

1 BRIAN M. BOYNTON, Acting Assistant Attorney General, Civil Division  
 2 ARUN G. RAO, Deputy Assistant Attorney General  
 3 GUSTAV W. EYLER, Director, Consumer Protection Branch  
 4 LISA K. HSIAO, Assistant Director  
 5 ZACHARY A. DIETERT  
 6 DAVID G. CROCKETT  
 7 Trial Attorneys  
 8 Consumer Protection Branch  
 9 Civil Division, U.S. Department of Justice  
 10 450 5<sup>th</sup> Street, NW, Suite 6400-South  
 11 Washington, D.C. 20530  
 12 Telephone: (202) 616-9027 (Dietert)  
 13 (202) 305-7196 (Crockett)  
 14 Facsimile: (202) 514-8742  
 15 Zachary.A.Dietert@usdoj.gov  
 16 David.G.Crockett@usdoj.gov

17 Attorneys for Plaintiff  
 18 UNITED STATES OF AMERICA

19 UNITED STATES OF AMERICA,  
 20 Plaintiff,  
 21 v.  
 22 OPENX TECHNOLOGIES, INC.,  
 a Delaware Corporation,  
 Defendant.

Case No. 2:21-cv-09693

23 Plaintiff, the United States of America, acting upon notification and  
 24 authorization to the Attorney General by the Federal Trade Commission (“FTC” or  
 25 “Commission”), filed its Complaint for Civil Penalties, Permanent Injunction, and  
 26 Other Equitable Relief (“Complaint”), in this matter, pursuant to Sections 5(a)(1),  
 27 5(m)(1)(A), 13(b), 16(a)(1), and 19, of the Federal Trade Commission Act (“FTC  
 28 Act”), 15 U.S.C. §§ 45(a)(1), 45(m)(1)(A), 53(b), 56(a)(1), and 57(b), and Sections



1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

including such acts or practices involving foreign commerce that cause or are likely to cause reasonably foreseeable injury within the United States, or involve material conduct occurring within the United States.

For the purpose of this Order, the following definitions apply:

A. means any of Defendant’s products or services that enable or facilitate the marketing, sale, or purchase of digital or mobile advertising.

B.

1 a specific consumer, computer or device: (a) Personal Information;  
2 (b) Location Information; (c) behavioral data (e.g., videos viewed, ads  
3 viewed, pages clicked, etc.); and (d) profile data (e.g., age, gender,  
4 ethnicity, income net worth, political affiliation, etc.).

5 G. means OpenX Technologies, Inc. (“OpenX”), a  
6 corporation, and its successors and assigns.

7 H. means, with respect to Personal Information:

- 8 1. The Release of Personal Information Collected by an Operator  
9 from a Child in identifiable form for any purpose, except where an  
10 Operator provides such information to a person who provides  
11 Support for the Internal Operations of the Web site or Online  
12 Service; and
- 13 2. Making Personal Information Collected by an Operator from a  
14 Child publicly available in identifiable form by any means,  
15 including but not limited to a public posting through the Internet,  
16 or through a personal home page or screen posted on a Web site or  
17 online service; a pen pal service; an electronic mail service; a  
18 message board; or a chat room.

19 I. means collectively the myriad of computer and  
20 telecommunications facilities, including equipment and operating  
21 software, which comprise the interconnected world-wide network of  
22 networks that employ the Transmission Control Protocol/Internet  
23 Protocol, or any predecessor or successor protocols to such protocol, to  
24 communicate information of all kinds by wire, radio, or other methods of  
25 transmission.

26 J. means the following information, when  
27 linkable to a specific consumer, computer, or device: (a) information  
28 about a consumer’s location that is collected through an application

1 programming interface; or (b) information about a consumer's location  
2 that is inferred from basic service set identifiers (BSSIDs).

