DePaul University
University Libraries

DePaul Journal of Art, Technology & Intellectual Property Law

Volume 33
Issue 1 *Spring 2023*

Article 4

ACLU v. Clearview Ai, Inc.,

Isra Ahmed
DePaul University College of Law, IAHMED20@depaul.edu

ACLU v. Clearview Ai, Inc., 2021 Ill. Cir. LEXIS 292.

*Isra Ahmed**

I. BACKGROUND OF THE CASE

ACLU v. Clearview AI[1] highlights the dangers that facial recognition software and lack of regulations can have on our society. The information Clearwater AI's facial recognition database collected was available for anyone with the money to pay for it with no restrictions on how they use it. To protect the safety of marginalized communities, the ACLU filed an action against Clearview AI. In a consent order, the court has banned Clearwater from making the database available to other private actors, including most businesses, and sends out a severe warning for companies collecting biometric data.[2]

The ACLU is a non-profit public interest law firm that routinely appears before the United States Supreme Court in its efforts to the civil liberties of American people.[3] The ACLU of Illinois is a state chapter of the ACLU. The CAASE, SWOP-Chicago, Illinois PIRG, and Mujeres (collectively, Public Interest Groups) are all also public interest organizations based in Illinois suing on behalf of their members, clients and program participants affected by Clearview's practices.

---

* Isra Ahmed is a 2024 DePaul University College of Law J.D. Candidate. Isra is a writer on the DePaul Journal of Art, Technology, and Intellectual Property. Isra graduated from Texas Woman's University with a Bachelor of Science in Computer Science and a minor in Mathematics, which has continued over in her interest in Information Technology, Cybersecurity, and Data Privacy law. She is also the Founder and President of the Part Time Law Student Organization and a member of the International Association of Privacy Professionals, where she is pursuing privacy certifications as well. Due to her personal international background, Isra is specially interested in IT law related to digital assets and data privacy laws on a global scale.

[1] *ACLU v. Clearview Ai, Inc.*, 2021 Ill. Cir. LEXIS 292.

[2] *See* Press Release, *ACLU, In Big Win, Settlement Ensures Clearview AI Complies with Groundbreaking Illinois Biometric Privacy Law* (May 9, 2022), https://www.aclu.org/press-releases/big-win-settlement-ensures-clearview-ai-complies-with-groundbreaking-illinois#:~:text=As%20part%20of%20the%20settlement,businesses%20and%20other%20private%20actors.

[3] ACLU History, https://www.aclu.org/about/aclu-history, (last visited February 12, 2023).

Clearview AI is a U.S. software company with facial recognition technology.[4] Clearview AI's algorithm takes facial recognition data from public sources to deliver an image-search solution.[5] Prior to the lawsuit, this intelligence platform was available for anyone who wished to purchase it, such as universities, wealthy individuals, and other private businesses. As agreed in the settlement contract, this platform is now only available for law enforcement agencies from the local to federal levels.

On January 18, 2020, the New York Times published an article on Clearview AI.[6] This article shed light on the company, a young start up at the time, and its potential dangers regarding data privacy as it built a tracking and surveillance tool using biometric identifiers. The biometric identifier at issue is the faceprint, which as defined by the ACLU complaint, is a print of your face, much like a thumbprint, that can be used to discern or verify an individual's identity.[7] Facial recognition systems work in two distinct phases: enrollment and identification.[8] The enrollment phase is the creation of the first logging of a faceprint.[9] To create a faceprint from a picture, the face recognition algorithm scans the image for a human face, noting facial feature data often based on the roughly 80 nodal points such as the distance between a person's eyes, the shape of their nose, the pattern of freckles or any discerning birth marks or moles that amount to an individual's immutable biological characteristic.[10] The software then assigns that data an overall faceprint in the form of a numerical value which is then typically stored in a database, with faceprints representing faces that look similar grouped together.[11]

During the identification phase, the facial recognition

[4] *Company Overview*, Clearview AI, https://www.clearview.ai/overview, (last visited February 12, 2023).
[5] *Id*.
[6] Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, (Nov. 2, 2021), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.
[7] ACLU, *supra* note 1.
[8] *Id*. at 8.
[9] *Id*.
[10] *Id*.
[11] *Id*. at 9.

algorithm searches the existing database to see if the recently made faceprint matches any existing faceprints. If the algorithm finds a match, it can then build a reliable faceprint of the person's features in its database, increasing the likelihood of them being identified. This occurs each time a faceprint is captured, adding more details as it runs. Clearview AI is no longer a young start up and now boasts the world's largest law enforcement database of 20+ billion images. It is the #1 algorithm in the U.S. and western worlds out of 650+ algorithms tested by the National Institute of Standards and Technology Facial Recognition Vendor 1:1 Verification Test.[12] This means that even if a person changes their hair, starts wearing color contacts, or gets a nose job, this algorithm with access to billions of pictures will still have no problem identifying them.

