BURSOR & FISHER, P.A.
L. Timothy Fisher (State Bar No. 191626)
1990 North California Boulevard, Suite 940
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
Email: ltfisher@bursor.com

HEDIN HALL LLP
David W. Hall (State Bar No. 274921)
Four Embarcadero Center, Suite 1400
San Francisco, CA 94111
Telephone: (415) 766-3534
Facsimile: (415) 402-0058
Email: dhall@hedinhall.com

Counsel for Plaintiff and the Putative Class

[Additional Counsel on Signature Page]

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

H.K. and J.C., through their father and legal guardian CLINTON FARWELL, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

GOOGLE, LLC,

Defendant.

Case No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

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 (collectively, "Plaintiffs"), 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 violation of California's Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code §17200, predicated on violation of the federal Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. § 501, *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 THE ACTION

1. Plaintiffs bring this action for damages and other legal and equitable remedies resulting from the illegal actions of Google in collecting, storing, and using their and other similarly situated childrens' biometric identifiers[1] and biometric information[2] (referred to collectively as "biometrics"), as well as numerous other forms of personally identifying information, without them requisite consent of their legal guardians – in direct violation of both BIPA and COPPA.

2. In 1999, to better protect the privacy of children under the age of 13, the United States Congress enacted COPPA in response to a growing concern over the collection of children's data on the Internet. In passing COPPA, Congress specifically sought to increase parental involvement in children's online activities, ensure children's safety during their participation in online activities, and most importantly, protect children's personal information. Ultimately, Congress enacted COPPA with the specific goal of placing parents in control over what information is collected from their young children online. To that end, COPPA requires, in relevant part, that websites and online services fully and clearly disclose their data collection, use, and disclosure practices, and obtain "verifiable parental consent" before collecting, using, or

[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.

disclosing personal information from children under 13. Further, COPPA requires websites and online services to permit parents to review all personal information they collect and maintain from children under 13, and to allow parents to refuse further use or maintenance of those data. Similarly, websites and online services may not condition a child's use of a site or service on the collection of more personal information than is reasonably necessary, and must take reasonable steps to keep confidential and safe any personal information in their possession.

3. More recently, 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.*

4. 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).

5. Incredibly, Google has managed to violate both of these important consumer protection statutes (COPPA and BIPA) at the same time, by collecting, storing, and using the personally identifying biometric data of millions of school children throughout the country (including thousands in Illinois), most of whom are under the age of 13, without seeking, much less obtaining the requisite informed written consent from any of their parents or other legal guardians.

6. 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, most of whom are under the age of 13. 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

7. 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 uniquely identifies 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.

8. Thus, in direct violation of both BIPA and COPPA, Google has collected, stored, and used (and continues to collect, store, and use) – without providing notice, obtaining informed or verifiable parental consent, or publishing data retention policies – the biometrics and other personally identifying information of millions of school children under the age of 13 across the country, including tens of thousands of young children in Illinois.

9. Plaintiffs, individually and on behalf of other similarly situated children, by and through their father and legal guardian Clinton Farwell, bring this action to stop Google from

further violating the BIPA-protected privacy rights of children in Illinois and the COPPA-protected privacy rights of children under 13 all across the country 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

10. Plaintiffs H.K. and J.C., and their father and natural legal guardian, Clinton Farwell are, and at all relevant times have been, citizens of the State of Illinois residing in Bushnell, Illinois. Plaintiffs H.K. and J.C. were under the age of 13 when they used Google's "G Suite for Education" platform at their elementary school in Bushnell, Illinois, which is within Prairie City Community Unit School District #170, and they are still under the age of 13 today. Neither Plaintiff H.K. nor Plaintiff J.C. was asked for verifiable or written parental consent authorizing Google extraction, collection, storage, and use of their personally and uniquely identifying "biometric identifiers" or "biometric information," nor was Plaintiffs' father, Clinton Farwell, notified of or asked to provide his written authorization to permit Google's collection, storage, or use of such data.

