E-FILED
Thursday, 01 July, 2021 04:54:49 PM
Clerk, U.S. District Court, ILCD

IN THE UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF ILLINOIS
ROCK ISLAND DIVISION

H.K. and J.C., through their father and legal guardian CLINTON FARWELL, and M.W., through her mother and legal guardian ELIZABETH WHITEHEAD, individually and on behalf of all others similarly situated, Plaintiffs, v. GOOGLE, LLC, Defendant.	Case No.: 1:21-cv-01122-SLD-JEH Chief Judge Sara L. Darrow **JURY TRIAL DEMANDED**

FIRST AMENDED CLASS ACTION COMPLAINT

On behalf of themselves and all others similarly situated, Plaintiffs H.K. and J.C., minor children, by and through their father and legal guardian Clinton Farwell, and Plaintiff M.W., a minor child, by and through her mother and legal guardian Elizabeth Whitehead, bring this Class Action Complaint against Google LLC ("Google") for violation of Illinois' Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/1, *et seq.*, and allege as follows based on personal knowledge as to themselves, on the investigation of their counsel and the advice and consultation of certain third-party agents as to technical matters, and on information and belief as to other matters, and demand trial by jury.

NATURE OF ACTION

1. Plaintiffs bring this action for damages and other legal and equitable remedies resulting from the illegal actions of Google in collecting, storing, using, and failing provide basic information concerning its usage of or its guidelines for retaining and destroying, Plaintiffs' and

other similarly situated children's biometric identifiers[1] and biometric information[2] (referred to collectively as "biometrics") – in direct violation of BIPA.

2. In 2008, the Illinois Legislature recognized the importance of protecting the privacy of individuals' biometric data, finding that "[b]iometrics are unlike other unique identifiers that are used to access finances or other sensitive information." 740 ILCS 14/5(c). "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, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions." *Id.*

3. In recognition of these concerns over the security of individuals' biometrics, the Illinois Legislature enacted BIPA, which provides, *inter alia*, that a private entity like Google may not obtain and/or possess an individual's biometrics unless it: (1) informs that person in writing that biometric identifiers or information will be collected or stored, *see id.*; (2) informs that person in writing of the specific purpose and length of term for which such biometric identifiers or biometric information is being collected, stored, and used, *see id.*; (3) receives a written release from the person for the collection of her biometric identifiers or information, *see id.*; and (4) publishes publicly available written retention schedules and guidelines for permanently destroying biometric identifiers and biometric information, 740 ILCS 14/15(a).

4. Google has systematically violated this important consumer protection statute by collecting, storing, and using the biometric data of millions of school children throughout the

[1] A "biometric identifier" is any personal feature that is unique to an individual, including fingerprints, iris scans, DNA and "face geometry," among others.

[2] "Biometric information" is any information captured, converted, stored, or shared based on a person's biometric identifier used to identify an individual.

country (including in Illinois) without seeking, much less obtaining the requisite informed written consent from any of their parents or other legal guardians.

5. Google has infiltrated the primary and secondary school system in this country by providing access to its "ChromeBook" laptops, which come pre-installed with its "G Suite for Education" platform (formerly referred to as Google Apps for Education), to over half of the nation's school children, including those in Illinois. When these children use Google's "G Suite for Education" platform on the company's ChromeBook laptops at school, Google creates, collects, stores and uses their "face templates" (or "scans of face geometry") and "voiceprints" – highly sensitive and immutable biometric data – as well as various other forms of personally identifying information pertaining to these children, including:

a. their physical locations;
b. the websites they visit;
c. every search term they use in Google's search engine (and the results they click on);
d. the videos they watch on YouTube;
e. personal contact lists;
f. voice recordings;
g. saved passwords; and
h. other behavioral information

6. Each voiceprint and face template that Google extracts from a child and catalogues in its vast biometrics database is unique to that child, in the same way that a fingerprint is unique to one and only one person. Google supplements this biometric data with other personally identifying information pertaining to each child, including the child's e-mail address and name.

7. Thus, in direct violation of BIPA, Google has collected, stored, and used (and continues to collect, store, and use) – without obtaining the requisite signed written release or publishing the mandated data retention policies – the biometrics of millions of school children across the country, including tens of thousands of young children in Illinois.

8. Plaintiffs H.K. and J.C., by and through their father and legal guardian Clinton Farwell, and Plaintiff M.W., by and through her mother and legal guardian Elizabeth Whitehead, individually and on behalf of other similarly situated children, , bring this action to stop Google from further violating the BIPA-protected privacy rights of children in Illinois in connection with their use of the "G Suite for Education" platform, and to recover statutory damages for Google's unauthorized collection, storage, and use of Illinois students' biometric data in violation of BIPA.

