DePaul University
University Libraries

DePaul Journal of Art, Technology & Intellectual Property Law

Volume 31
Issue 1 *2021 Issue*

Article 5

Fighting to Protect Individual Privacy in a Rapidly Advancing Technological World

Farzana Ahmed
DePaul University College of Law

FIGHTING TO PROTECT INDIVIDUAL PRIVACY IN A RAPIDLY ADVANCING TECHNOLOGICAL WORLD

*Farzana Ahmed**

I. INTRODUCTION

You open social media to post pictures of the amazing trip you just went on. You are working on creating a brand where you make short films and post them on different platforms. These both have one important feature in common, the social media applications automatically tag the people in those videos and photos. Sounds great, right? Maybe not so much. During a pandemic where technology is proving to be crucial to today's society, there has been a rise in cases dealing with biometric data, like facial recognition. Recently, states have begun enacting and proposing biometric data protection laws, and courts in states with biometric information protection laws have given more attention to the issues.[1] On June 1st, 2020, in *Acaley v. Vimeo, Inc*., an Illinois district court held an arbitration clause in a user policy notice does not prevent trial for a claim under the Illinois Biometric Information Privacy Act (BIPA).[2] The court's reasoning focuses on people's right to privacy and BIPA's similarity to common law torts.[3] This case lends insight into one of the many ways companies will attempt to avoid BIPA claims and highlights the significance of BIPA violations.

* Farzana Ahmed is a 2022 DePaul University College of Law J.D. Candidate. Farzana is the Junior Editor for the DEPAUL JOURNAL OF ART, TECHNOLOGY AND INTELLECTUAL PROPERTY. Farzana graduated from Knox College in 2018, where she received her Bachelor of Arts majoring in both Economics and International Studies and elected for membership of Omicron Delta Epsilon, the International Economics Honor Society. Farzana is a member of the International Association of Privacy Professionals and pursuing privacy certifications.

[1] Natalie A Prescott, *The Anatomy of Biometric Laws: What U.S. Companies Need to Know in 2020*, Vol. X No. 15 NAT'L L. REV. (2020), https://www.natlawreview.com/article/anatomy-biometric-laws-what-us-companies-need-to-know-2020.

[2] *Acaley v Vimeo, Inc.*, 464 F.Supp.3d 959, 971 (N.D. Ill. 2020).

[3] *Id.*

The court's decision in *Acaley*, explains how BIPA may not be a common law tort, but the law is still a protection from an invasion of privacy for contractual definition purposes. [4] The court believes the Congress of Illinois intended for this reading of BIPA so that there are definite protections to prevent against real injuries including injuries that are not sustained to someone's physical self or property.[5] Vimeo believes the words in its contracts are superfluous and BIPA should not be included in its exceptions.[6]

The central argument of this note is the court correctly sets importance on Congress' intent to protect consumers in a rapidly advancing industry and sector of society, technology. Therefore, the court directs that arbitration contracts must clearly delineate whether or not BIPA claims fall under their arbitration clause if they do not mean to include it in their terms for invasion of privacy.[7] Part II of this note provides background on the historical trend presented by state courts with existing and recently enacted versions of a biometric privacy act.[8] Part III of this note discusses the opinion by the United States District Court for the Northern District of Illinois in *Acaley v. Vimeo, Inc.* including the requested further proceedings, holding, and reasoning.[9] Part IV examines the social, legal, and business effects of the Illinois BIPA.[10] Part IV will also look at the affects cases such as *Acaley* and state BIPA laws are having in federal government law making.[11] Part V concludes with the importance of biometric data protection in a world where technology has quickly and aptly integrated into the most intimate parts of our lives.

II. **BACKGROUND**

[4] *Id.* at 969.
[5] *Id*.
[6] *Id.* at 970.
[7] *Id.*
[8] Jeffrey Rosenthal and David Oberly, *Biometric Privacy in 2020: The Current Legal Landscape*, LAW360 (2020); *See also* Prescott, *supra* note 1.
[9] *Acaley v Vimeo, Inc.*, 464 F.Supp.3d 959, 965-71 (N.D. Ill. 2020).
[10] *Id.*
[11] Jeffrey Rosenthal and David Oberly, *What Cos. Could Expect From National Biometric Privacy Bill*, LAW360 (2020); *See also* National Biometric Information Privacy Act, S. 4400, 116th Cong. (2020).