3 K. means making any  
4 reasonable effort (taking into consideration available technology) to  
5 ensure that before Personal Information is Collected from a Child, a  
6 Parent of the Child:

- 7 1. Receives notice of the Operator's Personal Information Collection,  
8 use, and Disclosure practices; and
- 9 2. Authorizes any Collection, use, and/or Disclosure of the Personal  
10 Information.

11 L. means an e-mail address or any other  
12 substantially similar identifier that permits direct contact with a person  
13 online, including but not limited to an instant messaging user identifier, a  
14 voice over internet protocol (VOIP) identifier, or a video chat user  
15 identifier.

16 M. means any person who operates a Web site located on the  
17 Internet or an online service and who Collects or maintains Personal  
18 Information from or about the users of or visitors to such Web site or  
19 online service, or on whose behalf such information is Collected or  
20 maintained, or offers products or services for sale through that Web site  
21 or online service, where such Web site or online service is operated for  
22 commercial purposes involving commerce among the several States or  
23 with one or more foreign nations; in any territory of the United States or  
24 in the District of Columbia, or bevins or

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

- Operator; or
- 2. The Operator benefits by allowing another Person to Collect Personal Information directly from users of such Web site or online service.
- N. includes a legal guardian.
- O. means any individual, partnership, corporation, trust, estate, cooperative, association, or other entity.
- P. means individually identifiable information about an individual Collected online, including:
  - 1. A first and last name;
  - 2. A home or other physical address including street name and name of a city or town;
  - 3. Online Contact Information;
  - 4. A screen or user name where it functions in the same manner as Online Contact Information;
  - 5. A telephone number;
  - 6. A Social Security number;
  - 7. A persistent identifier that can be used to recognize a user over time and across different Web sites or online services. Such persistent identifier includes but is not limited to a customer number held in a cookie, an IP address, a processor or device serial number, or unique device identifier;
  - 8. A photograph, video, or audio file where such file contains a Child's image or voice;
  - 9. Geolocation information sufficient to identify street name and name of a city or town; or
  - 10. Information concerning the Child or the Parents of that Child that the Operator Collects online from the Child and combines with an

1 identifier described in this definition.

2 Q. means the sharing, selling, renting,  
3 or transfer of Personal Information to any Third Party.

4 R. means an entity that performs services for and at the  
5 direction of Defendant. Provided, however, that an entity does not  
6 become a Service Provider solely because of that entity's marketing,  
7 purchase, or sale of digital advertisements in an Ad Tech Service  
8 operated by Defendant.

9 S.  
10 means

- 11 1. Those activities necessary to:
  - 12 a. Maintain or analyze the functioning of the Web site or  
13 online service;
  - 14 b. Perform network communications;
  - 15 c. Authenticate users of, or personalize the content on, the Web  
16 site or online service;
  - 17 d. Serve contextual advertising on the Web site or online  
18 service or cap the frequency of advertising;
  - 19 e. Protect the security or integrity of the user, Web site, or  
20 online service;
  - 21 f. Ensure legal or regulatory compliance; or
  - 22 g. Fulfill a request of a Child as permitted by § 312.5(c)(3) and  
23 (4) of the COPPA Rule;
- 24 2. So long as the information Collected for the activities listed in  
25 (1)(a) – (g) of this definition is not used or Disclosed to contact a  
26 specific individual, including through behavioral advertising, to  
27 amass a profile on a specific individual, or for any other purpose.

28 T. means any Person who is not:

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

1. An Operator with respect to the Collection or maintenance of Personal Information on the Web site or online service; or
2. A Person who provides Support for the Internal Operations of the Web site or Online Service and who does not use or Disclose information protected under this part for any other purpose.

U. means a commercial Web site or online service, or portion thereof that is targeted to Children.

IT IS ORDERED that Defendant and Defendant's officers, agents, employees, and attorneys who receive actual notice of this Order, whether acting directly or indirectly, in connection with Defendant operating a Web site or Online Service Directed to Children or operating a Web site or online service that has actual knowledge that it is Collecting or maintaining Personal Information from a Child, are hereby permanently restrained a



1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

- A. Consumers' ability to opt out of Defendant's Collection, maintenance, use, Disclosure of, or provision of access to Covered Information;
- B. The extent to which Defendant Collects, maintains, uses, Discloses, or provides access to Covered Information;
- C. The extent to which Defendant complies with the COPPA Rule and the measures Defendant takes to comply with the COPPA Rule; or
- D. The extent to which Defendant otherwise protects the privacy, security, availability, confidentiality, or integrity of Covered Information.

