YES / (NO)

EXHIBITS

CASE NO. 2020 CH 1810

DATE: 2/13/20

CASE TYPE: CLASS ACTION

PAGE COUNT: 20

CASE NOTE

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

JORDAN STEIN, individually and on behalf of others similarly situated,	)	
Plaintiffs,	)	Case No. 2020CH01810
v.	)	**JURY TRIAL DEMANDED**
CLARIFAI, INC.,	)	
Defendant.	)	

CLASS ACTION COMPLAINT

Plaintiff, Jordan Stein, individually and on behalf of all others similarly situated, brings this class action complaint pursuant to 735 ILCS 5/2-801, *et seq.*, against Defendant Clarifai, Inc. ("Clarifai" or "Defendant") for its violations of the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.* ("BIPA") and alleges as follows:

NATURE OF THE ACTION

1. Plaintiff brings this action for damages and other legal and equitable remedies resulting from the illegal actions of Clarifai in surreptitiously collecting, capturing, storing, using, and profiting from Plaintiff's and other similarly-situated individuals' biometric identifiers without informed written consent, in direct violation of BIPA.

2. A "biometric identifier" is any personal feature that is unique to an individual, including, but not limited to fingerprints, iris scans, and scans of face or hand geometry. 740 ILCS 14/10.

3. The Illinois Legislature has found that "[b]iometrics are unlike other unique identifiers," such as social security numbers which can be changed if compromised. 740 ILCS

14/5(c). "Biometrics . . . are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions." *Id.*

4. Recognizing the need to protect citizens from these risks, Illinois enacted BIPA, which generally prohibits private entities like Clarifai from obtaining and/or possessing an individual's biometrics unless it first: (1) informs that person in writing that biometric identifiers or information will be collected or stored; (2) provides that person with written notice of the specific purpose and length of term for which such biometric identifiers and/or information is being collected, stored, and used; (3) receives a written release from the person authorizing the collection of his or her biometric identifiers and/or information; and (4) publishes a publicly-available retention schedule and guidelines for permanently destroying biometric identifiers and/or information. *See* 740 ILCS 14/15(a)-(b).

5. In direct violation of these requirements, Clarifai harvested biometric identifiers from tens (if not hundreds) of thousands of unwitting Illinois residents. With the assistance of its Chicago-based investors, Clarifai secretly accessed profile photographs OKCupid users had uploaded to OKCupid, one of the world's largest dating websites. After obtaining these images, Clarifai scanned the facial geometry of each individual depicted therein to create unique "face templates," which it used to develop and train its facial recognition technology.

6. BIPA also makes it unlawful for private entities such as Clarifai to profit from a person's biometric identifiers. *See* 740 ILCS 14/15(c). Nevertheless, Clarifai has continuously and systematically marketed and sold the facial recognition technology derived from the illegally-obtained biometric identifiers described above.

7. Accordingly, Plaintiff, on behalf of herself and all other similarly-situated

individuals, brings this action to prevent Clarifai from further violating the privacy rights of those Illinois residents affected by its biometric-harvesting scheme, and to recover statutory damages for Clarifai's unlawful collection, storage, use, and commercial exploitation of those individuals' biometric identifiers.

PARTIES

8. Plaintiff Jordan Stein is, and has been at all relevant times, a resident and citizen of Illinois.

9. Defendant Clarifai is a private, for-profit corporation organized under Delaware law, and headquartered in New York, New York.

10. Founded in 2013, Clarifai is an artificial intelligence company that offers a variety of autonomous image recognition services including, but not limited to, facial recognition technology. Clarifai markets this technology throughout the United States, including in Illinois.

JURISDICTION AND VENUE

11. This Court has jurisdiction over Clarifai pursuant to 735 ILCS 5/2-209 based on the commission of a tortious act in Illinois. As discussed herein, Clarifai illegally obtained images of Plaintiff and the Class members who reside in Illinois. Moreover, Clarifai's conduct arose from its commercial contacts with Illinois, as Clarifai requested and received access to Plaintiff's and the Class members' photographs from one of Clarifai's Illinois-based investors.

