

1 James M. Wagstaffe (95535)
Frank Busch (258288)
2 WAGSTAFFE, VON LOEWENFELDT,
BUSCH & RADWICK LLP
3 100 Pine Street, Suite 725
San Francisco, CA 94111
4 Tel: (415) 357-8900
Fax: (415) 357-8910
5 wagstaffe@wvbrlaw.com
busch@wvbrlaw.com

6 *Counsel for Plaintiffs and the Proposed*
7 *Classes*

LABATON SUCHAROW LLP
Jonathan Gardner (*pro hac vice* to be
submitted)
Melissa H. Nafash (*pro hac vice* to be
submitted)
Jonathan D. Waisnor (*pro hac vice* to be
submitted)
140 Broadway
New York, NY 10005
Tel: (212) 907-0700
Fax: (212) 818-0477
jgardner@labaton.com
mnafash@labaton.com
jwaisnor@labaton.com

Counsel for Plaintiffs and the Proposed
Classes

10 **UNITED STATES DISTRICT COURT**
11 **NORTHERN DISTRICT OF CALIFORNIA**

12 L.P., a minor, E.P., a minor, S.P., a minor,)
13 D.P., a minor, F.P., a minor, R.P., a minor, and)
A.P., a minor, by and through their legal)
14 guardian Esther Yona Posner; N.T., a minor,)
by and through her legal guardian Ilya Tsorin;)
15 and C.D., a minor, by and through her legal)
guardian Katherine Delgado, V.M., a minor, by)
16 and through her legal guardian Eunice Morris;)
A.S., a minor, Y.S., a minor, S.S., a minor,)
17 D.S., a minor, and M.S., a minor by and)
through their legal guardian Dina Shallman,)
18 Individually and on Behalf of All Others)
Similarly Situated,)

Case No.

CLASS ACTION COMPLAINT AND
REQUEST FOR JURY TRIAL

19)
20)
21)
22)
23)
24)
25)
26)
27)
28)
Plaintiff(s),)

vs.)

SHUTTERFLY, INC.,

Defendant.

1 **CLASS ACTION COMPLAINT**

2 Plaintiffs L.P., a minor, E.P., a minor, S.P., a minor, D.P., a minor, F.P., a minor, R.P., a
3 minor, and A.P., a minor, by and through their parent and legal guardian Esther Yona Posner;
4 N.T., a minor, by and through her parent and legal guardian Ilya Tsorin; C.D., a minor, by and
5 through her parent and legal guardian Katherine Delgado; V.M., a minor, by and through her
6 legal guardian Eunice Morris; A.S., a minor, Y.S., a minor, S.S., a minor, D.S., a minor, and
7 M.S., a minor by and through their legal guardian Dina Shallman, bring this Class Action
8 Complaint against Defendant Shutterfly, Inc. to put a stop to its surreptitious collection, use,
9 storage, and disclosure of Plaintiffs’ and the proposed Classes’ sensitive biometric data in
10 violation of Illinois’ Biometric Information Privacy Act, the Children’s Online Privacy
11 Protection Act, California’s Online Privacy Protection Act, and California’s Consumer Privacy
12 Act. The Classes include minors whose rights were wronged pursuant to violations of the
13 Illinois Biometric Information Privacy Act, the Children’s Online Privacy Protection Act,
14 California’s Online Privacy Protection Act, California’s Consumer Privacy Act, or a
15 combination of two or more. Plaintiffs allege as follows upon personal knowledge as to
16 themselves and their own acts and experiences, and, as to all other matters, upon information,
17 belief, and research into Shutterfly’s platform and patents, which includes investigation
18 conducted by their attorneys.

19 **NATURE OF THE ACTION**

20 1. Defendant Shutterfly is a leading retailer and manufacturing platform for
21 personalized photos and services. Shutterfly can be accessed online and through its “app” that
22 can be downloaded by users to devices such as a smartphone or tablet.

23 2. Shutterfly users can use its platform to, among other things, upload, organize, and
24 maintain photographs, as well as share photographs with friends and relatives. Once a user
25 uploads a photograph on Shutterfly, the user can “tag” (*i.e.*, identify by name) all of the faces
26 that appear in the photograph. Shutterfly users can then use this feature to gather, organize,
27 share, and transform the photos into personalized items. If the user does not “tag” the faces in
28 the photos, Shutterfly will still apply its technology to the photos and organize photos by face,

1 showing a person’s face and how many photos have been uploaded of them underneath their
2 face.

3 3. Shutterfly’s use of facial recognition technology followed its acquisition of
4 ThisLife in January 2013¹, which offered what Shutterfly claimed to be a best-in-class memory
5 solution comprising facial recognition, duplicate detection, chronological organization and
6 instant product creation. It also included Shutterfly’s “Smart Facial Tagging” feature. Smart
7 Facial Tagging functions by scanning photographs uploaded by the user and identifying faces
8 appearing in those photographs. If Smart Facial Tagging recognizes and identifies one of the
9 faces appearing in the photograph, Shutterfly will automatically tag it. If not, Shutterfly will
10 suggest tagging the unidentified face.

11 4. Shutterfly conceals the fact that it utilizes proprietary facial recognition software
12 to extract from user-uploaded photographs the unique biometric identifiers (*i.e.*, graphical
13 representations of facial features, also known as facial geometry) associated with people’s faces
14 in order to identify them. Shutterfly then stores the biometric information of users and non-users
15 in its database. Shutterfly does not disclose its biometric data collection to its users, nor does it
16 ask users or non-users in the photographs to acknowledge, let alone consent to, these practices.

17 5. Through these practices, Shutterfly not only disregards the users’ and non-users’
18 privacy rights; it also violates the Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.*
19 (“BIPA”), which was specifically designed to protect Illinois residents from practices like
20 Shutterfly’s. In particular, Shutterfly violated (and continues to violate) BIPA because it did not:

- 21 • Properly inform Plaintiffs or the Classes in writing that their biometric
22 identifiers (face geometry) were being generated, collected or stored;
- 23 • Properly inform Plaintiffs or the Classes in writing of the specific purpose
24 and length of time for which their biometric identifiers were being
25 collected, stored, and used;

26 _____
27 ¹ Shutterfly began using the tagging feature in August 2014. *See* Shutterfly’s August 12, 2014
28 Press Release at <http://ir.shutterfly.com/news-releases/news-release-details/thislife-shutterfly-provides-best-class-memory-management>.

- 1 • Provide and follow a publicly available retention schedule and guidelines
2 for permanently destroying the biometric identifiers of Plaintiffs and the
Classes; and
- 3 • Receive a written release from Plaintiffs or the Classes to collect, capture,
4 or otherwise obtain their biometric identifiers.

5 6. Through these practices, Shutterfly also violated and continues to violate the
6 Children’s Online Privacy Protection Act, 15 U.S.C. § 6502(a)(1, *et seq.* (“COPPA”), which is
7 specifically designed to protect children from practices like Shutterfly’s. In particular, Shutterfly
8 violated and continues to violate COPPA because it does not:

- 9 • Post a notice on the website indicating (a) what information the operator
10 collects from children, (b) how the operator uses this information, and (c)
11 what the operator’s disclosure practices are for this information;
- 12 • Obtain verifiable parental consent for the collection, use or disclosure of
13 personal information obtained from a child;
- 14 • Provide to a parent, upon verifying the identification of the parent, (a) a
15 description of the types of personal information collected from a child, (b)
16 an opportunity at any time to refuse to permit the operator’s further use or
17 maintenance in retrievable form of the personal information collected
from the child or to permit future online collection of personal information
from the child; and
- 18 • Establish and maintain reasonable procedures to protect the
19 confidentiality, security, and integrity of personal information collected
20 from children.

21 7. Through these practices, Shutterfly also violated and continues to violate
22 California’s Online Privacy Protection Act, Cal. Bus. & Prof. Code § 22575, *et seq.*
23 (“CalOPPA”), which is designed to put users on notice of personal information being collected.
24 In particular, Shutterfly violated and continues to violate CalOPPA because it does not:

- 25 • Identify in its privacy policy the categories of personally identifiable information
26 that the operator collects through the website or online service about individual
27 consumers who use or visit its commercial website or online service and the
28 categories of third-party persons or entities with whom the operator may share
that personally identifiable information; and

1 11. Plaintiff N.T., a minor, is a natural person whose pictures were uploaded to
2 Shutterfly. N.T. and her parent and guardian, Ilya Tsorin, who brings this action on her behalf,
3 are residents and citizens of the State of Illinois.

4 12. Plaintiff C.D., a minor, is a natural person whose pictures were uploaded to
5 Shutterfly. C.D. and her parent and guardian, Katherine Delgado, who brings this action on her
6 behalf, are residents and citizens of the State of Illinois.

7 13. Plaintiff V.M., a minor is a natural person whose pictures were uploaded to
8 Shutterfly. V.M., a minor, and her parent and guardian, Eunice Morris, who brings this action on
9 her behalf, are residents and citizens of the State of California.

10 14. Plaintiffs A.S., a minor, Y.S., a minor, S.S., a minor, D.S., a minor, and M.S., a
11 minor A.S., a minor, Y.S., a minor, S.S., a minor, D.S., a minor, and M.S., a minor, and their
12 parent and guardian, Dina Shallman, who brings this action on their behalf, are residents of the
13 State of California.

14 15. Defendant Shutterfly, Inc. (“Defendant” or “Shutterfly”) is a Delaware
15 corporation with its headquarters and principal executive office at 2800 Bridge Parkway,
16 Redwood City, California 94065. Shutterfly conducts business throughout the State of
17 California and the United States.

18 **JURISDICTION AND VENUE**

19 16. Jurisdiction is proper in this Court pursuant to the Class Action Fairness Act, 28
20 U.S.C. §1332(d) (“CAFA”), because (i) the proposed Classes consist of well over 100 members;
21 (ii) Plaintiffs and all Class Members are United States citizens and nine of the Plaintiffs and
22 many class members are citizens of a state different from Defendant’s principal place of
23 business; and (iii) the aggregate amount in controversy exceeds \$5,000,000, exclusive of interest
24 and costs.

25 17. Jurisdiction over the Children’s Online Privacy Protection Act (“COPPA”), 15
26 U.S.C. § 6501, *et seq.* is also proper in this Court pursuant to 28 U.S.C. § 1331.

27 18. Jurisdiction over the California Consumer Privacy Act (“CCPA”) Class is proper
28 in this Court pursuant to 28 U.S.C. § 1367(a), because the CCPA claims are so related to claims

1 over which this Court has original jurisdiction that they form part of the same case or
2 controversy under Article III of the United States Constitution.

3 19. This Court has personal jurisdiction over Plaintiffs because the nonresident
4 Plaintiffs submit to the Court's jurisdiction and the California Plaintiffs live within the Court's
5 jurisdiction. This Court has personal jurisdiction over Defendant Shutterfly because Shutterfly's
6 corporate headquarters and principal place of business is in Redwood City, California.
7 Defendant is a citizen of the states of Delaware and California.

8 20. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant
9 maintains its corporate headquarters and principal place of business in this District.

10 **INTRADISTRICT ASSIGNMENT**

11 21. Pursuant to Civil Local Rule 3-2(d), this case should be assigned to the San
12 Francisco Division.