On May 28, 2020, the American Civil Liberties Union (ACLU), the ACLU of Illinois, and the law firm Edelson PC on behalf of Chicago Alliance Against Sexual Exploitation ("CAASE"), Sex Workers Outreach Project Chicago ("SWOP-Chicago"), Illinois State Public Interest Research Group, Inc. ("Illinois PIRG"), and Mujeres Latinas en Acción ("Mujeres"), all filed a complaint against Clearview AI, Inc. ("Clearview") alleging a violation of Illinois residents' privacy rights under the Illinois Biometric Information Privacy Act (BIPA).[13]

ACLU and the ACLU of Illinois filed this lawsuit in Circuit Court of Cook County, Illinois, attempting to prevent the company from making their database and platform available to private companies, individuals, public institutions, and law enforcement agencies. The Public Interest Groups filing suit have constituents who have been subject to faceprinting by Clearview AI without consent and risk suffering some of the gravest consequences, such as a higher risk of identity theft as well as the endangerment of the lives of domestic violence and sexual assault victims, undocumented immigrants, communities of color, and members of other vulnerable communities. This lawsuit is the first

[12] *Facial Recognition*, Clearview AI, https://www.clearview.ai (last visited Apr. 10, 2022).
[13] Compl. at 1, *ACLU v. Clearview AI*, (May 28, 2020) (No. 9337839), https://www.aclu.org/legal-document/aclu-v-clearview-ai-complaint.

to focus explicitly on the harm that Clearview's unprecedented intelligence program inflicts on vulnerable communities and minorities. ACLU claimed that Clearview's algorithm clearly violated BIPA and urged the court to demand that the company cease operations until they both comply with BIPA's consent requirements and delete existing faceprints created without consent. Clearview AI filed a motion to Dismiss.

II. BACKGROUND OF PRIVACY LAW AND THE ILLINOIS BIOMETRIC INFORMATION PRIVACY ACT

This case highlights the gap between our current privacy laws and technological advances. Online privacy and security is difficult to govern when it keeps advancing faster than our regulations. Although most U.S. residents have a technological footprint, we still lack a uniform federal code or statute that regulates data privacy.

The closest thing we have to a federal act protecting data privacy is the U.S. Privacy Act of 1974**.**[14] This act establishes the rights and restrictions on the collection, use, and disclosure of personal information held by government agencies. We have some regulations to protect certain types of personal information, such as individuals' medical information under The Health Insurance Portability and Accountability Act (HIPAA)[15], personal information collected on children under the Children's Online Privacy Protection Act (COPPA)[16], and restrictions on financial institutions' collection, use, and disclosure of consumer data under the Gramm-Leach-Bliley Act (GLBA).[17] However, any personal information not covered by these acts, such as biometric data, can be seen as free game by private businesses.

This leaves companies to collect, use and disclose personal information as they like. To combat this issue, states have begun implementing their own data privacy laws. Some states like

[14] 5 U.S.C. § 552a.
[15] 42 U.S.C. 1320d.
[16] 15 U.S.C. § 6501.
[17] 12 U.S.C. § 1811.

California have great data privacy regulations set in place, such as the California Consumer Privacy Act and soon the California Consumer Privacy Rights Acts, while other states are catching up and some still have none.

Currently, Illinois has one of the toughest laws in the United States regarding biometric data. Before the enactment of this law, major national corporations had chosen Illinois as their pilot testing sites for new applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias.[18]

Thus, in 2008, Illinois enacted BIPA to regulate the collection, use and storage of biometric data. BIPA requires private entities to (1) obtain informed, written consent from individuals prior to collecting their biometric information and (2) develop a written, publicly available policy on retention and destruction of such information.[19] BIPA also prohibits entities from profiting from the biometric data and permits only a limited right to disclosure of the information.[20]

BIPA defines "private entity" as “any individual, partnership, corporation, limited liability company, association, or other group, however organized.”[21] BIPA also defines “biometric information” as any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual.[22] Biometric information does not include information derived from items or procedures excluded under the definition of biometric identifiers.[23] The biometric identifiers definition under BIPA includes a “scan of hand or face geometry.”[24] Thus, the faceprints captured by Clearview AI are not excluded as biometric information under BIPA.