A. The Emergence of Biometric Information Protection Legislation

In 2008, with internet, technology, and applications widely available to people in their homes for personal use, Illinois' Congress enacted the first biometric regulation in the United States.[12] Biometric information covers identifying data such as retina scans, fingerprints, voice recognition, facial-geometry recognition, DNA recognition, and many other forms of identifying information.[13] The Illinois BIPA applies to all industries and regulates private entities and individuals who collect biometric information to provide their services and make their services more efficient.[14] Illinois Congress' intent is to protect consumers and workers who interact with biometric information collecting data services and employers.[15] BIPA is meant to help deal with the constituents' concerns about their biometric data that is collected with the ease of a one second scan which can be used by a company or employer easily and unbeknownst to the constituent.[16]

A year after Illinois passed BIPA, Texas enacted their own biometric privacy act.[17] In more recent years, Washington, California, New York, and Arkansas, followed suit and enacted their own biometric privacy legislation.[18] Other states have introduced bills, but have yet to enact them.[19] Unlike Illinois' BIPA, these states' biometric privacy legislation does not give an express private right of action. However, they provide relief in the form of the attorney general's enforcement of the laws or private right of action under other laws that are violated by a violation of their biometric information privacy acts and statutes.[20] These laws show there are growing concerns about the use of biometric

[12] *See* Prescott, *supra* note 1.
[13] *Id.*
[14] 740 Ill. Comp. Stat. 14/15 (2008).
[15] *Id.* at 14/5.
[16] *Id.*
[17] *See* Prescott, *supra* note 1.
[18] *Id*.
[19] *Id.*
[20] *Id.*

information data which is becoming an intricate part of citizens' daily lives.[21]

In addition to states enacting laws, Democratic Senator of Oregon, Jeff Merkley, and Independent Senator of Vermont, Bernie Sanders, introduced the National Biometric Information Privacy Act which would provide the same protections to U.S. citizens as the state legislations which have been passed.[22] The act would be most similar to Illinois' BIPA which provides for more extensive requirements and broader protections than other states' legislations including a private right of action.[23]

B. Patel v. Facebook: Broadening the Protections for Consumers

In *Patel v. Facebook*, the court considered standing by deciding if the Illinois statute provided relief for real harms or potential risk of harm to those protected in the statute.[24] The court held the plaintiffs' did have standing under the Illinois' BIPA for Facebook's violation of the law with their facial-recognition technology.[25] The court reasoned BIPA expressly provides protected privacy interests and violations do cause real harm or potential risk of harm to individuals.[26] This harm gives the user standing under the Illinois BIPA in federal courts.[27] This holding is crucial to confirming a right of private action and that federal courts can hear cases for BIPA violations.

The court also considered whether damages of monetary value could be provided as relief. [28] The court held monetary damages may be awarded and the district court did not abuse its discretion.[29] The court reasoned there was no express indication that the statutory damages prevented a court from providing relief

[21] *Id.*
[22] *See* Rosenthal, *supra* note 11.
[23] *Id.*
[24] *Patel v. Facebook, Inc.*, 932 F.3d 1264, 1267 (9th Cir. 2019).
[25] *Id.* at 1271-75.
[26] *Id*.
[27] *Id.*
[28] *Id.* at 1267.
[29] *Id.* at 1277.

through monetary means and the statutory damages actually provide for some monetary relief.[30] This holding shows the importance of protecting the individuals affected by violations under BIPA as the law provides for serious damages. This case also shows violations will not bode well for the companies or individuals who violate the Illinois BIPA.

C. Bryant v. Compass: Federal Court Jurisdiction for Only Some BIPA Claims

In *Bryant v. Compass*, the court considered two claims from the same case and whether standing existed for either claim.[31] The court reasoned that failing to make requisite disclosures to plaintiff or obtain her informed consent to collect her fingerprints is an invasion of personal rights under BIPA and provides standing for her nonconsensual biometric data collection claim.[32] The court also reasoned that violating a procedural requirement of BIPA does not create standing in federal courts because no concrete harm is created by this violation.[33] This case is crucial in establishing federal court standing for Illinois BIPA claims as it delineates not all claims can be brought to federal courts and must remain in state court unless federal procedural rules apply.