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28 .78003 797

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19

- 1 F. Assess, at least once every twelve (12) months, the sufficiency of any  
2 safeguards in place to address the internal and external risks to the  
3 privacy of Covered Information, and modify the Privacy Program based  
4 on the results;
- 5 G. Test and monitor the effectiveness of the safeguards at least once every  
6 twelve (12) months, and modify the Privacy Program based on the  
7 results;
- 8 H. Select and retain Service Providers capable of safeguarding Personal  
9 Information they access through or receive from Defendant, and  
10 contractually require Service Providers to implement and maintain  
11 safeguards sufficient to address the internal and external risks to the  
12 privacy of Personal Information; and
- 13 I. Evaluate and adjust the Privacy Program in light of any changes to  
14 Defendant's operations or business arrangements, new or more efficient  
15 technological or operational methods to control for the risks identified in  
16 Provision IV.D of this Order, or any other circumstances that Defendant  
17 knows or has reason to know may have an impact on the effectiveness of  
18 the Privacy Program or any of its individual safeguards. At a minimum,  
19 Defendant must evaluate the Privacy Program at least once every twelve  
20 (12) months and modify the Privacy Program based on the results.

21  
22 IT IS FURTHER ORDERED that, in connection with Defendant's  
23 compliance with Provision IV of this Order titled Mandated Privacy Program,  
24 Defendant must obtain initial and biennial assessments ("Assessments"):

- 25 A. The Assessments must be obtained from a qualified, objective,  
26 independent third-party professional ("Assessor"), who: (1) uses  
27 procedures and standards generally accepted in the profession;  
28 (2) conducts an independent review of the Privacy Program; (3) retains

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

evidence that the Assessor examined is (a) appropriate for assessing an enterprise of Defendant’s size, complexity, and risk profile; and (b) sufficient to justify the Assessor’s findings. No finding of any Assessment shall rely primarily on assertions or attestations by Defendant’s management. The Assessment must be signed by the Assessor, state that the Assessor conducted an independent review of the Privacy Program and did not rely primarily on assertions or attestations by Defendant’s management, and state the number of hours that each member of the assessment team worked on the Assessment. To the extent that Defendant revises, updates, or adds one or more safeguards required under Provision IV of this Order during an Assessment period, the Assessment must assess the effectiveness of the revised, updated, or added safeguard(s) for the time period in which it was in effect, and provide a separate statement detailing the basis for each revised, updated, or additional safeguard.

E. Each Assessment must be completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Unless otherwise directed by a Comm003.ssition 003.ssitionw2feguar567-.0007 Tw[(Ea



1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

(a) corrected or (b) disclosed to the Commission. The certification must be based on the personal knowledge of the senior corporate manager, senior officer, or subject matter experts upon whom the senior corporate manager or senior officer reasonably relies in making the certification.

B. Unless otherwise directed by a Commission representative in writing, submit all annual certifications to the Commission pursuant to this Order via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580. The subject line must begin, “United States v.



1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

payment or monetary judgment pursuant to this Order.

C. Defendant acknowledges that its Ta

1 responsibilities relating to the Collection, retention, storage, or security of  
2 Covered Information, and all agents and representatives who have  
3 managerial responsibility for the operation of any of Defendant's Web  
4 sites or online services; and (3) any business entity resulting from any  
5 change in structure as set forth in the Provision titled Compliance  
6 Reporting. Delivery must occur within seven (7) days of entry of this  
7 Order for current personnel. To all others, delivery must occur before  
8 they assume their responsibilities.