13 **FACTUAL BACKGROUND**

14 **I. Biometrics and Consumer Privacy**

15 22. "Biometrics" refers to technologies used to identify an individual based on unique
16 physical characteristics. Common biometric identifiers include retina or iris scans, fingerprints,
17 voiceprints, or hand or face geometry scans. One of the most prevalent uses of biometrics is in
18 facial recognition technology, which works by scanning a photograph or image for human faces,
19 extracting facial feature data from that photograph or image, generating a "faceprint" from the
20 image through the use of facial recognition algorithms, and then comparing, or "matching," the
21 resultant faceprint to other faceprints stored in a "faceprint database." If a database match is
22 found, a person may be identified.

23 23. The recent sophistication of facial recognition software has generated many
24 commercial applications of the technology, but it has also raised serious privacy concerns about
25 its massive scale, scope, and surreptitiousness. During a 2012 hearing before the United States
26 Senate Subcommittee on Privacy, Technology, and the Law, U.S. Senator Al Franken stated that
27 "there is nothing inherently right or wrong with facial recognition technology . . . [b]ut if we do
28 not stop and carefully consider the way we use [it], it could also be abused in ways that could

1 threaten basic aspects of our privacy and civil liberties.”² Senator Franken noted, for example,
2 that facial recognition technology could be “abused to not only identify protesters at political
3 events and rallies, but to target them for selective jailing and prosecution.”³

4 24. Indeed, Senator Franken’s concern became a reality. During a May 22, 2019
5 hearing, Senator Elijah Cummings shared that he was part of a march in protest to the tragic
6 death of Freddie Gray at the hands of police in 2015, and he later learned “the police used facial
7 recognition technology to find and arrest protestors. It is likely that I and other members of our
8 community who were simply exercising our rights under the Constitution were scanned,
9 identified, and monitored by using this technology. Think about what I just said. Whatever walk
10 of life you may come from, you may very well be a part of this process. You could be at a rally
11 supporting gun rights or protesting gun violence. You could be marching for the right to life or a
12 woman’s right to choose. You could be pressing for the repeal of the ACA or the expansion of
13 health care. In all of these cases the government can monitor you without your knowledge and
14 enter your face into a data base that could be used in virtually unrestricted ways.”⁴

15 25. Approximately one year after Senator Cummings’ statement and in the wake of
16 protests surrounding the death of George Floyd, Senator Edward J. Markey, Senator Jeff
17 Merkley, Congresswoman Pramila Jayapal, and Congresswoman Ayanna Pressley introduced
18 “bicameral legislation to stop government use of biometric technology, including facial
19 recognition tools.”⁵ If passed, the Facial Recognition and Biometric Technology Moratorium

21 ² *What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before*
22 *the S. Comm. on Privacy, Tech., & the Law of the Comm. on the Judiciary*, 112th Cong. (2012),
23 *available at* [https://www.govinfo.gov/content/pkg/CHRG-112shrg86599/pdf/CHRG-](https://www.govinfo.gov/content/pkg/CHRG-112shrg86599/pdf/CHRG-112shrg86599.pdf)

24 ³ *Id.*

25 ⁴ *Facial Recognition Technology: Part I, It’s Impact on Our Civil Rights and Liberties: Hearing*
26 *Before the Comm. on Oversight and Reform*, 116th Cong. (2019), *available at*
27 [https://docs.house.gov/meetings/GO/GO00/20190522/109521/HHRG-116-GO00-Transcript-](https://docs.house.gov/meetings/GO/GO00/20190522/109521/HHRG-116-GO00-Transcript-20190522.pdf)

28 ⁵ Press Release, *Senators Markey and Merkley, and Reps. Jayapal, Pressley to Introduce*
Legislation to Ban Government Use of Facial Recognition, Other Biometric Technology (June
25, 2020), *available at* [CLASS ACTION COMPLAINT
CASE NO.](https://www.markey.senate.gov/news/press-releases/senators-markey-</p></div><div data-bbox=)

1 Act would “prohibit biometric surveillance by the Federal Government without explicit statutory
 2 authorization and to withhold certain Federal public safety grants from State and local
 3 governments that engage in biometric surveillance.”⁶ Not only does this Act prohibit the
 4 collection and use of biometrics by federal entities, but it also provides for a “private right of
 5 action for individuals whose biometric data is used in violation of the Act and allows for
 6 enforcement by state Attorneys General.”⁷

7 26. California is now taking additional steps to protect biometric data by amending
 8 the current version of the CCPA. The California Privacy Rights Act (“CPRA”) recently
 9 qualified for the November 2020 ballot. The CPRA would amend the CCPA to create additional
 10 privacy rights and obligations in California. The CPRA would add a new category of protected
 11 information called “Sensitive Personal Information” and give consumers new rights surrounding
 12 that information. Sensitive Personal information includes “Social Security Number, driver’s
 13 license number, passport number, financial account information, precise geolocation, race,
 14 ethnicity, religion, union membership, personal communications, genetic data, **biometric or**
 15 **health information**, and information about sex life or sexual orientation.”⁸ This amendment
 16 also specifically includes additional protections for children. The CPRA enhances the
 17 protections for children by “tripling fines for violations of the CCPA’s opt-in to sale right and
 18

19 and-merkley-and-reps-jayapal-pressley-to-introduce-legislation-to-ban-government-use-of-
 20 facial-recognition-other-biometric-technology.

21 ⁶ Facial Recognition and Moratorium Act, *available at*
 22 [https://www.markey.senate.gov/imo/media/doc/acial%20Recognition%20and%20Biometric%20](https://www.markey.senate.gov/imo/media/doc/acial%20Recognition%20and%20Biometric%20Technology%20Moratorium%20Act.pdf)
 23 [Technology%20Moratorium%20Act.pdf](https://www.markey.senate.gov/imo/media/doc/acial%20Recognition%20and%20Biometric%20Technology%20Moratorium%20Act.pdf).

24 ⁷ See Press Release, *Senators Markey and Merkley, and Reps. Jayapal, Pressley to Introduce*
 25 *Legislation to Ban Government Use of Facial Recognition, Other Biometric Technology* (June
 26 25, 2020), *supra* note 5.

27 ⁸ Hunton Andrews Kurth LLP, *BREAKING: Californians for Consumer Privacy Introduces*
 28 *California Privacy Rights Act for November 2020 Ballot* (May 5, 2020), *available at*
[https://www.natlawreview.com/article/breaking-californians-consumer-privacy-introduces-](https://www.natlawreview.com/article/breaking-californians-consumer-privacy-introduces-california-privacy-rights-act)
[california-privacy-rights-act.](https://www.natlawreview.com/article/breaking-californians-consumer-privacy-introduces-california-privacy-rights-act) See also, Submission of Amendments to The California Privacy
 Rights and Enforcement Act of 2020, Version 3, No. 19-0021 (Nov. 4, 2019), *available at*
[https://privacyblogfullservice.huntonwilliamsblogs.com/wp-](https://privacyblogfullservice.huntonwilliamsblogs.com/wp-content/uploads/sites/28/2020/05/19-0021A1-Consumer-Privacy-Version-3_1.pdf)
[content/uploads/sites/28/2020/05/19-0021A1-Consumer-Privacy-Version-3_1.pdf](https://privacyblogfullservice.huntonwilliamsblogs.com/wp-content/uploads/sites/28/2020/05/19-0021A1-Consumer-Privacy-Version-3_1.pdf).

1 creating a new requirement to obtain opt-in consent to sell or share data from consumers under
2 the age of 16.”⁹

3 27. Unlike other identifiers such as Social Security or credit card numbers, which can
4 be changed if compromised or stolen, biometric identifiers linked to a specific voice or face
5 cannot. These unique and permanent biometric identifiers, once exposed, leave victims with no
6 means to prevent identity theft and unauthorized tracking. Recognizing this, the Federal Trade
7 Commission urged companies using facial recognition technology to ask for consent *before* ever
8 scanning and extracting biometric data from their digital photographs.¹⁰ For years, Shutterfly
9 has deliberately ignored this prevailing view, which is expressly required under BIPA and
10 COPPA; failed to obtain user consent before launching its wide-spread facial recognition
11 program; failed to notify users of the biometric information being collected in violation of
12 CalOPPA and the CCPA; and violated millions of Illinois and California residents’ legal privacy
13 rights.

14 **II. Illinois’s Biometric Information Privacy Act**

15 28. BIPA was enacted in 2008. Under BIPA, companies may not:

16 collect, capture, purchase, receive through trade, or otherwise
17 obtain a person’s or a customer’s biometric identifier . . . unless it
18 first:

19 (1) informs the subject . . . in writing that a biometric identifier . . .
20 is being collected or stored;

21 (2) informs the subject . . . in writing of the specific purpose and
22 length of term for which a biometric identifier . . . is being
23 collected, stored, and used; and

24 (3) receives a written release executed by the subject of the
25 biometric identifier.

26 740 ILCS 14/15(b).

27 ⁹ *Id.*

28 ¹⁰ *See 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>.

1 29. The statute defines “biometric identifier” to include “a retina or iris scan,
2 fingerprint, voiceprint, or scan of hand or face geometry.” 740 ILCS 14/10.

3 30. The statute defines “biometric information” as “any information, regardless of
4 how it is captured, converted, stored, or shared, based on an individual’s biometric identifier
5 used to identify an individual.” 740 ILCS 14/10.

6 31. BIPA also regulates how companies must handle Illinois consumers’ biometric
7 data. *See, e.g.*, 740 ILCS 14/15(c)–(d). For instance, BIPA prohibits selling, leasing, trading, or
8 otherwise profiting from a person’s biometric data, 740 ILCS 14/15(c), and requires that
9 companies develop a publicly available written policy establishing a retention schedule and
10 guidelines for permanently destroying biometric data when the initial purpose for collecting such
11 data has been satisfied or within three years of the individual’s last interaction with the company,
12 whichever occurs first. It also requires companies to comply with the established retention
13 schedule and destruction guidelines. 740 ILCS 14/15(a).

14 **III. The Federal Children’s Online Privacy Protection Act**

15 32. In 1998, recognizing the vulnerability of children in the Internet Age, Congress
16 enacted the COPPA. *See* 15 U.S.C. §§ 6501-6506. COPPA’s primary goal is to place parents in
17 control over what information is collected from their young children online. COPPA applies to
18 operators of general audience websites or online services with actual knowledge that they are
19 collecting, using, or disclosing personal information from children under 13. Under COPPA,
20 websites like Shutterfly cannot lawfully obtain personally identifiable information of children
21 under 13 years of age without first obtaining verifiable consent from their parents.

22 33. Under COPPA, personally identifiable information includes first and last name;
23 home or other physical address including street name and name of a city or town; online contact
24 information; screen or user name that functions as online contact information; telephone number;
25 social security number; persistent identifier that can be used to recognize a user over time and
26 across different websites or online services; *photograph, video, or audio file, where such file*
27 *contains a child’s image or voice*; geolocation information sufficient to identify street name and
28

1 name of a city or town; or information concerning the child or the parents of that child that the
2 operator collects online from the child and combines with an identifier described above.

3 34. In order to lawfully collect, use, or disclose personally identifiable information,
4 COPPA requires that an operator meet specific requirements, including:

- 5 • Posting a privacy policy on its website or online service providing clear,
6 understandable, and complete notice of its information practices including what
7 information the website operator collects from children online, how it uses such
8 information, its disclosure practices for such information, and other specific
9 disclosures as set forth in the Rule;
- 10 • Providing clear, understandable, and complete notice of its information practices,
11 including specific disclosures, directly to parents; and
- 12 • Obtaining verifiable parental consent prior to collecting, using, and/or disclosing
13 personally identifiable information from children.

