12-Person Jury

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

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.:

COMPLAINT

Plaintiffs American Civil Liberties Union ("ACLU"), American Civil Liberties Union of Illinois ("ACLU-IL"), 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") bring this Complaint against Defendant Clearview AI, Inc. ("Clearview") to put a stop to its unlawful surreptitious capture and storage of millions of Illinoisans' sensitive biometric identifiers. Plaintiffs, for their Complaint, allege as follows upon personal knowledge as to themselves and their own acts and experiences and, as to all other matters, upon information and belief.

NATURE OF THE ACTION

1. This case seeks to remedy an extraordinary and unprecedented violation of Illinois residents' privacy rights by Clearview, a company seeking to profit off its use of "face

recognition technology" to capture billions of personally identifying "faceprints." A "faceprint," much like a thumbprint or a DNA profile, is a biometric identifier that is used to discern or verify an individual's identity. "Face recognition technology" is the system used to create faceprints.

2. Like other biometrics, faceprints rely on an individual's immutable biological characteristics—from the distance between one's eyes and the shape of one's cheekbones to the pattern of freckles on one's forehead—to capture their biometric signature. This process is akin to identifying the loops, whorls, and arches on one's finger (for a fingerprint), or the unique patterns and gradations of the eye (for an iris or retina scan).

3. Given the immutability of our biometric information and the difficulty of completely hiding our faces in public, face recognition poses severe risks to our security and privacy. The capture and storage of faceprints leaves people vulnerable to data breaches and identity theft. It can also lead to unwanted tracking and invasive surveillance by making it possible to instantaneously identify everyone at a protest or political rally, a house of worship, a domestic violence shelter, an Alcoholics Anonymous meeting, and more. And, because the common link is an individual's face, a faceprint can also be used to aggregate countless additional facts about them, gathered from social media and professional profiles, photos posted by others, and government IDs.

4. In prescient recognition of these threats, more than a decade ago the Illinois General Assembly enacted the Illinois Biometric Information Privacy Act ("BIPA"), which protects people against the surreptitious and nonconsensual capture of their biometric identifiers, including faceprints. 740 ILCS 14/15(b). In enacting the BIPA, the Legislature explained: "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." 740 ILCS 14/5(c).

5. Plaintiffs are organizations representing the interests of thousands of Illinois residents. The ability to control their biometric identifiers and to move about in public, free from the threat of surreptitious unmasking or surveillance, is essential to Plaintiffs' members, clients, and program participants in Illinois.

6. Clearview has violated and continues to violate the BIPA rights of Plaintiffs' members, clients, and program participants and other Illinois residents at staggering scale. Using face recognition technology, Clearview has captured more than three billion faceprints from images available online, all without the knowledge—much less the consent—of those pictured. Clearview claims that, through this enormous database, it can instantaneously identify the subject of a photograph with unprecedented accuracy, enabling covert and remote surveillance of Americans on a massive scale. This technology is so dangerous, in fact, that this little-known startup "might end privacy as we know it."[1]

7. In capturing these billions of faceprints and continuing to store them in a massive database, Clearview has failed, and continues to fail, to take the basic steps necessary to ensure that its conduct is lawful, including by obtaining the prior written consent of the individuals' who appear in the photos; informing those individuals of when their biometric data will be deleted; or even telling them to whom Clearview will be disclosing or selling their faceprints.

8. This secrecy is deeply concerning, as public reporting indicates that Clearview has provided thousands of entities and individuals with access to the billions of faceprints it has

[1] Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, The New York Times (Jan. 18, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

captured. Its users include more than 200 companies, including Kohl's, Walmart, Wells Fargo, Bank of America, and the Chicago Cubs, as well as law enforcement agencies and other governmental entities in Illinois, throughout the United States at the federal, state, and local levels, and around the world. And they include private individuals—including celebrities and wealthy businesspeople—in their personal capacities, and many individuals—including police officers and corporate employees—who use the surveillance technology as part of a 30-day free trial or other arrangement, without any contract between Clearview and their employers. According to news reports, by February 2020, people associated with 2,228 companies, law enforcement agencies, and other institutions had collectively performed nearly 500,000 searches of Clearview's faceprint database.[2]

9. Clearview's brazen disregard for individual privacy rights violates Illinoisans' rights under the BIPA, which was specifically designed to protect Illinois residents from practices like Clearview's.

10. Accordingly, this Complaint seeks an Order declaring that Clearview's conduct violates the BIPA and requiring Clearview to cease the unlawful activities discussed throughout this Complaint.

PARTIES

11. Plaintiff ACLU is a non-profit, nonpartisan nationwide membership organization headquartered in New York. Plaintiff ACLU-IL is a state affiliate of the ACLU, and is a separately incorporated non-profit, nonpartisan statewide membership organization that shares

[2] Ryan Mac, Caroline Haskins, & Logan McDonald, *Clearview's Facial Recognition App Has Been Used By The Justice Department, ICE, Macy's, Walmart, And The NBA*, Buzzfeed News (Feb. 27, 2020), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement.

members with the ACLU in Illinois. Both organizations are dedicated to protecting and expanding the civil rights and civil liberties enshrined in the constitutions and laws of the United States and the State of Illinois. One of the ACLU's and ACLU-IL's primary purposes is ensuring that individuals are able to enjoy their right to privacy, particularly in the face of advancing technological capabilities of corporations and the government. The ACLU and ACLU-IL have more than 35,000 dues-paying members in Illinois, many of whom have been, and will continue to be, subjected to surreptitious and nonconsensual capture of their faceprints by Clearview. The ACLU and ACLU-IL sue on behalf of their members.

12. Plaintiff CAASE is a Chicago-based non-profit organization dedicated to protecting and advancing the rights of survivors of sexual violence and exploitation. One of CAASE's primary purposes is ensuring that victims' and survivors' rights are respected and upheld, including their rights to privacy, safety, and consideration. CAASE has helped thousands of individuals in Illinois, many of whom have been, and will continue to be, subjected to surreptitious and nonconsensual capture of their faceprints by Clearview. CAASE sues on behalf of its clients and program participants.

