

IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS
COUNTY DEPARTMENT, CHANCERY DIVISION
GENERAL CHANCERY SECTION

AMERICAN CIVIL LIBERTIES UNION,
AMERICAN CIVIL LIBERTIES UNION OF
ILLINOIS, CHICAGO ALLIANCE AGAINST
SEXUAL EXPLOITATION, SEX WORKERS
OUTREACH PROJECT CHICAGO, ILLINOIS STATE
PUBLIC INTEREST RESEARCH GROUP, INC., and
MUJERES LATINAS EN ACCIÓN,

Plaintiffs,

v.

CLEARVIEW AI, INC., a Delaware corporation,

Defendant.

CASE No. 20 CH 4353

CALENDAR 11

MEMORANDUM OPINION AND ORDER

This matter came before the Court on Defendant's motion to dismiss the Complaint. For the reasons explained below, the motion is denied.

BACKGROUND

The central conflict in this case is the clash between privacy rights and First Amendment protections in an age of ever-more-powerful technology. Defendant Clearview AI, Inc. ("Clearview") used facial recognition technology to capture more than three billion faceprints from publicly-available photos on the internet¹. A faceprint is a biometric identifier used to verify a person's identity. To create a faceprint, Clearview's system scans the photo, measures and records data such as the shape of the cheekbones and the distance between eyes, nose, and ears, and assigns that data a numerical value. These faceprints are then collected into a database, with faceprints for similar-looking faces clustered together. Clearview sells access to its technology, database, and investigative tools—the "world's best facial-recognition technology combined with the world's largest database of headshots"—by subscription to public and private entities. When a user wants to identify someone, the user uploads a photo. The system then processes the request, finds matches, and returns links to publicly-available images on the internet. Often, the linked websites will include additional information about the person identified.

¹ The facts recited here are derived from Plaintiffs' Complaint and its exhibits, and are accepted as true for purposes of Defendant's motion to dismiss. See *Kedzie & 103rd Currency Exchange v. Hodge*, 156 Ill. 2d 112, 115 (1993).

Clearview does not seek or receive permission to create and store faceprints of the persons depicted in the photos.

On May 28, 2020, Plaintiffs filed their one-count Complaint in this action, seeking relief under the Illinois Biometric Information and Privacy Act (“BIPA”), 740 ILCS 14/1 et seq. Plaintiffs are the national and Illinois American Civil Liberties Union organizations and four other organizations suing on behalf of their members, clients and program participants. The Complaint alleges that these individuals—including survivors of domestic violence and sexual assault, undocumented immigrants, current and former sex workers, and individuals who regularly exercise their constitutional rights to protest and to access reproductive healthcare—live in Illinois and have particular reasons to fear loss of privacy, anonymity and security.

The Complaint alleges that Clearview violated Section 15(b) of BIPA, which provides:

(b) No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person’s or a customer’s biometric identifier or biometric information, unless it first:

(1) informs the subject or the subject’s legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;

(2) informs the subject or the subject’s legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and

(3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject’s legally authorized representative.

Plaintiffs allege that Clearview “systematically and automatically captured, used and stored their biometric identifiers without first obtaining the written release” as required. Cplt. at ¶ 70.

In addition, Plaintiffs allege that Clearview did not publicly provide a retention schedule or guidelines for permanently destroying individuals’ biometric identifiers, in violation of Section 15(a) of BIPA:

(a) A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual’s last interaction with the private entity, whichever occurs first. Absent a valid warrant or subpoena issued by a court of competent jurisdiction, a private entity in possession of biometric identifiers or biometric information must comply with its established retention schedule and destruction guidelines.

Cplt. at ¶ 72.

Plaintiffs seek an injunction ordering Clearview to destroy all biometric identifiers that Clearview collected and stored in violation of BIPA, to comply with BIPA's disclosure and consent requirements in the future, and to award Plaintiffs their attorneys' fees and costs.

Clearview moved to dismiss. The parties briefed the motion and the Court also received amicus briefs from the Electronic Frontier Foundation and from two groups of law professors (one in support and one in opposition to the motion). The Court heard oral argument by Zoom on April 2, 2021 and took the matter under advisement.