14 35. Under COPPA:

15 [o]btaining verifiable consent means making any reasonable effort
16 (taking into consideration available technology) to ensure that
17 before personal information is collected from a child, a parent of
18 the child:

19 (1) [r]eceives notice of the operator's personal information
20 collection, use, and disclosure practices; and

21 (2) [a]uthorizes any collection, use, and/or disclosure of the
22 personally identifiable information.

23 16 C.F.R. § 312.2.

24 36. The FTC issued acceptable methods for obtaining verifiable parental consent,
25 which include:

- 26 • A signed consent form sent back to the operator via fax, mail, or electronic
27 scan;
- 28 • Use of a credit card, debit card, or other online payment system that
provides notification of each separate transaction to the account holder;
- Call to a toll-free number staffed by trained personnel;
- Connect to trained personnel via video conference;

- 1 • Provide a copy of a form of government issued ID that is checked against
2 a database, as long as the identification is deleted from the operator's
records when it finishes the verification process;
- 3 • Answer a series of knowledge-based challenge questions that would be
4 difficult for someone other than the parent to answer; or
- 5 • Verify a picture of a driver's license or other photo ID submitted by the
parent and comparing that photo to a second photo submitted by the
6 parent, using facial recognition technology.

7 37. As alleged below, Shutterfly's practices of collecting, using, storing, and
8 disclosing biometric identifiers of children under 13, without the requisite verifiable parental
9 consent, are in clear violation of COPPA.

10 **IV. California's Online Privacy Protection Act**

11 38. California's Department of Justice once wrote "[m]eaningful privacy
12 policy statements safeguard consumers by helping them make informed decisions about which
13 companies they will entrust with their personal information."¹¹ Indeed, in 2003, California
14 became the first in the nation to enact broad requirements for privacy policies when it enacted its
15 Online Privacy Protection Act. CalOPPA applies to operators of commercial websites and
16 online services that collect personally identifiable information. Cal. Bus. & Prof. Code § 22575,
17 *et seq.* Under CalOPPA, websites like Shutterfly cannot lawfully obtain personally identifiable
18 information of anyone unless it discloses the data it is collecting in its privacy policy and
19 conspicuously posts its privacy policy on its website. *Id.*

20 39. Under CalOPPA, personally identifiable information includes first and
21 last name; home or other physical address, including street name and name of a city or town; e-
22 mail address; telephone number; social security number; any other identifier that permits the
23 physical or online contacting of a specific individual; ***information concerning a user that the
24 website or online service collects online from the user and maintains in personally identifiable***

25
26 ¹¹ *Making Your Privacy Practices Public, Recommendations on Developing a Meaningful
27 Privacy Policy*, California Department of Justice (May 2014), available at
28 https://oag.ca.gov/sites/all/files/agweb/pdfs/cybersecurity/making_your_privacy_practices_public.pdf.

1 *form in combination with an identifier described in this subdivision.* Cal. Bus. & Prof. Code §
2 22577.

3 40. In order to lawfully collect personally identifiable information, CalOPPA requires
4 that an operator meet specific requirements, including:

- 5 • Conspicuously posting its privacy policy on its website;
- 6 • Identifying in its privacy policy the categories of personally identifiable
7 information that the operator collects through the website or online service about
8 individual consumers who use or visit its commercial website or online service and
9 the categories of third-party persons or entities with whom the operator may share
10 that personally identifiable information; and
- 11 • Describing in its privacy policy the process by which the operator notifies
12 consumers who use or visit its commercial website or online service of material
13 changes to the operator’s privacy policy for that website or online service.

14 41. As alleged below, Shutterfly’s practices of collecting, using, storing, and
15 disclosing biometric identifiers of children, without identifying it in its privacy policy as data it
16 collects, are in clear violation of CalOPPA.

17 **V. California’s Consumer Privacy Act**

18 42. “Knowledge is power, and in the internet age knowledge is derived from data.
19 Our personal data is what powers today’s data-driven economy and the wealth it generates. It’s
20 time we had control over the use of our personal data. That includes keeping it private.”¹² In
21 June 2018, California took “a historic step forward [...] to protect Californians’ inalienable right
22 to privacy,”¹³ when it enacted California’s Consumer Privacy Act.

23 43. The CCPA requires businesses to disclose data collection and sharing practices,
24 allow consumers to request their data be deleted, allow consumers to opt out of the sale or

25
26 ¹² Press Release, *Attorney General Becerra Publicly Releases Proposed Regulations under the*
27 *California Consumer Privacy Act* (Oct. 10, 2019), available at <https://oag.ca.gov/news/press-releases/attorney-general-becerra-publicly-releases-proposed-regulations-under-california>.

28 ¹³ *Id.*

1 sharing of their personal information, and it prohibits businesses from selling personal
 2 information of consumers under the age of 16 without explicit consent. Cal. Civ. Code §
 3 1798.100, *et seq.*

4 44. Under the Act, “personal information means information that identifies, relates to,
 5 describes, is reasonably capable of being associated with, or could reasonably be linked, directly
 6 or indirectly, with a particular consumer or household. Personal information includes, but is not
 7 limited to, . . . biometric information.” Biometric information is defined as:

8 an individual’s physiological, biological, or behavioral
 9 characteristics . . . Biometric information includes, but is not
 10 limited to, imagery of the iris, retina, fingerprint, *face*, hand, palm,
 11 vein patterns, and voice recordings, from which an identifier
 12 template, such as a *faceprint*, a minutiae template, or a voiceprint,
 can be extracted, and keystroke patterns or rhythms, gait patterns
 or rhythms, and sleep, health, or exercise data that contain
 identifying information.¹⁴

13 “Sell,” “selling,” “sale,” or “sold,” is defined as “selling, renting, releasing, disclosing,
 14 disseminating, making available, transferring, or otherwise communicating orally, in writing, or
 15 by electronic or other means, a consumer’s personal information by the business to another
 16 business or a third party for monetary or other valuable consideration.”¹⁵

17 45. In order to lawfully collect personally identifiable information, the CCPA requires
 18 that an operator meet specific requirements *before* collection of that data, including:

- 19 • Informing consumers as to the categories of personal information to be
 20 collected;
- 21 • Informing consumers as to the purposes for which the categories of
 22 personal information collected shall be used;
- 23 • Provide multiple ways in which consumers can request their data be
 24 deleted;
- 25 • Allow consumers to opt out of the sale or sharing of their personal
 26 information;

27 ¹⁴ *Id.* (emphasis added.)

28 ¹⁵ *Id.*

- 1 • Obtain explicit parental or guardian consent before selling, releasing,
2 disclosing, disseminating personal information of consumers under the age
3 of 16 without explicit consent; and
- 4 • Disclose the personally identifiable information collected in its online
5 privacy policy and in any California-specific description of consumers’
6 privacy rights.

7 46. As alleged below, Shutterfly’s practices of collecting, using, storing, and
8 disclosing biometric identifiers of children under 16, without the requisite explicit parental
9 consent, are in clear violation of the CCPA.

10 **VI. Shutterfly Violates the Privacy of Illinois and Californian Children**

11 47. Shutterfly applies its proprietary facial recognition technology to every photo
12 uploaded to its website and uses “Smart Facial Tagging,” which “automate[s] the process of
13 identifying and, if the user chooses, tagging friends in the photos he or she uploads.”¹⁶

14 48. In a press release dated January 7, 2013, Shutterfly states, “[i]n the coming
15 months, Shutterfly will layer ThisLife’s technology onto the Shutterfly platform to enable richer
16 storytelling and easier product creation. Consumers will be able to safely and easily preserve,
17 organize and share their memories, regardless of where photos are stored — from Facebook to
18 Picasa to mobile phones. ThisLife’s intelligent organization platform offers features like facial
19 recognition and presents photos and albums in an elegant timeline for convenient sharing and
20 product creation.”¹⁷ Shutterfly boasted that it “make[s] face tagging quick and easy with our
21 facial recognition [technology] **that even works with kids and babies.**”¹⁸

23 ¹⁶ *Testimony of Robert Sherman, What Facial Recognition Technology Means for Privacy and*
24 *Civil Liberties: Hearing Before the S. Comm. on Privacy, Tech., & the Law of the Comm. on the*
25 *Judiciary*, 112th Cong. (2012), available at [http://www.judiciary.senate.gov/imo/media/doc/12-](http://www.judiciary.senate.gov/imo/media/doc/12-7-18ShermanTestimony.pdf)

26 ¹⁷ Shutterfly acquired ThisLife in January 2013, and the press release is available at
27 [https://www.businesswire.com/news/home/20130107005787/en/Shutterfly-Acquires-ThisLife-](https://www.businesswire.com/news/home/20130107005787/en/Shutterfly-Acquires-ThisLife-Power-Generation-Photo-Solution)
28 [Power-Generation-Photo-Solution.](https://www.businesswire.com/news/home/20130107005787/en/Shutterfly-Acquires-ThisLife-Power-Generation-Photo-Solution)

¹⁸ See <http://blog.thislife.com/post/65531549805/introducing-the-new-thislife-r-by-shutterfly>.

1 49. During a February 5, 2014 earnings call with analysts, Shutterfly reported that
2 “ThisLife provide[s] easy-to-use features like facial recognition, duplicate detection,
3 chronological organization, and image search, so users can interact with their memories by
4 person, place or event.” It announced that it planned on rolling out the new capabilities and
5 features “over the next couple of quarters.”

6 50. By the end of 2014, the facial recognition technology was live. On November 10,
7 2014, Shutterfly presented at the RBC Capital Markets Technology, Internet, Media & Telecom
8 Conference and announced:

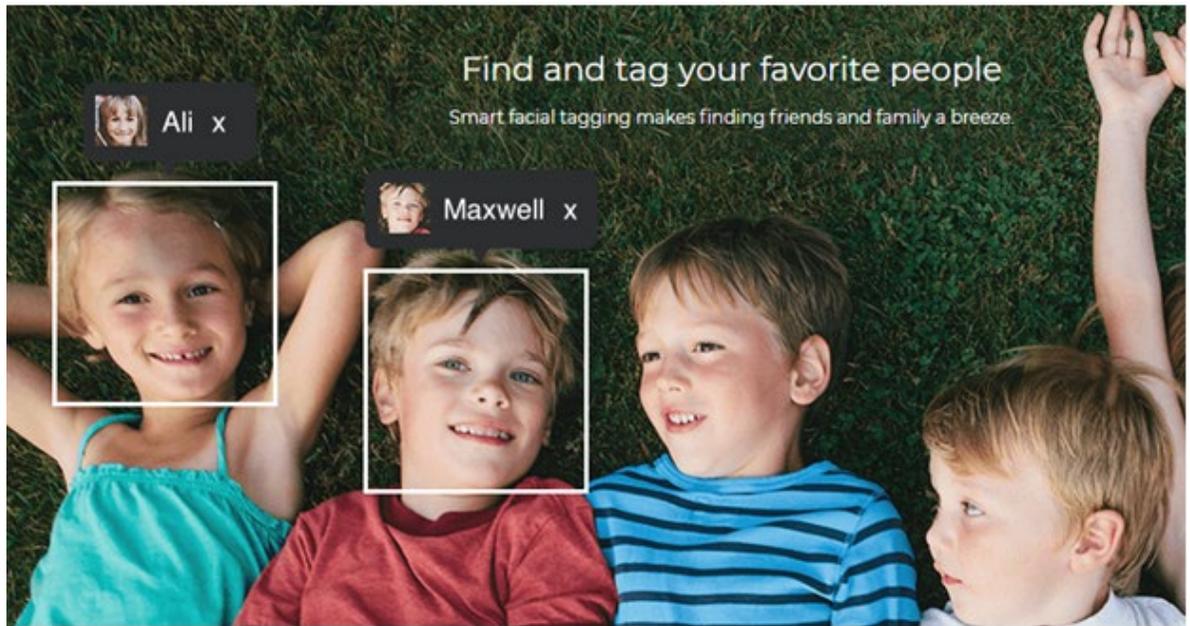
9 ThisLife [...] goes in and it aggregates all your photos across all
10 the different devices that you’re storing them on, whether it’s your
11 smartphone, whether it’s your digital SLR, whether it’s on your
12 hard drive, whether it’s at a social site like Facebook, or SmugMug
13 or Instagram, and what we do is then apply technology to allow it
14 to then organize, in a structured way, so that you can then query
15 that archive of photos whether it be by facial recognition
16 technology, whether it be by date, whether it be by the tags that
17 you’ve added to that photo.

