feature. Thereafter they filed claims against the defendant contending the following violations under BIPA:

- I Collection of biometric data without informed consent;
- II Dissemination of biometric data to others during game play without informed consent;
- III failure to inform in writing of the specific purpose and length of term for which biometric data would be stored;



Page: 85


- IV failure to make a retention schedule publicly available and guidelines for permanently destroying plaintiffs' biometric data; and
- V failure to store, transmit, or protect from disclosure plaintiffs' biometric data by using a reasonable standard of care or in a manner that is at least as protective as the manner in which it stores, transmits, and protects other confidential and sensitive information.

The district court took up two issues - firstly, the scope of the procedural right conferred by the statute; and secondly, whether a mere procedural violation would raise a material risk of harm. Though the parties did not contest the first issue, the second issue was answered in the negative. The court held that procedural violations in terms of non-use of the term 'face geometry', non-disclosure of the duration for which data would be stored, do not amount to a material risk of harm⁵⁹ to the plaintiff and the consent obtained by them is a valid consent under the statute. The district court therefore granted defendant's motion to dismiss on the ground that the plaintiffs have failed to establish a just cause of action and that they have a constitutional standing for a procedural violation of law.⁶⁰ While the US Courts has been inconsistent over time, it has now settled upon the rule that 'at an irreducible minimum', the constitutional requisites under Article III for the existence of standing are that the party seeking to sue must personally have suffered some actual or threatened injury that can fairly be traced to the challenged action of defendant and that the injury is likely to be redressed by a favourable decision.⁶¹

The Court of Appeal upheld the decision of the district court in part. While it agreed with the verdict of the district court on the issue that the plaintiffs have failed to showcase Article III standing, it disagreed on the issue that the plaintiffs have failed to establish a cause of action, therefore the district court was remanded with instruction that the dismissal shall be without prejudice.

The *Take-Two* verdict elucidates two important aspects for the subjects enforcing rights and seeking damages under BIPA. First that the violation should have raised or at the least should have the potential of raising material risk in terms of being improperly accessed by third parties. Second, that Article III standing requirements as

propounded under *Spokeo* can be an important limitation on claims based on bare procedural violations of the notice and consent provisions of BIPA.⁶² In addition, the Court of Appeal clarified

 Page: 86

that the plaintiff's inability to show actual injury does not point out that they have failed to establish a cause of action and therefore were afforded another opportunity to amend the complaint.


A similar situation arose in *Rosenbach v. Six Flags Entertainment Corp*⁶³ where the defendants were owners of a themed amusement park and collected fingerprinting data from all the visitors entering the park. The plaintiff's grievance arises out of the said transaction when they purchased a season ticket for the park and the defendant fingerprinted them without obtaining due consent and complying with other regulatory requirements of BIPA. Like *Vigil*, the defendants contended that since no actual damage occurred to the plaintiffs, they are not "aggrieved" as required by the statute and thus the claim brought about is bad in law.

Essentially, the three pronged consent requirement of informing the data subject of the information being collected, purpose and length of time for which the data is being collected and to receive a written consent from the data subjects was alleged to be not followed by the defendants. The plaintiffs claimed that in addition to violating BIPA, the defendants' unjust enrichment from the collection of data. The defendants' challenge rested on the following grounds:

- I whether a person who has not shown any actual injury can be considered as aggrieved based on proper consent not being obtained and proper disclosures not being made;
- II whether a person who has received the benefits of the purchase claim that the purchase itself caused the injury; and
- III whether a plaintiff who fails to establish actual injury is entitled to liquidated damages under BIPA.

The trial court denied the defendants' motion to dismiss. Thereupon, they filed a motion for reconsideration. The appellate court considered the question of whether only the injury because violation of notice and consent requirement would render the plaintiff aggrieved and be sufficient to make them entitled for liquidated damages and/or injunctive relief.

The court applied the principles of statutory interpretation laid down in *People v. Chapman*⁶⁴, which provides that "where the language is clear and unambiguous, this court will apply the statute without further aids of statutory construction". While relying on the definition of 'aggrieved'⁶⁵ and 'aggrieved

 Page: 87

party'⁶⁶ as provided in the *Black's Law Dictionary*, it concluded that an actual injury needs to be showcased before the plaintiff can bring an action under section 20 of BIPA.

The court further upheld *McCullough v. Smarte Carte Inc.*⁶⁷ and *Vigil v. Take-Two Interactive Software Inc.*⁶⁸ on their observation that a mere technical violation without any element of right being adversely affected is not sufficient to bring a private claim

under BIPA. It relied heavily on *Avudria v. McGlone Mortgage Co.*⁶⁹ to interpret the term 'aggrieved', wherein it was treated as synonymous with the term 'injured'. The court however concluded on the note that although depiction of an injury is necessary, such injury may not be pecuniary at all times.