ANALYSIS

Clearview describes itself as a "small technology company" that helps law enforcement agencies identify perpetrators and victims of crimes using publicly-available images from the internet. (Clearview Memo at 1). Plaintiffs describe Clearview's business model as a "nightmare scenario." (Complaint at ¶ 41). Whichever description is closer to the truth, this case touches on matters of significant public interest.

Clearview makes a variety of constitutional, common law and statutory arguments in support of dismissal. First, Clearview contends it is not subject to personal jurisdiction in Illinois. Second, it argues that the extraterritoriality doctrine and the dormant Commerce Clause preclude the application of BIPA to Clearview's conduct. Next, it argues that BIPA is unconstitutional, as applied to Clearview, under the First Amendment to the U.S. Constitution and Article I, Section 4 of the Illinois Constitution. Finally, it argues that BIPA by its terms does not apply to Clearview's collection of biometric data from publicly-available photos.

Procedural Standard

To begin, Clearview does not specify the section of the Illinois Code of Civil Procedure under which it brings this motion. The Court assumes Clearview's request to dismiss for lack of jurisdiction is brought under 735 ILCS 5/2-301, which deals with objections to jurisdiction over the person. Such a motion may be brought either singly as the first substantive motion in a case, or combined with another motion as described in Section 2-619.1 of the Code.

Clearview has chosen to combine its motion to dismiss for lack of jurisdiction with a motion to dismiss on other grounds, but does not specify whether its other arguments are made under section 2-615 or 2-619 of the Code. It makes a difference. A section 2-615 motion to dismiss challenges the legal sufficiency of a complaint based on defects apparent on its face. *Marshall v. Burger King Corp.*, 222 Ill. 2d 422, 429 (2006). The court must consider, in a light most favorable to the plaintiff, if the complaint is sufficient to state a cause of action upon which relief can be granted. *Id.* On the other hand, a section 2-619 motion admits the legal sufficiency of the complaint and raises defects, defenses, or other affirmative matters that defeat the plaintiff's claim. Those defects may appear on the face of the complaint or be established by affidavit or other evidence. *Spirit of Excellence v. Intercargo Ins. Co.*, 334 Ill. App. 3d 136, 145 (1st Dist. 2002).

While it is not entirely clear, Clearview's non-jurisdictional arguments appear to challenge the legal sufficiency of the Complaint, rather than admitting the legal sufficiency of the Complaint and raising affirmative matter to defeat it. Therefore, the Court will treat the non-jurisdictional arguments as being brought under section 2-615.

Jurisdiction

To analyze an Illinois court's jurisdiction over a case, we start from Illinois' long-arm statute, 735 ILCS 5/2-209. Subsection (c) is a catchall provision allowing Illinois courts to exercise jurisdiction "on any other basis now or hereafter permitted by the Illinois Constitution and the Constitution of the United States." So if the contacts between a defendant and Illinois are sufficient to satisfy federal due process concerns, the requirements of Illinois' long-arm statute have been met, and no further inquiry is necessary. *Morris v. Halsey Enters. Co.*, 379 Ill. App. 3d 574, 579 (1st Dist. 2008).

Personal jurisdiction may be general or specific. Clearview is incorporated in Delaware and has its principal place of business in New York, so it is not "at home" in Illinois and general jurisdiction does not apply—nor do Plaintiffs say it does. Rather, Plaintiffs contend the Court has specific jurisdiction over Clearview.

Specific jurisdiction applies when a defendant is "less intimately connected with a State" and yet is still sufficiently connected to meet the requirements of due process. *Ford Motor Co. v. Montana Eighth Judicial Dist. Court*, 141 S. Ct. 1017, 1024 (2021).

To determine whether the due process standard has been met, we consider whether (1) the nonresident defendant had "minimum contact" with Illinois such that there was "fair warning" that the nonresident defendant may be haled into an Illinois court; (2) the action arose out of or related to the defendant's contacts with Illinois; and (3) it is reasonable to require the defendant to litigate in Illinois. In other words, the defendant should be able to "reasonably anticipate" being called into an Illinois court. *Burger King Corp. v. Rudzewicz*, 471 U.S. 462 (1985).

Morgan, Lewis & Bockius LLP v. City of E. Chicago, 401 Ill. App. 3d 947, 954 (1st Dist. 2010) (internal citation omitted).