PARTIES

9. Plaintiff H.K., and her father and legal guardian, Clinton Farwell are, and at all relevant times have been, citizens of the State of Illinois residing in Bushnell, Illinois, which is within McDonough County. Plaintiff J.C. has used Google's "G Suite for Education" platform at her elementary school in Bushnell, Illinois, which is within Community Unit School District #170. Plaintiff H.K. has never been informed of or asked to provide a written release authorizing Google's extraction, collection, storage, and use of her unique "biometric identifiers" or "biometric information," nor was her father, Clinton Farwell, informed or asked to provide a written release authorizing Google's collection, storage, and use of such data..

10. Plaintiff J.C., and her father and legal guardian, Clinton Farwell are, and at all relevant times have been, citizens of the State of Illinois residing in Bushnell, Illinois, which is within McDonough County. Plaintiff J.C. has used Google's "G Suite for Education" platform

at her middle school in Bushnell, Illinois, which is within Community Unit School District #170. Plaintiff J.C. was 13 years old when she used Google's "G Suite for Education" platform. Plaintiff J.C. has never been informed of or asked to provide a written release authorizing Google's extraction, collection, storage, and use of her unique "biometric identifiers" or "biometric information," nor was her father, Clinton Farwell, informed or asked to provide a written release authorizing Google's collection, storage, and use of such data.

11. Plaintiff M.W., and her mother and natural legal guardian, Elizabeth Whitehead are, and at all relevant times have been, citizens of the State of Illinois residing in Hampshire, Illinois, which is within Kane County. Plaintiff M.W. has used Google's "G Suite for Education" platform at her middle school in Hampshire, Illinois, which is within Community Unit School District #300. Plaintiff M.W. was 13 years old when she used Google's "G Suite for Education" platform. Plaintiff M.W. has never been informed of or asked to provide a written release authorizing Google's extraction, collection, storage, and use of her unique "biometric identifiers" or "biometric information," nor was her mother, Elizabeth Whitehead, informed of or asked to provide a written release authorizing Google's collection, storage, or use of such data.

12. Google, LLC is a Delaware corporation with its headquarters at 1600 Amphitheatre Parkway, Mountain View, California 94043. Google is also registered to do business in Illinois (No. 65161605).

JURISDICTION AND VENUE

13. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A) because this case is a class action where the aggregate claims of all members of the proposed class are in excess of $5,000,000, exclusive of interest and costs, and because the proposed class

is comprised of more than 100 members, at least one of which is a citizen of a state different from the state of Defendant.

14. Personal jurisdiction exists over Defendant in Illinois and venue is proper in this Court because Plaintiffs reside in McDonough County, Illinois, which is within this District; because Plaintiffs had their biometrics collected by Defendant while they were using Google Chromebook laptops that Defendant had supplied and shipped to their school in McDonough County, Illinois, within this District; because Google failed to but should have (as required by BIPA) obtained statutorily compliant written releases authorizing the collection of Plaintiffs' biometrics from Plaintiffs while they were within Illinois and within in this District; and because Plaintiffs' biometrics were used by Defendant while Plaintiffs were physically present in within Illinois and within in this District, such that the Plaintiffs' privacy was violated in Illinois and within this District and Defendant violated BIPA (as alleged herein) in Illinois and in substantial part within this District. Venue is additionally proper in this judicial district pursuant to 28 U.S.C. § 1391 because Defendant conducts business throughout this district.

FACTUAL BACKGROUND

I. Biometric Technology Implicates Consumer Privacy Concerns

15. "Biometrics" refers to unique physical characteristics of an individual. One of the most prevalent uses of biometrics 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 can be identified.

16. 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, a member of the U.S. Senate 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."[3] 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."[4]

17. The Federal Trade Commission ("FTC") has raised similar concerns, and recently released a "Best Practices" guide for companies using facial recognition technology.[5] In the guide, the Commission underscores the importance of companies' obtaining affirmative consent from consumers before extracting and collecting their biometric identifiers and biometric information from digital photographs.

II. The Illinois Biometric Information Privacy Act

18. In 2008, Illinois enacted the BIPA due to the "very serious need [for] protections for the citizens of Illinois when it [comes to their] biometric information." Illinois House Transcript, 2008 Reg. Sess. No. 276. The BIPA makes it unlawful for a company to*, inter alia*,

---

[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), *available at* https://www.eff.org/files/filenode/jenniferlynch_eff-senate-testimony-face_recognition.pdf (last visited Feb. 18, 2020).

[4] *Id*.

[5] *Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies*, Federal Trade Commission (Oct. 2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf (last visited Feb. 18, 2020).

"collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers[6] or biometric information, unless it first:

> (l) 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 or the subject's legally authorized representative."