9 C. From each individual or entity to which Defendant delivered a copy of  
10 this Order, Defendant must obtain, within thirty (30) days, a signed and  
11 dated acknowledgment of receipt of this Order.

12  
13 IT IS FURTHER ORDERED that Defendant make timely submissions to  
14 the Commission:

15 A. One year after entry of this Order, Defendant must submit a compliance  
16 report, sworn under penalty of perjury, which does the following: (a)  
17 identify the primary physical, postal, and email address and telephone  
18 number, as designated points of contact, which representatives of the  
19 Commission and Plaintiff may use to communicate with Defendant; (b)  
20 identify all of Defendant's businesses by all of their names, telephone  
21 numbers, and physical, postal, email, and Internet addresses; (c) describe  
22 the activities of each business; (d) describe in detail whether and how  
23 Defendant is in compliance with each Provision of this Order; (e) provide  
24 a copy of each different version of any privacy notice posted on each  
25 Web site or online service operated by Defendant; (f) provide a statement  
26 setting forth OpenX's treatment of Child-directed Web sites and online  
27 services; and (g) provide a copy of each Order Acknowledgment  
28 obtained pursuant to this Order, unless previously submitted to the

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

Commission.

- B. For ten (10) years after entry of this Order, Defendant must submit a compliance notice, sworn under penalty of perjury, within fourteen (14) days of any change in the following: (a) any designated point of contact; or (b) the structure of Defendant or any entity that Defendant has any ownership interest in or controls directly or indirectly that may affect compliance obligations arising under this Order, including: creation, merger, sale, or dissolution of the entity or any subsidiary, parent, or affiliate that engages in any acts or practices subject to this Order.
- C. Defendant must submit to the Commission notice of the filing of any bankruptcy petition, insolvency proceeding, or similar proceeding by or against each Defendant within fourteen (14) days of its filing.
- D. Any submission to the Commission required by this Order to be sworn under penalty of perjury must be true and accurate and comply with 28 U.S.C. § 1746, such as by concluding: “I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on: \_\_\_\_\_” and supplying the date, signatory’s full name, title (if applicable), and signature.
- E. Unless otherwise directed by a Commission representative in writing, all submissions to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580. The subject line must begin: “United States v. OpenX Technologies, Inc.”

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

IT IS FURTHER ORDERED that Defendant must create certain records for ten (10) years after entry of the Order, and retain each such record for five (5) years. Specifically, Defendant must create and retain the following records:

- A. Accounting records showing the revenues from all goods or services sold;
- B. All records necessary to demonstrate full compliance with each provision of this Order, including all submissions to the Commission;
- C. Copies of all consumer complaints relating to Defendant’s Collection, maintenance, use, or Disclosure of Covered Information, whether received directly or indirectly, such as through a Third Party, and any response; and
- D. A copy of each materially different document widely disseminated or caused to be widely disseminated by Defendant containing any representation regarding Defendant’s Collection, maintenance, use, or Disclosure practices pertaining to Covered Information.

IT IS FURTHER ORDERED that, for the purpose of monitoring Defendant’s compliance with this Order, including any failure to transfer any assets as required by this Order:

- A. Within fourteen (14) days of receipt of a written request from a representative of the Commission or Plaintiff, Defendant must: submit additional compliance reports or other requested information, which must be sworn under penalty of perjury; appear for depositions; and produce documents for inspection and copying. The Commission and Plaintiff are also authorized to obtain discovery, without further leave of court, using any of the procedures prescribed by Federal Rules of Civil Procedure 29, 30 (including telephonic depositions), 31, 33, 34, 36, 45, and 69.