[18] 740 ILCS 14/5(b) (2008).
[19] *Id*. at §15 (a), (b), and (e).
[20] *Id*. at §15(c)-(d).
[21] *Id*. at §10.
[22] *Id*.
[23] *Id*.
[24] *Id*.

BIPA creates a private right of action for individuals "aggrieved" by a violation of the statute.[25] However, because there were millions of Illinois residents affected by the issue at hand, it made more sense for the aforementioned groups to represent them in them in this lawsuit.

III. CIRCUIT COURT OF COOK COUNTY, ILLINOIS, DENIES CLEARVIEW AI'S MOTION TO DISMISS

On August 27, 2021, the Circuit Court of Cook County, Illinois, denied Clearview AI's Motion to Dismiss.[26]

Plaintiffs, the ACLU and four other organizations suing on behalf of their members, clients, and program participants, had filed a complaint alleging Clearview AI violated Section 15 of BIPA.

The Complaint alleges that Clearview AI 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 subjects' 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.[27]

Specifically, the complaint alleges that Clearview AI "systematically and automatically captured, used and stored their biometric identifiers without first obtaining the written release."[28] It also alleges that Clearview AI did not publicly provide a

[25] *Id*. at § 20.
[26] Mot. to Dismiss, *ACLU v. Clearview Ai, Inc.*, 20 CH 4353 (Ill. Cir. Ct. 2021).
[27] *Id.* at § 15(b).
[28] Compl. at ¶ 70.

retention scheme or any guidelines for permanently destroying individuals' biometric identifiers.[29] This violates 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.[30]

Clearview AI moved to dismiss. The Court received amici briefs from the Electronic Frontier Foundation and from two groups of law professors, one in support and one in opposition to Clearview AI's motion to dismiss. After hearing oral arguments on Zoom, it came to the following conclusions on 4 issues.

First, Clearview AI contended that it is not subject to personal jurisdiction in Illinois. The Court denied the motion to dismiss on jurisdictional grounds immediately based on the decision the U.S. District Court for the Northern District of Illinois made in *Mutnick v. Clearview AI, Inc*.[31] In[32] As the Court points out, in our case Plaintiffs also showed that Clearview AI targeted Illinois by marketing its faceprint database to a substantial number of Illinois customers.

Second, Clearview AI contended that the Complaint fails under Illinois' extraterritoriality doctrine because BIPA cannot

[29] Compl. at ¶ 72.
[30] *Id*. at § 15(a).
[31] *Mutnick v. Clearview AI, Inc.*, 2020 U.S. Dist. LEXIS 144583 *7 (N.D. Ill. 2020).
[32] *Id.* at 7.

regulate out-of-state conduct; and under the U.S. Constitution's dormant Commerce Clause applying BIPA to Clearview would be regulating commerce in another state, thereby precluding its application to Clearview AI's conduct.

The Court held that the extraterritoriality doctrine does not warrant a dismissal of Plaintiff's Complaint based on BIPA's legislative findings. The Ninth Circuit Court of Appeals found it reasonable to conclude that the General Assembly intended for BIPA's application to include individuals who are located in Illinois, even if some relevant activities occur outside the state. In this case, Plaintiffs suggest that many millions of images uploaded by Illinois residents and collected by Clearview AI were uploaded from Illinois and that Clearview's Illinois customers used Clearview to search for Illinois residents.[33] Thus, BIPA is still applicable.

The Court also rejects Clearview's dormant Commerce Clause argument because it would be too dangerous to accept. Clearview AI argued that BIPA is not applicable in this case because it would have the practical effect of controlling its conduct outside of Illinois. Their business would be majorly affected as it would be "impossible to identify where a photo on the Internet comes from – or where the person in the photo resides" and that Illinois residents were a "small percentage of Clearview's database of 'three billion' publicly-available photographs."[34] As the Court points out, this argument is weak and a small percentage of three billion is still a considerable number of people. A "too big to comply" excuse is not enough for Clearview AI to be let off the hook.

The third argument is that BIPA's application to Clearview AI is unconstitutional under the First Amendment and Article 1 Section 4 of the Illinois Constitution. It contends that its system and practices are classified as protected speech under the First Amendment, for which the proper standard of review is strict scrutiny, and that BIPA cannot survive strict scrutiny.