The judges in *Rosenbach* have taken a very conservative approach by bringing literal rule of interpretation into play. In situations wherein something as vulnerable as biometric data is at stake, the application of mischief rule would have been ideal. It would have helped capture the essence of the intention of the legislature in terms of the prominence being afforded to a biometric identifier. The result would naturally be a higher degree of compliance of BIPA by private entities.

The court rendered a contrasting judgment on this issue in *Alejandro Monroy v. Shutterfly Inc.*⁷⁰. Shutterfly operated a website that allowed its users to upload and share their photographs. The website had default facial recognition software which used face mapping technology to create a unique template for each face. The templates were stored in a massive database and every time a new picture is uploaded the website would compare it with the templates in its database and if there is a match found, it would suggest 'tagging' the individual with his/her name - a feature like Facebook's 'Tag Suggestions'. In case no match is found, it prompted the user to add a name.

Monroy contended that while he himself never used Shutterfly, he was tagged in one such picture by a stranger and basis the name, he was able to extract his other personal data such as gender, age, location and age. Monroy had in no point in time consented to storage and processing of his data by the defendant. Monroy therefore brought a class action suit on behalf of similarly situated plaintiffs in Illinois.

The court evaluated the matter considering the following issues - Whether BIPA applies to facial scans obtained from photographs; whether the current suit requires an impermissible extraterritorial application of the statute; and whether the plaintiff need to establish actual damages to bring an action under

BIPA. We have analyzed the first issue in the previous segment; the second is not pertinent to the scope of this article and we would now proceed to evaluate the last one.

One of the most highly contested issues in BIPA suits is whether actual damages is a pre-requisite to any claims made therein. This is made significantly uncertain by the statute as it simply states each prevailing party may recover liquidated or actual damages for each violation. Further, contradictory judgments on the point enhance the uncertainty on the point. An interpretation of the term 'actual damages' by the US Supreme Court in *Federal Aviation Admn v. Cooper*⁷¹ observes that "*the term 'actual damages' has this chameleon-like quality,*" and that while in some contexts it has been "*construed narrowly to authorize damages for only pecuniary harm,*" in other contexts it has been "*understood to include nonpecuniary harm*".

Monroy's plight is distinguishable from *McCullough*⁷² and *Vigil*⁷³ on the ground that in these two scenarios, the plaintiffs had voluntarily given their biometric data to the defendants with only some procedural lapses in the consent and information notices. This nullified their claim for actual damages under the Act. Whereas Monroy had not consented to his data being collected or processed in the first place, therefore raising an additional aspect of invasion of privacy which drove the court towards a more lenient approach.

There is an obvious legislative gap highlighted by the aforementioned judgments, which is, in the event there is a procedural violation under BIPA not causing actual damages, the plaintiffs would be left without a remedy and they need to wait for harm to be caused in order to enforce their right to privacy under the statute. Further, in the absence of a statutory authority being established under the legislation, no adequate action could be taken against the perpetrators. This has been remedied to some extent under CUBI and HB 1493.

TREATMENT OF BIOMETRIC DATA UNDER THE DATA PROTECTION DIRECTIVE (DPD) AND GDPR

The starting point of this discussion in the EU was the opinion of the Working Party established by Article 29 of the Directive 95/46/EC on biometrics of 1 August 2003 (hereinafter opinion WP80).⁷⁴ The opinion WP80 focuses primarily on biometric applications for verification purposes.⁷⁵ The reason for this could be the status of technological advancement in biometric verification back in 2003.



Page: 89

However, since then the techniques have grown leaps and bounds, and there is no doubt about the identification capabilities of biometrics now. So much so that the EU as well member states have established central national register for storage of biometrics (European Dactyloscopy (EURODAC); UK National Identity Register (established under the Identity Cards Act, 2006)).