12. Venue is proper under 735 ILCS 5/1-108 and 735 ILCS 5/2-101 as a substantial portion of the transactions giving rise to the claims alleged herein occurred in Cook County. Specifically, the activities giving rise to the claims occurred within the City of Chicago, Illinois, where Plaintiff resides and engaged in transactions relevant to her claim. Further, the sole Defendant does not reside in Illinois, and thus, pursuant to 735 ILCS 5/2-101, this action may be

brought in any Illinois county.

FACTUAL BACKGROUND

Illinois' Biometric Information Privacy Act

13. Biometrics are unlike other identifiers because they are a permanent, biologically unique identifier associated with the individual. Thus, once compromised, the individual has no recourse and is at heightened risk for identity theft. *See* 740 ILCS 14/5(c).

14. In the 2000's, major national corporations started using Chicago and other locations in Illinois to test new applications of biometric-facilitated transactions. *See* 740 ILCS 14/5(b).

15. In late 2007, a biometrics company called Pay by Touch—which provided major retailers throughout the State of Illinois with biometric scanners to facilitate consumer transactions—filed for bankruptcy. That bankruptcy was alarming to the Illinois legislature because suddenly there was a serious risk that citizens' biometric records—which 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. The bankruptcy also highlighted that many persons who used the biometric scanners were unaware that the scanners were transmitting their data to the now-bankrupt company, and that their biometric identifiers could then be sold to unknown third parties.

16. Recognizing the "very serious need [for] protections for the citizens of Illinois when it [came to their] biometric information," Illinois enacted BIPA in 2008. Illinois House Transcript, 2008 Reg. Sess. No. 276, p.249 (May 30, 2008); *see also* 740 ILCS 14/5(g).

17. BIPA makes it unlawful for a company to collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier unless it first:

a) informs the subject in writing that a biometric identifier is being collected or stored;

b) 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

c) receives a written release executed by the subject of the biometric identifier.

740 ILCS 14/15(b).

18. BIPA defines a "written release" as "informed written consent." 740 ILCS 14/10.

19. BIPA also requires companies to develop and comply with a written policy—made available to the public—establishing a retention schedule and guidelines for permanently destroying biometric identifiers when the initial purpose for collecting such identifiers has been satisfied, or within three years of the individual's last interaction with the company, whichever occurs first. 740 ILCS 14/15(a).

20. BIPA further prohibits a private entity in possession of a biometric identifier from selling, leasing, trading, or otherwise profiting from that identifier. 740 ILCS 14/15(c)-(d).

21. One of the most prevalent uses of biometric identifiers is in facial recognition technology, which works by scanning a human face or an image thereof, extracting facial feature data based on specific "biometric identifiers" (*i.e.* details about the face's geometry as determined by facial points and contours), and comparing the resulting "face template" (or "faceprint") against the face templates stored in a face template database. If a database match is found, an individual may be identified.

22. The use of facial recognition technology in the commercial context presents numerous consumer privacy concerns. During a 2012 hearing before the United States Senate Subcommittee on Privacy, Technology, and the Law, U.S. Senator Al Franken stated that "there is nothing inherently right or wrong with [facial recognition technology, but] if we do not stop and carefully consider the way we use [it], it may also be abused in ways that could threaten basic

aspects of our privacy and civil liberties."[1] Senator Franken noted, for example, that facial recognition technology could be "abused to not only identify protesters at political events and rallies, but to target them for selective jailing and prosecution."[2]

The Need to Train Facial Recognition Algorithms

23. Facial recognition technology is based on algorithms that learn how to recognize human faces and the hundreds of ways in which each one is unique.

24. These algorithms create a unique "face template" of a person's facial geometry by scanning, identifying and measuring various facial landmarks, such as the location of the mouth, chin, nose, ears, eyes and eyebrows.

25. To automatically extract face templates from new images, a facial recognition algorithm must be "trained" to identify and measure the relevant facial landmarks.

26. This is typically accomplished by the algorithm evaluating "triplet" sets of photographs—*i.e.* two images of the same person (known as the "anchor" and "positive sample"), and one of a completely different person (known as the "negative sample").