11. 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

12. The Court has original subject-matter jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d) ("CAFA"), because: (i) the proposed BIPA Class consists of at least tens of thousands of members; (ii) at least one member of the proposed BIPA Class, including both of the Plaintiffs as well as their father, is a citizen of a state different from Google; and (iii) the aggregate amount in controversy exceeds $5,000,000.00, exclusive of interests and costs. Google has extracted, collected, stored, and used thousands of minor school childrens' voiceprints and scans of face geometry in connection with their use of Google's "G Suite for Education" platform on the company's "ChromeBook" laptops at primary and secondary schools in Illinois. The estimated number of children who have been impacted by Google's conduct in

Illinois multiplied by the BIPA's statutory liquidated damages figure ($5,000.00 for each intentional or reckless violation and $1,000.00 for each negligent violation) easily exceeds CAFA's $5,000,000.00 threshold. The Court also has supplemental jurisdiction over Plaintiffs' UCL claim for injunctive relief arising from Google's violations of COPPA pursuant to 28 U.S.C. § 1367.

13. Personal jurisdiction and venue are proper in California and within this District because Defendant maintains its corporate headquarters and principal place of business within this District, in Mountain View, California.

FACTUAL BACKGROUND

I. Biometric Technology Implicates Consumer Privacy Concerns

14. "Biometrics" refers to unique physical characteristics used to identify 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.

15. 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]

---

[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.*

16. 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

17. 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*, "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).

18. 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).

---

[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).

[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.

19. 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.

III. The Federal Children's Online Privacy Protection Act

20. In 1999, recognizing the vulnerability of children in the Internet age, Congress enacted the Children's Online Privacy Protection Act (COPPA). *See* 15 U.S.C. §§ 6501–6506. COPPA's express goal is to protect children's privacy while they are connected to the internet. Under COPPA, developers of child-focused applications like Google's "G Suite for Education" service cannot lawfully obtain the personally identifiable information of children under 13 years of age without first obtaining verifiable consent from their parents.

21. COPPA applies to any operator of a commercial website or online service (including an app) that is directed to children and that: (a) collects, uses, and/or discloses personally identifiable information from children, or (b) on whose behalf such information is collected or maintained. Under COPPA, personally identifiable information is "collected or maintained on behalf of an operator when…[t]he operator benefits by allowing another person to collect personally identifiable information directly from users of" an online service. 16 C.F.R. § 312.2. In addition, COPPA applies to any operator of a commercial website or online service that has actual knowledge that it collects, uses, and/or discloses personally identifiable information from children.

22. Under COPPA, "personally identifiable information" includes information like names, email addresses, and social security numbers. COPPA's broad definition of "personally identifiable information" is as follows:

> "individually identifiable information about an individual collected online," which includes (1) a first and last name; (2) a physical address including street name and name of a city or town; (3) online contact information (separately defined as "an email address or any other substantially similar identifier that permits direct contact with a person online"); (4) a screen name or user name; (5) telephone number; (6) social security number; (7) a media file containing a

> child's image or voice; (8) geolocation information sufficient to identify street name and name of a city or town; (9) a "persistent identifier that can be used to recognize a user over time and across different Web sites or online services" (including but not limited to "a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or unique device identifier"); and (10) any information concerning the child or the child's parents that the operator collects then combines with an identifier.

23. The FTC regards "persistent identifiers" as "personally identifiable" information that can be reasonably linked to a particular child. The FTC amended COPPA's definition of "personally identifiable information" to clarify the inclusion of persistent identifiers.[7]

24. In order to lawfully collect, use, or disclose personally identifiable information, COPPA requires that an operator meet specific requirements, including each of the following:

a. Posting a privacy policy on its website or online service providing clear, understandable, and complete notice of its information practices, including what information the website operator collects from children online, how it uses such information, its disclosure practices for such information, and other specific disclosures as set forth in the Rule;

b. Providing clear, understandable, and complete notice of its information practices, including specific disclosures, directly to parents; and

c. Obtaining verifiable parental consent prior to collecting, using, and/or disclosing personally identifiable information from children.