III. **SUBJECT OPINION**

A. Acaley v. Vimeo: BIPA Is an Invasion of Privacy Protection for Individuals' Data

In *Acaley v. Vimeo, Inc.*, the US District Court for the Northern District of Illinois considered the applicability of arbitration in a browsewrap agreement to terms contract in one of Vimeo's subbranch websites, Magisto.[34] The court also considered whether an invasion of privacy exclusion from the arbitration agreement existed.[35] Plaintiff claims he did not assent to the terms of service in the browsewrap agreement because he was not able to

[30] *Patel*, 932 F.3d at 1269.
[31] *Bryant v. Compass Grp. USA, Inc*., 958 F.3d 617, 622 (7th Cir. 2020).
[32] *Id.* at 626-27.
[33] *Id.* at 626.
[34] *Acaley v Vimeo, Inc.*, 464 F.Supp.3d 959, 965-66 (N.D. Ill. 2020).
[35] *Id.* at 967.

opt-out of the inconspicuous agreement hidden by additional pop-ups and shrouded in the background.[36] Plaintiff also claims Vimeo violated BIPA using facial recognition to collect data on his and others' face geometries from media they uploaded to Magisto without satisfying BIPA's requirements.[37] While the court rules against plaintiff's first claim because plaintiff had multiple occasions to opt-out of the browsewrap agreement, the court holds Vimeo did violate BIPA.[38] The court also holds BIPA is an invasion of privacy violation and is included in the exclusion from arbitration clause in the terms of service agreement.[39]

1. The Rational Reasoning and Examining Illinois Congress Intent on Application

Before addressing the key issue of defining invasion of privacy, the court considered the scope of the agreement and the exclusion clause. The court reasoned there was no language in the arbitration exclusion clause that provided only Vimeo could bring claims outlined in the clause.[40] The court concluded the clause must be interpreted broadly and expansively to include any claim related to or arising from invasions of privacy.[41] Thus, the plain language of the terms of service excluded arbitration requirements on invasion of privacy claims brought by users.[42]

With the conclusion that users have a valid claim for a trial hearing for violation of invasion of privacy under Vimeo's agreement, the court addressed whether BIPA was an invasion of privacy. The court addressed the trend that lawsuits brought under BIPA are characterized as invasion of privacy lawsuits.[43] The court also looked to the Illinois Supreme Court which explained BIPA codifies the principle that individuals possess a right to privacy over their biometric information and biometric identifier

[36] *Id.* at 966-77.
[37] *Id.* at 964.
[38] *Id.* at 968, 971.
[39] *Id.* at 971.
[40] *Acaley*, 464 F.Supp.3d at 970.
[41] *Id.*
[42] *Id.*
[43] *Id.* at 969.

data.[44] The supreme court relied on the Illinois General Assembly's intent outlined in their legislative materials.[45]

The court reasoned a violation of BIPA is as harmful as theft or piracy because violating the statute would result in the theft, misuse, or other injury of an individual's privacy and property rights over their biometric data.[46] The court explained while common-law tort invasion of privacy and statute invasion of privacy issues have different statute of limitations, an invasion of privacy protection exists in both.[47] In this case, the court finds an invasion of privacy protection exists because BIPA provides a statutory protection.[48] Therefore, BIPA is defined as an invasion of privacy of individuals' bona fide right to control their biometric data and a right to privacy in their biometric information.[49]

In addition to the holdings of the key issues in this case, the court denied plaintiff's guidance on how to rule and only ruled to deny Vimeo's motion. Plaintiff requested the court rule to deny further appeal by Vimeo because the appeal would not likely succeed and only be used as a tactic to further delay litigation on the reparations for and the extent to which Vimeo violated BIPA.[50] The court reasoned the requested ruling was premature.[51] Thus, the court ruled the case to proceed to trial and denied Vimeo's motion to stay this case and compel arbitration.[52]

IV. **ANALYSIS**

The importance of individuals' right and protection of their biometric information and identifiers is highlighted by this case. Technology and the use of biometric data is rapidly growing, and the Illinois BIPA is leading the way for defining the necessary regulations. The Illinois BIPA and Illinois Congress also shows

[44] *Id.*
[45] *Id.*
[46] *Acaley*, 464 F.Supp.3d at 970-71.
[47] *Id.*
[48] *Id.*
[49] *Id.* at 970.
[50] *Id.* at 971.
[51] *Id*.
[52] *Acaley*, 464 F.Supp.3d at 971.

the magnitude of importance for the care and safety of citizens who might be unaware of the significant personal rights violations that can occur from misuse and handling of biometric information. The court in *Acaley* correctly defines BIPA as a statutory invasion of privacy because this definition creates definitive protection of individuals' rights; notifies businesses of the magnitude of violation; and sets the stage for invasion of privacy claims brought under BIPA. Also, this definition corresponds with the importance of biometric information protection which other states are now adopting. Most importantly, this definition highlights the precedent the Illinois BIPA has set by influencing the US Congress to enact a similar law.