27. The algorithm reviews the measurements collected from each image, and then adjusts itself so that the measurements collected from the anchor sample are closer to those collected from the positive sample, and further apart from those collected from the negative sample.

28. After repeating this process millions of times with images of thousands of different people, the algorithm learns to reliably scan for and collect a face template of the geometry of any given face.

---

[1] *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), *available at* https://www.judiciary.senate.gov/download/statement-of-franken-pdf (last visited Feb. 7, 2020).

[2] *Id.*

Clarifai Secretly Harvests and Uses Biometric Identifiers in Violation of BIPA, and Clarifai's Violations are Intentional or Reckless and Ongoing

29. The process of training facial recognition algorithms requires vast quantities of images from a diverse array of faces.

30. As first revealed in a July 13, 2019 New York Times article, Clarifai built a massive "face database" (the "Database") of OKCupid users' profile photographs obtained from OKCupid, a popular dating website.[3]

31. Clarifai gained access to those profile photographs from one of its investors, a Chicago-based venture capital group launched by OKCupid's founders.

32. According to an OKCupid spokeswoman, Clarifai contacted the company in 2014 to inquire about collaborating on artificial intelligence and facial recognition technology.

33. Clarifai created the Database to develop and train the algorithms used in its facial recognition technology. To that end, Clarifai created thousands of unique face templates by scanning the biometric information in each photograph contained in the Database and extracting the unique geometry of each face detected therein.

34. In direct violation of BIPA, Clarifai did not notify those Illinois residents whose photographs appeared in the Database about the collection of their facial geometry, nor did it obtain a written release from any of those individuals. *See* 740 ILCS 14/15(b)(1), (3).

35. Clarifai also violated its statutory obligation to inform those individuals about the purpose and length of the term for which their biometric identifiers would be collected, stored, and used. *See* 740 ILCS 14/15(2).

36. Clarifai did not notify Plaintiff or the Class members that Clarifai (or anyone else)

[3] Cade Metz, *Facial Recognition Tech Is Growing Stronger, Thanks to Your Face*, New York Times, July 13, 2019, available at https://www.nytimes.com/2019/07/13/technology/databases-faces-facial-recognition-technology.html (last visited Feb. 7, 2020).

had gained access to their OKCupid profile photographs.

37. Given the secretive nature of the scheme, Plaintiff and the Class members had no way of knowing Clarifai had gained access to their OKCupid profile photographs or collected, used and profited from their biometric identifiers until those facts were revealed by a July 13, 2019 New York Times article.

38. In the same article, Clarifai's CEO, Matt Zeiler, revealed that the company signed an agreement with a large social media company to use the social media company's users' images for training facial recognition algorithms. Zeiler did not, however, disclose the name of this social media company.

39. Thus, Clarifai's surreptitious harvesting of biometric identifiers is ongoing.

40. To make matters worse, Zeiler has publicly stated that Clarifai would sell its facial recognition technology to foreign governments.

41. In January 2019, Clarifai employee Liz O'Sullivan posted an open letter to CEO Matt Zeiler (the "Open Letter") on the company message board.

42. Liz O'Sullivan managed Clarifai's face Database, and was originally tapped to serve as an ethics advisor of Clarifai.

43. The Open Letter to Matt Zeiler voiced Ms. Sullivan's and other employees' concerns, and posed several questions about where their work for Clarifai was headed. The Open Letter stated, *inter alia*, the following:

a) "[I]n conversations I've had with you and with other members of the executive team about our position on ethics in facial recognition, there have been mixed messages, and our values seem to be changing every day."

b) "New executives have indicated that there's no project we would fail to consider if the price is right"

c) "Google and Amazon employees' open letters have described some of the more obvious applications of CFR that are terrifying (mass surveillance, social credit

scoring, political oppression/registration), but there is a fourth elephant in the room that few are addressing: autonomous weapons."

d) "[W]ill Clarifai participate in projects that might lead to large scale warfare, mass invasions of privacy, or (perhaps a bit dramatically) genocide? Because that's the fear behind autonomous weapons, after all."