25. Under COPPA, "[o]btaining verifiable consent means making any reasonable effort (taking into consideration available technology) to ensure that before personally identifiable information is collected from a child, a parent of the child. . . [r]eceives notice of the operator's personally identifiable information collection, use, and disclosure practices; and [a]uthorizes any collection, use, and/or disclosure of the personally identifiable information." 16 C.F.R. § 312.2.

[7] *See* https://www.ftc.gov/news-events/blogs/business-blog/2016/04/keeping-onlineadvertising-industry (2016 FTC Blog post from Director of the FTC Bureau of Consumer Protection) (last visited November 22, 2019).

26. The FTC recently clarified acceptable methods for obtaining verifiable parental consent, which include:

a. providing a consent form for parents to sign and return;

b. requiring the use of a credit card/online payment that provides notification of each transaction;

c. connecting to trained personnel via video conference;

d. calling a staffed toll-free number;

e. emailing the parent soliciting a response email plus requesting follow-up information from the parent;

f. asking knowledge-based questions; or

g. verifying a photo ID from the parent compared to a second photo using facial recognition technology.[8]

27. As alleged below, Google's practices of collecting, storing and using biometric identifiers, biometric information, and other personally identifying information from school children under 13, without the requisite verifiable parental consent, are in clear violation of COPPA.

IV. Google Violates Both the Illinois BIPA and the Federal COPPA

28. In 2011, Google's then-CEO Eric Schmidt discussed the company's past development of facial recognition technology, and explained 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-

[8] *See* https://www.ftc.gov/tipsadvice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance (last visited November 22, 2019).

technology.html. Nonetheless, Mr. Schmidt predicted that "some company by the way is going to cross that line." *Id.*

29. 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.

30. 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.

31. 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.[9] 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.

32. But 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.

33. 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 under the age of 13 all across the country, including the state of Illinois.

34. 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.[10]

35. To reaffirm the 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

---

[9] 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.

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

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 collection, use, and maintenance of student data.[11] Though not an original signatory, and hesitant to sign on (only succumbing after public outrage), Googled eventually signed the Student Privacy Pledge[12] 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 Google collects, if any, and the purposes for which the information Google maintains is used or shared with third parties.

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

[12] 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-privacypledge/ (last visited March 26, 2020).

36. 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.

37. 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).

38. 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 used to identify a person—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 used to identify a person—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 13. *See* 740 ILCS 14/10.

39. 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.

40. 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.

41. 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.

42. 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.

43. Moreover, the "biometric identifiers" and "biometric information" Google collected (and continues to collect) from children who used (and continue to use) its "G Suite for Education" platform, at schools in both Illinois and elsewhere throughout the country, also constitute "personally identifiable information" within the meaning of COPPA. And Google, by making commercially available and operating its online, cloud-based "G Suite for Education" service with actual knowledge that it collects, uses, and/or discloses personally identifiable information from children, constitutes an "operator" of such a service within the meaning of COPPA.

44. Google collected, stored, and used this "personally identifiable information"—namely, the biometric identifiers and biometric information belonging to Plaintiffs and millions of other children under age 13 across the United States, as well as the names and other personal information capable of identifying the children to whom this sensitive biometric data belongs—without first "[o]btaining verifiable consent" within the meaning of COPPA. Indeed, by engaging in these practices as alleged herein, Google failed to "mak[e] any reasonable effort (taking into consideration available technology) to ensure that before personally identifiable information is collected from a child, a parent of the child. . . [r]eceives notice of the operator's personally identifiable information collection, use, and disclosure practices; and [a]uthorizes any collection, use, and/or disclosure of the personally identifiable information." 16 C.F.R. § 312.2.

45. Thus, both BIPA and COPPA 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 or COPPA at any point during that five-year period (be it by obtaining the requisite signed written release or verifiable consent from the from the parents or legal guardians of the children whose biometrics it collects in Illinois or by turning the technology off in Illinois' schools altogether).

V. Plaintiffs' Experiences

46. Google provides "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. 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.

47. At all times during the time period relevant to this action, Plaintiffs have resided in Illinois and attended a primary 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.

48. 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 used to identify them—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 used to identify them—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.

49. 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 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.