13. Plaintiff SWOP-Chicago is a Chicago-based non-profit organization dedicated to improving the lives of current and former sex workers in the Chicago area. SWOP-Chicago's members include current and former sex workers, sex educators, and academic and activist allies in Illinois. Through education, advocacy, and peer support programs, SWOP-Chicago seeks to provide its members and other similarly situated individuals with access to supportive community and health care, to end physical and psychological violence against current and former sex workers at the hands of police, clients, and employers that is fueled in part by criminalization of sex work, and to curb social stigma against this community. Protecting the

privacy and confidentiality of vulnerable individuals among its members and the populations it serves is central to SWOP-Chicago's work. Many of SWOP-Chicago's members have been, and will continue to be, subjected to surreptitious and nonconsensual capture of their faceprints by Clearview. SWOP-Chicago sues on behalf of its members and program participants.

14. Plaintiff Illinois PIRG is a non-profit, nonpartisan membership organization that advocates for the public interest. Similar to ACLU and ACLU-IL, Illinois PIRG is dedicated to protecting and expanding the civil rights and civil liberties enshrined in the constitutions and laws of the United States and the State of Illinois. In particular, one of Illinois PIRG's primary purposes is ensuring that individuals are able to enjoy their right to privacy, particularly in the face of advancing technological capabilities of corporations and the government. Illinois PIRG has thousands of dues-paying members in Illinois, many of whom have been, and will continue to be, subjected to surreptitious and nonconsensual generation of their faceprints by Clearview. Illinois PIRG sues on behalf of its members.

15. Plaintiff Mujeres is a multiservice, non-profit organization dedicated to improving the lives of Latinas and their families in the Chicago area. Founded in 1973, Mujeres is the longest standing incorporated Latina organization in the nation. Over the years, Mujeres has developed a comprehensive array of social services and advocacy initiatives that promote non-violence, reproductive health, and leadership development. The organization now serves more than 8,000 community residents annually, through counseling, crisis intervention, and court advocacy for survivors of domestic violence and sexual assault; parent support programs; court supervised visitation for noncustodial parents; entrepreneurship education, and leadership development programs. Also, through its Community Engagement and Mobilization Program, Mujeres educates participants so that they can become civically engaged about issues affecting

their lives and community. A significant proportion of the organization's program participants are survivors of domestic violence and sexual assault, and/or are undocumented immigrants. Many of Mujeres's program participants have been, and will continue to be, subjected to surreptitious and nonconsensual capture of their faceprints by Clearview. The organization is dedicated to protecting these individuals against unjustified incursions on their privacy that may threaten their safety. Mujeres sues on behalf of its program participants.

16. Defendant Clearview AI, Inc. is a Delaware corporation with its principal place of business located at 214 West 29th Street, 2nd Floor, New York City, New York 10001. Clearview conducts business throughout this County and the State of Illinois.

JURISDICTION AND VENUE

17. This Court has jurisdiction over Defendant pursuant to 735 ILCS 5/2-209 because Defendant conducts business transactions in Illinois (having offered its services for sale in Illinois and then actually selling its services to customers in Illinois), has committed tortious acts arising from and related to its conduct and contracts in Illinois, and has committed tortious acts expressly aimed at Illinois residents from which this action arises. This Court has jurisdiction over Plaintiffs because they have members, clients, and program participants in Illinois, and because ACLU-IL's, CAASE's, SWOP-Chicago's, Illinois PIRG's, and Mujeres's principal places of business are located in the State of Illinois.

18. Venue is proper in Cook County because Defendant conducts business in this State and in Cook County, and Plaintiffs ACLU-IL, CAASE, SWOP-Chicago, Illinois PIRG, and Mujeres have their principal places of business in Cook County.

FACTUAL BACKGROUND

I. The Use of Biometrics and Consumer Privacy.

19. "Biometrics" refers to signifiers used to identify individuals based on their unique physical and biological characteristics. Faceprints are one of the most prevalent examples of biometrics today. Like other forms of biometric data collection—such as those capturing fingerprints and DNA—face recognition technology captures biometric data from and about people's bodies.

20. To create a faceprint from a photograph, a face recognition system scans the image for human faces; captures facial feature data—often based on the roughly 80 nodal points of the human face, including the distance between their eyes, nose, and ears, and the shape of their cheekbones; and finally assigns that data a faceprint, often a numerical value. Faceprints are then typically stored in a database, with faceprints representing faces that look similar clustered near one another.

21. Faceprints are created during two distinct phases in a face recognition system: enrollment and identification. During the enrollment phase, the algorithm captures biometric information from a picture of a person's face and stores the resulting faceprint in a database ready for future identification queries. The identification phase generally involves capturing a faceprint from a new photo using the same algorithm, and then querying the database to determine if the new faceprint matches any of the existing faceprints in the database. If a database match is found, a person may be identified.

22. This is similar to other biometric identification technologies—including fingerprints or DNA—which typically involve the capture of a biometric identifier at two distinct phases: first, to enroll the individual and link the biometric to a known identity, and second to

match a biometric of unknown origin to that known identity.

23. Face recognition technology poses an unprecedented threat to individuals' privacy and security. During a hearing captioned "What Facial Recognition Technology Means for Privacy and Civil Liberties," Senator Al Franken asserted that "if we do not stop and carefully consider the way we use [face recognition technology], it may . . . be abused in ways that could threaten basic aspects of our privacy and civil liberties."[3] For example, Sen. Franken continued, it is possible to use the technology to identify people at a distance and in crowds, and the technology could be "abused to not only identify protesters at political events and rallies, but to target them for selective jailing and prosecution."[4]

24. At the same hearing, an expert testified that face recognition technology takes the "risks inherent in . . . biometrics to a new level because Americans cannot take precautions to prevent the collection of their image," and that "[f]ace recognition allows for the covert, remote and mass capture and identification."[5] A person's faceprint can be used to find their "name [and] social networking account," and to "find and track [them] in the street, in the stores [they] visit, the government buildings [they] enter, and the photos [their] friends post online."[6]

25. As the U.S. Court of Appeals for the Ninth Circuit recently explained, "the facial-

---

3 *What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the Subcomm. On Privacy, Tech. & the law of the S. Comm. On the Judiciary*, 112th Cong. 1 (2012) (statement of Sen. Al Franken, Chairman, Subcomm. on Privacy, Tech., & the Law of the S. Comm. on the Judiciary).