A. Social, Business, and Legal Implications of Defining BIPA as a Protection

Defining BIPA as a protection of invasion of privacy has many implications. The implications include protection of people's rights to a seemingly intangible property, sets the tone for business compliance, and provides a streamlined legal process for claims under BIPA. The implication to individuals' and businesses are especially important because the law provides a right of private action.[53] In light of the Covid-19 pandemic, these implications are applying to an increasing number of Illinois citizens and entities operating in Illinois. Also, considering the nationwide exponential increased use of technology due to the pandemic, the policy reasons for enacting biometric information privacy protection laws in other states with the right of private action may be ever more important.[54]

1. Protecting Citizens in a Rapidly Advancing Technological World

[53] *See generally* 740 Ill. Comp. Stat. 14/20 (2008); Rosenthal, *supra* note 11, at 2.

[54] *See generally* Kenneth D. Walsh and Mary Smigielski, *Insight: Illinois Biometric Privacy Law Has Nationwide Potential in Pandemic* (April 24, 2020), BLOOMBERG LAW, https://news.bloomberglaw.com/tech-and-telecom-law/insight-illinois-biometric-privacy-law-has-nationwide-potential-in-pandemic?context=search&index=1.

The unprecedented rapid expansion of remote work and e-learning due to the pandemic requires lawmakers to investigate the privacy issues technology and biometric information presents. Presently, the issues of using biometric information goes beyond people's social lives in social media, creating a growing concern amongst citizens.

Many companies already used biometric information such as fingerprints, retina scans, and various other identifiers to help increase employee productivity, surveillance, security, and other business operations.[55] Relying on the analysis of *Bryant*, an Illinois court in *Snider v. Heartland Beef*, noted the inherent risk an employee is forced to accept mandates businesses acquire actively provided consent to biometric information data collection.[56]

A current case, *H.K. et al. v. Google LLC*, in California which has similar biometric information privacy laws as Illinois, represents the crossovers between other privacy laws such as the Children's Online Privacy Protection Act (COPPA).[57] COPPA protects the privacy and personal information of children under the age of 13.[58] This issue of the case addresses the concerns of parents across the nation whose children's biometric information is being used by Google G Suite without proper notification and parental consent of the collection, disposal, use, and other processes of such information.[59] The growing concern of technology and biometric data effecting more parts of people's

[55] Aaron C. Garavaglia, *When Increasing Productivity Can Backfire*, Vol. X No. 262 Nat'l L. Rev. (2020), https://www.natlawreview.com/article/when-increasing-productivity-can-backfire; David Oberly, *How to Avoid Becoming the Next Major BIPA Class Action Target When Using Facial Recognition for Security and Surveillance* (Sept. 16, 2020), BIOMETRIC UPDATE.COM, https://www.biometricupdate.com/202009/how-to-avoid-becoming-the-next-major-bipa-class-action-target-when-using-facial-recognition-for-security-and-surveillance.

[56] Jacob M. Davis, *Court Sua Sponte Dismisses Part of BIPA Claim Before Denying Rule 12(b)(6) Motion to Dismiss*, Vol. X No. 241 NAT'L L. REV. (2020), https://www.natlawreview.com/article/court-sua-sponte-dismisses-part-bipa-claim-denying-rule-12b6-motion-to-dismiss.

[57] Walsh, *supra* note 54.

[58] *Id.*

[59] *Id.*

lives calls for the lawmakers to address the policy issues the use of biometric information presents.