50. 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 or their father, Clinton Farwell, 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.

51. 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.

52. 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.

53. Neither Clinton Farwell (Plaintiffs' father, legal guardian, and authorized representative) nor any other BIPA 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.

54. Likewise, Google never provided Clinton Farwell (Plaintiffs' father, legal guardian, and authorized representative) or any other parent, legal guardian, or authorized representative of any member of the Classes 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.

55. Nevertheless, when Plaintiffs and the unnamed members of the BIPA 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 Classes, all in direct violation of BIPA and COPPA.

56. Additionally, in connection with Plaintiffs' and COPPA Class members' use of the "G Suite for Education" platform at schools in Illinois and across the country, Google has also collected and continues to collect, without first obtaining "verifiable parental consent," browsing histories, contact lists, and audio notes and memos pertaining to Plaintiffs and the other COPPA Class members under the age of 13 across the United States, including in Illinois, as well as the Plaintiffs' and COPPA Class members' names and uniquely identifying school email addresses in direct violation of COPPA, 16 C.F.R. § 31 2.4.

CLASS ALLEGATIONS

57. **Proposed Class Definition:** Plaintiffs, by and through their father and legal guardian, bring this action pursuant to Federal Rules of Civil Procedure 23(b)(2) and 23(b)(3) on behalf of two classes of similarly situated individuals. The first class Plaintiffs seek to represent is defined as follows (the "BIPA Class"):

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

The second class Plaintiffs seek to represent is defined as follows (the "COPPA Class"):

> All persons under the age of 13 who, while using the "G Suite for Education" platform at a primary or secondary school in the United States, had their voiceprint, face template, or other personally identifiable information collected by Google after March 26, 2016.

58. The BIPA Class and the COPPA Class are at times collectively referred to herein as the "Classes."

59. **Numerosity:** The number of persons within each of the Classes is substantial, believed to amount to millions of children for the COPPA Class and tens of thousands of children for the BIPA Class. It is, therefore, impractical to join all members of the Classes as named plaintiffs. Further, the size and relatively modest value of the claims of the individual members of the BIPA Class, and the purely injunctive relief sought on behalf of the members of the COPPA 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.

60. **Commonality and Predominance:** There are well-defined common questions of fact and law that exist as to all members of the Classes and that predominate over any questions affecting only individual members of the Classes. With respect to the BIPA 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 BIPA Class's "biometric identifiers" or "biometric information";

c. whether Google informed Plaintiffs and the BIPA 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 BIPA 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 BIPA Class, whichever occurs first;

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

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

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

61. With respect to the COPPA 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 "biometric identifiers" or "biometric information" from Plaintiffs and other children under the age of 13 in connection with their use of the "G Suite for Education" platform at primary and secondary schools in the United States during the preceding four years;

b. whether "biometric identifiers" and "biometric information" constitute "personally identifiable information" within the meaning of COPPA;

c. whether Google collected, captured, or otherwise obtained the "biometric identifiers," "biometric information," or other personally identifiable information from COPPA Class members in connection with their use of the "G Suite for Education" platform at primary and secondary schools;

d. whether Google properly informed COPPA Class members' parents or legal guardians and the BIPA Class that it would collect, capture, otherwise obtain

and then store their "biometric identifiers", "biometric information", or other collected personally identifiable information within the meaning of COPPA; and

e. whether Google obtained "verifiable parental consent" before collecting, using, or disclosing "biometric identifiers", "biometric information", or other collected personal information from COPPA Class members.

62. **Adequate Representation:** 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 Classes. Plaintiffs are able to fairly and adequately represent and protect the interests of the Classes. Plaintiffs have raised viable statutory claims of the type reasonably expected to be raised by members of the Classes, 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 Classes or to add additional claims or classes as may be appropriate.

63. **Superiority:** 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 Classes is impracticable. Even if every member of the Classes 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 Classes. Plaintiffs anticipate no difficulty in the management of this action as a class action. Class-wide relief is essential to compel compliance with BIPA and COPPA.

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

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

65. 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).

66. Plaintiffs' father and legal guardian, Clinton Farwell, is Plaintiffs' "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).