In the discussion about the principle of purpose and proportionality, opinion WP 80 discusses the example of the use of biometrics for access control purposes and hereby refers to the verification function.⁷⁶ The Working Party also goes on to identify and describe the generic risks associated with biometric data, such as secret capture, the false acceptance rate (hereinafter FAR) and false recognition rate (hereinafter FRR)⁷⁷ and theft. Other risks described, such as surveillance, incompatible re-use, usage as unique identifier and identification are dangers that in principle would only apply if the biometric data is used in a centralized way.⁷⁸

It is worth noting that the key difference on this point between the EU Data Protection Directive (Directive 95/46/EC) (hereinafter DPD) and GDPR is that while in the former the term 'biometrics' does not appear specifically, it is apparently indubitable that their processing would involve "capturing, transmitting, manipulating, recording, storing or communicating sound and image data relating to natural persons". Hence, the DPD applies to processing of such data, and it equates 'personal data' with any information relating to a data subject who can be identified, directly or indirectly, particularly by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.⁷⁹ Whereas the GDPR also makes a distinction between personal data and *sensitive personal data* which is information that relates to health, sex life, racial or ethnic origin, political opinions, religious or philosophical beliefs, and even trade-union membership.⁸⁰ Processing of sensitive personal data is prohibited under the GDPR except in certain exceptional circumstances. In particular, EU legislation explicitly mentions facial images and fingerprints as a form of sensitive personal data.⁸¹

One important exception that allows processing of sensitive personal data is when the data subject gives explicit, free consent.⁸² This is convenient, for example, in applications such as unlocking a mobile phone. However, the use of such applications is still conditional on: (i) sufficient data security is

applied; (ii) the data is not used for unspecified purposes or shared with third parties; and (iii) users are allowed to revoke their consent at any time.⁸³ For the same reason, employers are not typically required to obtain explicit free consent for technology they deploy.⁸⁴ This is because employees can leave organizations when they are uncomfortable with their working practices (which would lead to a revocation of consent), though in reality some may have little real choice.

Current methods of explicit consent often take the form of complex legal terms and conditions that are typically incomprehensible for the person giving consent. Furthermore, such terms often do not reflect actual privacy preferences but the person assents because he/she believes that there is no reasonable alternative.⁸⁵ This may not constitute explicit and free consent for the purpose of GDPR. Additionally, social media providers such as Facebook and Google, which use click-wrap and browse-wrap Terms of Service, might need to revamp their business model specifically for the EU.

CONCLUSION - COMBATING CHALLENGES AND THE WAY AHEAD

The dynamism with which the biometric technology has flooded the markets is commendable and at the same time daunting. The legislature as always has failed to keep pace with the technological developments. While venturing into these waters may seem foolproof at first sight, a closer look reveals the serious security risks. There is a rising concern around protecting privacy of an individual including their biometric and other personal data and though nation states across have taken steps to enact legislations to cope up with the situation, there still remains miles to go.

Every technological development comes with its own banes and so has the use of biometric data. The first and most significant one of the lot is data leakage. In simple terms data leakage is the unauthorized transfer of classified information from a computer or datacenter to the outside world.⁸⁶ It may range from something as simple as mentally remembering the data and reproducing it to sophisticated programming algorithm driven remote and untraceable hacking. If a data center's network is compromised, it may lead to disastrous results especially in terms of physical, financial and reputational security of an individual.

Secondly, data loss is also of major concern. If biometric data is lost, then depending upon pervasiveness of its usage an individual may lose access to even their financial data. A similar situation may arise in security checks at public places such as airports as well as private establishments. Further, if the data loss occurs at a large scale at central repositories, an individual may face identity crisis. The severity of the consequences would however be directly proportional to a system's dependency on biometric data.

Thirdly, biometric data of an individual does not remain static from birth to death. While retinal scans may remain the same, fingerprints and facial characteristics of a person change over years.⁸⁷ Information collected under a centralized scheme such as UID must be updated once the subject attains the age of eighteen years. In the event the information is not updated for any reason whatsoever, it may again lead to loss of access to all linked public services.

From an organization's perspective that collects, stores, or processes biometric data the coast can be secured by ensuring strict consent and information notice requirements. Even before collating biometrics, the individual must be informed of the purpose for which the data is being collected, the duration for which it shall be retained and the data destruction mechanism in place. Moreover, each organization must appoint a named authority whom an individual may contact in respect of such any concerns around his/her data. Further, an express written consent must be obtained; deemed consent is not acceptable in many jurisdictions including under the GDPR regime. Secondly, adequate mechanisms need to be in place to ensure the data collected, is destroyed on all fronts once the purpose for which it was collected is extinct. Lastly, click-wrap and browse-wrap agreements must be done away with and visible notice must be given to the individual on applicable Terms of Service. In situations where the data is being collected physically, notices must be displayed at all conspicuous locations. The above recommendations, if put in place would save the organization from the wrath of not only data privacy authorities but also data subjects.

Bearing in mind the above highlighted risks, the policymakers need to bring themselves to speed and salvage the situation by striking the perfect balance between ensuring privacy of an individual and securing commercial interests of enterprises. Since we are living in an age of extreme dependency on personal data in all walks of life and business, a robust system to secure usage of such data would bolster transactions manifold.