740 ILCS 14/15 (b).

19. Section 15(a) of the BIPA also provides:

> A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first.

740 ILCS 14/15(a).

20. As alleged below, Google's practices of collecting, storing, and using biometric identifiers and information from school children in Illinois without the requisite informed written consent violate all three prongs of § 15(b) of the BIPA. Google's failure to provide a publicly available written policy regarding its schedule and guidelines for the retention and permanent destruction of these childrens' biometrics also violates § 15(a) of the BIPA.

---

[6] BIPA's definition of "biometric identifier" expressly includes information collected about the geometry of the face (i.e., facial data obtained through facial recognition technology). *See* 740 ILCS 14/10.

III. Google Violates the Illinois BIPA

21. In 2011, Google's then-CEO Eric Schmidt recounted the company's past development of facial recognition technology and revealed that he had put the brakes on the program due to the profound implications he believed the technology would have on individuals' privacy rights. Characterizing facial recognition technology as "crossing the creepy line," Mr. Schmidt said at the time "that [Google] would not build a database capable of recognizing individual faces even though it is increasingly possible." Matt Warman, *Google Warns Against Facial Recognition Database*, THE TELEGRAPH, May 18, 2011, *available at* http://www.telegraph.co.uk/technology/google/8522574/Google-warns-against-facial-recognition-technology.html. Nonetheless, Mr. Schmidt predicted that "some company by the way is going to cross that line." *Id.*

22. In 2013, Mr. Schmidt wrote a piece for The Wall Street Journal, titled "The Dark Side of the Digital Revolution," in which he again cautioned against the collection of Americans' biometric data and advocated in favor of regulating the collection and use of such data in this country, writing in pertinent part:

> Today's facial-recognition systems use a camera to zoom in on an individual's eyes, mouth and nose, and extract a "feature vector," a set of numbers that describes key aspects of the image, such as the precise distance between the eyes. (Remember, in the end, digital images are just numbers.) Those numbers can be fed back into a large database of faces in search of a match. The accuracy of this software is limited today (by, among other things, pictures shot in profile), but the progress in this field is remarkable. A team at Carnegie Mellon demonstrated in a 2011 study that the combination of "off-the-shelf" facial recognition software and publicly available online data (such as social network profiles) can match a large number of faces very quickly. With cloud computing, it takes just seconds to compare millions of faces. The accuracy improves with people who have many pictures of themselves available online—which, in the age of Facebook, is practically everyone.

> By indexing our biometric signatures, some governments will try to track our every move and word, both physically and digitally. That's why we need to fight hard not just for our own privacy and security, but also for those who are not equipped to do so themselves. We can regulate biometric data at home in democratic countries, which helps.

Eric Schmidt, *The Dark Side of the Digital Revolution*, THE WALL STREET JOURNAL, Apr. 19, 2013, *available at* https://www.wsj.com/articles/SB10001424127887324030704578524650479285218.

23. Ironically, the company that Google's CEO predicted in 2011 would one day "cross that line" by diving into the consumer biometrics-collection business turned out to be none other than Google itself.

24. In May 2015, Google announced the release of its web- and mobile app-based photo sharing and storage service called Google Photos. Users of Google Photos immediately began uploading millions of photos per day through the service, and Google in turn began using its "FaceNet"-powered facial recognition technology to extract, collect, store, and catalog the biometric data of everyone whose faces appeared in all of those uploaded photographs, in real time.[7] Google has sold licenses to its Google Photos APIs, including APIs that enable the use of its facial recognition technology, to various mobile application developers, and derives substantial commercial profit from such sales. Thus, less than four years after warning of the immense dangers posed by facial recognition technology, Google began using that very technology to collect the immutable biometric data of hundreds of millions of its users worldwide.

[7] A research paper released by Google engineers at around the same time as the release of Google Photos describes FaceNet as "a unified system for face verification (is this the same person), recognition (who is this person) and clustering (find common people among these faces)." Schroff, Florian, et al., "FaceNet: A Unified Embedding for Face Recognition and Clustering," June 7, 2015, available at https://ieeexplore.ieee.org/document/7298682.

25. Google's pursuit of the world's biometric data didn't end there. Most recently, Google has unleashed its immensely powerful biometrics-collection technology on primary and secondary school children throughout the country, including across the state of Illinois.

26. Specifically, Google provides its "ChromeBook" laptops to grade schools, elementary schools, and high schools nationwide, who in turn make these computing devices available for use by children who attend their schools. The ChromeBooks that Google provides to schools come equipped with Google's "G Suite for Education" platform, a cloud-based service used by young students all across the country, including the state of Illinois.