18 51. Once ThisLife was live, Shutterfly focused on its plan to integrate facial
19 recognition technology into its entire platform, discussing that end product, “Shutterfly 3.0,”
20 during its February 3, 2016 earnings call and at its presentation at the Cantor Fitzgerald Internet
21 & Technology Conference on February 25, 2016. Shutterfly 3.0 would migrate all existing
22 Shutterfly users as well as ThisLife users. ThisLife would then cease to exist. At a September
23 13, 2016 meeting with analysts, Shutterfly revealed it began this migration in February 2016.

24 52. Shutterfly promotes its facial recognition technology as “the most comprehensive
25 memory solution on the market” that “allows customer[s] the ability to focus on reliving, sharing
26 and creating products with their favorite memories instead of spending hours tediously
27 cataloging and organizing images and video,”¹⁹ but altogether fails to disclose to anyone that it
28 collects and stores sensitive biometric identifiers in the process.

¹⁹ See August 12, 2014 Press Release available at <http://ir.shutterfly.com/news-releases/news-release-details/thislife-shutterfly-provides-best-class-memory-management>.

1 53. Unbeknownst to the public, Shutterfly’s “Smart Facial Tagging” relies on state-
 2 of-the-art facial recognition technology to extract biometric identifiers from user-uploaded
 3 photographs in order to determine the people in the photographs. Figure 1 below is taken from
 4 one of Shutterfly’s advertisements and is an example from Shutterfly’s “Smart Facial Tagging.”
 5 Notably, however, Shutterfly uses its facial recognition technology to extract biometric
 6 identifiers from user-uploaded photographs regardless of whether the user is availing itself of the
 7 Smart Facial Tagging feature.



18 **(Fig. 1.)**²⁰

19 54. In a press release dated December 1, 2015, in which Shutterfly announces the
 20 resignation of Jeffrey Housenbold, he states:

21 I am honored and privileged to have served as president and CEO
 22 of this great company . . . I would like to highlight my deep
 23 appreciation for the tens of millions of customers who have trusted
 24 us with 30 billion of their most precious memories. I would also
 25 like to thank Shutterfly employees, who have built an
 26 internationally recognized brand. Together, we pioneered and
 27 continue to lead our industry by developing the most innovative,
 28 intuitive and highest quality products and services with trend-

²⁰ See www.shutterfly.com/photos (last viewed on June 11, 2020).

1 forward designs and best-in-class customer service; all while
2 delivering the largest profit margins in our industry.²¹

3 As of December 31, 2016, Shutterfly had approximately 10.1 million users.²² As of December
4 31, 2017, Shutterfly had approximately 10 million users.²³ As of December 31, 2018, Shutterfly
5 had approximately 9.7 million users. *Id.*

6 VII. Shutterfly Violates Illinois' Biometric Information Privacy Act

7 55. Unbeknownst to consumers, and in direct violation of § 15(b)(1) of BIPA,
8 Shutterfly's proprietary facial recognition technology locates each and every face appearing in
9 each and every photo uploaded to its service from within the State of Illinois, and based on the
10 unique points and contours of each face, extracts scans of face geometry (i.e., biometric
11 identifiers) from each person appearing in each photo, including non-users – all without ever
12 informing anyone of this practice.²⁴ Indeed, Shutterfly's website states, “[i]f you notice some
13 faces not being suggested for tagging, sometimes that means we don't have enough photos of

14 ²¹ See [http://ir.shutterfly.com/news-releases/news-release-details/shutterfly-inc-announces-ceo-
15 transition-occur-2016](http://ir.shutterfly.com/news-releases/news-release-details/shutterfly-inc-announces-ceo-transition-occur-2016).

16 ²² See January 30, 2018 Press Release: Shutterfly Announces Fourth Quarter and Full Year 2017
17 Financial Results, <http://ir.shutterfly.com/node/18836/pdf>.

18 ²³ See February 5, 2019 Press Release: Shutterfly Announces Fourth Quarter and Full Year 2018
19 Financial Results, <http://ir.shutterfly.com/node/19556/pdf>.

20 ²⁴ Shutterfly holds several patents covering its facial recognition technology that detail its illegal
21 process of collecting and storing scans of face geometry without obtaining informed written
22 consent:

- 23 1. Patent No. 8798401: Image sharing with facial recognition models (granted on
24 August 5, 2014);
- 25 2. Patent No. 8861804: Assisted photo-tagging with facial recognition models (granted
26 on October 14, 2014);
- 27 3. Patent No. 9063956: Assisted photo-tagging with facial recognition models (granted
28 on June 23, 2015);
4. Patent No. 9241018: System and method for storing and sharing images (granted on
January 19, 2016);
5. Patent 9378408: Assisted photo-tagging with facial recognition models (granted on
June 28, 2016);
6. Patent No. 9569658: Image sharing with facial recognition models (granted on
February 14, 2017); and
7. Patent No. 10043059: Assisted photo-tagging with facial recognition models (granted
on August 7, 2018).

1 that person to recognize them right away. We recommend adding more photos of that face so
2 our system can learn from your uploads.”²⁵

3 56. The Smart Facial Tagging feature of Shutterfly – which automatically tags
4 previously identified individuals in the photo – works by comparing the scans of face geometry
5 of individuals who appear in newly-uploaded photos against the scans of face geometry already
6 saved in Shutterfly’s face database. Specifically, when a Shutterfly user uploads a new photo,
7 Shutterfly’s sophisticated facial recognition technology collects a scan of face geometry from
8 each person whose face is depicted in the photo, without regard for the age of that person or
9 whether that person is a user of Shutterfly, and compares that scan of face geometry against
10 Shutterfly’s face database. If no match is found, the user is prompted to “tag” (i.e., identify by
11 name) a person to that face, at which point the scan of face geometry and corresponding name
12 identification are saved in Shutterfly’s face database. However, if a scan of face geometry is
13 generated that matches a scan of face geometry already in Shutterfly’s database, then Shutterfly
14 suggests the user “tag” to that face the name already associated with that face.

15 57. In direct violation of §§ 15(b)(2) and 15(b)(3) of BIPA, Shutterfly never informed
16 anyone appearing in photos uploaded within the State of Illinois of the specific purpose and
17 length of term for which their biometric identifiers or information would be collected, stored and
18 used, nor did Shutterfly obtain a written release from any of these individuals.

19 58. In further violation of BIPA, Shutterfly shares biometric information. According
20 to Shutterfly’s Privacy Policy, “[f]rom time to time we share the personal information we collect
21 with trusted companies who work with or on behalf of us. We may share personal information
22 within our family of brands. We may also combine personal information with publicly available
23 information and information we receive from or cross-reference with our partners. These
24 companies may use your personal information to enhance and personalize your shopping
25
26

27 _____
28 ²⁵ See <https://support.shutterfly.com/s/article/Shutterfly-Photos--Search-and-Tagging-1>.

1 experience with us, to communicate with you about products and events that may be of interest
2 to you and for other promotional purposes.”²⁶

3 59. In direct violation of § 15(a) of BIPA, Shutterfly does not have written, publicly
4 available policies identifying its retention schedules nor guidelines for permanently destroying
5 individuals’ biometric identifiers or information.

6 60. Without even informing its users – let alone obtaining their informed written
7 consent – Shutterfly, through Smart Facial Tagging, automatically enrolled those users and any
8 non-user subjects of uploaded photos into Shutterfly’s facial recognition program, extracting
9 biometric identifiers from uploaded photographs and previously tagged pictures, and storing
10 these biometric identifiers and biometric information in a Shutterfly database.

11 **VIII. Shutterfly Never Notifies or Requires Users to Acknowledge Its Biometric**
12 **Data Collection Practices – Individually or on Behalf of their Children,**
13 **Never Obtains Their Express Written Consent to Collect the Same, and,**
Instead, Hides the Fact that It Systematically Collects Users’ Biometrics in
violation of BIPA, COPPA, CalOPPA, and the CCPA

14 61. Since Smart Facial Tagging debuted in 2014, Shutterfly has been intentionally
15 elusive in explaining how the technology works. First, Shutterfly does not directly inform users
16 that it collects, captures, and obtains faceprints from users and all of the individuals in the photos
17 uploaded by users. In fact, even though this technology has been in use for six years, Shutterfly
18 still does not require users to acknowledge its collection of their biometric data, much less obtain
19 a written release from them before collecting their faceprints. Instead, Shutterfly markets its
20 organization and Smart Facial Tagging as convenience features, often with advertisements under
21 the heading “Smart facial tagging makes finding friends and family a breeze.”²⁷ And nothing in
22 those seemingly innocuous advertisements gives any indication that use of the feature would
23 come at the cost of users’ biometric privacy rights.

24
25
26 ²⁶ See [http://www.shutterfly.com/shutterfly-](http://www.shutterfly.com/shutterfly-inc/privacy.html#:~:text=From%20time%20to%20time%20we,within%20our%20family%20of%20brands.)
27 [inc/privacy.html#:~:text=From%20time%20to%20time%20we,within%20our%20family%20of%20brands.](http://www.shutterfly.com/shutterfly-inc/privacy.html#:~:text=From%20time%20to%20time%20we,within%20our%20family%20of%20brands.)

28 ²⁷ See Figure 1.

1 62. Second, and despite it not preventing Shutterfly from collecting biometric data
2 even if a user did opt out, Shutterfly’s Smart Facial Tagging is an opt-out (not an opt-in)
3 program, so by default all users are automatically enrolled. Shutterfly makes it difficult to opt
4 out. In fact, since the Smart Facial Tagging feature was rolled out, Shutterfly has kept its
5 biometric data collection practices out of its privacy policies and has instead included ambiguous
6 statements about the true nature of its data collection practices and how a user can opt out.
7 According to its vague privacy policy, a user must affirmatively opt out by notifying Shutterfly
8 of the user’s preferences, but even then, Shutterfly makes no promises about its ability to respect
9 those preferences:

10 You can notify us of your preferences when you create an account
11 with us, and if you would like to review, correct or delete your
12 account information on our Sites and Apps, you can do so by
13 logging in to your account or by contacting us directly. There may
14 be times when we are unable to fulfill your request – for example,
15 if providing access to your personal information would reveal
16 confidential commercial or proprietary information or personal
17 information about someone else (and we cannot separate your
18 data), if we are prohibited by law from disclosing the information,
19 or if we have a legal obligation to retain certain data. We may
20 require additional personal information from you for the purposes
21 of verifying your identity and rights.