4 *Id*.

5 *What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the Subcomm. On Privacy, Tech. & the Law of the S. Comm. on the Judiciary*, 112th Cong. 1 (2012) (statement of Jennifer Lynch, Staff Attorney, Electronic Frontier Foundation), *available at* https://www.eff.org/files/filenode/jenniferlynch_eff-senate-testimony-face_recognition.pdf.

6 *Supra* note 3.

recognition technology at issue here can obtain information that is 'detailed, encyclopedic, and effortlessly compiled,' which would be almost impossible without such technology."[7] "Once a face template of an individual is created, [a company] can use it to identify that individual in any of the other hundreds of millions of photos uploaded to [the internet] each day, as well as determine when the individual was present at a specific location. . . . [T]he development of a face template using facial-recognition technology without consent (as alleged here) invades an individual's private affairs and concrete interests."[8]

26. Federal regulators have voiced similar concerns. In late 2011, the Federal Trade Commission ("FTC") hosted a series of wide-ranging discussions with researchers, academics, and industry representatives about face recognition technologies. Among the topics examined were the potential hazards of a third party maliciously breaching a database of biometric information. The consequences of such a breach would be especially harmful because unlike numerical identifiers (*e.g.*, Social Security numbers), which can be replaced or re-assigned, biometrics are biologically unique to each person and therefore, once exposed, an individual has no recourse to prevent falling prey to misconduct like identity theft and unauthorized tracking.

II. The Biometric Information Privacy Act.

27. In the early 2000's, major national corporations started using Chicago and other locations in Illinois to test "new [consumer] applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias." 740 ILCS 14/5(b). The privacy and security risks of this then-growing, yet unregulated, technology generated significant concern among members of the public. *See* 740

---

[7] *Patel v. Facebook, Inc.*, 932 F.3d 1264, 1273 (9th Cir. 2019) (quoting *Carpenter v. United States*, 138 S. Ct. 2206, 2216 (2018)).

[8] *Patel*, 932 F.3d at 1273.

ILCS 14/5.

28. In late 2007, the risks became acute when a biometrics company called Pay By Touch—which provided major retailers throughout the State of Illinois with fingerprint scanners to facilitate consumer transactions—filed for bankruptcy. That bankruptcy was alarming to the Illinois General Assembly because it created a specific risk that millions of fingerprint records—which, like faceprints, are unique biometric identifiers and can be linked to people's sensitive financial and personal data—could now be sold, distributed, or otherwise shared through the bankruptcy proceedings without adequate protections for Illinois residents.

29. Recognizing the "very serious need [for] protections for the citizens of Illinois when it [came to their] biometric information," Illinois enacted the BIPA in 2008. *See* Illinois House Transcript, 2008 Reg. Sess. No. 276; 740 ILCS 14/5.

30. The BIPA is an informed consent statute that achieves its goal of protecting individuals' privacy, anonymity, autonomy, and security by making it unlawful for a company to, among other things, "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers . . . , unless it *first*:

> (1) informs the subject . . . in writing that a biometric identifier . . . is being collected or stored;
>
> (2) informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier . . . is being collected, stored, and used; and
>
> (3) receives a written release executed by the subject of the biometric identifier."

740 ILCS 14/15(b).

31. Under the BIPA, biometric identifiers are defined to include retina and iris scans, voiceprints, fingerprints, and—most importantly here—scans of facial geometry. *See* 740 ILCS 14/10. Faceprints are scans of facial geometry.

32. The BIPA also establishes standards for how companies in possession of

biometric identifiers must handle them, including a requirement that companies develop and comply with a written policy—made available to the public—establishing a retention schedule and guidelines for permanently destroying biometric identifiers. *See* 740 ILCS 14/15(a), (c)–(d).

33. The BIPA's common-sense requirement that entities wishing to engage in the conduct of capturing biometric identifiers must provide notice to and obtain consent from individuals before doing so, such that individuals can maintain control over and security of their biometrics, is mirrored in other state statutes seeking to similarly protect against surreptitious and nonconsensual capture of biometric identifiers. *See* Tex. Bus. & Com. Code Ann. § 503.001; Wash. Rev. Code § 19.375.020.

III. Plaintiffs' Interests in Biometric Privacy and Security.

34. The ACLU and ACLU-IL have long advocated for the protection of the right to privacy of their members and all residents of Illinois and the nation. The ACLU and ACLU-IL recognize that face recognition technology poses a severe threat to individual privacy and security, and have advocated for the enactment and enforcement of laws and policies to curb abusive uses of biometric collection technology in general and face recognition technology in particular. ACLU-IL advocated for passage of the BIPA, and has continued to advocate against industry proposals to dilute its provisions. Clearview's practices pose a threat to the ACLU's and ACLU-IL's members by divesting them of the power to control their biometric identifiers, and by chilling their ability to exercise various constitutional rights—including the right to protest, to access reproductive healthcare services, and to travel—without being instantaneously identified and tracked.

35. CAASE also has a long history advocating for the protection of the rights to privacy for survivors of sexual harm and violation, including survivors of rape and commercial

sexual exploitation (prostitution and sex trafficking). Relevant here, survivors are often forced to flee abusive people and circumstances and, in extreme circumstances, change their identities in order to protect themselves from further harm and harassment. While traditional identifiers, like names, can be changed, there is no way for most individuals to change their biometric information. It is unique and once compromised, cannot be fully protected. For survivors who need to protect their identities in order to stay safe, biometric privacy is essential to their security, safety, and well-being. In addition:

i) CAASE is harmed by Clearview's actions. If Clearview's large-scale, surreptitious capture of faceprints is allowed to continue, CAASE's clients and program participants will be more susceptible to abusive practices by private citizens as well as police department employees (there is a long history of police officers targeting people in the sex trade for specific exploitation and harm), including the possibility that they will be afraid to travel to CAASE's offices or to meet with CAASE staff, for fear of being identified as survivors of sexual harm or commercial sexual exploitation. This chilling effect will harm CAASE by making it more difficult to meet with and assist its legal services clients, and participants in its community engagement programs.

ii) CAASE has a close relationship with its clients and program participants, such that it will be able to represent their interests in this suit. CAASE owes a fiduciary duty and a duty of care to clients of its legal services program. The legal services CAASE provides to its clients also include advocacy to protect those clients' rights to privacy and anonymity, including through motions to expunge criminal convictions, to change legal names, and to proceed by

pseudonym in litigation.

iii) CAASE's clients and program participants are hampered from bringing suit, as bringing suit in an individual capacity could reveal their true identities and expose them to abusers they have fled.