27. To drive adoption in more schools – and to alleviate legitimate concerns about its history of privacy abuses – Google publicly assured parents, students, and educators alike that the company takes student privacy seriously and that it only collects education-related data from students using its "G Suite for Education" platform. Google also publicly promised never to mine student data for its own commercial purposes. In particular, Google has stated that it recognizes that "trust is earned through protecting teacher and student privacy" and has made a number of public promises designed to convince parents, teachers, school districts, and students that it will protect the privacy of students who use the "G Suite for Education" platform.[8]

28. To reaffirm the various commitments it has made over the years to safeguard and protect student privacy, including to school districts, Google signed the K-12 School Service Provider Pledge to Safeguard Student Privacy (the "Student Privacy Pledge") in or around January 2015. The Student Privacy Pledge is a set of principles and promises developed by the Future of Privacy Forum and The Software & Information Industry Association regarding the

[8] Privacy and Security, Google LLC, http://services.google.com/th/files/misc/gsuite for_ education_ privacy_security.pdf (last visited March 26, 2020).

collection, use, and maintenance of student data.[9] Though not an original signatory, and hesitant to sign on (only succumbing after public outrage), Google eventually signed the Student Privacy Pledge[10] and affirmatively and expressly committed to:

a. Not collect, maintain, use or share student personal information beyond that needed for authorized educational/school purposes, or as authorized by the parent/student;

b. Not use or disclose student information collected through an educational/school service (whether personal information or otherwise) for behavioral targeting of advertisements to students;

c. Not build a personal profile of a student other than for supporting authorized educational/school purposes or as authorized by the parent/student;

d. Not knowingly retain student personal information beyond the time period required to support the authorized educational/school purposes, or as authorized by the parent/student;

e. Collect, use, share, and retain student personal information only for purposes for which Google was authorized by the educational institution/agency, teacher, or the parent/student; and

f. Disclose clearly in contracts or privacy policies, including in a manner easy for parents to understand, what types of student personal information

[9] Student Privacy Pledge Signatories, Future of Privacy Forum and The Software & Information Industry Association, https://studentprivacypledge.org/signatories/ (last visited March 26, 2020).

[10] Google Changes Course, Signs Student Data Privacy Pledge, Wall Street Journal, https://blogs. wsj .com/digits/2015/01 /20/ google-changes-course-signs-student-data-pri vacypledge/ (last visited March 26, 2020).

Google collects, if any, and the purposes for which the information Google maintains is used or shared with third parties.

29. Although Google publicly promoted its decision to sign the Student Privacy Pledge, and received positive coverage in the press for having done so, Google quickly began breaking the commitments it had made in the Pledge.

30. Specifically, since signing the Student Privacy Pledge, Google has implemented features on its "G Suite for Education" platform that instruct children to speak into the recording device on the ChromeBook laptops utilized at their schools (whereupon Google records the acoustic details and characteristics of their voices), and to look into the ChromeBook's camera as well (whereupon Google scans and images the geometry of their faces, including the contours of their faces and the distances between certain localized facial points, such as the distances between the eyes and noses and ears).

31. After Google has obtained the voice of a child using its "G Suite for Education" platform on one of its "ChromeBook" laptops, Google extracts, collects, stores, and catalogs the child's "voiceprint"—a unique, immutable, and highly sensitive biometric identifier—in its vast database of personally identifying biometric data. Likewise, after Google has scanned and imaged the face of a child using its "G Suite for Education" platform on one of its "ChromeBook" laptops, Google extracts, collects, stores, and catalogs the child's "scan of face geometry" (also known as a "face template")—another unique, immutable, and highly sensitive biometric identifier—in its vast database of personally identifying biometric data. Accordingly, Google collects the "biometric identifiers" of children whose voices are recorded and whose faces are scanned while using its "G Suite for Education" platform in schools in Illinois and

across the country, including of Plaintiffs and numerous other children under the age of 18. *See* 740 ILCS 14/10.

32. Google uses the voiceprints and face templates it collects to, *inter alia*, identify and track the children who use its ChromeBook laptops and the "G Suite for Education" platform that comes installed on them. This technology works by comparing the voiceprints and face templates of children whose voices are recorded and faces are scanned while using a ChromeBook with the voiceprints and facial templates already saved in Google's vast biometrics database. Specifically, when a child's face is scanned or voice is recorded using the "G Suite for Education" platform on a ChromeBook laptop, Google's sophisticated voice and facial recognition technology creates a voiceprint for the child's voice or a or a face template for the child's face, and then compares the generated voiceprint or face template against the voiceprints and face templates already stored in its database. If there is a match, then Google is able to confirm the identity of the child using its platform, enhancing the functionality of the various features available on the platform and enabling Google to further improve the quality of the child's voiceprint or face template stored in its database.