When a defendant is a nonresident, the plaintiff bears the burden of proof to establish personal jurisdiction. *Morris*, 379 Ill. App. 3d at 579. Here, Plaintiffs contend they have met that burden by showing that "Clearview has extensive contacts with Illinois, those contacts relate to Plaintiffs' cause of action, and it is reasonable to require Clearview to litigate in Illinois." (Pltfs' Resp at 5). Plaintiffs detail those contacts in their Complaint and in two declarations attached to their response. They assert that Clearview directly marketed its faceprint database in Illinois, offering its service to employees of the Illinois Secretary of State, Springfield Police Department, Chicago Police Department, and more. The Complaint alleges that Clearview provided its

faceprint database to over 105 public and private entities in Illinois and facilitated thousands of searches by those entities.

Clearview contends it does not target Illinois through advertising and marketing. Rather, it says, its app is marketed “nationwide.” (Schwartz Declaration ¶ 6, Exh. B to Def’s Memorandum).

Where, as here, there is a conflict between the facts set forth by plaintiff and defendant on a motion to dismiss for lack of personal jurisdiction, that factual conflict must be resolved in plaintiff’s favor. *Mutnick v. Clearview AI, Inc.*, 2020 U.S. Dist. LEXIS 144583 *7 (N.D. Ill. 2020). Clearview need not *especially* or *exclusively* target Illinois in its marketing; rather, Clearview must only have been able to reasonably foresee that its service would be sold here. *Id.* at *8. In *Mutnick*, the U.S. District Court for the Northern District of Illinois decided this very issue, finding it had personal jurisdiction over Clearview in Illinois because Clearview “took biometric information from Illinois residents, created a surveillance database, and then marketed and sold licenses to use this database to entities in Illinois.” *Id.* at *7.

Clearview argued in its motion that its actions in Illinois did not “give rise” to any alleged harm. At oral argument, the parties discussed the implications of the then-week-old U.S. Supreme Court decision in *Ford Motor Co. v. Montana Eighth Judicial Dist. Court*, 141 S. Ct. 1017 (2021). That case emphasized the second part of the requirement that an action “arise out of or relate to” a defendant’s contacts with a state. While “arise out of” requires a causal connection, “relate to” does not. The court cautioned that, while “relate to” is broader than “arise out of,” there are “real limits” to its reach. The court based those limits on concepts of fairness, reciprocity, and predictability. In *Ford*, the defendant advertised, sold, and serviced vehicles in Montana and Minnesota. Plaintiffs filed product liability actions against Ford in Montana and Minnesota in two separate cases. In both cases, the injury took place in the forum state, but the vehicle that caused the injury was not sold there. The court found sufficient grounds for the state courts to exercise jurisdiction, even though the injuries could not be said to “arise out of” the state contacts. The cases did “relate to” each of the states because “Ford had systematically served a market in Montana and Minnesota for the very vehicles that the plaintiffs alleged malfunctioned and injured them in those states.” *Id.* at 1028.

The same is true in our case. Taking Plaintiffs’ allegations and verified statements as true, Clearview deliberately and successfully marketed its services in Illinois to Illinois customers. Those Illinois customers (and others) were then able to search a database of faceprints that included faceprints of Illinois residents collected in violation of BIPA. Just as Ford was required to litigate in forums where it had marketed its allegedly defective products, Clearview’s regular activity in Illinois is sufficiently “related to” this case that it is reasonable to require Clearview to litigate it in Illinois.

Clearview relies upon *Gullen v. Facebook.com, Inc.*, 2016 U.S. Dist. LEXIS 6958 (N.D. Ill. 2016), but *Mutnick* and *Ford* are more recent and more on point. Further, *Gullen* is distinguishable from our case. *Gullen* was a proposed class action against Facebook under BIPA. Facebook’s alleged connections to Illinois consisted of registering to do business here,

maintaining a general sales and marketing office here, and making its website available to Illinois residents. *Id.* at *5. The court found that the first two contacts had “no relationship” to the face recognition technology at issue in the suit, and that making its website accessible to Illinois residents was not the same as intentionally *targeting* them. By contrast, Plaintiffs in our case showed that Clearview targeted Illinois by marketing its faceprint database to a substantial number of Illinois customers. Those activities related to the very product at issue in this case.