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

68. Plaintiffs and the BIPA 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 school in Illinois after March 26, 2015. *See* 740 ILCS 14/10.

69. Plaintiffs and all members of the BIPA 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.

70. Google systematically collected, captured, or otherwise obtained Plaintiffs' and the BIPA 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.

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

72. 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 BIPA Class members, as required by the BIPA. *See* 740 ILCS 14/15(a).

73. Google has denied BIPA's promise of privacy to those who need it most. By collecting, storing, and using Plaintiffs' and the other BIPA 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.

74. On behalf of themselves and the proposed BIPA Class members, by and through their father and natural legal guardian, Clinton Farwell, Plaintiffs seek: (1) injunctive and equitable relief as is necessary to protect the interests of Plaintiffs and the other members of the BIPA 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., 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., 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).

SECOND CAUSE OF ACTION
Violation of Cal. Bus. & Prof. Code § 17200, *et seq.*
(On Behalf of Plaintiffs and the COPPA Class)

75. Plaintiffs incorporate the allegations of paragraphs 1-63 as if fully set forth herein.

76. Google engaged in business acts and practices deemed "unlawful" under the UCL, because, as alleged above, Google unlawfully collected, stored, and used the biometric identifiers, biometric information, and other personally identifying information of Plaintiffs and the other COPPA Class members without first obtaining the requisite parental consent in violation of COPPA and Federal Trade Commission regulations.

77. Under COPPA, an operator of a website or online service that collects personal information from children must provide notice to the child's parent about its data collection practices and obtain verifiable parental consent prior to any collection or use of personal information from children. A violation of this regulation is deemed unlawful. 16 C.F.R. § 312.3.

78. COPPA defines a "child" as "an individual under the age of 13." 16 C.F.R. §312.2.

79. Google is required to comply with the requirements set out in COPPA because it has specifically developed the Google Education platform for use by students in grades K-12 at schools across the United States, including in Illinois, and has actual knowledge that children under the age of 13 use its apps and services.

80. Plaintiffs and the COPPA Class members are minor children under the age of 13 who had their "biometric identifiers," "biometric information," and other personally identifying information including their names and e-mail addresses collected, captured, received, or otherwise obtained by Google in connection with their use of Google's "G Suite for Education" platform at a school in the United States after March 26, 2016.

81. Google's "G Suite for Education" service utilized by Plaintiffs and members of the COPPA Class features "subject matter, visual content, use of animated characters or child-oriented activities and incentives, music or other audio content, age of models, presence of child celebrities

or celebrities who appeal to children, language or other characteristics of the Web site or online service, as well as . . . advertising promoting or appearing on the Web site or online service [that] is directed to children." *See* 16 C.F.R. § 312.2.

82. Google is an "operator" as contemplated by 16 C.F.R. § 312.2 because it operates a "Web site located on the Internet or an online service and who collects or maintains personal information from or about the users of or visitors to such Web site or online service . . . where such Web site or online service is operated for commercial purposes involving commerce among the several States or with 1 or more foreign nations." Indeed, students can access Google's services online and Google provides its Google Education platform to schools in Illinois and throughout the country.

83. Google "collects" personal information from children under the age of 13 across the United States, including in Illinois, because it requests, prompts, or encourages a child to submit personal information online and it passively collects highly sensitive biometric data (as alleged above) from children online as they use the "G Suite for Education" platform at school.

84. Specifically, Google collects and has collected, on information and belief, browsing histories, contact lists, and audio notes and memos of Plaintiffs and the other COPPA Class members under the age of 13 across the United States, including in Illinois, in the form of audio files containing the child's voice and digitized images of the child's facial geometry, as well as biometric identifiers and biometric information derived therefrom. Google attributed, and continues to attribute, all data it collects from children to their Google accounts with the child's name and uniquely identifying school email address.

85. Pursuant to 16 C.F.R. § 31 2.4(a), "[i]t shall be the obligation of the operator to provide notice and obtain verifiable parental consent prior to collecting, using, or disclosing personal information from children. Such notice must be clearly and understandably written, complete, and must contain no unrelated, confusing, or contradictory materials."