1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

BRIAN M. BOYNTON  
Acting Assistant Attorney General  
Civil Division

ARUN G. RAO  
Deputy Assistant Attorney General

GUSTAV W. EYLER  
Director  
Consumer Protection Branch

LISA K. HSIAO  
Assistant Director

/s/ Zachary A. Dietert  
ZACHARY A. DIETERT  
DAVID G. CROCKETT  
Trial Attorneys  
Consumer Protection Branch  
U.S. Department of Justice  
450 5<sup>th</sup> Street, NW, Suite 6400-South  
Washington, D.C. 20530  
Telephone: (202) 616-9027 (Dietert)  
                  (202) 305-7196 (Crockett)  
Facsimile: (202) 514-8742  
Zachary.A.Dietert@usdoj.gov  
David.G.Crockett@usdoj.gov

Dated: December 15, 2021

1 **FOR THE FEDERAL TRADE COMMISSION:**

2

3  
4 General Counsel

5 **KRISTIN COHEN**

Acting Associate Director

6

**MARK EICHORN**

Assistant Director

Division of Privacy and Identity Protection

8





1

DEFENDANT:

3

4

5

6

*Julia K Tama*

Date: Jun 15, 2021

7

Julia K Tama  
Venab LLP

8

Massachusetts Avenue, NW  
Washington, D.C. 20001

9

Tel: 202-344-4000

10

Email: J  
Counsel

nc.

11

12

13

14

DEFENDANT:

15

*Julia K Tama*

16

Date: 06/15/21

17

General Counsel  
OpenX Technologies, Inc.

18

19

20

21

22

23

26

28

# **APPENDIX A**

**List of Subjects in 16 CFR Part 312**

Children, Communications, Consumer protection, Electronic mail, Email, Internet, Online service, Privacy, Record retention, Safety, science and technology, Trade practices, Web site, Youth.

■ Accordingly, for the reasons stated above, the Federal Trade Commission revises part 312 of Title 16 of the Code of Federal Regulations to read as follows:

**PART 312—CHILDREN'S ONLINE  
PRIVACY PROTECTION RULE**

Sec.

- 312.1 Scope of regulations in this part.
- 312.2 Definitions.
- 312.3 Regulation of unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet.
- 312.4 Notice.
- 312.5 Parental consent.
- 312.6 Right of parent to review personal information provided by a child.
- 312.7 Prohibition against conditioning a child's participation on collection of personal information.

- 312.8 Confidentiality, security, and integrity of personal information collected from children.
- 312.9 Enforcement.
- 312.10 Data retention and deletion requirements.
- 312.11 Safe harbor programs.
- 312.12 Voluntary Commission Approval Processes.
- 312.13 Severability.

**Authority:** 15 U.S.C. 6501–6508.

**§ 312.1 Scope of regulations in this part.**

This part implements the Children's Online Privacy Protection Act of 1998, (15 U.S.C. 6501, *et seq.*) which prohibits unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet.

profile on a specific individual, or for any other purpose.

*t* means any person who is not:

(1) An operator with respect to the collection or maintenance of personal information on the Web site or online service; or

(2) A person who provides support for the internal operations of the Web site or online service and who does not use or disclose information protected under this part for any other purpose.

*t t t* means a commercial Web site or online service, or portion thereof, that is targeted to children.

(1) In determining whether a Web site or online service, or a portion thereof, is directed to children, the Commission will consider its subject matter, visual content, use of animated characters or child-oriented activities and incentives, music or other audio content, age of models, presence of child celebrities or celebrities who appeal to children, language or other characteristics of the Web site or online service, as well as whether advertising promoting or appearing on the Web site or online service is directed to children. The Commission will also consider competent and reliable empirical evidence regarding audience composition, and evidence regarding the intended audience.

(2) A Web site or online service shall be deemed directed to children when it has actual knowledge that it is collecting personal information directly from users of another Web site or online service directed to children.