Looking at the concerns posed in other cases, the court in *Acaley* rightly defined BIPA as an invasion of privacy. The overlap between COPPA and biometric information privacy laws shows the privacy of children is at stake in this increased use of technology. The use of biometric data in the workplace shows privacy concerns for employees who are subjected to data collection often without proper notice. Social media has long been known to use biometric information and recognition software to help make tagging people and saving their personal information easier as seen in *Patel*.[60]

In addition to correctly reading Illinois Congress' intent of applying BIPA claims as invasion of privacy disputes, these aforementioned areas of individuals' lives provide support for the Northern District of Illinois court's decision in defining BIPA as an invasion of privacy. Defining BIPA as an invasion of privacy provides concrete protection of individuals' rights to control their biometric information in all aspects of their lives that are increasingly using these individual identifying data for efficiency, security, and other purposes.

2. Providing Businesses Notice of and Enforcing People's Rights to Biometric Data

Defining BIPA as an invasion of privacy provides businesses clear and sufficient notice of the importance of the statute and the regulation requirements the statute outlines. As seen in *Acaley*, Vimeo tried to defend its arbitration mandate by claiming the invasion of privacy exclusion only applies to common law torts and that BIPA is not an invasion of privacy under that definition.[61] Businesses such as Lowe's, Home Depot, Macy's, and Kroger faced BIPA violations for using new surveillance technology that recorded customer and employee facial information.[62] Businesses are being forced to look into the regulation as they learn BIPA is

[60] *See generally Patel v. Facebook, Inc.*, 932 F.3d 1264, 1271-75 (9th Cir. 2019).
[61] *Acaley v Vimeo, Inc.*, 464 F.Supp.3d 959, 969 (N.D. Ill. 2020).
[62] Oberly, *supra* note 55.

an invasion of privacy on par with common law tort invasions of privacy.[63] Businesses can comply with regulations by implementing accuracy and bias testing, privacy policies, written notices for those affected by the data collection, written releases, data security, opt-out options, and rules that prohibit using the data for discriminatory purposes.[64]

Clearly, the rapid advancement of technology and the best regulation policies are as new and foreign to businesses as they are to individuals' whose rights are of the utmost importance. While policy makers, like the Illinois Congress, are implementing new laws to protect their citizens, the extent to which some of these biometric information privacy laws apply are unclear to businesses who must comply with these laws. So, by defining BIPA as an invasion of privacy protection, businesses have irrefutable notice that they must adjust their policies and practices of privacy accordingly. Thus, in the holding of *Acaley*, the court provided notice to businesses.

Moreover, this notification means businesses understand the extent to which they must notify unionized workers of their policies regarding biometric information collection. Only recently have Illinois courts found possible federal preemption defenses for businesses when dealing with unionized workers.[65] With judicial affirmation that BIPA applies as a statutory invasion of privacy claim, businesses have clear notification of how to defend themselves and assess a BIPA claim. Each BIPA case ruling, such as the ruling in *Acaley*, provides the details of BIPA which is crucial to accurate, efficient, and fair application of the statute in lawsuits.

Filling in these details which provide businesses with a preemption defense is increasing national momentum to prevent

[63] *Id.*
[64] *Id.*
[65] Jason E. Reisman, et al., *Insight: Class Action BIPA Rulings Further Successful Preemption Challenges* (Sept. 10, 2020), BLOOMBERG LAW, https://news.bloomberglaw.com/tech-and-telecom-law/insight-class-action-bipa-rulings-further-successful-preemption-challenges.

businesses' evasion of a serious violation. This momentum will be discussed further in a later part of this note.

The holding from *Acaley*, may not have a sweeping affect over all Illinois BIPA claims, but it provides proper notice on arbitration and contract compliance. Arbitration BIPA claims will be decided on facts and the different outcomes will help notify businesses on how they draft and update their terms of service agreements.[66] Agreements and contracts created between third party servicers and subbranches of businesses, as seen in *Acaley*, will all benefit from the notice provided by the court.

Notice is essential to businesses ability to efficiently and successfully operate, especially considering the number of various servicers and businesses that have to work together to complete the services they provide to the public. Proper notification of how to draft contracts with everyone from employees and customers to other businesses that will handle the biometric information collected by another business will increase the efficiency of compliance, ensure successful business operations, and complete the statute's purpose of protecting individuals' rights.