33. The unique voiceprints and face templates that Google has collected from children in Illinois and across the country are not only used by Google to identify children by name, they are also used by Google to recognize childrens' gender, age, and location. Accordingly, Google collects the "biometric information" of children whose voices are recorded and whose faces are scanned while using its "G Suite for Education" platform in schools in Illinois and across the country. *See* 740 ILCS 14/10.

34. In direct violation of §§ 15(b)(2) and 15(b)(3) of the BIPA, Google never informed the parents of the children in Illinois (or elsewhere in the country) whose voiceprints

and face templates it has collected of the specific purpose and length of term for which their children's biometric identifiers and information would be collected, stored, and used, nor did Google obtain a written release from the parents of any of these children.

35. In direct violation of § 15(a) of the BIPA, Google does not have written, publicly available policies identifying their retention schedules, or guidelines for permanently destroying the biometric identifiers and biometric information of these children.

36. Thus, BIPA clearly prohibits what Google has done, Google has known so since at least 2015, and yet Google has made no effort to come into compliance with BIPA at any point during that five-year period (be it by obtaining the requisite signed written releases authorizing these practices or by turning the technology off in Illinois' schools altogether).

IV. Plaintiffs' Experiences

37. Google provides "ChromeBook" laptops to grade schools, elementary schools, middle schools, and high schools nationwide, who in turn make these computing devices available for use by children who attend their schools. These Google-manufactured and provided laptops come equipped with Google's "G Suite for Education" platform, which requires the children using it to speak into a microphone on the laptop that records their voices and to look into a camera on the laptop that scans their faces.

38. At all times during the time period relevant to this action, Plaintiffs have resided in Illinois and attended a primary and/or middle school in Illinois, where they were provided access to Google-supplied "ChromeBook" laptops, pre-installed with Google's "G Suite for Education" platform by school officials. Using accounts linked to their names and other personal details that Google had established for them on its ChromeBook laptops and "G Suite for Education" platform, Plaintiffs frequently have logged into their accounts and used the "G

Suite for Education" platform on these ChromeBook laptops while attending school, including features of the platform that required Plaintiffs to speak into the laptop's audio recording device and look into the laptop's camera, at which point Google recorded Plaintiffs' voices and imaged their faces.

39. After Google obtained recordings of Plaintiffs' voices while they used the "G Suite for Education" platform on "ChromeBook" laptops, Google extracted, collected, stored, and cataloged each of their "voiceprints"—a unique, immutable, and highly sensitive biometric identifier—in its vast database of personally identifying biometric data. Likewise, after Google scanned and imaged Plaintiffs' faces while they used the "G Suite for Education" platform on "ChromeBook" laptops, Google extracted, collected, stored, and cataloged their "scans of face geometry" (i.e., "face templates")—another unique, immutable, and highly sensitive biometric identifier—in its vast database of personally identifying biometric data. Accordingly, unbeknownst to Plaintiffs or their father, Clinton Farwell, Google collected Plaintiffs' "biometric identifiers" as they used the company's "G Suite for Education" platform at their school in Illinois. *See* 740 ILCS 14/10.

40. Google uses the voiceprints and face templates that it extracted from Plaintiffs' voices and faces to, *inter alia*, identify them while using its ChromeBook laptops and "G Suite for Education" platform. Specifically, each time either of the Plaintiffs' faces is imaged or voices is recorded while they are using the "G Suite for Education" platform on a ChromeBook laptop at school, Google's sophisticated voice or facial recognition technology creates a voiceprint of the Plaintiff's voice or a face template of the Plaintiff's face, and then compares the newly generated voiceprint or face template against the collection of voiceprints or face templates already stored in its database, whereupon Google is able to match the newly collected

voiceprint or face template with the voiceprints or face templates previously collected from the Plaintiff that are stored in its database and linked to the Plaintiff's identity. If there is a match, Google is able to confirm the identity of the child using its platform, and also uses the information derived from the match to improve the quality and detail of the child's voiceprint or face template saved in its database and thus better train the functionality of the various features available on its platform—enhancing the formidability of its brand in the process.

41. The unique voiceprints and face templates Google extracted from Plaintiffs' voices and faces were not only collected and used by Google to identify Plaintiffs by name, they have also been used by Google to recognize Plaintiffs' gender, age, and location. Accordingly, unbeknownst to Plaintiffs H.K., J.C. or their father, Clinton Farwell, and unbeknownst to Plaintiff M.W. or her mother, Elizabeth Whitehead, Google collected Plaintiffs' "biometric information" as they used the company's "G Suite for Education" platform at their school in Illinois. *See* 740 ILCS 14/10.

42. In direct violation of §§ 15(b)(2) and 15(b)(3) of BIPA, Google never informed the parents of the children in Illinois (or elsewhere in the country) whose voiceprints and face templates it collected of the specific purpose and length of term for which their children's biometric identifiers and information would be collected, stored, and used, nor did Google obtain a written release from the parents of any of these children.