22 63. Third, and compounding the automatic enrollment violation, Shutterfly does not
23 notify its users, nor does it require its users to acknowledge or provide written consent to its
24 collection of biometric data. This violates BIPA, COPPA, CalOPPA, and the CCPA. In fact, in
25 its privacy policy, Shutterfly **explicitly denies that it collects personally identifiable**
26 **information of children:** “We will not knowingly collect personally identifiable information
27 from children. If we become aware that a child under the age of 13 has provided personal
28 information through our websites or apps, we will remove their personally identifiable
information from our files.”²⁸

 64. Fourth, and further compounding the automatic enrollment violation, Shutterfly
does not require its users to acknowledge or provide written consent to its collection of biometric

²⁸ See Shutterfly’s Privacy Policy, available at <https://www.shutterflyinc.com/privacy/#what-personal-info>, last accessed on July 8, 2020.

1 data, and in violation of BIPA, Shutterfly's website does not have a written, publicly available
2 policy identifying its biometrics retention schedule, nor guidelines for permanently destroying
3 users' biometric identifiers when they are no longer needed.

4 65. Thus, BIPA, COPPA, CalOPPA, and the CCPA clearly prohibit Shutterfly's
5 flagrant violations of the Classes' biometric privacy rights. Shutterfly has known that it is
6 collecting biometric data and personally identifying information of children since at least 2016,
7 has known this is a violation of BIPA, COPPA, CalOPPA, and now the recently enacted CCPA,
8 and yet has made no effort to come into compliance with any of these statutes at any point during
9 the past four years.

10 **IX. Facts Specific to Plaintiffs L.P., a minor, E.P., a minor, S.P., a minor, D.P., a**
11 **minor, F.P., a minor, R.P., a minor, and A.P., a minor**

12 66. Plaintiffs L.P., E.P., S.P., D.P., F.P., R.P., and A.P., all minors, do not have
13 Shutterfly accounts and have never consented, neither on their own behalf nor through their
14 parent or guardian, to Shutterfly's use, collection, and storage of their biometric data.

15 67. L.P., E.P., S.P., D.P., F.P., R.P., and A.P.'s parent and guardian, Esther Yona
16 Posner, has been a Shutterfly user since 2007. Since then, L.P., E.P., S.P., D.P., F.P., R.P., and
17 A.P.'s parent has uploaded thousands of photographs to her account that include images of L.P.,
18 E.P., S.P., D.P., F.P., R.P., or A.P.s' faces from 2008 to present.

19 68. L.P., E.P., S.P., D.P., F.P., R.P., and A.P.'s aunt has also uploaded photographs to
20 her Shutterfly account that include images of L.P., E.P., S.P., D.P., F.P., R.P., and A.P.'s faces.

21 69. L.P., E.P., S.P., D.P., F.P., R.P., and A.P., did not request or give permission –
22 written or otherwise – to Shutterfly to collect or store their biometric identifiers, nor did any of
23 them receive or sign a written release allowing Shutterfly to collect or store their biometric
24 identifiers. L.P., E.P., S.P., D.P., F.P., R.P., and A.P.'s parent did not request or give permission
25 – written or otherwise – to Shutterfly to collect or store the biometric identifiers of her children,
26 nor did she receive or sign a written release allowing Shutterfly to collect or store L.P., E.P.,
27 S.P., D.P., F.P., R.P., and A.P.'s biometric identifiers.

1 70. Shutterfly never even informed L.P., E.P., S.P., D.P., F.P., R.P., and A.P. or their
2 parent or guardian by written notice or otherwise that they could prevent Shutterfly from
3 collecting, storing or using L.P., E.P., S.P., D.P., F.P., R.P., and A.P.’s biometric identifiers.

4 71. Likewise, L.P., E.P., S.P., D.P., F.P., R.P., and A.P.’s parent was never provided
5 with an opportunity to prohibit or prevent Shutterfly from collecting, storing or using L.P., E.P.,
6 S.P., D.P., F.P., R.P., and A.P.’s biometric identifiers.

7 72. Nevertheless, when L.P., E.P., S.P., D.P., F.P., R.P., and A.P.’s parent uploaded
8 photographs of L.P., E.P., S.P., D.P., F.P., R.P., and A.P. to Shutterfly, Shutterfly extracted from
9 those photographs a unique faceprint or “template” for each child containing their biometric
10 identifiers, including their facial geometry, and identified who they were. Shutterfly
11 subsequently stored their biometric identifiers in its databases.

12 73. If L.P., E.P., S.P., D.P., F.P., R.P., and A.P.’s parent and guardian Yona Posner
13 had known about Shutterfly’s practices, she would not have uploaded photos of Plaintiffs L.P.,
14 E.P., S.P., D.P., F.P., R.P., and A.P.

15 74. Further, if L.P., E.P., S.P., D.P., F.P., R.P., and A.P.’s parent and guardian Yona
16 Posner had known about Shutterfly’s practices, she would have proactively requested that her
17 family members also not upload photos of her children to Shutterfly’s platform.

18 75. As a result of Shutterfly’s unauthorized collection and use of L.P., E.P., S.P.,
19 D.P., F.P., R.P., and A.P.’s biometric identifiers, L.P., E.P., S.P., D.P., F.P., R.P., and A.P. were
20 deprived of their control over that valuable information.

21 76. Accordingly, L.P., E.P., S.P., D.P., F.P., R.P., and A.P. have additionally suffered
22 damages in the diminution in value of their sensitive biometric identifiers.

23 **X. Facts Specific to Plaintiff N.T., a minor**

24 77. Plaintiff N.T., a minor, does not have a Shutterfly account and has never
25 consented, neither on her own behalf nor through her parent or guardian, to Shutterfly’s use,
26 collection, or storage of her biometric data.

1 78. N.T.'s parent and guardian, Ilya Tsorin, has been a Shutterfly user since 2018.
2 Since then, N.T.'s parent and guardian has uploaded 546 photographs to his account that include
3 images of N.T.'s face.

4 79. N.T. did not request or give permission – written or otherwise – to Shutterfly to
5 collect or store her biometric identifiers, nor did she receive or sign a written release allowing
6 Shutterfly to collect or store her biometric identifiers. N.T.'s parent did not request or give
7 permission – written or otherwise – to Shutterfly to collect or store the biometric identifiers of
8 his child, nor did he receive or sign a written release allowing Shutterfly to collect or store N.T.'s
9 biometric identifiers.

10 80. Shutterfly never even informed N.T. or her parent or guardian by written notice or
11 otherwise that they could prevent Shutterfly from collecting, storing or using N.T.'s biometric
12 identifiers.

13 81. Likewise, neither N.T. nor her parent or guardian were provided with an
14 opportunity to prohibit or prevent Shutterfly from collecting, storing or using N.T.'s biometric
15 identifiers.

16 82. Nevertheless, when N.T.'s parent uploaded photographs of N.T. to Shutterfly,
17 Shutterfly extracted from those photographs a unique faceprint or “template” for N.T.
18 containing her biometric identifiers, including her facial geometry, and identified who N.T. was.
19 Shutterfly subsequently stored N.T.'s biometric identifiers in its databases.

20 83. If N.T.'s parent and guardian, Ilya Tsorin, had known about Shutterfly's practices,
21 he would not have uploaded photos of Plaintiff N.T.

22 84. As a result of Shutterfly's unauthorized collection and use of N.T.'s biometric
23 identifiers, N.T. was deprived of her control over that valuable information.

24 85. Accordingly, N.T. has additionally suffered damages in the diminution in value of
25 her sensitive biometric identifiers.

26
27
28

1 **XI. Facts Specific to Plaintiff C.D., a minor**

2 86. Plaintiff C.D., a minor, does not have a Shutterfly account and has never
3 consented, neither on her own behalf nor through her parent or guardian, to Shutterfly’s use,
4 collection, and storage of her biometric data.

5 87. C.D.’s parent and guardian, Katherine Delgado, has been a Shutterfly user since
6 December 2015. Since then, C.D.’s parent has uploaded over 500 photographs to her account
7 that include images of C.D.’s face.

8 88. Lifetouch, a subsidiary of Shutterfly, has uploaded six photos of C.D. to
9 Katherine Delgado’s Shutterfly account.

10 89. When clicking the tab “people,” Shutterfly identifies C.D.’s name with her
11 pictures.

12 90. C.D. did not request or give permission – written or otherwise – to Shutterfly to
13 collect or store her biometric identifiers, nor did she receive or sign a written release allowing
14 Shutterfly to collect or store her biometric identifiers. C.D.’s parent did not request or give
15 permission – written or otherwise – to Shutterfly to collect or store the biometric identifiers of
16 her child, nor did she receive or sign a written release allowing Shutterfly to collect or store
17 C.D.’s biometric identifiers.

18 91. Shutterfly never even informed C.D. or her parent or guardian by written notice or
19 otherwise that they could prevent Shutterfly from collecting, storing or using C.D.’s biometric
20 identifiers.

21 92. Likewise, neither C.D. nor her parent or guardian were provided with an
22 opportunity to prohibit or prevent Shutterfly from collecting, storing or using C.D.’s biometric
23 identifiers.

24 93. Nevertheless, when C.D.’s parent uploaded photographs of C.D. to Shutterfly,
25 Shutterfly extracted from those photographs a unique faceprint or “template” for C.D. containing
26 her biometric identifiers, including her facial geometry. Shutterfly subsequently stored C.D.’s
27 biometric identifiers in its databases.

28

1 94. If C.D.'s parent and guardian, Katherine Delgado, had known about Shutterfly's
2 practices, she would not have uploaded photos of Plaintiff C.D.

3 95. As a result of Shutterfly's unauthorized collection and use of C.D.'s biometric
4 identifiers, C.D. was deprived of her control over that valuable information.

5 96. Accordingly, C.D. has additionally suffered damages in the diminution in value of
6 her sensitive biometric identifiers.

7 **XII. Facts Specific to Plaintiff V.M., a minor**

8 97. Plaintiff V.M., a minor, does not have a Shutterfly account and has never
9 consented, neither on her own behalf nor through her parent or guardian, to Shutterfly's use,
10 collection, and storage of her biometric data.

11 98. V.M.'s parent and guardian, Eunice Morris, has been a Shutterfly user since 2006.
12 Since then, V.M.'s parent has uploaded thousands of photographs to her account that include
13 images of V.M.'s face, including during the past four years and since January 2020.

14 99. Additionally, V.M.'s aunt and grandfather have also uploaded photographs to
15 their Shutterfly account that include images of V.M.'s faces.

16 100. V.M. did not request or give permission – written or otherwise – to Shutterfly to
17 collect or store her biometric identifiers, nor did she receive or sign a written release allowing
18 Shutterfly to collect or store her biometric identifiers. V.M.'s parent did not request or give
19 permission – written or otherwise – to Shutterfly to collect or store the biometric identifiers of
20 her child, nor did she receive or sign a written release allowing Shutterfly to collect or store
21 V.M.'s biometric identifiers.