* Senior Executives (Legal and Compliance), Wipro Limited.

¹ *Biometrics: Authentication and Identification (2018)* (Gemalto, 9 February 2018) <www.gemalto.com/govt/inspired/biometrics> accessed 31 January 2018.

² Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act 2016 (AA 2016), s. 2 (g).

³ Colin Soutar et al, '*Biometric Encryption*' in Randall K. Nicholls (ed), *ICSA Guide to Cryptography* (McGraw-Hill Professional 1999).

⁴ Henry C Lee & RE Gaensslen, *Advances in Fingerprint Technology* (Robert Ramotowski ed, 3rd edn, CRC Press 2012).

⁵ Colin Soutar (n 3).

⁶ Illinois Biometric Data Privacy Act, 2008 (BIPA 2008) (US).

⁷ BIPA 2008, s. 10.

⁸ BIPA 2008, s. 15(a).

⁹ BIPA 2008, s. 20(1).

¹⁰ BIPA 2008, s. 20(2).

¹¹ Texas Business & Commercial Code 2009 (TBCC 2009), s. 503.001(a)(US).

¹² TBCC 2009, s. 503.001(b).

¹³ TBCC 2009, s. 503.001(c)(1).

¹⁴ TBCC 2009, s. 503.001(c)(3).

¹⁵ TBCC 2009, s. 503.001(c)(2).

¹⁶ TBCC 2009, s. 503.001(d).

¹⁷ Engrossed Substitute House Bill 1493 (ESHB 1493), s. 3(1)(US).

¹⁸ ESHB 1493, s. 2(2).

- ¹⁹ General Data Protection Regulation, 2018 (GDPR 2018), art 4(14).
- ²⁰ GDPR 2018, art 77(1).
- ²¹ GDPR 2018, art 77(1).
- ²² GDPR 2018, art 82(1).
- ²³ GDPR 2018, art 84(1).
- ²⁴ Amended Act on the Protection of Personal Information 2016, art 2 (Japan).
- ²⁵ Information Privacy Act, 2014, s. 14(c)(Australia).
- ²⁶ The Personal Data (Protection) Bill 2013 (PDB 2013), s. 2(c).
- ²⁷ PDB 2013, s. 2(x)(i).
- ²⁸ AA 2016, preamble.
- ²⁹ AA 2016, s. 2(h).
- ³⁰ AA 2016, s. 2(n).
- ³¹ AA 2016, s. 2(g).
- ³² AA 2016, s. 2(j).
- ³³ AA 2016, s. 2(u).
- ³⁴ AA 2016, s. 8(1).
- ³⁵ AA 2016, s. 8(2)(a).
- ³⁶ AA 2016, s. 8(3).
- ³⁷ AA 2016, s. 28(5).
- ³⁸ *KS Puttaswamy v. Union of India*, (2017) 10 SCC 641.
- ³⁹ *Ibid.*.
- ⁴⁰ *Lujan v. Defenders of Wildlife*, 1992 SCC OnLine US SC 67 : 119 L Ed 2d 351 : 112 S Ct 2130, 2136 : 504 US 555 (1992).
- ⁴¹ *Rivera v. Google Inc.* No. 16 C 02714, 2017 WL 748590 (ND Ill, 27 February 2017).
- ⁴² *Ibid.*.
- ⁴³ BIPA 2008, s. 10.
- ⁴⁴ *Yates v. United States*, 2015 SCC OnLine US SC 57 : 191 L Ed 2d 64 : 135 S Ct 1074, 1086-88 : 574 US ____ (2015).
- ⁴⁵ Crimes and Criminal Procedure 18 USCA, s. 657 (US).
- ⁴⁶ BIPA 2008, s. 10.
- ⁴⁷ *Rivera* (n 41).
- ⁴⁸ BIPA 2008, s. 10.
- ⁴⁹ *Rivera* (n 41).
- ⁵⁰ *Ultsch v. Illinois Municipal Retirement Fund*, 874 NE 2d 1, 10 (2007).
- ⁵¹ IL HR Tran 2008, Reg Sess No. 249, 276 (30 May 2008).
- ⁵² *Rivera* (n 41).
- ⁵³ *In re Facebook Biometric Information Privacy Litigation*, 185 F Supp 3d 1155 (ND Cal 2016).