(3) A Web site or online service that is directed to children under the criteria set forth in paragraph (1) of this

practices required under paragraph (d)  
of this section.

operator must delete such information from its records;

(2) Where the purpose of collecting a parent's online contact information is to provide voluntary notice to, and subsequently update the parent about, the child's participation in a Web site or online service that does not otherwise collect, use, or disclose children's personal information. In such cases, the parent's online contact information may not be used or disclosed for any other purpose. In such cases, the operator must make reasonable efforts, taking into consideration available technology, to ensure that the parent receives notice as described in § 312.4(c)(2);

(3) Where the sole purpose of collecting online contact information from a child is to respond directly on a one-time basis to a specific request from the child, and where such information is not used to re-contact the child or for any other purpose, is not disclosed, and is deleted by the operator from its records promptly after responding to the child's request;

(4) Where the purpose of collecting a child's and a parent's online contact information is to respond directly more than once to the child's specific request, and where such information is not used for any other purpose, disclosed, or combined with any other information collected from the child. In such cases, the operator must make reasonable efforts, taking into consideration available technology, to ensure that the parent receives notice as described in § 312.4(c)(3). An operator will not be deemed to have made reasonable efforts to ensure that a parent receives notice where the notice to the parent was unable to be delivered;

(5) Where the purpose of collecting a child's and a parent's name and online contact information, is to protect the safety of a child, and where such information is not used or disclosed for any purpose unrelated to the child's safety. In such cases, the operator must make reasonable efforts, taking into consideration available technology, to provide a parent with notice as described in § 312.4(c)(4);

(6) Where the purpose of collecting a child's name and online contact information is to:

(i) Protect the security or integrity of its Web site or online service;

(ii) Take precautions against liability;

(iii) Respond to judicial process; or

(iv) To the extent permitted under other provisions of law, to provide information to law enforcement agencies or for an investigation on a matter related to public safety; and where such information is not be used for any other purpose;

(7) Where an operator collects a persistent identifier and no other personal information and such identifier is used for the sole purpose of providing support for the internal operations of the Web site or online service. In such case, there also shall be no obligation to provide notice under § 312.4; or

(8) Where an operator covered under paragraph (2) of the definition of *t t t* in § 312.2 collects a persistent identifier and no other personal information from a user who affirmatively interacts with the operator and whose previous registration with that operator indicates that such user is not a child. In such case, there also shall be no obligation to provide notice under § 312.4.

**§ 312.6 Right of parent to review personal information provided by a child.**

(a) Upon request of a parent whose child has provided personal information to a Web site or online service, the operator of that Web site or online service is required to provide to that parent the following:

(1) A description of the specific types or categories of personal information collected from children by the operator, such as name, address, telephone number, email address, hobbies, and extracurricular activities;

(2) The opportunity at any time to refuse to permit the operator's further use or future online collection of personal information from that child, and to direct the operator to delete the child's personal information; and

(3) Notwithstanding any other provision of law, a means of reviewing any personal information collected from the child. The means employed by the operator to carry out this provision must:

(i) Ensure that the requestor is a parent of that child, taking into account available technology; and

(ii) Not be unduly burdensome to the availa() es, and 8)ng colT\* (Std (tion )Tj T\* by vidvymscitct2(avait fo goocularatinology; and (matt)tmbntld's personal inf further )Tj -0.ion c\* (c\*). Tdirappaicl inf further Priparelogy; and

that they meet the following performance standards:

(1) Program requirements that ensure operators subject to the self-regulatory program guidelines (“subject operators”) provide substantially the same or greater protections for children as those contained in §§ 312.2 through 312.8, and 312.10.

(2) An effective, mandatory mechanism for the independent assessment of subject operators’ compliance with the self-regulatory program guidelines. At a minimum, this mechanism must include a comprehensive review by the safe harbor program, to be conducted not less than annually, of each subject operator’s information policies, practices, and representations. The assessment mechanism required under this paragraph can be provided by an independent enforcement program, such as a seal program.

(3) Disciplinary actions for subject operators’ non-compliance with self-regulatory program guidelines. This performance standard may be satisfied by:

(i) Mandatory, public reporting of any action taken against subject operators by the industry group issuing the self-regulatory guidelines;

(ii) Consumer redress;

(iii) Voluntary payments to the United States Treasury in connection with an industry-directed program for violators of the self-regulatory guidelines;

(iv) Referral to the Commission of operators who engage in a pattern or practice of violating the self-regulatory guidelines; or

(v) Any other equally effective action.