86. Google has failed to provide notice to Plaintiffs' father and legal guardian Clinton Farwell, and has failed to provide such notice to the parents and guardians of the other members of the COPPA Class of its data collection practices as required by 16 C.F.R. § 312.4. Specifically,

Google failed to give direct notice to parents stating the types of personal information it seeks to collect from the child. Any notice that Google provides is not intended for the child's parent and contains terms that no child under the age of 13 would comprehend or would have the capacity to accept.

87. Further, Google failed to obtain—or even adequately attempt to obtain—parental consent authorizing it to collect and use minors' personal and sensitive information from Plaintiffs' father and guardian Clinton Farwell or from the parents or guardians of any of the other COPPA Class members.

88. Each instance of Google's nonconsensual and unauthorized collection and use of Plaintiffs' and other members of the COPPA Class's personal information in one or more ways described above constitutes a separate violation of COPPA and is thus a separate violation of the UCL's "unlawful" prong.

89. Moreover, pursuant to Section 1303(c) of COPPA, 15 U.S.C. § 6502(c), a violation of COPPA constitutes an "unfair" or "deceptive" act or practice in or affecting commerce, in violation of the FTC Act and thus the UCL.

90. Google additionally engaged in business acts or practices deemed "unfair" under the UCL because, as alleged above, Google failed to disclose during the Class Period that it was collecting, storing, and using the biometric identifiers, biometric information, and other personally identifying information of Plaintiffs and the other COPPA Class members without obtaining the requisite parental consent in violation of COPPA and Federal Trade Commission regulations.

91. Unfair acts under the UCL have been interpreted using three different tests: (1) whether the public policy which is a predicate to a consumer unfair competition action under the unfair prong of the UCL is tethered to specific constitutional, statutory, or regulatory provisions; (2) whether the gravity of the harm to the consumer caused by the challenged business practice outweighs the utility of the defendant's conduct; and (3) whether the consumer injury is substantial, not outweighed by any countervailing benefits to consumers or competition, and is an injury that consumers themselves could not reasonably have avoided. Defendants' conduct is unfair under each of these tests. As described above, Google's conduct violates the policies underlying

privacy law, as well as COPPA itself. The gravity of the harm resulting from Google's secret collecting, storing, and using of biometric identifiers, biometric information, and other personally identifying information from children under the age of 13, without the requisite parental consent, is significant and there is no corresponding benefit to these children or their parents from such conduct. Lastly, because Plaintiffs and COPA Class members were completely unaware of Google's practices as alleged herein, they could not possibly have avoided the privacy-based harms such practices caused.

92. Additionally, Google's conduct constitutes deceptive business practices in violation of Cal. Bus. & Prof. Code §17200. Under the UCL, a business practice that is likely to deceive an ordinary consumer constitutes a deceptive business practice. Google's conduct as alleged herein was deceptive because Google intentionally and deceptively misled children under the age of 13, the parents of those children, and the public about their practices of collecting, storing, and using of biometric identifiers, biometric information, and other personally identifying information from children under the age of 13. Google has additionally made material misrepresentations and omissions, both directly and indirectly, to Plaintiffs and members of the COPPA Class, by and through their legal guardians, related to the invasive and unlawful practices alleged herein, including through its signing of the Student Privacy Pledge and through other public-facing documents such as websites, privacy policies, marketing materials, and public statements, in which it omits or otherwise conceals the full extent of its BIPA and COPPA violative conduct detailed herein and its practices of otherwise invading the privacy of children under the age of 13 in connection with their use of the "G Suite for Education" platform at school, as well as by misrepresenting, *inter alia*, the privacy-protective nature of its "G Suite for Education" platform and its suitability for children.