3. Streamlining a Technological Invasion of Privacy Legal Process

The court's decision and other case decisions have helped streamline the legal process for BIPA claims. In *Patel*, the extraterritorial impact of BIPA was established.[67] The court in *Bryant* established that not all BIPA claims have federal jurisdiction.[68] In *Acaley*, the court established the equal extent to which a BIPA statutory invasion of privacy violation and common law tort violation will be adjudicated.[69]

Other cases have defined that the information derived from photographs are still biometric information and identifying data

[66] Meghan A. Quinn, *Vimeo Will Face Facial Recognition BIPA Class Action in Federal Court, Despite Valid Arbitration Clause*, Vol. X No. 1567 NAT'L L. REV (2020).
[67] Walsh, *supra* note 54; *see generally Patel*, 932 F.3d at 1271-75.
[68] Garavaglia, *supra* note 55; *see generally Bryant*, 958 F.3d at 624-27.
[69] *Acaley v Vimeo, Inc.*, 464 F.Supp.3d 959, 970-71 (N.D. Ill. 2020).

protected by BIPA.[70] In *Rosenbach v. Six Flags Entertainment Corp*., the Illinois Supreme Court established plaintiffs could sue for technical violations even when no real harm was experienced by the plaintiff.[71] In another case it was established that a preemption defense can exist for businesses when the claim is brought by unionized workers.[72] A few of these cases provide more revolutionary impacts on BIPA law, but nonetheless, all of the holdings provide more guidance in BIPA procedures and streamlines the adjudication process.

The decision in *Acaley* is not a breakthrough landmark case such as *Patel*, but the holding is just as important. BIPA was enacted in 2008 and cases addressing BIPA claims have been steadily arising. Each clarification such as the court's definition in *Acaley* plays a major role in expounding the statute. The detailed development of BIPA case law also stands as a prime example for other states following in Illinois' footsteps. Most importantly, the case law development and the stringency of the Illinois BIPA acts as the muse for the new national BIPA proposal.

B. Influencing Biometric Data Protections Across the Nation

The Illinois BIPA has influenced other states biometric data protection laws. Currently, six states have some form of biometric data privacy protection laws. At the time *Patel* was decided California did not have a biometric data privacy protection law of its own, but the California district court still made a landmark decision on the Illinois BIPA which favored protecting Illinois citizens.[73] Notably, Texas, California, and Washington's biometric privacy information statutes are directly based off of the Illinois

[70] Christina Tabacco, *Court Denies Most of IBM's Motion to Dismiss in Biometric Data Suit* (Sept. 20, 2020), LAW STREET MEDIA, https://lawstreetmedia.com/tech/court-denies-most-of-ibms-motion-to-dismiss-in-biometric-data-suit/.
[71] Jeffrey Rosenthal and David Oberly, *Biometric Privacy in 2020: What Companies Can expect*, LAW360 (2020).
[72] Reisman, *supra* note 65.
[73] *Patel v. Facebook, Inc.*, 932 F.3d 1264, 1271-75 (9th Cir. 2019); *see generally* Prescott, *supra* note 1.

BIPA.[74] Other states have amended their laws and introduced proposals based on the Illinois BIPA and case law formation.[75]

Holdings, such as in *Acaley*, support the views these states' legislation present: biometric data information protection and control is a critical personal and property right. The Illinois BIPA is a crucial player in legislation across the nation, as more states recognize the increasing importance of individuals' rights to biometric data privacy. Biometric information collection has become a significant tool in various areas of individuals' lives from social media to the government. Illinois BIPA case law provides insight into novel issues in a world where technology is intertwining into the most personal areas of individuals' lives like voice recognition tools such as Alexa or Google Home.

Biometric information use is not going anywhere and is only likely to be used in new areas of peoples' lives. Laws such as the Illinois BIPA are crucial for the success of an advancing technological world.

C. Push for Federal Protection of Biometric Data

In August, the National Biometric Information Privacy Act of 2020 was introduced by Senators Jeff Merkley and Bernie Sanders.[76] The bill almost mirrors the Illinois BIPA and provides a private right of action.[77] The national bill proposal differs in that it provides more protections to consumers and reflects lessons learned from Illinois BIPA case law.[78] With the increased use of tools which collect biometric data for Covid-19 screening and the surge in remote work and e-learning, the concerns of invasion of privacy have prevailed.[79] The pandemic likely helped push the bill to introduction considering the rising concerns and prevalence of