The motion to dismiss on jurisdictional grounds is denied, and the Court will consider the arguments on the merits.

Application of BIPA to Faceprints

Clearview argued that BIPA by its terms does not apply to photographs, or to faceprints derived from photographs. It’s important to distinguish between the two. While BIPA provides that “biometric identifiers do not include ... photographs,” it also defines “biometric identifiers” to include a “scan of ... face geometry.” 740 ILCS 14/10. The Complaint describes a faceprint as just that, a scan of face geometry. The fact that the scan was made from a photo and not from a live person does not change that fact. Federal district court cases have considered this issue and concluded that BIPA’s protections apply to faceprints created from photos. *Rivera v. Google Inc.*, 238 F. Supp. 3d 1088, 1096 (N.D. Ill. 2017); *In re Facebook Biometric Privacy Info. Litig.*, 185 F. Supp. 3d 1155, 1172 (N.D. Cal. 2016); *Monroy v. Shutterfly Inc.*, 2017 U.S. Dist. LEXIS 149604, *11-12 (N.D. Ill. 2017). Clearview essentially conceded this point at oral argument, choosing simply to rest on its briefs and not argue the matter further.

The Court holds that BIPA’s protections apply to faceprints.

Extraterritoriality

In related arguments, Clearview contends that the Complaint fails under Illinois’ extraterritoriality doctrine because BIPA cannot regulate out-of-state conduct; and that the Complaint fails under the U.S. Constitution’s dormant Commerce Clause because applying BIPA to Clearview would have the practical effect of regulating commerce in another state.

Concerning extraterritoriality, Illinois courts have recognized a “long-standing rule of construction” that a statute will not have extraterritorial effect “unless a clear intent in this respect appears from the express provisions of the statute.” *Avery v. State Farm Mut. Auto. Ins. Co.*, 216 Ill. 2d 100, 184-85 (2005). While that intent may not have been expressed explicitly in BIPA, its legislative findings come close. The Ninth Circuit Court of Appeals found it “reasonable to infer [from the BIPA’s legislative findings] that the General Assembly contemplated BIPA’s application to individuals who are located in Illinois, even if some relevant activities occur outside the state.” Specifically, the court noted the statute’s finding that “[m]ajor *national* corporations” were targeting locations in Illinois as “pilot testing sites for new

applications of biometric-facilitated financial transactions.” *Patel v. Facebook, Inc.*, 932 F.3d 1264, 1276 (9th Cir. 2019) (emphasis added); 740 ILCS 14/5(b).²

The court in *Rivera v. Google*, 238 F. Supp. 3d 1088, 1100 (N.D. Ill. 2017) denied a motion to dismiss a BIPA complaint on extraterritoriality grounds, holding that discovery was needed to develop facts concerning where the violation “primarily and substantially” took place. In *Rivera*, plaintiffs claimed that their Google Droid device uploaded photos automatically to the cloud, scanned the photos, and made a template (what our Plaintiffs call a “faceprint”) without their knowledge or consent. The *Rivera* court noted that plaintiffs were residents of Illinois, the photos in question were taken in Illinois and uploaded to the cloud from an Illinois IP address, and the defendant failed to give plaintiffs the required notice and get their consent in Illinois. The court held that these facts, if proven true, “tip toward a holding that the alleged violations primarily happened in Illinois.” *Id.* at 1101-1102.

The Court holds that the extraterritoriality doctrine does not warrant dismissal of Plaintiffs’ Complaint. When considering a 2-615 motion to dismiss, the court must take as true all well-pled allegations of a complaint *and* all reasonable inferences that could be drawn from those facts. *Village of Wheeling v. Stavros*, 89 Ill. App. 3d 450, 453 (1st Dist. 1980). The Complaint alleges that Plaintiffs are Illinois residents and that photos of them appear on the internet. It is reasonable to infer, as Plaintiffs suggest, that “of the many millions of images uploaded by Illinoisans and collected by Clearview, many were uploaded from Illinois” and that Clearview’s Illinois customers used Clearview to search for Illinois residents. Pltf. Resp at 11.