36. SWOP-Chicago is dedicated to defending the right to privacy and confidentiality of current and former sex workers. Members of these communities experience much higher rates of violence, intimidation, and harassment than the general population, and the social stigma directed at them contributes to a variety of harms, including poor health outcomes and denial of housing and employment. SWOP-Chicago regularly helps its members and other similarly situated individuals mitigate the risk of violence, intimidation, and harassment and the effects of stigma by advising them on ways to keep sensitive information about themselves, including their identities, private. Clearview's practices threaten SWOP-Chicago's members and program participants by denying them the right to control their biometric identifiers and making it easy to identify, track, and target them as they go about their lives, thus increasing the risk of violence, intimidation, harassment, and discrimination.

i) SWOP-Chicago's membership is self-identified and includes their volunteers, who carry out the majority of their outreach and other operations, and attendees of their monthly community meetings or other events such as the organization's monthly support group. Many, but not all, of SWOP-Chicago's followers on social media and subscribers to their emails also consider themselves members. SWOP-Chicago's membership also includes their leadership board, which currently includes three members but may include as many as nine, all of whom are current or former sex workers.

ii) Clearview's surveillance threatens not only SWOP-Chicago's membership, but the organization's program and activities, which are carried out with strict attention to the privacy of its members and other current and former sex workers. For example, SWOP-Chicago volunteers often conduct outreach outdoors, in neighborhoods where many of those they serve do their work. That outreach includes providing food, clothing, hygiene supplies, and harm-reduction supplies, including Narcan dose packs and clean needles. Sometimes SWOP-Chicago's volunteers bring the organization's van to a neighborhood at a pre-arranged time and place near the areas where their constituents work, and those seeking services approach the van. A Clearview user could quickly identify SWOP-Chicago volunteers and those who seek its services, interfering with SWOP-Chicago's ability to carry out its mission.

iii) Likewise, SWOP-Chicago allows photography at its meetings and events only with the express verbal consent of every individual in the photo, both to be photographed and to have the image posted online. Without this assurance of privacy, volunteers, members, and supporters would not feel comfortable attending these meetings and events. Maintaining that level of privacy and comfort is difficult in any case; it is all the more difficult if attendees can be instantly identified entering or leaving an event using Clearview's software.

iv) If Clearview's large-scale, surreptitious collection of faceprints is allowed to continue, SWOP-Chicago will be harmed because its members and other individuals who receive its services will be afraid to meet with SWOP-

Chicago's volunteers, for fear of being identified as current or former sex workers, and some will likely cease receiving services from the organization.

v) SWOP-Chicago has a close relationship with its program participants, such that it will be able to represent their interests in this suit. The services SWOP-Chicago provides to current and former sex workers include a monthly support group, condom distribution, and street outreach, as well as organizing a free, full-service legal clinic. The sensitivity of these services requires SWOP-Chicago to zealously guard the confidentiality of communications with its program participants, and to maintain privacy over their personal information.

vi) SWOP-Chicago's program participants are hampered from bringing suit. Due to the stigma and opprobrium directed at former and current sex workers, bringing suit in an individual capacity could reveal their identities and expose them to harassment, violence, or discrimination.

37. Like the ACLU, Illinois PIRG also has long advocated for protection of the right to privacy of their members and all residents of Illinois. Illinois PIRG recognizes that face recognition technology poses a severe threat to individual privacy and security, and has advocated for the preservation and enforcement of laws and policies to curb abusive uses of the biometric collection technology in general and face recognition technology in particular. Illinois PIRG is a staunch advocate in the Illinois General Assembly against industry proposals to dilute the BIPA.

38. Mujeres provides a range of services to the Latina community in Chicago, including court advocacy, individual and group counseling, and individual therapy for survivors

of domestic violence and sexual assault; counseling for children who have witnessed or been exposed to domestic violence; and medical advocacy for survivors of sexual assault who require hospitalization or other medical treatment. Many of Mujeres's program participants are undocumented immigrants. Central to the work of Mujeres work is the need to protect the privacy and security of its vulnerable program participants and their families, including helping them shield their whereabouts and identities from individuals who seek to harm them. Clearview's nonconsensual capture of faceprints poses a grave threat to the privacy and security of Mujeres's members and program participants, by removing their ability to control their sensitive biometric identifiers, and threatening to make it trivially easy to identify and track them as they move about their lives online and in the physical world, thus exposing them to stalking, harassment, and violence. In addition:

i) Mujeres is harmed by Clearview's actions. If Clearview's large-scale, surreptitious capture of faceprints is allowed to continue, Mujeres's program participants will be afraid to travel to Mujeres's offices, to attend court hearings, or to meet with Mujeres staff, for fear of being identified as survivors of sexual harm. This chilling effect will harm Mujeres by making it more difficult to meet with and serve its program participants.

ii) Mujeres has a close relationship with its program participants, such that it will be able to represent their interests in this suit. Mujeres employs masters level counselors and licensed clinical professional counselors who provide individual therapy, trained bachelors and masters level counselors who provide individual and group counseling, trained legal advocates who accompany and advise survivors of domestic violence and sexual assault

through civil and criminal proceedings, and trained medical advocates who accompany and support survivors of sexual assault through any necessary medical treatment. Mujeres also trains volunteers to staff a 24-hour crisis hotline for individuals in domestic violence situations. As a Domestic Violence Prevention and Intervention community-based provider in Illinois, Mujeres complies with the confidentiality clause of the Illinois Domestic Violence Act of 1986 (750 ILCS 60/227) and informs each victim of the victim's right to confidential communications with the organization. As a Rape Crisis Center in Illinois, Mujeres complies with the confidentiality statute of Confidentiality of Statements Made to Rape Crisis Personnel (735 ILCS 5/8-802.1), which provides significant protection to communications between a victim and a rape crisis worker. Mujeres owes duties of care and confidentiality to the participants and recipients of these services, and is committed to advancing those individuals' best interests, including helping them preserve their privacy, security, and overall well-being.