43. In direct violation of § 15(a) of BIPA, Google does not have written, publicly available policies identifying their retention schedules, or guidelines for permanently destroying the biometric identifiers and biometric information of these school children.

44. Neither Clinton Farwell (Plaintiffs H.K and J.C.'s father, legal guardian, and authorized representative), Elizabeth Whitehead (Plaintiff M.W.'s mother, legal guardian, and

authorized representative) nor any other Class member's parent, legal guardian, or authorized representative received a disclosure from Google that it would collect, capture, otherwise obtain, or store unique biometric identifiers or biometric information extracted from their child's face or voice, and neither Clinton Farwell nor any other Class member's parent, legal guardian, or authorized representative ever consented, agreed or gave permission—via a written release or otherwise—to authorize or permit Google to collect, capture, otherwise obtain, or store their child's sensitive biometric data or in this way.

45. Likewise, Google never provided Clinton Farwell (Plaintiffs H.K and J.C.'s father, legal guardian, and authorized representative), Elizabeth Whitehead (Plaintiff M.W.'s mother, legal guardian, and authorized representative), or any other parent, legal guardian, or authorized representative of any member of the Class with an opportunity to prohibit or prevent the collection, storage, or use of their child's unique biometric identifiers, biometric information, or other personally identifying information.

46. Nevertheless, when Plaintiffs and the unnamed members of the Class spoke to or had their faces imaged in connection with their use of Google's "G Suite for Education" platform in Illinois, Google's sophisticated face and voice recognition technologies scanned the recordings of their voices and the geometry of their faces that it had collected, and created unique "voiceprints" and "face templates" corresponding to Plaintiffs and each member of the proposed Class, all in direct violation of BIPA.

CLASS ALLEGATIONS

47. **Class Definition**: Plaintiffs H.K. and J.C., by and through their father and legal guardian, and Plaintiff M.W., by and through her mother and legal guardian, bring this action

pursuant to 735 ILCS 5/2-801 on behalf of a class of similarly situated individuals defined as follows (the "Class"):

> All persons who, while using the "G Suite for Education" platform at a primary, middle, or secondary school in Illinois, had their voiceprint or face template collected by Google after March 26, 2015.

The following are excluded from the Class: (1) any Judge presiding over this action and members of his or her family; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, and any entity in which Defendant or its parent has a controlling interest (including current and former employees, officers, or directors); (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiffs' counsel and Defendant's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

48. **Numerosity**: Pursuant to 735 ILCS 5/2-801(1), the number of persons within the Class is substantial, believed to amount to at least tens of thousands of children for the Class. It is, therefore, impractical to join all members of the Class as named plaintiffs. Further, the size and relatively modest value of the claims of the individual members of the Class renders joinder impractical. Accordingly, utilization of the class action mechanism is the most economically feasible means of determining and adjudicating the merits of this litigation.

49. **Commonality and Predominance**: Pursuant to 735 ILCS 5/2-801(2), there are well-defined common questions of fact and law that exist as to all members of the Class and that predominate over any questions affecting only individual members of the Class. These common legal and factual questions, which do not vary from member to member, and which may be

determined without reference to the individual circumstances of any individual member, include but are not limited to the following:

a. whether Google collected, captured, or otherwise obtained Plaintiffs' and other Illinois school children's "biometric identifiers" or "biometric information" in connection with their use of the "G Suite for Education" platform at primary and secondary schools in Illinois during the preceding five years;

b. whether Google stored Plaintiffs' and the Class's "biometric identifiers" or "biometric information";

c. whether Google informed Plaintiffs and the Class that it would collect, capture, otherwise obtain and then store their "biometric identifiers" or "biometric information";

d. whether Google obtained a written release (as defined in 740 ILCS 14/10) prior to collecting, capturing, or otherwise obtaining, and then storing, Plaintiffs' and the Class's "biometric identifiers" or "biometric information";

e. whether Google developed a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying "biometric identifiers" and "biometric information" when the initial purpose for collecting, capturing, or otherwise obtaining these "biometric identifiers" and "biometric information" has been satisfied or within 3 years of their last interaction with Plaintiffs and members of the Class, whichever occurs first;

f. whether Google complied with any such policy;

g. whether Google used Plaintiffs' and the Class's "biometric information" to identify them;

h. whether Google's violations of the BIPA were committed negligently; and

i. whether Google's violations of the BIPA were committed intentionally or recklessly.