The Court, as well as the Plaintiffs and amici concede that Clearview's activities involve expression, which entitles it to some

[33] Pltf. Resp. at 11.
[34] *ACLU v. Clearview AI, Inc.*, 2021 WL 4164452, at *6 (Ill.Cir.Ct.).

protection under the First Amendment. However, this does not fully protect Clearview AI's actions.

Clearview AI argues that BIPA is subject to strict scrutiny because it is a content-based regulation of speech due to its target of biometric information. However, the Court rejects this contention, stating that if BIPA regulated the types of faceprints that could be seen as content-based distinction but as it stands today, there is no such thing. Clearview AI also attempts to apply strict scrutiny because BIPA distinguishes between which speakers are subject to the law and which are not, specifically excluding "subcontractor[s]. contractor[s], or agent[s] of a state agency."[35] The Court rejects this argument as well, finding that BIPA's speaker-based exemptions are content-neutral.

On the other hand, Plaintiffs argue that BIPA is subject to intermediate scrutiny because it is content-neutral that only incidentally burdens speech. Amici Law Professors in Opposition to Defendant's Motion emphasize the content and source distinction, citing *Bartnicki*[36], which held that the Electronic Communications Privacy Act did not have any content-based speech restrictions. The Court sides with these parties, agreeing that BIPA is content-neutral and thus subject to intermediate scrutiny.

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

> [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.[37]

[35] 740 ILCS 14/25(e).
[36] *Bartnicki v. Vopper*, 532 U.S. 514, 526 (2016).
[37] *United States v. O'Brien*, 391 U.S. 367, 377 (1968).

BIPA meets all of these requirements. As the Court stated in its decision, (1) Illinois legislature had the power to enact the statute, (2) BIPA furthers an important governmental interest, specifically to prevent a person's biometric identifiers from being compromised and to provide meaningful recourse if it does happen, (3) this governmental interest, "the substantial and irreversible harm that could result if biometric identifiers and information are not properly safeguarded," is unrelated to the suppression of free expression, and (4) 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 simply requires Clearview to first provide notice and receive consent from any Illinois individual whose information may be involved.

As the Amicus brief by the Electronic Frontier Foundation states, "Illinois has a substantial interest in protecting the information security of its residents."[38] BIPA's consent requirement for Clearview AI's faceprinting is narrowly drawn to Illinois' substantial interests. Illinois' substantial interests in protecting its residents' biometric privacy, free speech, and information security, and its requirement that Clearview AI obtain an individual's opt-in consent before collecting their faceprint is a "close fit" as defined in *McCullen*.[39]

Clearview AI argues that the photos from which they make faceprints are public, and thus there should be no expectation of privacy regarding them. The Court immediately shuts this down, stating that just because something is public does not mean that anyone can do what they please with that material, and this is especially true in our case because law enforcement is not always allowed to use technology to analyze public material.

Finally, Clearview AI proposes a 'reduced effectiveness' argument which is essentially another side of the 'too-big-to-comply' argument. They state that BIPA's requirement would majorly impact their business model and it would be nearly impossible to comply with as finding out the residence of a person in a photo is extremely difficult. While the Court understands this

[38] Electronic Frontier Foundation Amicus Brief ¶ C.
[39] *McCullen*, 573 U.S. 486.

imposition will have a major impact on Clearview AI's business model, the 'reduced effectiveness' argument does not hold because "BIPA's restriction on Clearview First Amendment freedoms are no greater than what's essential to further Illinois' interest in protecting its citizens' privacy and security." Requiring an opt-in consent method for Illinois residents is the least restrictive and most reasonable solution in this case.

The fourth and final argument is that BIPA is unconstitutionally overboard "because its application would suppress a large amount of speech that is fully protected under the First Amendment." Again, this argument relies upon the fact that finding the state of residence of a person in their photographs will be impossible. The Court finds that BIPA is not overboard because it only concerns Illinois residents.

The Complaint states a valid cause of action and because of the aforementioned reasons, the Court denied Clearview AI's motion to dismiss.