Dormant Commerce Clause

The Commerce Clause of the U.S. Constitution provides that Congress has the exclusive power to “regulate Commerce ... among the several States.” U.S. Const. Art. I, § 8, Cl 3. The dormant Commerce Clause “precludes the application of a state statute to commerce that takes place wholly outside of the State’s borders, whether or not the commerce has effects within the State. . . . The critical inquiry is whether the practical effect of the regulation is to control conduct beyond the boundaries of the State.” *Healy v. Beer Inst.*, 491 U.S. 324, 336 (1989).

Clearview argues that BIPA cannot be applied to it in this case because that would have the practical effect of controlling its conduct outside of Illinois, given that “in many cases it is in fact impossible to identify where a photo on the Internet comes from—or where the person in the photo resides.” Clearview objects to being made subject to BIPA’s constraints “merely because some small percentage of Clearview’s database of ‘three billion’ publicly-available photographs contain images of Illinois residents.” Def. Memo at 14-15.

² The legislature was concerned about what national actors might do with Illinois residents’ biometric information, because “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; therefore, once compromised, the individual has no recourse [and] is at heightened risk for identity theft ...” Further, “The full ramifications of biometric technology are not fully known.” 740 ILCS 14/5(c) and (f).

This argument is troubling. A “small percentage” of three billion is a very large number. One percent of three billion is thirty million. Maybe the percentage is not exact, but *many* Illinois residents have indisputably had their biometric information captured by Clearview. Yet Clearview argues that BIPA should not apply to it because Clearview built a system and a business model—the “world’s best facial-recognition technology combined with the world’s largest database of headshots”—in such a way that it cannot identify which of its faceprints are associated with Illinois residents, so it cannot comply with Illinois law.

The dangers of accepting this argument are apparent. It would reward reckless disregard of the law in blind deference to technology—a kind of “too big to comply” argument. The Court rejects Clearview’s dormant Commerce Clause argument.

The *Facebook* court in California also soundly rejected the dormant Commerce Clause argument:

Facebook's cursory reference to the specter of inconsistent regulations is equally unavailing. Facebook says that the Commerce Clause “precludes Illinois from overriding the decisions of California and other states” to not regulate biometric information ..., but there is no risk of Illinois law overriding the laws of the other states. This suit involves Facebook's conduct with respect to Illinois users only, and even so, evidence in the record shows that Facebook can activate or deactivate features for users in specific states with apparent ease when it wants to do so. ... Nothing indicates that liability under BIPA would force Facebook to change its practices with respect to residents of other states.

In re Facebook Biometric Info. Privacy Litig., 2018 U.S. Dist. LEXIS 81044, at *14 (N.D. Cal. 2018).

First Amendment

Clearview argues that BIPA is unconstitutional as applied in this case. Clearview contends it is engaged in protected speech under the First Amendment, that the proper standard of review is strict scrutiny, and that BIPA cannot survive strict scrutiny. Clearview emphasizes that all the photos it uses in its system were obtained from publicly-available online sources.

Is it Speech?

The First Amendment protects not just expression, but some necessary predicates to expression such as making an audio recording (*ACLU v Alvarez*, 679 F.3d 583 (7th Cir. 2012)) or observing a trial (*Richmond Newspapers, Inc. v. Virginia*, 448 U.S. 555). It can protect not just words but also symbolic notations such as musical scores and computer code. (*Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 449 (2d Cir. 2001)).

Clearview describes the creation and use of its app as the “creation and dissemination of information,” which constitutes speech under *Sorrell v. IMS Health Inc.*, 564 U.S. 552, 570

(2011) and *People v Austin*, 2019 IL 123910 ¶ 31. All the amici agreed or assumed that Clearview’s activities involve speech entitled to some level of First Amendment protection. Plaintiffs argue that Clearview’s activities involve conduct, not speech. At the same time, they concede that applying BIPA to Clearview has an incidental effect on Clearview’s speech.

The Court finds that Clearview’s activities involve expression and its predicates, which are entitled to some First Amendment protection. That does not end the inquiry. The First Amendment does not fully protect every act that involves collection or analysis of data. For instance, stealing documents and private wiretapping involve collection of data, but they are not protected by the First Amendment even if the purpose is to obtain information for a news story. *Branzburg v. Hayes*, 408 U.S. 665, 691 (1972). To determine whether a law violates the First Amendment, the Court must first decide what level of scrutiny to apply.