e) "We in the industry know that all technology can be compromised. Hackers hack. Bias is unavoidable. . . . And that's why it's concerning that certain executives on the team have indicated in private conversations that autonomous weapons would be perfectly ok for us to build."

f) "We very nearly went live with a version of CFR that had 10% more errors when predicting on people with dark skin. If this technology had been sold to a government for security purposes, it would certainly have a negative effect on all the dark-skinned people who would be disproportionately mistaken for criminals."

g) "[T]he last questions we have relate our philosophy on data collection. Because the way we treat consumer data is an important part of our ethical framework. It demonstrates how far we are willing to go in the interest of profit, at the expense of privacy and consent. And just this month, we've been asked to download data from cameras whose owners haven't given consent at all (Insecam), and a few other sources that may walk a legal line but are sketchy at best. There are even rumors going around that the photos in the dataset used to build the general model were stolen from a stock photo site."

h) "All of these things combined with the change in plan regarding our board ethics committee lead us to ask the following questions: . . .

- Will Clarifai vet every military contract to ensure that our work does not get used in the creation of autonomous weapons? . . .
- Will Clarifai sign the open letter [written by Stephen Hawking and Elon Musk in 2014], guaranteeing that we never intend to work on autonomous weapons, even if a large enough contract comes along?
- Will Clarifai promise not to sell CFR (or any similar technology that has the potential to be used for oppression) to any totalitarian or otherwise oppressive government for any purpose ever? . . .
- Will Clarifai promise to evaluate every algorithm we build for racial/age/gender/disability bias as part of our process, and not just as an ad hoc afterthought? . . .
- Will Clarifai promise never to use illegally obtained or otherwise ethically dubious data?"

i) "[W]e should not be willing to risk the safety, privacy, or survival of humans globally just so that Clarifai can have an IPO."

44. Approximately one week later, Clarifai CEO Matt Zeiler called a company-wide meeting and announced that Clarifai's facial recognition technology would be used for autonomous weapons. Zeiler explained that, while Clarifai would not be building missiles, its technology was going to be useful for those and will make its way into autonomous weapons through Clarifai's partnerships.

Facts Pertaining to Plaintiff Stein

45. In 2013, Plaintiff created a user profile with OKCupid.

46. At this time, Plaintiff uploaded approximately five (5) digital photographs of herself to OKCupid.

47. Plaintiff created, managed, and uploaded those photographs from computers and/or mobile devices located in Illinois.

48. Plaintiff maintained an OKCupid user profile from 2013 through present day.

49. Plaintiff maintained an OKCupid user profile when Clarifai obtained the profile photographs it used to create the Database. Thus, Plaintiff's profile photographs are contained in the Database.

50. As with the other photographs in the Database, Clarifai has captured biometrics from Plaintiff's profile photographs by identifying, scanning and measuring her facial landmarks, and using that data to create a unique template of Plaintiff's face.

51. Clarifai used Plaintiff's face template (scans of face geometry) in the same manner as the others collected from photographs in the Database—to train and develop the facial recognition technology that it sells to customers throughout the world.

52. At no time did Clarifai inform Plaintiff, in writing or otherwise, about the

collection, receipt, storage, or use of her biometric identifiers.

53. At no time did Clarifai notify Plaintiff, in writing or otherwise, about the purpose and length of time for which her biometric identifier was being collected, stored, and used.

54. At no time did Plaintiff provide Clarifai with an executed written release authorizing the collection, receipt, storage, and/or use of her biometric identifier.

55. Plaintiff has never given informed written consent for Clarifai to collect, capture, receive, store or use her facial geometric data.

56. Plaintiff would not have given informed written consent for Clarifai to use her biometric information for the purpose of training facial recognition software for its own profit.

57. Plaintiff was not informed of any biometric data retention policy of Clarifai, nor has she ever been informed as to whether and when Clarifai will ever permanently delete her facial geometric data.

58. As a result of Clarifai's actions, Plaintiff continues to worry about how the biometric data Clarifai collected from her photographs has been and will continue to be used, what has and will happen her biometric data Clarifai collected, whether Clarifai will ever delete her biometric information, and whether (and with whom) Clarifai shared her biometric information.