iii) Mujeres's program participants are hampered from bringing suit. Many of Mujeres's program participants are monolingual Spanish speakers, who face obstacles in understanding their legal rights and navigating the English-language legal system. Many of Mujeres's program participants are undocumented immigrants, who are hampered from vindicating their rights by the threat that federal authorities may exploit their participation in litigation to arrest and deport them and their families. Mujeres's program participants who are survivors of domestic violence and sexual assault are hampered from

bringing suit by the threat that they may be publicly identified as survivors of domestic violence and sexual assault, or that the individuals who have caused them harm in the past may exploit their participation in a lawsuit to further harass or harm them.

IV. Clearview Violates Individuals' Privacy Rights On An Unprecedented Scale.

39. Clearview has set out to do what many companies have intentionally avoided out of ethical concerns: create a mass database of billions of faceprints of people, including millions of Illinoisans, entirely unbeknownst to those people, and offer paid access to that database to private and governmental actors worldwide.

40. Other private companies have refused to create this type of technology because it represents a "radical erosion of privacy." Even technology giants like Google, which have the capability to create a database like this, have declined to do so out of ethical concerns, i.e., that it could be used "in a very bad way."[9] And recently, Apple blocked Clearview's app from its App Store and suspended it from its developer program.[10]

41. Indeed, Clearview's business model appears to embody the nightmare scenario the FTC and 2012 Senate Subcommittee envisioned: a private company capturing untold quantities of biometric data for purposes of surveillance and tracking without notice to the individuals affected, much less their consent.

42. Reports suggest that neither the United States Government nor any American company has ever compiled such a massive trove of biometrics.

---

[9] Hill, *supra* note 1.

[10] Rishi Iyengar, *Apple Suspends Controversial Facial Recognition App Clearview AI From Its Developer Program*, CNN (Feb. 28, 2020), https://www.cnn.com/2020/02/28/tech/clearview-ai-apple-account-disabled/index.html.

43. In an age where companies spend huge amounts of money on dedicated information security personnel and infrastructure in order to secure sensitive information, it is likely that Clearview lacks even remotely sufficient security controls. Based on media reports, the entire Clearview operation has been bare bones.[11] Indeed, recently, over the course of only two months, Clearview's secret internal client list was leaked to an online news organization,[12] and separately, "a misconfigured server exposed the company's internal files, apps and source code for anyone on the internet to find."[13]

44. Clearview's namesake software functions by comparing faceprints generated from individuals' images to a database of more than three billion faceprints for purposes of ascertaining their identities. Clearview captured the faceprints from photographs available online—including on news sources and social media sites like Facebook, YouTube, and Twitter—without the pictured individuals' knowledge, much less their consent. Clearview then stored those faceprints in its database, which it continues to maintain without those individuals' knowledge or consent.

45. Plaintiffs' members, clients, and program participants, like millions of other Illinois residents, have uploaded numerous photos of themselves to social media sites and other websites. For example:

i) Kenneth L. Page is a resident of Illinois and a member of the ACLU and the ACLU of Illinois. Mr. Page is active in his church, the alumni chapter of his college fraternity, the Prince Hall Freemasons, and the Springfield chapter of

---

11 Hill, *supra* note 1.

12 Mac, *supra* note 2.

13 Zach Whittaker, *Security Lapse Exposed Clearview Source Code*, TechCrunch (Apr. 16, 2020), https://techcrunch.com/2020/04/16/clearview-source-code-lapse/.

the ACLU of Illinois, and photographs of him are or have been publicly available on the internet in all of those capacities. He served four years as the president of the Springfield Branch of the NAACP and 20 years as the Environmental Justice Officer for the Illinois Environmental Protection Agency, and was frequently pictured online in those roles as well. Mr. Page is active on Facebook, where he has a private account (but a publicly accessible profile page on which his photo sometimes appears), though he does not know how many of his over 3,000 friends have public accounts. Mr. Page has never received notice from Clearview that it has created faceprints from his online photographs, and has never given Clearview consent to do so.

ii) Marcia Liss is a resident of Illinois and a member of the ACLU and the ACLU of Illinois. She has posted multiple photographs of herself on her Facebook page, which is public, and she has 441 Facebook friends. In her role as an active member of ACLU of Illinois and her former role as its development director for 20 years, her photos have appeared online with board members and fundraisers. Ms. Liss has never received notice from Clearview that it has created faceprints from her online photographs, and has never given Clearview consent to do so.

iii) Sara Paretsky is a resident of Illinois and a member of the ACLU and the ACLU of Illinois. She is the author of more than 20 books, and her photograph frequently appears on the internet in connection with book tours and other public events. Her two public Facebook pages, which have thousands of followers, also include multiple photographs of her. Ms.

Paretsky has never received notice from the Defendant that it has created faceprints from her online photographs, and has never given Defendant consent to do so.

iv) Kathryn Rosenfeld is a resident of Illinois and a member of SWOP-Chicago and of the organization's leadership board. She has uploaded photos of herself to numerous websites, including Facebook, Instagram, and elsewhere, and is aware of additional photos of her posted online by relatives and acquaintances. Ms. Rosenfeld has never received notice from Clearview that it has created faceprints from her online photos, and has never given Clearview consent to do so.

v) Numerous of ACLU's, ACLU-IL's, Illinois PIRG's, CAASE's, SWOP-Chicago's, and Mujeres's members, clients, and program participants have posted photos online on numerous social media sites and other websites. Being subjected to surreptitious, nonconsensual faceprinting exposes them to the threat of identity theft; to the dangers of being found by the individuals who have caused them harm in the past, both online and in the physical world, notwithstanding any efforts they have made to alter their official identities; and to the threat of having their private histories exposed if they are surveilled and identified when at the CAASE, SWOP-Chicago, Mujeres, or other organizations' offices or service locations or in unidentified images on their websites. Moreover, such surreptitious, nonconsensual faceprinting robs them of control over their own bodies, stories, and physical freedom.