50. **Adequate Representation**: Pursuant to 735 ILCS 5/2-801(3), Plaintiffs have retained and are represented by qualified and competent counsel who are highly experienced in complex consumer class action litigation. Plaintiffs and their counsel are committed to vigorously prosecuting this class action. Neither of the Plaintiffs, nor any of their counsel, have any interest adverse to, or in conflict with, the interests of the absent members of the Class. Plaintiffs are able to fairly and adequately represent and protect the interests of the Class. Plaintiffs have raised viable statutory claims of the type reasonably expected to be raised by members of the Class, and will vigorously pursue those claims. If necessary, Plaintiffs may seek leave of this Court to amend this Complaint to include additional representatives to represent the Class or to add additional claims or classes as may be appropriate.

51. **Superiority**: Pursuant to 735 ILCS 5/2-801(4), a class action is superior to other available methods for the fair and efficient adjudication of this controversy because individual litigation of the claims of all members of the Class is impracticable. Even if every member of the Class could afford to pursue individual litigation, the Court system could not. It would be unduly burdensome to the courts in which individual litigation of numerous cases would proceed. Individualized litigation would also present the potential for varying, inconsistent or contradictory judgments, and would magnify the delay and expense to all parties and to the court

system resulting from multiple trials of the same factual issues. By contrast, the maintenance of this action as a class action, with respect to some or all of the issues presented herein, presents few management difficulties, conserves the resources of the parties and of the court system and protects the rights of each member of the Class. Plaintiffs anticipate no difficulty in the management of this action as a class action. Class-wide relief is essential to compel compliance with BIPA.

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

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

53. 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 or biometric information, unless it 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 or the subject's legally authorized representative." 740 ILCS 14/15(b).

54. Plaintiffs H.K and J.C.'s father and legal guardian, Clinton Farwell, is their "legally authorized representative" within the meaning of BIPA, and served in such capacity at all times relevant to this action. *See* 740 ILCS 14/15(b).

55. Plaintiff M.W.'s mother and legal guardian, Elizabeth Whitehead, is her "legally authorized representative" within the meaning of BIPA, and served in such capacity at all times relevant to this action. *See* 740 ILCS 14/15(b).

56. Google is a corporation and thus qualifies as a "private entity" under the BIPA. *See* 740 ILCS 14/10.

57. Plaintiffs and the Class members are minor children who had their "biometric identifiers," including their voiceprints and scans of face geometry, collected, captured, received, or otherwise obtained by Google in connection with their use of Google's "G Suite for Education" platform at a primary and/or middle school in Illinois after March 26, 2015. *See* 740 ILCS 14/10.

58. Plaintiffs and all members of the Class are minor children who had their "biometric information" collected by Google (in the form of their gender, age, and location) through Google's collection and use of personally identifying information derived from their "biometric identifiers" that Google has used to identify them.

59. Google systematically collected, captured, or otherwise obtained Plaintiffs' and the Class members' "biometric identifiers" and "biometric information" without first obtaining signed written releases, as required by 740 ILCS 14/15(b)(3), from any of them or their "legally authorized representatives," i.e., their parents or legal guardians.

60. In fact, Google failed to properly inform Plaintiffs or members of the Class, or any of the foregoing's parents, legal guardians, or other "legally authorized representatives," in writing that Plaintiffs' or the Class members' "biometric identifiers" and "biometric information" were being "collected or stored" by Google, nor did Google inform Plaintiffs or members of the Class, or any of the foregoing's parents, legal guardians, or other "legally authorized representatives," in writing of the specific purpose and length of term for which Plaintiffs' or the Class members' "biometric identifiers" and "biometric information" were being "collected, stored and used" as required by 740 ILCS 14/15(b)(1)-(2).

61. In addition, Google does not publicly provide a retention schedule or guidelines for permanently destroying the "biometric identifiers" and "biometric information" of Plaintiffs or the Class members, as required by the BIPA, or otherwise indicate that it permanently destroys biometric identifiers and biometric information when the initial purpose for collecting, capturing, or otherwise obtaining such information has been satisfied or within 3 years of its last interaction with Plaintiffs and members of the Class, whichever occurs first. See 740 ILCS 14/15(a).

62. At all times relevant to this action, Google has been aware of BIPA and the requirements it imposes on entities that collect and store biometric data, and could have readily complied with those requirements in Illinois by simply obtaining written releases from, and providing the information and other disclosures required by the statute to, the children who use the Google Education platform in Illinois and their legal guardians. Unfortunately, Google chose not to do any of those things or make any other reasonable efforts to comply with BIPA in Illinois – despite having been sued years earlier for engaging in similar conduct in violation of BIPA. *See, e.g., Rivera et al. v. Google, LLC*, No. 1:16-cv-02714 (N.D. Ill.) (alleging BIPA violations arising from Googles nonconsensual collection of biometric data from users of its Google Photos platform in Illinois).