CLASS ALLEGATIONS

59. Plaintiff brings this action on behalf of herself class of similarly-situated individuals, defined as follows:

> All Illinois residents who had scans of their face geometry collected, captured, purchased, received through trade, or otherwise obtained by Clarifai within five years of the filing of this lawsuit.

The following people are excluded from the Class: (1) any judge presiding over the action and their families and staff; (2) Defendant and its owners, officers, directors, parents, subsidiaries,

successors, predecessors; and (3) Plaintiff's and Defendant's counsel and their staffs.

60. Certification of Plaintiff's claim for classwide treatment is appropriate because Plaintiff can prove the elements of her claims on a classwide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

61. **Numerosity – 735 ILCS 5/2-801(1)**. The members of the Class are so numerous that individual joinder of all Class members is impracticable. Clarifai unlawfully harvested biometric identifiers from more than 60,000 OKCupid users residing in Illinois. While the exact number of Class member is currently unknown to Plaintiff, this information can be ascertained from Clarifai's books and records, as well as OKCupid's records. Class members can be notified about the pendency of this action through recognized, Court-approved methods of notice dissemination, such as U.S. Mail, electronic mail, internet postings, and/or published notice.

62. **Commonality and Predominance – 735 ILCS 5/2-801(2)**. This action involves common questions of law and fact, which predominate over any questions affecting Class members, including, without limitation;

a) whether Clarifai collected, captured, or otherwise obtained the Class members' biometric identifiers;

b) whether Clarifai informed Class members in writing of the specific purposes for collecting, using, and storing their biometric identifiers;

c) whether Clarifai obtained a written release (as defined in 740 ILCS 14/10) to collect, use, and store the Class members' biometric identifiers;

d) whether Clarifai disclosed or re-disclosed the Class members' biometric identifiers to any third party;

e) whether Clarifai sold, leased, traded, or otherwise profited from the Class members' biometric identifiers;

f) whether Clarifai maintained a publicly-available written policy establishing a retention schedule and guidelines for the destruction of biometric identifier and/or information at the time it collected Plaintiff's

and the Class members' biometric identifiers;

g) whether Clarifai complies with any such written policy;

h) whether Clarifai violated BIPA; and

i) whether Clarifai's BIPA violations were negligent, reckless, or intentional.

63. **Adequacy of Representation – 735 ILCS 5/2-801(3).** Plaintiff will fairly and adequately represent and protect the interests of the Class, and has retained counsel competent and experienced in complex and class action litigation. Plaintiff has no interests antagonistic to those of the Class.

64. **Superiority – 735 ILCS 5/2-801(4).** A class action is appropriate to resolve the claims at issue because: (i) the prosecution of separate actions by the members of the Class would wastefully burden the judicial system with the need to resolve the common factual and legal questions this case presents over and over; (ii) requiring members of the Class to prosecute their own individual lawsuits would work an injustice, as it would prevent Class members who are unaware they have a claim, or lack the time, ability, or wherewithal to bring their own lawsuit and find a lawyer willing to take their case, to obtain relief; (iii) requiring individual Class member lawsuits would create a risk of adjudications with respect to individual members of the Class that would, as a practical matter, be dispositive of the interests of the other members not parties to the adjudications, or substantially impair or impede their ability to protect their interests, or create conflicting and incompatible standards of conduct; and (iv) proceeding on a class basis will not create any significant difficulty in the management of this litigation, as the Class members will be easily identified from the business records of third parties (*e.g.* OkCupid), and the Class members' claims can be proven using common evidence. Thus, there will be no difficulty maintaining this case as a class action.

COUNT I
Violation of 740 ILCS 14/15(b)
(On Behalf of Plaintiff and the Class)

65. Plaintiff incorporates the above allegations as if fully set forth herein.

66. BIPA requires private entities such as Clarifai to obtain informed written consent from individuals before acquiring their biometric data. Specifically, BIPA makes it unlawful for any private entity to "collect, capture, purchase, receive through trade, or otherwise obtain a person's …. biometric identifier or biometric information, unless [the entity] first: (1) informs the subject .... in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject .... 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…." 740 ILCS 14/15(b).