46. Upon information and belief, Clearview has captured the faceprints of Plaintiffs'

members, clients, and program participants from their photos found online. The extraordinary breadth and volume of online photos used by Clearview to capture faceprints for its database means that it is a near certainty that anyone whose photos are posted to publicly accessible portions of the internet will have been subjected to surreptitious and nonconsensual faceprinting by Clearview. For example, when a reporter recently used California's newly-enacted Consumer Privacy Act to obtain a copy of the information Clearview had collected and generated about her, Clearview's faceprint database returned links to images of her posted online as far back as 2004; images posted on web pages that are no longer functional (*e.g.*, a photo from the all-but-defunct social media platform MySpace); and images scraped from social media and posted to various unsavory websites, such as Insta Stalker (which scrapes Instagram photos *en masse*) and conspiracy theory websites.[14] Another California resident has similarly described the results of his information request to Clearview as revealing that the a query of the company's database returned photos posted on Facebook, in his "alma mater's alumni magazine from 2012, and a follow-up article published a year later," and "a profile page from a Python coders' meetup group I had forgotten I belonged to, as well as a wide variety of posts from a personal blog my wife and I had started just after getting married."[15]

47. There is also a substantial likelihood that Plaintiffs' members, clients, and program participants will be subject to faceprinting by Clearview in the future. The sheer volume of photos ingested by Clearview's system on an ongoing basis creates a substantial likelihood

---

[14] Anna Merlan, *Here's the File Clearview AI Has Been Keeping on Me, and Probably on You Too*, VICE (Feb. 28, 2020), https://www.vice.com/en_us/article/5dmkyq/heres-the-file-clearview-ai-has-been-keeping-on-me-and-probably-on-you-too.

[15] Thomas Smith, *I Got My File From Clearview AI, and It Freaked Me Out*, OneZero (March 24, 2020), https://onezero.medium.com/i-got-my-file-from-clearview-ai-and-it-freaked-me-out-33ca28b5d6d4.

that any photos newly uploaded to publicly available social media websites and other webpages will be obtained by Clearview and used to capture faceprints.

48. Although Clearview recently announced several "voluntary" measures it asserts are intended to avoid capturing faceprints of Illinois residents, those measures are unlikely to meaningfully reduce the volume of faceprints of Illinois residents that Clearview captures or retains. For example, Clearview has stated that it intends to avoid capturing faceprints from any image file that contains metadata that includes geolocation information indicating it was taken at longitude and latitude coordinates within Illinois. However, most social media websites and many other websites routinely strip geolocation information out of image files before posting the photos publicly, as a means to preserve their users' privacy and avoid inadvertent disclosure of people's home addresses and other sensitive locations. Moreover, many smartphone users enable the location privacy settings in their phones' operating systems, which prevents geolocation information from being included in photos' metadata in the first place, and many digital cameras lack GPS capabilities, and therefore cannot include geolocation information in photos' metadata at all. Therefore, a significant proportion of photos of Illinois residents that appear online will not contain geolocation information and so will not be excluded from Clearview's system.

49. Clearview has also stated that it intends to exclude photos from its system if it can tell that those photos were uploaded from internet protocol ("IP") addresses in Illinois. However, few photos on publicly available websites include metadata showing the IP address from which they were uploaded. And, even for those rare photos with such metadata, IP address geolocation databases are notoriously unreliable for determining a user's location, and often cannot accurately provide location information beyond a multi-state region, or even a nation.

50. Clearview has additionally stated that it intends to avoid photos posted on

webpages with "URLs or page titles that contain the terms 'Chicago' and 'Illinois.'" This does nothing to protect Illinois residents pictured in photos on the vast majority of webpages, which do not contain the terms "Chicago" and "Illinois" in their URLs or page titles, from nonconsensual faceprinting or to keep them out of Clearview's database.

51. Clearview captured, and will continue to capture, faceprints of Plaintiffs' members without their knowledge or consent. Further, Clearview stored, and continues to maintain, Plaintiffs' members' faceprints in its massive database, again without their knowledge or consent.

52. Clearview's inventor Ton-That describes the company's algorithm as a "state-of-the-art neural net" that organizes photos with similar vectors into "neighborhoods."[16] A neural network is a type of artificial intelligence that mimics the way a human brain functions by using a series of algorithms that recognize underlying relationships in a dataset through deep learning. Simply put, Clearview uses artificial intelligence in order to group together similar photos of the same individual by capturing and comparing faceprints.

53. Clearview's database contains not only individuals' faceprints, but also links to the webpages from which Clearview obtained the photographs used to capture those faceprints. Those webpages often contain additional information about the individual, furthering the privacy and security harms.

54. A memo produced for Clearview by the Kirkland & Ellis law firm titled "Legal Implications of Clearview Technology" describes what happens after a photo is uploaded by a Clearview user to the system via a computer or cell phone:[17]

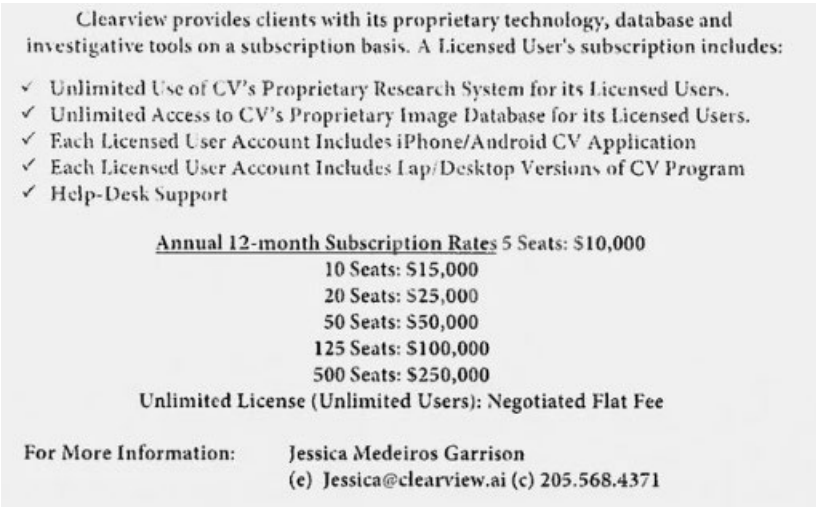
"When a Clearview user uploads an image, Clearview's proprietary

[16] Hill, *supra* note 1.