IV. SIGNED SETTLEMENT AGREEMENT BETWEEN CLEARVIEW AI AND PLAINTIFFS

On May 4, 2022, Plaintiffs and Clearview AI entered a Signed Settlement Agreement, intended to fully, finally, and forever resolve, discharge, and settle all the claims specified within it based on the agreed terms and conditions.[40]

The first term of agreement between the parties involves a permanent nationwide injunction against Clearview AI, prohibiting the company from granting paid or free access to the Clearview AI database of alleged facial vectors at issue in Plaintiffs' complaint and Clearview AI's counterclaim to: (1) any private entity or individuals except as consistent with BIPA Section 15 and 25; and (2) any individual government employee who is not acting in their official capacity on behalf of a local, State, or federal government agency. Essentially this agreement

[40] *In Big Win, Settlement Ensures Clearview AI Complies with Groundbreaking Illinois Biometric Privacy Law*, ACLU (May 9, 2022, 11:45 AM), https://www.aclu.org/press-releases/big-win-settlement-ensures-clearview-ai-complies-with-groundbreaking-illinois.

permanently prohibits Clearview AI from selling or providing its database of biometric data for free to anyone, except government officials in their official capacity, without first getting opt-in consent from the person involved. Exceptions under BIPA will still apply to this injunction.

The second term of agreement between the parties is a temporary injunction for a period of five (5) years from the date of entry of the Consent Order prohibiting Clearview AI from granting either paid or free access to Illinois state, county, local or other government agencies and contractors working for those agencies in Illinois, including state and local police departments and other state and local law agencies to the Clearview AI App. This section also temporarily prohibits Clearview AI from granting either paid or free access to any private entity located in Illinois, even if the transaction in question would be otherwise permissible under BIPA Sections 15 and 25. In addition, Clearview AI agrees to a temporary injunction prohibiting the granting of either paid or free access to any individual employee of the Illinois State and Local agencies during this period, including when they are in their official capacities. Essentially, this Illinois State Ban prohibits Clearview AI from operating in Illinois until May 11, 2027.

The third term of the agreement between the parties clarifies the restrictions on Clearview's ability to contract with third parties. Specifically, excluding the private entity and individual ban in Section 1n and time limited Illinois State Ban in Section 2, no provision of this Settlement Agreement shall be construed to limit Clearview's ability to work with federal government agencies, including those in Illinois, and any other State or local government agencies outside of Illinois or contractors engaged in authorized support for and under contracts with such government agencies. This Settlement cannot prevent Clearview AI from working with federal government agencies or from doing business outside of Illinois.

The fourth term of agreement between the parties' releases Clearview AI from any actions arising under or relating to BIPA or other federal, state, local, statutory, or common law actions arising from Plaintiffs' allegations.

The fifth term of agreement is a standard covenant not to sue, stating that Plaintiffs cannot sue Clearview for any and all future

claims under BIPA or other claims arising from Plaintiffs' allegations. This is contingent upon Clearview AI's compliance with the Consent Order and Settlement, expiration by operation of the terms of the injunction in Paragraph 2 and lack of a material amendment to BIPA or other laws that would prohibit or limit Clearview AI from granting access to the Clearview App to the Illinois State and local agencies.

The sixth term of agreement is an injunction against Clearview requiring them to delete all facial vectors in the Clearview App that existed before Clearview ceased providing or selling access to the Clearview App to private individuals and entities within fourteen (14) days of the Consent Order. However, Clearview AI will be able to re-create or use pre-existing facial vectors when it operates under an exception to BIPA as detailed in 740 ILCS 14/25, and this does not violate the Settlement Agreement.

The seventh term of agreement is a requirement for Clearview to maintain a publicly available internet-based opt-out request form for Illinois residents. A person can use this form to submit a photograph of themselves which will then only be used by Clearview to block any search results that include photographs containing the Illinois resident to the best of Clearview AI's ability. In addition, Clearview AI agrees to pay a one-time payment of $50,000 to advertise an Internet notice via Google, Facebook, or other reasonable Internet-based advertisements to publish the opt-out program to Illinois residents within fourteen (14) days of entry of the Consent Order by a contractor to be approved by both parties.

Finally, the eighth term of the agreement requires Clearview AI to maintain for five (5) years from the date of the entry of the Consent Order Clearview's filter program of screening out, to the best of its ability, Illinois-based photographs from the Clearview App. Except for litigation purposes, Clearview AI cannot access or use any images that are geotagged as being uploaded in Illinois or have metadata that associating them with a geolocation within Illinois from search results in the Clearview AI app.

The other terms of the Settlement Agreement are standard terms including terms and conditions about attorneys' fees,

dismissal, enforceability of consent order and settlement agreement and so forth.