67. Clarifai is a corporation, and thus constitutes a "private entity" under BIPA. *See* 740 ILCS 14/10.

68. Plaintiff and the Class members are individuals whose "biometric identifiers," as defined by the BIPA—specifically, scans of their facial geometry—were collected, captured, purchased, received through trade or otherwise obtained, stored, and used by Clarifai.

69. Clarifai violated BIPA by failing to inform Plaintiff and the Class, in writing, about the collection and storage of their biometric identifiers and/or biometric information before it occurred. *See* 740 ILCS 14/15(b)(1).

70. Clarifai violated BIPA by failing to inform Plaintiff and the Class, in writing before the fact, of the specific purpose and length of term for which their biometric identifiers and/or biometric information were being "collected, stored, and used." *See* 740 ILCS 14/15(b)(2).

71. Clarifai violated BIPA by collecting, capturing, purchasing, receiving through trade, and obtaining Plaintiff's and the Class members' biometric identifiers and/or biometric information without first obtaining a written release. *See* 740 ILCS 14/15(b)(3).

72. In so doing, Clarifai deprived Plaintiff and the Class of their statutory right to maintain the privacy of their biometric identifiers.

73. Clarifai carried out a deliberate scheme to secretly harvest biometric identifiers from millions of individuals, including Plaintiff and the Class members, without their knowledge or consent.

74. Clarifai's conduct intentionally or recklessly violated BIPA with respect to Plaintiff and the Class members.

75. In the alternative, Clarifai's conduct negligently violated BIPA with respect to Plaintiff and the Class members.

76. Accordingly, Plaintiff, on behalf of herself and the Class, seeks to recover: (1) statutory damages of $5,000 for each intentional or reckless violation of BIPA, or in the alternative, $1,000 for each such negligent violation; (2) injunctive and other equitable relief as is necessary to require Clarifai to comply with BIPA's requirements for the collection, storage, and use of biometric identifiers, as described herein; and (3) reasonable attorney's fees and costs of litigation.

COUNT II
Violation of 740 ILCS 14/15(c)
(On Behalf of Plaintiff and the Class)

77. Plaintiff restates and re-alleges all paragraphs of this Complaint as though fully set forth herein.

78. BIPA makes it unlawful for private entities in possession of biometric identifiers or biometric information to "sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information." 740 ILCS 14/15(c).

79. Clarifai is a corporation, and thus constitutes a "private entity" under BIPA. *See* 740 ILCS 14/10.

80. Clarifai is in possession of Plaintiff's and the Class members' biometric identifiers (*i.e.* their facial geometry).

81. Clarifai used Plaintiff's and the Class members' biometric identifiers to train and develop its facial recognition technology, which it sells to customers throughout the world.

82. In so doing, Clarifai violated BIPA by profiting from Plaintiff's and the Class members' biometric identifiers. *See* 740 ILCS 14/15(c).

83. Clarifai carried out a premeditated plan to commercially exploit the biometric identifiers that it illegally harvested from Plaintiff and the Class.

84. Clarifai's conduct intentionally or recklessly violated BIPA with respect to Plaintiff and the Class members.

85. In the alternative, Clarifai's conduct negligently violated BIPA with respect to Plaintiff and the Class members.

86. Accordingly, Plaintiff, on behalf of herself and the Class, seeks to recover: (1) statutory damages of $5,000 for each intentional or reckless violation of BIPA, or in the alternative, $1,000 for each such negligent violation; (2) injunctive and other equitable relief as is necessary to prevent Clarifai from continuing to commercially exploit Plaintiff's and the Class's biometric identifiers; and (3) reasonable attorney's fees and costs of litigation.

COUNT III
Violation of 740 ILCS 14/15(a)
(On Behalf of Plaintiff and the Class)

87. Plaintiff restates and re-alleges all paragraphs of this Complaint as though fully set forth herein.

88. BIPA requires private entities in possession of biometric data to establish and maintain a publicly-available retention schedule and guidelines for permanently destroying biometric identifiers and biometric information. *See* 740 ILCS 14/15(a).