[17] Hill, *supra* note 1.

> technology processes the image and returns links to publicly available images that match the person pictured in the uploaded image. Clearview does not itself create any images, and it does not collect images from any private, secure, or proprietary sources. Clearview links only to images collected from public-facing sources on the Internet, including images from public social media, news media, public employment and educational websites, and other public sources. Frequently, the linked websites containing the matched image include additional publicly available information about the person identified in the matched images. Clicking on a matched image will send the user to the linked external website, outside the Clearview application."

55. Clearview describes its offering as the "World's best facial recognition technology combined with the world's largest database of headshots" and offers its clients access to its proprietary technology, database, and investigative tools via a subscription. It also provides individuals and entities with 30-day free trials. *See also* Figures 1 and 2, showing Clearview's internal marketing materials describing its service.



Clearview provides clients with its proprietary technology, database and investigative tools on a subscription basis. A Licensed User's subscription includes:

- ✓ Unlimited Use of CV's Proprietary Research System for its Licensed Users.
- ✓ Unlimited Access to CV's Proprietary Image Database for its Licensed Users.
- ✓ Each Licensed User Account Includes iPhone/Android CV Application
- ✓ Each Licensed User Account Includes Lap/Desktop Versions of CV Program
- ✓ Help-Desk Support

Annual 12-month Subscription Rates 5 Seats: $10,000
10 Seats: $15,000
20 Seats: $25,000
50 Seats: $50,000
125 Seats: $100,000
500 Seats: $250,000
Unlimited License (Unlimited Users): Negotiated Flat Fee

For More Information: Jessica Medeiros Garrison
(e) Jessica@clearview.ai (c) 205.568.4371

(**Fig. 1.**)

(**Fig. 2.**)

56. At no point does Clearview—on its own, through its clients, customers, or through any other party—even attempt to inform individuals that their images and sensitive biometric data are being collected. It does not obtain (or even try to obtain) those individuals' consent.

57. Clearview similarly fails to provide individuals with a written, publicly available policy identifying its retention schedule, and guidelines for permanently destroying the faceprints in its database, as required by the BIPA. An individual with a faceprint in Clearview's database has no knowledge of when their biometric data will be removed from the database—or if it ever will be. Public information indicates that the company will keep faceprints captured from photos it has scraped from the internet even if the photos are later deleted, or if the settings on a social media account are changed to bar public access.

58. Clearview claims that its technology is immensely powerful, such that Clearview can produce accurate biometric identifiers even from imperfect images. According to the company, no matter whether a person's face is obscured (by hats, glasses, a hand) or shows only

a partial image (like in a profile photo), Clearview can still capture faceprints that produce matches. A forensic review of Clearview's mobile application also revealed that it contains code that can pair its face recognition technology with other technology—like augmented-reality glasses—which could potentially identify every person the wearer sees walking through a neighborhood. As the *Times* describes it, Clearview could "herald the end of public anonymity."[18]

59. Sadly, but perhaps unsurprisingly, revelations about the extent of Clearview's conduct have resulted only in obfuscation by the company. Initially, in response to public reporting about Clearview's face recognition technology, the company's CEO publicly claimed that it "strictly" and solely worked with law enforcement entities in "USA and Canada." While it certainly has done this—including by offering a free trial to, and later signing a contract with, police departments in Illinois—Clearview has neither limited its clientele to public entities, nor to entities in these countries. According to a February 2020 report by *BuzzFeed News*, Clearview has "aggressively pursu[ed] clients in industries such as law, retail, banking, and gaming, and push[ed] into international markets in Europe, South America, Asia Pacific, and the Middle East."[19]

60. Clearview's leaked client list revealed a list of people "associated with 2,228 law enforcement agencies, companies, and institutions [that] have created accounts and collectively performed nearly 500,000 searches – all of them tracked and logged by the company." Companies—or their employees—that have used Clearview include major retail chains (including Best Buy, Macy's, Kohl's, Walmart, Home Depot, Albertsons, and Rite Aid), event

---

18 Hill, *supra* note 1.

19 Mac, *supra* note 2.

venues and casinos (including Madison Square Garden, Las Vegas Sands, and the Pachanga Resort Casino), communications and financial services companies (including AT&T, Verizon, T-Mobile, Coinbase, Wells Fargo, and Bank of America), private universities (including Columbia University and Southern Methodist University), private security firms (including Gavin de Becker and Associates and SilverSEAL), the National Basketball Association, and the gym and fitness company Equinox. Numerous police departments and other government agencies throughout the country have also used Clearview, including federal law enforcement agencies within the Department of Homeland Security (including U.S. Immigration and Customs Enforcement, U.S. Customs and Border Protection, and U.S. Secret Service) and the Department of Justice (including the Federal Bureau of Investigation, U.S. Marshals Service, and Drug Enforcement Administration).

61. For law enforcement agencies, one of Clearview's main marketing strategies has involved offering trials to individual officers—often without knowledge or approval of the agency itself—in the hope that the officers will later convince their agency to pay for a subscription. Clearview has also offered access to its service to private individuals, such as New York billionaire John Catsimatidis, venture capitalist David Scalzo, and, upon information and belief, actor turned venture capitalist Ashton Kutcher.[20]

62. Clearview has specifically marketed its service in Illinois. According to reports, more than 105 entities in Illinois have used Clearview.[21] The Chicago Cubs had run at least 15

---

[20] *See* Kashmir Hill, *Before Clearview Became a Police Tool, It Was a Secret Plaything of the Rich*, N.Y. Times (Mar. 5, 2020), https://www.nytimes.com/2020/03/05/technology/clearview-investors.html.