V. CONSENT ORDER OF PERMANENT AND TIME-LIMITED INJUNCTIONS AGAINST CLEARVIEW AI, INC.

On May 11, 2022, the Court entered the Consent Order of Permanent and Time-Limited Injunctions against Clearview AI, Inc. This court order against Clearview AI enters the judgement, ordering Clearview AI to adhere to the same eight term agreements mentioned in the section above from the Settlement Agreement. It also dismisses the Action on the merits and with prejudice.

VI. IMPACT ON FUTURE LITIGATION AND COMPANY DATA PRIVACY PRACTICES

As best put by Nathan Freed Wessler, a deputy director of the ACLU Speech, Privacy and Technology Project, "[b]y requiring Clearview to comply with Illinois' pathbreaking biometric privacy law not just in the state, but across the country, this settlement demonstrates that strong privacy laws can provide real protections against abuse. Clearview can no longer treat people's unique biometric identifiers as an unrestricted source of profit. Other companies would be wise to take note, and other states should follow Illinois' lead in enacting strong biometric privacy laws."[41]

Just a few weeks before the Settlement Agreement was signed and the Consent order decreed, Clearview AI had announced its ambitious plan to put every single human face in its

[41] *See* Press Release, *In Big Win, Settlement Ensures Clearview Complies with Groundbreaking Illinois Biometric Privacy Law*, ACLU (May 9, 2022), https://www.aclu.org/press-releases/big-win-settlement-ensures-clearview-ai-complies-with-groundbreaking.-illinois#:~:text=As%20part%20of%20the%20settlement,businesses%20and%20other%20private%20actors.

database.[42] It was aiming for 100 billion pictures in its database, which would strengthen the AI and make it capable of recognizing pretty much everyone. With £50m in funding from investors, this is a goal Clearview AI can achieve sooner than we think. It already has 30 billion plus images in its database, and with the new U.S. patent for its highly accurate, bias-free facial recognition algorithm, its possibilities are endless.[43] For example, the algorithm is currently being used in the Russia-Ukraine war, aiding Ukrainian officials to uncover Russian assailants, combat misinformation and identify the dead for free.[44] While we may think this is good and even helpful for everyone, there aren't any laws keeping Clearview AI from providing the same tools and resources to Russia in the future.

This is alarming to say the least, and although this case has helped regulate the company's power in the U.S. for now, it is still going strong abroad. Certain countries such as the U.K., Australia, and Canada have already stepped up to prevent Clearview AI from mishandling its citizens data, including a possible £17m fine for "serious breaches" of data privacy laws in the U.K. and a similar consent order in Australia ordering Clearview AI to stop the collection of facial images and biometric templates of Australian citizens, and to delete its current data.

BIPA will continue to protect not only Illinois residents' data privacy and security as well as other U.S. citizens as a byproduct. Courts are in favor of protecting information more than they are of allowing companies to do as they please, and we are likely to continue seeing this trend in the near future. Just a month

[42] Leigh McGowran, *Clearview AI plans to put almost every human face in its database*, (Feb. 17, 2022), https://www.siliconrepublic.com/enterprise/clearview-ai-100-billion-photos-facial-recognition-database#:~:text=Controversial%20facial%20recognition%20company%20Clearview,obtained%20by%20The%20Washington%20Post.

[43] *See* Press Release, *Clearview AI Awarded U.S. Patent for Highly Accurate, Bias-Free Facial Recognition Algorithm*, Clearview AI (Sep. 28, 2022), https://www.clearview.ai/clearview-ai-awarded-us-patent-for-highly-accurate-bias-free-facial-recognition-algorithm).

[44] *War In Ukraine*, Clearview AI, https://www.clearview.ai/ukraine, (last visited February 12, 2023).

ago, a jury entered a $228m verdict against BNSF Railway Company for intentionally violating BIPA 45,600 times in the first ever Illinois BIPA trial.[45] This verdict is a wakeup call for private entities that collect, use, or store biometric data, especially in the U.S., as it demonstrates the potential exposure for failing to follow the statute's consent requirement.[46]

[45] *Rogers v. BNSF Ry. Co.*, 19 C 3083, 2019 WL 5635180 (N.D. Ill. Oct. 31, 2019).

[46] *$228M Verdict in First Illinois Biometric Information Privacy Act Trial*, Perkins Coie Updates (Oct. 18, 2022), https://www.perkinscoie.com/en/news-insights/dollar228m-verdict-in-first-illinois-biometric-information-privacy-act-trial.html.