(c) *t* . A proposed safe harbor program’s request for approval shall be accompanied by the following:

(1) A detailed explanation of the applicant’s business model, and the technological capabilities and mechanisms that will be used for initial and continuing assessment of subject operators’ fitness for membership in the safe harbor program;

(2) A copy of the full text of the guidelines for which approval is sought and any accompanying commentary;

(3) A comparison of each provision of §§ 312.2 through 312.8, and 312.10 with the corresponding provisions of the guidelines; and

(4) A statement explaining:

(i) How the self-regulatory program guidelines, including the applicable assessment mechanisms, meet the requirements of this part; and

(ii) How the assessment mechanisms and compliance consequences required

under paragraphs (b)(2) and (b)(3) provide effective enforcement of the requirements of this part.

(d) *t* . Approved safe harbor programs shall:

(1) By July 1, 2014, and annually thereafter, submit a report to the Commission containing, at a minimum, an aggregated summary of the results of the independent assessments conducted under paragraph (b)(2) of this section, a description of any disciplinary action taken against any subject operator under paragraph (b)(3) of this section, and a description of any approvals of member operators’ use of a parental consent mechanism, pursuant to § 312.5(b)(4);

(2) Promptly respond to Commission requests for additional information; and

(3) Maintain for a period not less than three years, and upon request make available to the Commission for inspection and copying:

(i) Consumer complaints alleging violations of the guidelines by subject operators;

(ii) Records of disciplinary actions taken against subject operators; and

(iii) Results of the independent assessments of subject operators’ compliance required under paragraph (b)(2) of this section.

(e) *P t- t t* .

Approved safe harbor programs must submit proposed changes to their guidelines for review and approval by the Commission in the manner required for initial approval of guidelines under paragraph (c)(2) of this section. The statement required under paragraph (c)(4) of this section must describe how the proposed changes affect existing provisions of the guidelines.

(f) *t t -* . The

Commission reserves the right to revoke any approval granted under this section if at any time it determines that the approved self-regulatory program guidelines or their implementation do not meet the requirements of this part. Safe harbor programs that were approved prior to the publication of the Final Rule amendments must, by March 1, 2013, submit proposed modifications to their guidelines that would bring them into compliance with such amendments, or their approval shall be revoked.

(g) *t ’ t t* . An operator will be deemed to be in compliance with the



---

<sup>401</sup> 15 U.S.C. 6501–6506.

<sup>402</sup> COPPA, 15 U.S.C. 6501(2), defines the term “operator” as “any person who operates a Web site located on the Internet or an online service and who collects or maintains personal information from or about users of or visitors to such Web site or online service, or on whose behalf such information is collected and maintained \* \* \*” As stated in the Statement of Basis and Purpose for the original COPPA Rule, “The definition of ‘operator’ is of central importance because it determines who is covered by the Act and the Rule.” Children’s





Important Information About Our Privacy Practices:

On [TO BE UPDATED], OpenX Technologies, Inc. (“OpenX”) reached a settlement with the Federal Trade Commission (“FTC”) to resolve allegations that OpenX collected, used, and transferred precise location data in the form of basic service set identifiers (“BSSIDs”), through software development kits (“SDKs”) offered prior to October 2018. At issue is that the BSSIDs were collected under circumstances where users had not granted or had denied requisite location permissions. The FTC also alleged that we failed to adequately comply with the Children’s Online Privacy Protection Act (“COPPA”) because, despite our policy of banning child-directed apps from participating in our Ad Exchange, we allowed some of these apps to participate in the Ad Exchange, resulting in targeted advertising to children absent parental notice and consent.

We have taken steps to address these issues. We stopped collecting BSSIDs in 2018, and we have tightened our practices to ensure that they comply with COPPA. That includes re-reviewing mobile apps to properly identify those that are child-directed and then banning those apps from participating in the OpenX Ad Exchange.