Level of Scrutiny

Clearview argues that BIPA is subject to strict scrutiny, because it is a content-based regulation of speech. Plaintiffs argue that BIPA is subject to intermediate scrutiny because it is a content-neutral regulation that only incidentally burdens speech.

Clearview contends that BIPA is content-based because it targets specific content—biometric information such as faceprints, but not other content such as photos. This is a distinction between types of media, not their content. If BIPA regulated, say, capture of faceprints of people yelling but not faceprints of people smiling, *that* would be a content-based distinction. BIPA does nothing of the sort.

Amici Law Professors in Opposition to Defendant’s Motion emphasize the content/source distinction and suggest that intermediate scrutiny is proper. The fact that BIPA grants privacy protections for certain kinds of communications does not make it a content-based speech restriction, they contend. They cite *Bartnicki v. Vopper*, 532 U.S. 514, 526 (2016), which held that the Electronic Communications Privacy Act’s prohibition on intercepting and disseminating the contents of wire, oral, and electronic communications was not a content-based speech restriction. The communications were “singled out ... by virtue of the source, rather than the subject matter.” *Id.*³ The Court finds that BIPA imposes content-neutral time, place or manner restrictions.

Clearview also argues that strict scrutiny is appropriate because BIPA distinguishes between which speakers are subject to the law and which are not, by exempting from the statute’s coverage any “subcontractor, contractor, or agent of a State agency.” 740 ILCS 14/25(e); see *Sorrell v. IMS Health Inc.*, 564 U.S. 552, 570-571 (2011). Speaker-based distinctions should lead to strict scrutiny only if those exemptions are hiding content- or viewpoint-based preferences. In *Sorrell*, the court found that a speaker-based distinction

³ Amici Professors in Support of Defendant’s motion suggest strict scrutiny is appropriate. They contend BIPA is content-based because it prohibits faceprints of humans but not of cats. A true content-based distinction would focus on what the subject communicates, not the subject’s species. So if a law allowed a cat to say “Mow” but not “Mew,” that would be content-based.

(regulating who could and who could not talk about certain drugs) reflected a viewpoint-based distinction in favor of speech promoting generic drugs. In summarizing its holding, the court focused on the effect of the law on suppressing certain ideas: “Privacy is a concept too integral to the person and a right too essential to freedom to allow its manipulation to support just those ideas the government prefers.” *Id.* at 580.

By contrast, BIPA’s speaker-based exemptions do not appear to favor any particular viewpoint. As BIPA’s restrictions are content-neutral, the Court finds that intermediate scrutiny is the proper standard.

BIPA Survives Intermediate Scrutiny

The U.S. Supreme Court described the application of intermediate scrutiny as follows:

- [A] government regulation is sufficiently justified
 - [1] if it is within the constitutional power of the Government;
 - [2] if it furthers an important or substantial governmental interest;
 - [3] if the governmental interest is unrelated to the suppression of free expression; and
 - [4] if the incidental restriction on alleged First Amendment freedoms is no greater than is essential to the furtherance of that interest.

United States v. O'Brien, 391 U.S. 367, 377 (1968) (numbering and formatting added).

BIPA meets all these requirements. First, the Illinois legislature unquestionably had the power to enact the statute. Second, BIPA furthers an important governmental interest, which the statute describes explicitly. The Illinois Supreme Court in *Rosenbach v. Six Flags Entm’t Corp.*, 2019 IL 123186 ¶ 35, pointed out that BIPA contains the General Assembly’s “stated assessment of the risks posed by the growing use of biometrics by businesses and the difficulty in providing meaningful recourse once a person’s biometric identifiers or biometric information has been compromised.” The court stated that BIPA tries “to head off such problems before they occur,” by imposing safeguards and punishing violators. *Id.* at ¶ 36.

This governmental interest is unrelated to the suppression of free expression. BIPA proscribes non-consensual face printing not for what it expresses, but for the risks it poses to the subject’s privacy and security. The legislature was concerned about “the substantial and irreversible harm that could result if biometric identifiers and information are not properly safeguarded.” It was concerned about “public welfare, security, and safety.” *Id.* at ¶ 37.