- ⁵⁴ *BedRoc Ltd LLC v. United States*, 2004 SCC OnLine US SC 27 : 158 L Ed 2d 338 : 541 US 176, 183 (2004); *State ex rel Pusateri v. Peoples Gas Light & Coke Co.*, 21 NE 3d 437, 441 (2014).
- ⁵⁵ *Facebook* (n 53).
- ⁵⁶ *Lebowitz v. City of New York*, 2014 US Dist LEXIS 25515 (SDNY, 25 February 2014); *Norberg v. Shutterfly Inc et al*, 152 F Supp 3d 1103 (2015).
- ⁵⁷ 2017 US Dist LEXIS 149604.
- ⁵⁸ 2017 WL 5592589.
- ⁵⁹ *Spokeo Inc. v. Robins*, 136 SCt 1540, 1550 (2016).
- ⁶⁰ *Strubel v. Comenity Bank*, 842 F 3d 181 (2nd Cir 2016); *Crupar-Weinmann v. Paris Baguette America Inc.*, 861 F3d 76 (2nd Cir 2017); *Katz v. Donna Karan Co LLC*, 872 F 3d 114 (2nd Cir 2017).
- ⁶¹ *Lujan* (n 40).
- ⁶² J. Neuburger, 'Appeals Court Affirms Dismissal on Standing Grounds of Biometric Privacy Suit over Videogame Facial Scan Feature' (*Lexology*, 28 November 2017) <www.lexology.com/library/detail.aspx?g=64998efe-6fa9-4242-bacc-3aab43dd3736> accessed 12 February 2018.
- ⁶³ 2017 IL App (2d) 170317.
- ⁶⁴ 2012 IL 111896, 965 NE 2d 1119, para 23.
- ⁶⁵ Bryan A. Garner (ed), *Black's Law Dictionary* (10th ed, 2014).
- ⁶⁶ *Ibid.*.
- ⁶⁷ 2016 WL 4077108 (ND Ill, 1 August 2016).
- ⁶⁸ 235 F Supp 3d 499, 519-20 (SDNY 2017).
- ⁶⁹ 2011 WI App 95.
- ⁷⁰ 2017 US Dist LEXIS 149604.
- ⁷¹ 2012 SCC OnLine US SC 35 : 182 L Ed 2d 497 : 566 US 284, 294 (2012).
- ⁷² 2016 WL 4077108 (ND Ill, 1 August 2016).
- ⁷³ 235 F Supp 3d 499, 519-20 (SDNY 2017).
- ⁷⁴ *Article 29 Data Protection Working Party'* (*Europa*, 1 August 2003) <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp80_en.pdf> accessed 12 February 2018.
- ⁷⁵ Colin Soutar (n 3).
- ⁷⁶ BIPA 2008.
- ⁷⁷ 'The Relation between FAR and FRR' (*ABI Institute*, 2016) <<http://abibiometrics.org/the-relation-between-frr-and-far.html>> accessed 14 February 2018.
- ⁷⁸ BIPA 2008, s. 15(a).
- ⁷⁹ A. Sprokkereef, 'Data Protection and the Use of Biometric Data in the EU' in S. Fischer-Hübner et al, *IFIP International Federation for Information Processing, The Future of Identity in the Information Society* (Boston Springer 2008) 277-84.
- ⁸⁰ GDPR 2018, art 9.
- ⁸¹ GDPR 2008, art 4(14).
- ⁸² GDPR 2008, art 9(2)(a).
- ⁸³ J. Bustard, *The Impact of EU Privacy Legislation on Biometric System Deployment: Protecting Citizens but Constraining Applications* (2015) 104 (32)5 IEEE Signal Processing Magazine.
- ⁸⁴ GDPR 2018, art 9(2)(b).

⁸⁵ E. Luger et al, '*Consent for All: Revealing the Hidden Complexity of Terms and Conditions*' in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (ACM 2013) 2687-2696.

⁸⁶ '*PC Encyclopedia*' (*PCmag*) <www.pcmag.com/encyclopedia/term/61834/data-leakage> accessed 13 February 2018.

⁸⁷ C. Engelking, '*Fingerprints Change over the Course of a Person's Life*' (*Discover*, 29 June 2015) <<http://blogs.discovermagazine.com/d-brief/2015/06/29/fingerprints-change-over-the-course-of-a-persons-life/#.WoMS4Ohua00>> accessed 13 February 2018.

Disclaimer: While every effort is made to avoid any mistake or omission, this casenote/ headnote/ judgment/ act/ rule/ regulation/ circular/ notification is being circulated on the condition and understanding that the publisher would not be liable in any manner by reason of any mistake or omission or for any action taken or omitted to be taken or advice rendered or accepted on the basis of this casenote/ headnote/ judgment/ act/ rule/ regulation/ circular/ notification. All disputes will be subject exclusively to jurisdiction of courts, tribunals and forums at Lucknow only. The authenticity of this text must be verified from the original source.