22 101. Shutterfly never even informed V.M. or her parent or guardian by written notice
23 or otherwise that they could prevent Shutterfly from collecting, storing or using V.M.'s biometric
24 identifiers.

25 102. Likewise, neither V.M. nor her parent or guardian were provided with an
26 opportunity to prohibit or prevent Shutterfly from collecting, storing or using V.M.'s biometric
27 identifiers.

28

1 103. Nevertheless, when V.M.’s parent uploaded photographs of V.M. to Shutterfly,
2 Shutterfly extracted from those photographs a unique faceprint or “template” for V.M.
3 containing her biometric identifiers, including her facial geometry. Shutterfly subsequently
4 stored V.M.’s biometric identifiers in its databases.

5 104. If V.M.’s parent and guardian, Eunice Morris, had known about Shutterfly’s
6 practices, she would not have uploaded photos of Plaintiff V.M.

7 105. Further, if V.M.’s parent and guardian Eunice Morris had known about
8 Shutterfly’s practices, she would have proactively requested that her family members also not
9 upload photos of her child to Shutterfly’s platform.

10 106. As a result of Shutterfly’s unauthorized collection and use of V.M.’s biometric
11 identifiers, V.M. was deprived of her control over that valuable information.

12 107. Accordingly, V.M. has additionally suffered damages in the diminution in value
13 of her sensitive biometric identifiers.

14 **XIII. Facts Specific to Plaintiffs A.S., a minor, Y.S., a minor, S.S., a minor, D.S., a**
15 **minor, and M.S., a minor**

16 108. Plaintiffs A.S., Y.S., S.S., D.S., and M.S., all minors, do not have Shutterfly
17 accounts and have never consented, neither on their own behalf nor through their parent or
18 guardian, to Shutterfly’s use, collection, and storage of their biometric data.

19 109. A.S., Y.S., S.S., D.S., and M.S.’s parent and guardian, Dina Shallman, has been a
20 Shutterfly user since 2001. Since then, A.S., Y.S., S.S., D.S., and M.S.’s parent has uploaded
21 thousands of photographs to her account that include images of A.S., Y.S., S.S., D.S., and M.S.’s
22 faces, including during the past four years and since January 2020.

23 110. Additionally, A.S., Y.S., S.S., D.S., and M.S.’s aunt has also uploaded
24 photographs to her Shutterfly account that include images of A.S., Y.S., S.S., D.S., and M.S.’s
25 faces.

26 111. A.S., Y.S., S.S., D.S., and M.S., did not request or give permission – written or
27 otherwise – to Shutterfly to collect or store their biometric identifiers, nor did any of them
28 receive or sign a written release allowing Shutterfly to collect or store their biometric identifiers.

1 A.S., Y.S., S.S., D.S., and M.S.’s parent did not request or give permission – written or otherwise
2 – to Shutterfly to collect or store the biometric identifiers of her children, nor did she receive or
3 sign a written release allowing Shutterfly to collect or store A.S., Y.S., S.S., D.S., and M.S.’s
4 biometric identifiers.

5 112. Shutterfly never even informed A.S., Y.S., S.S., D.S., and M.S. or their parent or
6 guardian by written notice or otherwise that they could prevent Shutterfly from collecting,
7 storing or using A.S., Y.S., S.S., D.S., and M.S.’s biometric identifiers.

8 113. Likewise, A.S., Y.S., S.S., D.S., and M.S.’s parent was never provided with an
9 opportunity to prohibit or prevent Shutterfly from collecting, storing or using A.S., Y.S., S.S.,
10 D.S., and M.S.’s biometric identifiers.

11 114. Nevertheless, when A.S., Y.S., S.S., D.S., and M.S.’s parent uploaded
12 photographs of A.S., Y.S., S.S., D.S., and M.S. to Shutterfly, Shutterfly extracted from those
13 photographs a unique faceprint or “template” for each child containing their biometric
14 identifiers, including their facial geometry, and identified who they were. Shutterfly
15 subsequently stored their biometric identifiers in its databases.

16 115. If A.S., Y.S., S.S., D.S., and M.S.’s parent and guardian Dina Shallman had
17 known about Shutterfly’s practices, she would not have uploaded photos of Plaintiffs A.S., Y.S.,
18 S.S., D.S., and M.S..

19 116. Further, if A.S., Y.S., S.S., D.S., and M.S.’s parent and guardian Dina Shallman
20 had known about Shutterfly’s practices, she would have proactively requested that her family
21 members also not upload photos of her children to Shutterfly’s platform.

22 117. As a result of Shutterfly’s unauthorized collection and use of A.S., Y.S., S.S.,
23 D.S., and M.S.’s biometric identifiers, A.S., Y.S., S.S., D.S., and M.S. were deprived of their
24 control over that valuable information.

25 118. Accordingly, A.S., Y.S., S.S., D.S., and M.S. have additionally suffered damages
26 in the diminution in value of their sensitive biometric identifiers.

27
28

CLASS ALLEGATIONS

119. **Class Definitions:** Plaintiffs L.P., a minor, E.P., a minor, S.P., a minor, D.P., a minor, F.P., a minor, R.P., a minor, and A.P., a minor, by and through their legal guardian Esther Yona Posner; N.T., a minor, by and through her legal guardian Ilya Tsorin; and C.D., a minor, by and through her legal guardian Katherine Delgado, V.M., a minor, by and through her legal guardian Eunice Morris; A.S., a minor, Y.S., a minor, S.S., a minor, D.S., a minor, and M.S., a minor by and through their legal guardian Dina Shallman, bring this action pursuant to Fed. R. Civ. P. 23 on behalf of themselves and four classes of similarly situated individuals. The first Class Plaintiffs seek to represent is the “BIPA Class” and is defined as follows:

All individuals who as a minor under the age of 18 had their biometric identifiers, faceprints, or face templates collected, captured, received, or otherwise obtained by Shutterfly while residing in Illinois during the period from February 1, 2016 to present.

The second Class Plaintiffs seek to represent is the “COPPA Class” and is defined as follows:

All individuals who while under the age of 13 had their biometric identifiers, faceprints, or face templates collected, captured, received, or otherwise obtained by Shutterfly while residing in the United States during the period from July 24, 2016 to present.

The third Class Plaintiffs seek to represent is the “CalOPPA Class” and is defined as follows:

All individuals who while under the age of 16 had their biometric identifiers, faceprints, or face templates collected, captured, received, or otherwise obtained by Shutterfly while residing in the United States during the period from July 24, 2016 to present.

The fourth Class Plaintiffs seek to represent is the “CCPA Class” and is defined as follows:

All individuals who while under the age of 16 had their biometric identifiers, faceprints, or face templates collected, captured, received, or otherwise obtained by Shutterfly while residing in California during the period from January 1, 2020 to present.

The following people are excluded from the Classes: (1) any Judge or Magistrate presiding over this action and members of their immediate families; (2) Defendant’s and its parent’s and subsidiaries’ current or former employees, officers and directors, and members of their

1 immediate families; (3) persons who properly submit a timely request for exclusion from the
2 Class(es) of which they are a member; (4) persons whose claims in this matter have been finally
3 adjudicated on the merits or otherwise released; (5) Plaintiffs' counsel and Defendant's counsel
4 and members of their immediate families; and (6) the legal representatives, successors, and
5 assigns of any such excluded persons.

6 120. The BIPA, COPPA, CalOPPA, and CCPA Classes are, at times, collectively
7 referred to as the "Classes."

8 121. **Numerosity:** The exact number of members of the Classes is unknown to
9 Plaintiffs at this time, but it is clear that individual joinder is impracticable. Defendant has
10 collected, captured, received, or otherwise obtained biometric identifiers from at least thousands
11 (and potentially even millions) of individuals who fall into the definitions of the Classes.
12 Ultimately, members of the Classes will be easily identified through Defendant's records.

13 122. **Commonality and Predominance:** There are many questions of law and fact
14 common to the claims of Plaintiffs and the Classes, and those questions predominate over any
15 questions that may affect individual members of the Classes. The facts common to all Classes
16 include:

- 17 • whether Shutterfly collected, captured, received, or otherwise obtained the
18 biometric information of Plaintiffs and the Classes;
- 19 • whether Shutterfly properly informed Plaintiffs and the Classes that it collected,
20 used, and stored their biometric information;
- 21 • whether Shutterfly has sold, leased, traded, or otherwise profited from the
22 biometric information of Plaintiffs and the Classes;
- 23 • whether Shutterfly had and made available to the public, written policies
24 concerning the collection and retention of biometric information and, if so,
25 whether Shutterfly followed its written policies; and

26 123. With respect to the BIPA Class, common questions include:

- 27 • whether Shutterfly collected, captured, received, or otherwise obtained
28 Plaintiffs' and the Class's biometric identifiers over the past four years;

1 • whether Shutterfly properly informed Plaintiffs and the Class that it
2 collected, used, and stored their biometric identifiers;

3 • whether Shutterfly obtained a written release, as defined in 740 ILCS
4 14/10, from Plaintiffs and the Class to collect, capture, or otherwise obtain their biometric
5 identifiers;

6 • whether Shutterfly has sold, leased, traded, or otherwise profited from
7 Plaintiffs' and the Class's biometrics identifiers;

8 • whether Shutterfly had and made available to the public, a written policy
9 establishing a retention schedule and guidelines for permanently destroying biometric identifiers
10 in compliance with BIPA; and

11 • whether Shutterfly's violations of BIPA were committed intentionally,
12 recklessly, or negligently.

13 With respect to the COPPA Class, common questions include:

14 • whether Shutterfly collected, captured, received, or otherwise obtained
15 biometric identifiers from Plaintiffs and other children under the age of 13 over the past four
16 years;

17 • whether Shutterfly properly informed Plaintiffs and the Class that it
18 collected, used, and stored their biometric identifiers; and

19 • whether Shutterfly obtained "verifiable parental consent" before
20 collecting, using, storing, or disclosing biometric identifiers of COPPA Class members.

21 With respect to the CalOPPA Class, common questions include:

22 • whether Shutterfly collected, captured, received, or otherwise obtained
23 biometric identifiers from Plaintiffs and other children under the age of 16;

24 • whether Shutterfly conspicuously posted its privacy policy on its website;

25 • whether Shutterfly's privacy policy identifies the categories of personally
26 identifiable information that it collects through the website or online service about individual
27 consumers who use or visit its website; and

28

1 • whether Shutterfly’s privacy policy identifies the third-party persons or
2 entities with whom the operator may share that personally identifiable information.

3 With respect to the CCPA Class, common questions include:

4 • whether Shutterfly collected, captured, received, or otherwise obtained
5 biometric identifiers from Plaintiffs and other children under the age of 16 over the past four
6 years;

7 • whether Shutterfly properly informed Plaintiffs and the Class that it
8 collected, used, and stored their biometric identifiers;

9 • whether Shutterfly obtained “explicit parental consent” before collecting,
10 using, storing, or disclosing biometric identifiers of CCPA Class members; and

11 • whether Shutterfly improperly sold, leased, traded, or otherwise profited
12 from Plaintiffs and the Class’ biometric information.

13 124. **Typicality:** Plaintiffs’ claims are typical of the claims of all other members of the
14 Classes. Plaintiffs and members of the Classes sustained substantially similar damages as a
15 result of Defendant’s uniform wrongful conduct, based upon the same transactions that were
16 made uniformly with Plaintiffs and the Classes.