93. Finally, Google's secret and unlawful practices of collecting, storing, and using the biometric identifiers, biometric information, and other personally identifying information of Plaintiffs and the other COPPA Class members without obtaining the requisite parental consent, in violation of COPPA and Federal Trade Commission regulations, take advantage of the lack of knowledge, ability, experience, or capacity of the children, parents, and educators across the United

States to a grossly unfair degree. Google purposefully misrepresents and obfuscates its COPPA-violative conduct, which in tum results in the children of the United States being forced to use its "G Suite for Education" service in order to participate in school. Google has complete control over the data collection, use, and retention practices of the "G Suite for Education" service, including the biometric data and other personally identifying information collected through the use of the service, and uses this control not only to secretly and unlawfully monitor and profile children, but to do so without the knowledge or consent of those children's parents. Such exploitation by Google, with its unique knowledge of its wrongful practices, occurs to the detriment of the children and their parents across the United States, and has invaded the privacy of Plaintiffs and the other members of the COPPA Class.

94. Google's violations of the UCL were, and are, willfully unlawful, deceptive, and unfair. Google is aware of its violative conduct, yet has failed to adequately and affirmatively take steps to cure such misconduct.

95. Plaintiffs and the other members of the COPPA Class were directly and proximately harmed by Google's violations of Cal. Bus. & Prof. Code §17200.

96. Plaintiffs, individually and on behalf of the COPPA Class, by and through their father and legal guardian Clinton Farwell, seek: (1) an injunction requiring Google to obtain consent prior to collecting the "biometric identifiers," "biometric information," and other personally identifiable information within the meaning of COPPA from children under the age of 13, to delete such "biometric identifiers," "biometric information," and other personally identifiable information already collected without parental consent, and to implement functionality sufficient to prevent the unlawful collection of such "biometric identifiers," "biometric information," and other personally identifiable information in the future; and (2) reasonable attorney's fees (pursuant to Cal. Code of Civ. Proc. § 1021.5).

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, seek judgment against Defendant as follows:

(a) Certifying this case as a class action on behalf of the Classes defined above, appointing Plaintiffs, by and through their father and legally authorized guardian, Clinton Farwell, as representatives of the Classes, and appointing their counsel as Class Counsel on behalf of the Classes;

(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 BIPA Class;

(c) Declaring that Google's actions, as set out above, violate the COPPA and thus the UCL, Cal. Bus. & Prof. Code § 17200, *et seq.,* with respect to Plaintiffs and members of the COPPA Class;

(d) Awarding $1,000.00 statutory damages to Plaintiff H.K., Plaintiff J.C., and each member of the BIPA 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;

(e) Awarding injunctive and other equitable relief pursuant to BIPA as is necessary to protect the interests of Plaintiffs and members of the BIPA 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 BIPA Class members to date;

(f) Awarding injunctive and other equitable relief pursuant to the California UCL as is necessary to protect the interests of Plaintiffs and members of the COPPA Class, including, *inter alia*, an order requiring Google to collect, store, and use the biometric identifiers, biometric information, and other personally identifying information (within the meaning of COPPA) of children under the ages of 13 across the United States in compliance with COPPA, and to permanently destroy the biometric identifiers, biometric information, and other personally identifying

information covered by COPPA that it has collected from Plaintiffs and COPPA Class members to date;

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

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

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

DEMAND FOR JURY TRIAL

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, demand a trial by jury pursuant to Federal Rule of Civil Procedure 38(b) on all claims and issues so triable.

Dated: April 2, 2020

BURSOR & FISHER, P.A.

By: /s/ *L. Timothy Fisher*
L. Timothy Fisher

L. Timothy Fisher (State Bar No. 191626)
1990 North California Blvd., Suite 940
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
Email: ltfisher@bursor.com

BURSOR & FISHER, P.A.
Scott A. Bursor (State Bar No. 276006)
2665 S. Bayshore Dr., Suite 220
Miami, FL 33133-5402
Telephone: (305) 330-5512
Facsimile: (305) 676-9006
E-Mail: scott@bursor.com

HEDIN HALL LLP
David W. Hall (State Bar No. 274921)
Four Embarcadero Center, Suite 1400
San Francisco, CA 94111
Telephone: (415) 766-3534
Facsimile: (415) 402-0058

Email: dhall@hedinhall.com

Counsel for Plaintiffs, by and through their father and legal guardian Clinton Farwell, and the Putative Class