89. Clarifai is a corporation, and thus constitutes a "private entity" under BIPA. *See* 740 ILCS 14/10.

90. Clarifai is in possession of Plaintiff's and the Class members' biometric identifiers (*i.e.* their facial geometry).

91. In violation of BIPA, Clarifai did not maintain the statutorily-mandated retention schedule and destruction guidelines at the time it collected Plaintiff's and the Class member's biometric identifiers. *See* 740 ILCS 14/15(a).

92. Clarifai's conduct intentionally or recklessly violated BIPA with respect to Plaintiff and the Class members.

93. In the alternative, Clarifai's conduct negligently violated BIPA with respect to Plaintiff and the Class members.

94. Accordingly, Plaintiff, on behalf of herself and the Class, seeks to recover: (1) statutory damages of $5,000 for each intentional or reckless violation of BIPA, or in the alternative, $1,000 for each such negligent violation; and (2) reasonable attorney's fees and costs of litigation.

COUNT IV
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

95. Plaintiff restates and re-alleges all paragraphs of this Complaint as though fully set forth herein.

96. Clarifai obtained a monetary benefit from Plaintiff and the Class members, to their detriment, by profiting from the covert collection and use of their biometric identifiers.

97. Plaintiff and the Class members did not authorize Clarifai to collect, capture, receive, otherwise obtain, use, or profit from their biometric identifiers.

98. Clarifai appreciated, accepted, and retained the benefit bestowed upon it under inequitable and unjust circumstances arising from its conduct toward Plaintiff and the Class as described herein.

99. In particular, Clarifai secretly obtained Plaintiff's and the Class members' profile photographs from a third-party website for the sole purpose of harvesting their biometric identifiers, without permission and in violation of Illinois law.

100. Clarifai used and profited from Plaintiff's and the Class member's biometric identifiers without providing any compensation for the commercial benefits it received.

101. Under the principles of equity and good conscience, it would be unjust and unfair for Clarifai to be permitted to retain any of the benefits obtained from its unlawful collection and use of Plaintiff's and the Class members' biometric identifiers.

102. Clarifai should be compelled to disgorge into a common fund or constructive trust all proceeds it unjustly received from the collection and use of Plaintiff's and the Class members' biometric identifiers.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Jordan Stein, on behalf of herself and the Class, respectfully requests that the Court enter an Order:

A. Certifying this case as a class action on behalf of the Class defined above (or on behalf of any other class the Court deems appropriate);

B. Appointing Plaintiff as representative of the Class, and her undersigned attorneys as class counsel;

C. Awarding liquidated of $5,000 for each intentional or reckless violation of BIPA that Clarifai committed, and $1,000 for each negligent violation;

D. Providing such injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and the Class, including an order requiring Clarifai to comply with BIPA's requirements for the collection, storage, and use of biometric identifiers, to cease its unlawful practice of profiting from Plaintiff's and the Class's biometric identifiers, and to permanently destroy Plaintiff's and the Class members' biometric identifiers;

E. Requiring Clarifai to disgorge all profits it received from the collection and use of Plaintiff's and the Class members' biometric identifiers into a common fund or constructive trust;

F. Awarding Plaintiff and the Class their reasonable attorneys' fees and costs; and

G. Granting such other and further relief as equity and justice may require.

JURY DEMAND

Plaintiff, individually and on behalf of all others similarly situated, hereby demands trial by jury on all issues so triable.

Dated: February 13, 2020

Respectfully submitted,

JORDAN STEIN, individually and on behalf of all others similarly situated,

By: /s/ Keith J. Keogh

Keith J. Keogh
Theodore H. Kuyper
Gregg M. Barbakoff
KEOGH LAW, LTD.
55 W. Monroe St., Suite 3390
Chicago, Illinois 60603
(312) 726-1092
(312) 726-1093 (fax)
keith@keoghlaw.com
tkuyper@keoghlaw.com
gbarbakoff@keoghlaw.com

Attorneys for Plaintiff and the Putative Class