[74] Prescott, *supra* note 1; *see generally* Rosenthal, *supra* note 71.
[75] Prescott, *supra* note 1.
[76] National Biometric Information Privacy Act, S. 4400, 116th Cong. (2020).
[77] *Id.* at § 4; *see also* Rosenthal, *supra* note 11.
[78] Rosenthal, *supra* note 11.
[79] Walsh, *supra* note 54, at 1; *see also* Joseph J Lazzarotti, *National Biometric Information Privacy Act, Proposed Sens. Jeff Merkley and Bernie*, Vol. X No. 218 Nat'l L. Rev. (2020), https://www.natlawreview.com/article/national-biometric-information-privacy-act-proposed-sens-jeff-merkley-and-bernie.

applicability compared to last year's attempts to introduce a national bill.[80]

Returning to the previously mentioned holdings which support a business' defense by preemption in cases brought by unionized workers, a national BIPA law would eliminate this defense.[81] The recent rise of defenses by preemption likely also influenced the newly charged momentum to pass a national BIPA law. There is a large concern for individuals' privacy, especially in the workplace. Establishing the magnitude of importance biometric information invasions of privacy present in states like Illinois helps address nationwide concerns. Establishing the importance also helps lawmakers pinpoint issues to address so they can protect individuals, workers, students, and others.

The Illinois BIPA highlighted the importance of biometric information protection. Illinois BIPA case law also provides insight on the issues presented regarding biometric information collection. As seen in some cases, the Illinois BIPA overlaps with other national privacy laws such as COPPA, the Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), and Gramm-Leach-Bliley Act (GLBA).[82] The national bill proposal shows the influence and importance of the Illinois BIPA and proposes laws like it. The nation cannot overlook the importance of biometric data privacy any longer. The push for a national BIPA exemplifies Congress addressing the growing concerns and protections necessary for US citizens as technology continues to increasingly dominate various aspects of people's lives.

V. **CONCLUSION**

The court's holding in *Acaley* establishes an important fact. The court is correct to establish such a definite definition and

[80] *See generally* Rosenthal, *supra* note 8.
[81] *See generally* Reisman, *supra* note 65.
[82] Walsh, *supra* note 54; Family Educational Rights Privacy Act, 20 U.S.C. § 1232g (2013); Health Insurance Portability Accountability Act, 42 U.S.C. § 1320d (2010); 15 U.S.C. § 6801 (2011) (requires financial institutions provide information and notice of their information and data sharing practices to customers and to protect customers' sensitive data).

comparison to common law tort invasions of privacy.[83] The need for policy protections demonstrates the impact of the court's holding. The holding helps expound the details of the Illinois BIPA and provides significant implications for businesses as they draft new policies and contracts.

The court's holding and the Illinois BIPA provide influential privacy concepts which reverberate through other state biometric privacy laws. The Illinois BIPA provides a prime outline of what the national BIPA proposal should look like.[84] Illinois BIPA case law has provided the US Congress insight on what issues need to be filled in for a national statute.[85] Moreover, Illinois case law and the pandemic have shown the need to push harder for a national BIPA law in order to protect individuals.

Looking forward, paying attention to further litigation is critical to understanding the Illinois BIPA. As the US Congress works on enacting a national BIPA, they should follow new cases and cases such as *Acaley.* As suspected by plaintiff, Vimeo motioned for an appeal a little more than two weeks after the court's decision.[86] The case's appeal had a joint status report at the end of November 2020 and the future date of the appeal was still pending in March 2021.[87] Perhaps Congress can come up with clauses that will help prevent other businesses from prolonging reparations for invasions of privacy under a national BIPA law to help protect constituents.

Biometric information and identifiers are seemingly intangible to the individual they belong to, but they are personal property. It is crucial that biometric data be protected, and individuals be given full control over their data. Technology has made peoples' lives more efficient and interconnected, but the process of promoting efficiency and interconnectedness has stepped into people's personal privacy. For some this invasion of

[83] *Acaley v Vimeo, Inc.*, 464 F.Supp.3d 959, 969 (N.D. Ill. 2020).
[84] Lazzarotti, *supra* note 78.
[85] Rosenthal, *supra* note 11.
[86] *Acaley*, Notification of Docket Entry (June 18, 2020).
[87] *Acaley v. Vimeo*, N.D. Illinois, Dec. 1, 2020, (1:19-cv-07164) Docket Number 56.

privacy has occurred without their knowledge or understanding of how dire biometric information invasion of privacy is. As the United States continues to embrace technology and all it can offer, governments need to make sure citizens are protected by enforcing and enacting biometric information privacy protections.