Finally, the incidental restrictions on Clearview’s First Amendment freedoms are no greater than necessary to further the governmental interest of protecting citizens’ privacy and security. BIPA does not prohibit Clearview from collecting or republishing publicly-available photographs or expressing an opinion about who is pictured in them. Nor does BIPA prohibit *all* use of faceprints. Instead, it requires Clearview to first provide notice and receive consent from the Illinois individuals involved. This is “to insure that individuals’ and customers’ privacy rights

in their biometric identifiers and biometric information are properly honored and protected to begin with, before they are or can be compromised.” *Id.*

Clearview emphasizes that the photos from which they make faceprints are publicly available and that Plaintiffs have no “expectation of privacy” in them. We must distinguish between the publicly-available photos Clearview harvested and what Clearview does with them. Clearview says it “collects publicly-available images from the Internet, analyzes them, and returns search results to licensed users of Clerview’s service.” Dft’s Memo at 1. BIPA comes in at the “analysis” stage, regulating the particular manner in which biometric information is captured from the photos, used, and stored.

The fact that something has been made public does not mean anyone can do with it as they please. In the Fourth Amendment context, where the “expectation of privacy” concept is most common, law enforcement is not always allowed to use technology to analyze what is public and visible. For instance, the U.S. Supreme Court held in *Kyllo v. United States*, 533 U.S. 27, 35-36, that law enforcement could not aim an infrared heat scanner at the exterior of a house to search for drugs. So, too, in our case the photos may be public, but making faceprints from them may be regulated.

In discussing the burden BIPA imposes upon its expression, Clearview focuses on BIPA’s practical effect. Clearview relies heavily on *Sorrell*, 564 U.S. at 565, for the proposition that “the First Amendment prohibits the application of laws that have the purpose and/or *practical effect* of burdening speech by *reducing the effectiveness* of its content.” Dft’s Memo at 21 (emphasis added). Clearview argues that the “inevitable effect” of BIPA would be to cripple its app—“nothing less than preventing the identification of individuals whose published photographs were on the Internet.” Dft’s Memo at 21. They contend it is “quite literally impossible to know based on publicly-available photos on the Internet from whom BIPA requires consent.” Trans. of 4/2/21 argument at 51.

The debate over Clearview’s “reduced effectiveness” argument can be simplified as follows:

Clearview: In our business, we scrape billions of photos off the internet, download them blindly,⁴ turn them into faceprints and allow our customers to search them.

Plaintiffs: You can’t do that to people from Illinois without their permission.

Clearview: We can’t possibly get their permission.

⁴ “that is, without knowledge of who the subject of the image is”—Declaration of Clearview General Counsel Thomas Mulcaire, Exh. A to Clearview’s Memo.

In balancing privacy rights and the First Amendment, should the Court's response be:

A: Then go ahead.

or

B: Then figure out a way, or you might be liable under BIPA.

The Court favors B, fully recognizing that this may have an effect on Clearview's business model. Inevitably, Clearview may experience "reduced effectiveness" in its service as it attempts to address BIPA's requirements. That is a function of having forged ahead and blindly created billions of faceprints without regard to the legality of that process in all states.

Suppose a company collected pictures of naked young people from the internet and shared the links with its customers without regard to whether or not the subjects were under 18. Suppose they did it blindly and said, "we have no way of knowing." Applying child pornography laws to this company would surely reduce the effectiveness of their service. But that would not excuse the company from complying with those laws. By the same reasoning, Clearview is not excused from complying with BIPA.

In sum, BIPA's restrictions on Clearview's First Amendment freedoms are no greater than what's essential to further Illinois' interest in protecting its citizens' privacy and security. Requiring notice and opt-in consent is a reasonable and well-tailored solution that returns control over citizens' biometrics to the individuals whose identities could be compromised.

Clearview's final First Amendment argument is that BIPA is unconstitutionally overbroad because its application would suppress a large amount of speech that is fully protected under the First Amendment. This argument also hinges on the fact that Clearview cannot identify where its images came from. The Court finds that BIPA is not overbroad, as it does not concern the rights of non-Illinois residents.

Of course, today's decision does not mean the Court has found Clearview liable for violating BIPA. Rather, today the Court rules that it has jurisdiction over the case and that the Complaint states a cause of action for which relief may be granted.

Clearview's motion to dismiss is denied.

Judge Pamela McLean Meyerson

ENTERED:

AUG 27 2021

Circuit Court - 2097

Judge Pamela McLean Meyerson