17 125. **Adequate Representation:** Plaintiffs will fairly and adequately represent and
18 protect the interests of the Classes. Plaintiffs have retained counsel with substantial experience
19 in prosecuting complex class actions. Plaintiffs and their counsel are committed to vigorously
20 prosecuting this action on behalf of the members of the Classes and have the financial resources
21 to do so. Neither Plaintiffs nor their counsel have any interest adverse to those of the other
22 members of the Classes, and Defendant has no defense unique to Plaintiffs.

23 126. **Policies Generally Applicable to the Classes:** Defendant has acted or failed to
24 act on grounds generally applicable to Plaintiffs and the other members of the Classes, requiring
25 the Court’s imposition of uniform relief to ensure compatible conduct towards the Classes.

26 127. **Superiority:** A class action is superior to all other available methods for the fair
27 and efficient adjudication of this controversy and joinder of all members of the Classes is
28 impracticable. The damages suffered by the individual members of the Classes are likely to have

1 been small relative to the burden and expense of individual prosecution of the complex litigation
 2 necessitated by Defendant's wrongful conduct. Thus, it would be virtually impossible for the
 3 individual members of the Classes to obtain effective relief from Defendant's misconduct. Even
 4 if members of the Classes could sustain the cost of such individual litigation, it would not be
 5 preferable to a class action because individual litigation would increase the delay and expense to
 6 all parties due to the complex legal and factual controversies presented in this Complaint, lead to
 7 potentially inconsistent individual decisions affecting members of the Classes, and present a
 8 tremendous burden for the courts. By contrast, a class action presents far fewer management
 9 difficulties and provides the benefits of single adjudication, economies of scale, and
 10 comprehensive supervision by a single court. Economies of time, effort, and expense will be
 11 fostered and uniformity of decisions affecting all members of the Classes will be achieved.

12 128. Plaintiffs reserve the right to revise the foregoing class allegations and definitions
 13 based on facts learned and legal developments following additional investigation, discovery or
 14 otherwise.

15 **FIRST CAUSE OF ACTION**

16 **Violation of 740 ILCS 14/15(b)** 17 **(On Behalf of the BIPA Class)**

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

19 130. BIPA makes it unlawful for any private entity to, among other things,

20 collect, capture, purchase, receive through trade, or otherwise
 21 obtain a person's or a customer's biometric identifier . . . unless it
 22 first: (1) informs the subject . . . in writing that a biometric
 23 identifier . . . is being collected or stored; (2) informs the subject
 24 . . . in writing of the specific purpose and length of term for which
 25 a biometric identifier . . . is being collected, stored, and used; *and*
 26 (3) receives a written release executed by the subject of the
 27 biometric identifier.

28 740 ILCS 14/15(b) (emphasis added).

131. Shutterfly is a Delaware corporation and thus qualifies as a "private entity" under
 BIPA. *See* 740 ILCS 14/10.

1 132. As explained in detail in Section III above, Plaintiffs’ and the Classes’ faceprints
2 or face geometry are “biometric identifiers” pursuant to 740 ILCS 14/10.

3 133. Shutterfly systematically and automatically collected, used, and stored Plaintiffs’
4 and the Classes’ biometric identifiers without first obtaining the specific written release required
5 by 740 ILCS 14/15(b)(3).

6 134. As explained in Section III.A, Shutterfly did not properly inform Plaintiffs or the
7 Classes in writing that their biometric identifiers were being collected and stored, nor did it
8 inform them in writing of the specific purpose and length of term for which their biometric
9 identifiers were being collected, stored, and used, as required by 740 ILCS 14/15(b)(1)–(2).

10 135. By collecting, storing, and using Plaintiffs’ and the Classes’ biometric identifiers
11 as described herein, Shutterfly violated Plaintiffs’ and the Classes’ rights to privacy of their
12 biometric identifiers, as set forth in BIPA, 740 ILCS 14/1, *et seq.*

13 136. On behalf of themselves and the Classes, Plaintiffs seek: (i) injunctive and
14 equitable relief as is necessary to protect the interests of Plaintiffs and the Classes by requiring
15 Shutterfly to comply with BIPA’s requirements for the collection, storage, and use of biometric
16 identifiers; (ii) statutory damages of \$5,000 per intentional or reckless violation of BIPA
17 pursuant to 740 ILCS 14/20(2), and statutory damages of \$1,000 per negligent violation of BIPA
18 pursuant to 740 ILCS 14/20(1); and (iii) reasonable attorneys’ fees and costs and other litigation
19 expenses pursuant to 740 ILCS 14/20(3).

20 **SECOND CAUSE OF ACTION**

21 **Violation of 740 ILCS 14/15(a)**
22 **(On Behalf of the BIPA Class)**

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

24 138. Section 15(a) of BIPA requires that any
25 private entity in possession of biometric identifiers . . . must
26 develop a written policy, made available to the public, establishing
27 a retention schedule and guidelines for permanently destroying
28 biometric identifiers . . . when the initial purpose for collecting or
obtaining such identifiers . . . has been satisfied or within 3 years
of the individual’s last interaction with the private entity,
whichever occurs first[, and] . . . a private entity in possession of

1 biometric identifiers or biometric information must comply with its
2 established retention schedule and destruction guidelines.

3 740 ILCS 14/15(a).

4 139. Shutterfly does not publicly provide a retention schedule or guidelines for
5 permanently destroying Plaintiffs' biometric identifiers as specified by BIPA. *See* 740 ILCS
6 14/15(a).

7 140. Consequently, Shutterfly does not comply with any established retention schedule
8 or destruction guidelines. *Id.*

9 141. Accordingly, on behalf of themselves and the Classes, Plaintiffs seek:
10 (i) injunctive and equitable relief as is necessary to protect the interests of Plaintiffs and the
11 Classes by requiring Shutterfly to establish and make publicly available a policy for the
12 permanent destruction of biometric identifiers compliant with 740 ILCS 14/15(a); (ii) statutory
13 damages of \$5,000 per intentional or reckless violation of BIPA pursuant to 740 ILCS 14/20(2),
14 and statutory damages of \$1,000 per negligent violation of BIPA pursuant to 740 ILCS 14/20(1);
15 and (iii) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS
16 14/20(3).

17 **THIRD CAUSE OF ACTION**

18 **Violation of Cal. Bus. & Prof. Code § 17200, *et seq.***
19 **(On Behalf of the COPPA Class)**

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

21 143. Shutterfly engaged in business acts and practices deemed "unlawful" under the
22 Unfair Competition Law ("UCL") found at Section 17200, *et seq.*, of the Bus. & Prof. Code,
23 because, as alleged above, Shutterfly unlawfully collected, stored, and used the biometric
24 identifiers, biometric information, and other personally identifying information of Plaintiffs and
25 the other COPPA Class members without first obtaining the requisite parental consent in
26 violation of COPPA and FTC regulations.

27 144. Under COPPA, an operator of a website or online service that collects personal
28 information from children must provide notice to a child's parent about its data collection

1 practices and obtain verifiable parental consent prior to any collection or use of personal
2 information from children. A violation of this regulation is deemed unlawful. 16 C.F.R. § 312.3.

3 145. COPPA defines a “child” as “an individual under the age of 13.” 16 C.F.R.
4 §312.2.

5 146. Shutterfly is required to comply with the requirements set out in COPPA because
6 it has developed a platform for and strongly encourages the upload of pictures of babies and
7 children on its website across the United States, including in Illinois, and has actual knowledge
8 that babies and children under the age of 13 are in pictures uploaded to its website.

9 147. Plaintiffs and the COPPA Class members are minor children under the age of 13
10 who had their “biometric identifiers” collected, captured, stored, and disclosed by Shutterfly.

11 148. Shutterfly is an “operator” as contemplated by 16 C.F.R. § 312.2 because it:

12 operates a Web site located on the Internet or an online service and
13 [] collects or maintains personal information from or about the
14 users of or visitors to such Web site or online service, or on whose
15 behalf such information is collected or maintained, or offers
16 products or services for sale through that Web site or online
17 service, where such Web site or online service is operated for
18 commercial purposes involving commerce among the several
19 States[.]

20 149. Shutterfly “collects” personal information from children under the age of 13
21 across the United States, including Illinois, because it takes the biometric identifiers in the form
22 of a face scan of every child’s face that is included in a photo uploaded to its website.

23 150. Pursuant to 16 C.F.R. § 312.4(a), “[i]t shall be the obligation of the operator to
24 provide notice and obtain verifiable parental consent prior to collecting, using, or disclosing
25 personal information from children. Such notice must be clearly and understandably written,
26 complete, and must contain no unrelated, confusing, or contradictory materials.”

27 151. As required by 16 C.F.R. § 312.4, Shutterfly failed to provide notice of its data
28 collection practices to Plaintiffs’ parents and to the parents of the other members of the COPPA
Class. Specifically, Shutterfly failed to give direct notice to parents stating the type of personal
information it collects from photographs.

1 152. Further, Shutterfly failed to obtain—or even adequately attempt to obtain—
2 parental consent authorizing it to collect and use minors’ personal and sensitive information from
3 Plaintiffs’ parents nor from the parents of any other COPPA Class member.

4 153. Each instance of Shutterfly’s nonconsensual and unauthorized collection and use
5 of Plaintiffs’ and other members of the COPPA Class’s personal information in one or more
6 ways described above constitutes a separate violation of COPPA and is thus a separate violation
7 of the UCL’s “unlawful” prong.

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

11 155. Shutterfly additionally engaged in business acts or practices deemed “unfair”
12 under the UCL because, as alleged above, Shutterfly failed to disclose during the Class Period
13 that it was collecting, storing, and using the biometric identifiers of Plaintiffs and the other
14 COPPA Class members without obtaining the requisite parental consent in violation of COPPA
15 and Federal Trade Commission regulations.

16 156. Unfair acts under the UCL have been interpreted using three different tests: (1)
17 whether the public policy, which is a predicate to a consumer unfair competition action under the
18 unfair prong of the UCL, is tethered to specific constitutional, statutory, or regulatory provisions;
19 (2) whether the gravity of the harm to the consumer, caused by the challenged business practice,
20 outweighs the utility of the defendant’s conduct; and (3) whether the consumer injury is
21 substantial, not outweighed by any countervailing benefits to consumers or competition, and is
22 an injury that consumers themselves could not reasonably have avoided. Defendant’s conduct is
23 unfair under each of these tests. As described above, Shutterfly’s conduct violates the policies
24 underlying privacy law, as well as COPPA itself. The gravity of the harm resulting from
25 Shutterfly’s secret collecting, storing, and using of biometric identifiers from children under the
26 age of 13, without the requisite parental consent, is significant and there is no corresponding
27 benefit to these children or their parents from such conduct. Lastly, because Plaintiffs and
28

1 COPPA Class members were completely unaware of Shutterfly's practices as alleged herein,
2 they could not possibly have avoided the privacy-based harms such practices caused.

3 157. Additionally, Shutterfly's conduct constitutes deceptive business practices in
4 violation of Cal. Bus. & Prof. Code §17200. Under the UCL, a business practice that is likely to
5 deceive an ordinary consumer constitutes a deceptive business practice. Shutterfly's conduct as
6 alleged herein was deceptive because Shutterfly intentionally and deceptively misled Plaintiffs,
7 by and through their legal guardians, by explicitly stating it does not collect personally
8 identifying information of children 13 and under in its privacy policy. Shutterfly made material
9 misrepresentations and omissions, both directly and indirectly, to Plaintiffs and members of the
10 COPPA Class, by and through their legal guardians, related to the invasive and unlawful
11 practices alleged herein.