[21] Ryan Mac, Caroline Haskins, & Logan McDonald, *Clearview AI Has Promised To Cancel All Relationships With Private Companies*, BuzzFeed News (May 7, 2020), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-no-facial-recognition-private-companies.

searches using Clearview's system as of April 2019. As of late February, 2020, the Macon County Sheriff's Office and the Naperville Police Department had used Clearview nearly 2,000 and 1,700 times, respectively. The Springfield Police Department has also used Clearview.

63. Clearview has recently asserted that it is canceling the accounts of all non-government users, as well as all accounts belonging to any entity in Illinois. This "voluntary" measure, for which Clearview has offered no proof and which Clearview could unilaterally reverse at any time, does not redress the violation of Plaintiffs' members', clients', and program participants' rights, as it does not address or end the nonconsensual capture of those individuals' faceprints from photos of them located online. Further, Clearview's past conduct casts doubt on the reliability of the company's claims. As noted above, Mr. Ton-That's prior statements that Clearview is "strictly for law enforcement"[22] have been belied by revelations soon thereafter—not by any voluntary transparency by Clearview, but due to a data breach that revealed the company's customer list.[23] In addition, ending all accounts belonging to an "entity" in Illinois says nothing of accounts held by individuals in Illinois.

64. The Pay By Touch bankruptcy that catalyzed the passage of the BIPA highlights why conduct such as Clearview's is so dangerous. That bankruptcy spurred Illinois citizens and legislators to realize a critical truth: when it comes to biometric data, it is crucial for people to retain controls, and to understand and consent to who exactly is collecting it, who it will be transmitted to, for what purposes, and for how long.

65. Clearview disregards these obligations, and instead unlawfully captures, stores, profits from and otherwise uses individuals' biometric identifiers without providing prior written

---

22 *New facial recognition tech 'loved' by law enforcement: Clearview AI CEO*, Fox Business (Feb. 19, 2020), https://video.foxbusiness.com/v/6133890195001/#sp=show-clips.

23 Mac, *supra* note 2.

notice and obtaining consent.

FIRST CAUSE OF ACTION
Violation of 740 ILCS 14/1, *et seq.*
(On Behalf of Plaintiffs)

66. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

67. The BIPA makes it unlawful for any private entity to, among other things, "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers . . ., unless it first: (1) informs the subject . . . in writing that a biometric identifier . . . is being collected or stored; (2) informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier . . . is being collected, stored, and used; *and* (3) receives a written release executed by the subject of the biometric identifier . . . ." 740 ILCS 14/15(b) (emphasis added).

68. Clearview AI is a Delaware corporation and thus qualifies as a "private entity" under the BIPA. *See* 740 ILCS 14/10.

69. Plaintiffs' members, clients, and program participants include thousands of individuals who had their "biometric identifiers" captured by Clearview's face recognition software (in the form of their facial geometries extracted from uploaded digital photographs), as explained in detail above. *See* 740 ILCS 14/10.

70. Clearview systematically and automatically captured, used, and stored their biometric identifiers without first obtaining the written release required by 740 ILCS 14/15(b)(3).

71. In fact, as explained above, Clearview didn't properly inform Illinoisans in writing that their biometric identifiers were being captured and stored, nor did it inform them in writing of the specific purpose and length of term for which their biometric identifiers were

being captured, stored, and used as required by 740 ILCS 14/15(b)(1)–(2).

72. In addition, Clearview does not publicly provide a retention schedule or guidelines for permanently destroying individuals' biometric identifiers as required by the BIPA. *See* 740 ILCS 14/15(a).

73. By capturing, storing, and using Illinoisans' biometric identifiers as described herein, Clearview violated Illinoisans' rights to privacy in their biometric identifiers as set forth in the BIPA, 740 ILCS 14/1, *et seq*.

74. As a result, Plaintiffs seek: (1) injunctive and equitable relief as is necessary to protect the interests of Illinois residents by requiring Clearview to comply with the BIPA's requirements for the collection, storage, and use of biometric identifiers; and (2) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs ACLU, ACLU-IL, CAASE, SWOP-Chicago, Illinois PIRG, and Mujeres, respectfully request that the Court enter an Order:

A. Declaring that Clearview's actions, as set out above, violate the BIPA;

B. Awarding injunctive and other equitable relief as is necessary to protect the interests of Illinois residents, including ordering Clearview to (i) destroy all biometric identifiers within its possession, except where otherwise provided by law, that were collected and stored in violation of the BIPA, (ii) inform in writing and obtain written consent from all persons before capturing their biometric identifiers, (iii) inform those persons in writing that their faceprint or other biometric data is being collected or stored and of the specific purpose and length of term for which biometric data is being collected, stored, or used, and (iv) establish a written policy, made available to the public, creating a retention schedule and guidelines for permanently

destroying any biometrics or any information based on biometrics as required by the BIPA;

C. Awarding Plaintiffs their reasonable litigation expenses and attorneys' fees; and

D. Awarding such other and further relief as equity and justice may require.

Respectfully submitted,

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,

Dated: May 28, 2020

By: /s/ Benjamin H. Richman
One of Plaintiffs' Attorneys

Jay Edelson
jedelson@edelson.com
Benjamin H. Richman
brichman@edelson.com
David I. Mindell
dmindell@edelson.com
J. Eli Wade-Scott
ewadescott@edelson.com
EDELSON PC
350 North LaSalle Street, 14th Floor
Chicago, Illinois 60654
Tel: 312.589.6370
Fax: 312.589.6378
Firm ID: 62075

Rebecca K. Glenberg
rglenberg@aclu-il.org
Karen Sheley
ksheley@aclu-il.org
Juan Caballero
jcaballero@aclu-il.org
ROGER BALDWIN FOUNDATION OF ACLU, INC.
180 North Michigan Avenue, Suite 2300
Chicago, Illinois 60601
Tel: 312.201.9740

Nathan Freed Wessler*
nwessler@aclu.org
Vera Eidelman*
veidelman@aclu.org
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Floor
New York, New York 10004
Tel: 212.549.2500
Fax: 212.549.2654

**Application for admission pro hac vice forthcoming*