63. Google has denied BIPA's promise of privacy to those who need it most. By collecting, storing, and using Plaintiffs' and the other Class members' "biometric identifiers" and "biometric information" as described herein, Google recklessly or intentionally violated each of BIPA's requirements, and infringed Plaintiffs' and the other Class members' rights to keep their sensitive, immutable, and uniquely identifying biometric data private.

64. On behalf of themselves and the proposed Class members, Plaintiffs H.K and J.C., by and through their father and natural legal guardian, Clinton Farwell, and Plaintiff M.W., by and through her mother and natural legal guardian, Elizabeth Whitehead, seeks: (1) injunctive and equitable relief as is necessary to protect the interests of Plaintiffs and the other members of the Class by requiring Google to comply with the BIPA's requirements for the collection, capture, and storage of "biometric identifiers" and "biometric information" as described herein, including to permanently destroy the biometric data it has collected from minor children in Illinois to date and to refrain from collecting such data in the future absent the requisite prior informed written authorization of their legally authorized representatives; (2) statutory damages of $1,000.00 to Plaintiff H.K., Plaintiff J.C., Plaintiff M.W., and each Class member pursuant to 740 ILCS 14/20 for each negligent violation of BIPA committed by Google; (3) statutory damages of $5,000.00 to Plaintiff H.K., Plaintiff J.C., Plaintiff M.W., and each Class member pursuant to 740 ILCS 14/20 for each intentional or reckless violation of BIPA committed by Google; and (4) reasonable attorneys' fees and costs and other litigation expenses to Plaintiffs' counsel and proposed Class counsel pursuant to 740 ILCS 14/20(3).

PRAYER FOR RELIEF

WHEREFORE, on behalf of themselves and all others similarly situated, Plaintiffs H.K. and J.C., minor children, by and through their respective father and legal guardian, Clinton Farwell, and Plaintiff M.W., a minor child, by and through her mother and legal guardian, Elizabeth Whitehead, seek judgment against Defendant as follows:

(a) Certifying this case as a class action on behalf of the Class defined above, appointing Plaintiffs H.K. and J.C., by and through their father and legally authorized guardian, Clinton Farwell, and Plaintiff M.W., by and through her

mother and legal authorized guardian, Elizabeth Whitehead, as representatives of the Class, and appointing their counsel as Class Counsel on behalf of the Class;

(b) Declaring that Google's actions, as set out above, violate the BIPA, 740 ILCS 14/1, *et seq.,* with respect to Plaintiffs and members of the Class;

(c) Awarding $1,000.00 statutory damages to Plaintiff H.K., Plaintiff J.C., Plaintiff M.W., and each member of the Class pursuant to 740 ILCS 14/20(1) for each violation of BIPA committed by Google negligently, or $5,000.00 pursuant to 740 ILCS 14/20(2) for each violation of BIPA committed by Google intentionally or recklessly;

(d) Awarding injunctive and other equitable relief pursuant to BIPA as is necessary to protect the interests of Plaintiffs and members of the Class, including, *inter alia*, an order requiring Google to collect, store, and use the biometric identifiers and biometric information of children in Illinois in compliance with BIPA, and to permanently destroy the biometric identifiers and biometric information it has collected from Plaintiffs and Class members to date;

(e) Awarding Plaintiffs' counsel and proposed Class counsel their reasonable litigation expenses and attorneys' fees pursuant to BIPA;

(f) Awarding Plaintiffs and the Class pre- and post-judgment interest, to the extent allowable;

(g) Awarding Plaintiffs and the Class such other and further relief as equity and justice may require.

JURY TRIAL

Plaintiffs demand a trial by jury on all claims and issues so triable.

Dated: July 1, 2021

Respectfully submitted,

/s/ Andrew Stuckart

Andrew Struckart
LUCIE, BOUGHER & ASSOCIATES
Attorneys at Law, P.C.
202 N. Lafayette Street
Macomb, IL 61455
Tel: (309) 833-1702
Fax: (309) 833-1701
andrew@lucielaw.com

Local Counsel for Plaintiffs and the Putative Class

BURSOR & FISHER, P.A.
Scott A. Bursor*
Joseph I. Marchese
Joshua D. Arisohn*
Philip L. Fraietta
888 Seventh Avenue
New York, NY 10019
Tel: (646) 837-7150
Fax: (212) 989-9163
E-Mail: scott@bursor.com
jmarchese@bursor.com
jarisohn@bursor.com
pfraietta@bursor.com

HEDIN HALL LLP
Frank S. Hedin*
David W. Hall*
1395 Brickell Avenue, Suite 1140
Miami, Florida 33131
Tel: (305) 357-2107
Fax: (305) 200-8801
E-mail: fhedin@hedinhall.com
dhall@hedinhall.com

*Petition for Admission Forthcoming

Counsel for Plaintiffs and the Putative Class

ClassAction.org