12 158. Shutterfly's website, privacy policies, and marketing materials are silent as to its
13 BIPA and COPPA violative conduct detailed herein and its practices of otherwise invading the
14 privacy of children under the age of 13.

15 159. Finally, Shutterfly's secret and unlawful practices of collecting, storing, and using
16 the biometric identifiers of Plaintiffs and the other COPPA Class members without obtaining the
17 requisite parental consent, in violation of COPPA and Federal Trade Commission regulations,
18 take advantage of the lack of knowledge, ability, experience, or capacity of children and parents
19 across the United States to a grossly unfair degree.

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

23 161. Upon information and belief, Shutterfly's conduct surrounding the application of
24 facial recognition technology to all faces in the photos uploaded to its platform, including
25 children, was directed from its headquarters in California.

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

28

1 168. Biometric data is “personally identifiable information.”

2 169. Shutterfly violates CalOPPA because it does not identify in its privacy policy that
3 it collects biometric data through its website about individual consumers and all other
4 individuals, including children, in the photos uploaded to its platform.

5 170. Shutterfly violates CalOPPA because its privacy policy does not identify the
6 categories of third-party persons or entities with whom Shutterfly may share that biometric data.

7 171. Shutterfly violates CalOPPA because its privacy policy does not instruct
8 consumers regarding how the consumer can review and request changes to Shutterfly’s
9 collection of their biometric data.

10 172. Plaintiffs, individually and on behalf of the CalOPPA Class, by and through their
11 parents, seek: (i) an injunction requiring Shutterfly to revise its privacy policy to include that it
12 collects “biometric identifiers” from all faces, including of children, appearing in the pictures
13 uploaded to its platform; to delete such “biometric identifiers” already collected; and to
14 implement functionality sufficient to prevent the unlawful collection of such “biometric
15 identifiers” in the future; (ii) relief under Cal. Bus. & Prof. Code § 17200, *et seq.*, including, but
16 not limited to, restitution to Plaintiffs and other members of the CalOPPA class of money or
17 property Shutterfly acquired by means of its unlawful business practices; and, as a result of
18 bringing this action to vindicate and enforce an important right affecting the public interest, (iii)
19 reasonable attorney’s fees (pursuant to Cal. Code of Civ. P. § 1021.5).

20 **FIFTH CAUSE OF ACTION**

21 **Violation of the California Consumer Privacy Act**
22 **Cal. Civ. Code § 1798.100, *et seq.***
23 **(On Behalf of the CCPA Class)**

24 173. Plaintiffs incorporate by reference the foregoing allegations as if fully set forth
25 herein.

26 174. The California Consumer Privacy Act of 2018 (“CCPA”) went into effect on
27 January 1, 2020. This comprehensive privacy law was enacted to protect consumers’ personal
28 information from collection and use by businesses without appropriate notice and consent.

1 175. Through the above-detailed conduct, Shutterfly violated the CCPA by, among
2 other things, collecting and using personal information of minors without providing consumers
3 with adequate notice consistent with the CCPA, in violation of Civil Code section 1798.100(b).

4 176. Through the above-detailed conduct, Shutterfly violated the CCPA by, among
5 other things, collecting and using personal information of minors without providing consumers
6 with the right to have their information deleted consistent with the CCPA, in violation of Civil
7 Code section 1798.100(b).

8 177. Through the above-detailed conduct, Shutterfly violated the CCPA by, among
9 other things, selling the personal information of minors without requiring children under the age
10 of 16 to provide opt-in consent or parental or guardian consent for children under the age of 13
11 consistent with the CCPA, in violation of Civil Code section 1798.100(b).

12 178. In fact, the sale of personal information of minors equates to that of a data breach
13 wherein Shutterfly disclosed Plaintiffs' and the Class members' nonencrypted and nonredacted
14 personal information to other companies, likely for monetary gain. Such unauthorized disclosure
15 violates section 1798.150 and puts into the hands of other companies Plaintiffs' and the Class
16 members' highly sensitive biometric information as defined by section 1798.140.

17 179. In accordance with Civil Code section 1798.150(b), Plaintiff has served
18 Defendant with notice of these CCPA violations and a demand for relief by certified mail, return
19 receipt requested. However, in light of Shutterfly's policy proactively stating that it regularly
20 shares personal information it collects, without indicating such information includes biometric
21 data, it is unlikely Shutterfly can cure the violation by clawing back the data shared -- or know
22 whether that data has been further shared with additional parties.

23 180. On behalf of members of the CCPA Classes, Plaintiffs seek injunctive relief in the
24 form of an order enjoining Defendant from continuing to violate the CCPA. If Defendant fails to
25 properly respond to Plaintiffs' notice letter or agree to timely and adequately rectify the
26 violations detailed above, or, more likely, cannot rectify the violations detailed above, Plaintiffs
27 also will seek actual, punitive, and statutory damages in an amount not less than one hundred
28 dollars (\$100) and not greater than seven hundred and fifty (\$750) per consumer per incident,

1 whichever is greater; restitution; attorneys' fees and costs (pursuant to Cal. Code of Civ. P. §
2 1021.5) as a result of bringing this action to vindicate and enforce an important right affecting
3 the public interest; and any other relief the Court deems proper as a result of Defendant's CCPA
4 violations.

5 **PRAYER FOR RELIEF**

6 WHEREFORE, Plaintiffs L.P., a minor, E.P., a minor, S.P., a minor, D.P., a minor, F.P.,
7 a minor, R.P., a minor, and A.P., a minor, by and through their legal guardian Esther Yona
8 Posner; N.T., a minor, by and through her legal guardian Ilya Tsorin; and C.D., a minor, by and
9 through her legal guardian Katherine Delgado, V.M., a minor, by and through her legal guardian
10 Eunice Morris; A.S., a minor, Y.S., a minor, S.S., a minor, D.S., a minor, and M.S., a minor by
11 and through their legal guardian Dina Shallman, on behalf of themselves and the Classes,
12 respectfully request that this Court enter an Order:

13 A. Certifying this case as a class action on behalf of the Classes defined above,
14 appointing Plaintiffs L.P., a minor, E.P., a minor, S.P., a minor, D.P., a minor, F.P., a minor,
15 R.P., a minor, and A.P., a minor, by and through their legal guardian Esther Yona Posner; N.T., a
16 minor, by and through her legal guardian Ilya Tsorin; and C.D., a minor, by and through her
17 legal guardian Katherine Delgado, V.M., a minor, by and through her legal guardian Eunice
18 Morris; A.S., a minor, Y.S., a minor, S.S., a minor, D.S., a minor, and M.S., a minor by and
19 through their legal guardian Dina Shallman, as representatives of the Classes, and appointing
20 their counsel as Class Counsel for the Classes;

21 B. Declaring that Shutterfly's actions, as set out above, violate BIPA, 740 ILCS
22 14/1, *et seq.*;

23 C. Declaring that Shutterfly's actions, as set out above, violate COPPA and thus the
24 UCL, Cal. Bus. & Prof. Code §17200, *et seq.*, with respect to Plaintiffs and the COPPA Class;

25 D. Declaring that Shutterfly's actions, as set out above, violate CalOPPA and thus
26 the UCL, Cal. Bus. & Prof. Code §17200, *et seq.*, with respect to Plaintiffs and the CalOPPA
27 Class;

28

1 E. If Shutterfly does not cure the CCPA violations, Declaring that Shutterfly's
2 actions, as set out above, violate the CCPA, Cal. Civ. Code § 1798.100, *et seq.*, with respect to
3 California Plaintiffs and the CCPA Class;

4 F. Awarding statutory damages of \$5,000 per intentional or reckless violation of
5 BIPA pursuant to 740 ILCS 14/20(2) and statutory damages of \$1,000 per negligent violation of
6 BIPA pursuant to 740 ILCS 14/20(1);

7 G. Awarding injunctive and other equitable relief as is necessary to protect the
8 interests of the BIPA Class, including, among other things, an order requiring Shutterfly to
9 collect, store, and use biometric identifiers in compliance with BIPA, and to permanently destroy
10 the biometric identifiers it has collected from Plaintiffs and the BIPA Class members;

11 H. Awarding damages under Cal. Bus. & Prof. Code § 17200, *et seq.*, including, but
12 not limited to, restitution to Plaintiffs and other members of the COPPA class of money or
13 property Shutterfly acquired by means of its unfair, unlawful, and deceptive business practices;

14 I. Awarding injunctive and other equitable relief as is necessary to protect the
15 interests of the COPPA Class, including, among other things, an order requiring Shutterfly to
16 collect, store, and use biometric identifiers in compliance with COPPA, and to permanently
17 destroy the biometric identifiers it has collected from Plaintiffs and COPPA Class members;

18 J. Awarding damages under Cal. Bus. & Prof. Code § 17200, *et seq.*, including, but
19 not limited to, restitution to Plaintiffs and other members of the CalOPPA class of money or
20 property Shutterfly acquired by means of its unfair, unlawful, and deceptive business practices;

21 K. Awarding injunctive and other equitable relief as is necessary to protect the
22 interests of the CalOPPA Class, including, among other things, an order requiring Shutterfly to
23 collect, store, and use biometric identifiers in compliance with CalOPPA, and to permanently
24 destroy the biometric identifiers it has collected from Plaintiffs and CalOPPA Class members;

25 L. If Shutterfly does not cure the CCPA violations, awarding statutory damages of
26 \$750.00 per violation of the CCPA pursuant to Cal. Civ. Code § 1798.150;

27 M. Awarding injunctive and other equitable relief as is necessary to protect the
28 interests of the CCPA Class, including, among other things, an order requiring Shutterfly to

1 collect, store, and use biometric identifiers in compliance with CCPA, and to permanently
2 destroy the biometric identifiers it has collected from Plaintiffs and CCPA Class members;

3 G. Awarding Plaintiffs and the Classes their reasonable litigation expenses and
4 attorneys' fees pursuant to BIPA, the UCL, the common fund doctrine, and Cal. Code Civ. Proc.
5 § 1021.5;

6 H. Awarding Plaintiffs and the Classes pre- and post-judgment interest, to the extent
7 allowable; and

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

9 **JURY TRIAL**

10 Plaintiffs demand a trial by jury for all issues so triable.

11 DATED: July 23, 2020

12 /s/
13 James M. Wagstaffe (95535)
14 Frank Busch (258288)
15 WAGSTAFFE, VON LOEWENFELDT,
16 BUSCH & RADWICK LLP
17 100 Pine Street, Suite 725
18 San Francisco, CA 94111
19 Tel: (415) 357-8900
20 Fax: (415) 357-8910
21 wagstaffe@wvbrlaw.com

22 *Counsel for Plaintiffs and the Proposed Classes*

23 LABATON SUCHAROW LLP
24 Jonathan Gardner (*pro hac vice* to be submitted)
25 Melissa H. Nafash (*pro hac vice* to be submitted)
26 Jonathan D. Waisnor (*pro hac vice* to be
27 submitted)
28 140 Broadway
New York, NY 10005
Tel: (212) 907-0700
Fax: (212) 818-0477
jgardner@labaton.com
mnafash@labaton.com
jwaisnor@labaton.com

Counsel for Plaintiffs and the Proposed Classes