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
ZACHARY A. DIETERT
DAVID G. CROCKETT
Trial Attorneys
Consumer Protection Branch
Civil Division, U.S. Department of Justice
450 5th 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

Attorneys for Plaintiff
UNITED STATES OF AMERICA

IN THE UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA
WESTERN DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. OPENX TECHNOLOGIES, INC., a Delaware Corporation, Defendant.	Case No. 2:21-cv-09693 **STIPULATED ORDER FOR PERMANENT INJUNCTION AND CIVIL PENALTY JUDGMENT**

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

1303(c) and 1306(d) of the Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. §§ 6502(c) and 6505(d), and the Children's Online Privacy Protection Rule ("COPPA Rule"), 16 C.F.R. Part 312. Defendant has waived service of the summons and the Complaint. The parties have been represented by the attorneys whose names appear hereafter. Plaintiff and Defendant stipulate to the entry of this Stipulated Order for Permanent Injunction and Civil Penalty Judgment ("Order") to resolve all matters in dispute in this action between them.

THEREFORE, IT IS ORDERED as follows:

FINDINGS

1. This Court has jurisdiction over this matter.
2. The Complaint charges that Defendant violated the FTC Act by misrepresenting its Collection, use, and Disclosure of Covered Information and by misrepresenting its COPPA obligations and practices. The Complaint also charges that Defendant violated COPPA by failing to provide notice to Parents of their information practices and failing to Obtain Verifiable Parental Consent prior to Collecting, using, or Disclosing Personal Information from Children.
3. Defendant neither admits nor denies any of the allegations in the Complaint, except as specifically stated in this Order. Only for purposes of this action, Defendant admits the facts necessary to establish jurisdiction.
4. Defendant waives any claim that it may have under the Equal Access to Justice Act, 28 U.S.C. § 2412, concerning the prosecution of this action through the date of this Order, and agrees to bear its own costs and attorney fees.
5. Defendant and Plaintiff waive all rights to appeal or otherwise challenge or contest the validity of this Order.
6. This Order relates to activities in or affecting interstate commerce,

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.

DEFINITIONS

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

A. **"Ad Tech Service"** means any of Defendant's products or services that enable or facilitate the marketing, sale, or purchase of digital or mobile advertising.

B. **"Ad Request Data"** means data that Defendant collects or receives from any entity to prompt the service of an advertisement, to the extent that the data includes information capable of identifying a specific individual or individual's device.

C. **"Affirmative Express Consent"** means that, prior to the collection of any Location Information, the consumer has made an affirmative action to assent to the collection of that data. Provided, however, that an affirmative action does not include obtaining a consumer's approval for a preselected default option.

D. **"Child"** means an individual under the age of 13.

E. **"Collects"** or **"Collection"** means, with respect to Personal Information, the gathering of any Personal Information from a Child by any means, including but not limited to:

1. Requesting, prompting, or encouraging a Child to submit Personal Information online;
2. Enabling a Child to make Personal Information publicly available in identifiable form; or
3. Passive tracking of a Child online.

F. **"Covered Information"** means information linkable to a specific consumer, computer, or device, including the following when linkable to

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

G. **"Defendant"** means OpenX Technologies, Inc. ("OpenX"), a corporation, and its successors and assigns.

H. **"Disclose" or "Disclosure"** means, with respect to Personal Information:

1. The Release of Personal Information Collected by an Operator from a Child in identifiable form for any purpose, except where an Operator provides such information to a person who provides Support for the Internal Operations of the Web site or Online Service; and

2. Making Personal Information Collected by an Operator from a Child publicly available in identifiable form by any means, including but not limited to a public posting through the Internet, or through a personal home page or screen posted on a Web site or online service; a pen pal service; an electronic mail service; a message board; or a chat room.

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

J. **"Location Information"** means the following information, when linkable to a specific consumer, computer, or device: (a) information about a consumer's location that is collected through an application

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

K. **"Obtaining Verifiable Parental Consent"** means making any reasonable effort (taking into consideration available technology) to ensure that before Personal Information is Collected from a Child, a Parent of the Child:

1. Receives notice of the Operator's Personal Information Collection, use, and Disclosure practices; and

2. Authorizes any Collection, use, and/or Disclosure of the Personal Information.

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

M. **"Operator"** means 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 the users of or visitors to such Web site or online service, or on whose behalf such information is Collected or maintained, or offers products or services for sale through that Web site or online service, where such Web site or online service is operated for commercial purposes involving commerce among the several States or with one or more foreign nations; in any territory of the United States or in the District of Columbia, or between any such territory and another such territory or any State or foreign nation; or between the District of Columbia and any State, territory, or foreign nation. Personal Information is Collected or maintained on behalf of an Operator when:

1. It is Collected or maintained by an agent or service provider of the

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. **"Parent"** includes a legal guardian.

O. **"Person"** means any individual, partnership, corporation, trust, estate, cooperative, association, or other entity.

P. **"Personal Information"** 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

identifier described in this definition.

Q. **"Release of Personal Information"** means the sharing, selling, renting, or transfer of Personal Information to any Third Party.

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

S. **"Support for the Internal Operations of the Web site or Online Service"** means

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

T. **"Third Party"** 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.

U. **"Web site or Online Service Directed to Children"** means a commercial Web site or online service, or portion thereof that is targeted to Children.

ORDER

I. INJUNCTION CONCERNING COLLECTION OF PERSONAL INFORMATION FROM 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 and enjoined from (A) Collecting, using, and Disclosing Personal Information from Child-directed properties without Verifiable Parental Consent unless the Children's Online Privacy Protection Rule, 16 C.F.R. Part 312 (attached as Appendix A), provides an exception to Obtaining Verifiable Parental Consent, or (B) violating the Children's Online Privacy Protection Rule, 16 C.F.R. Part 312 (attached as Appendix A).

II. INJUNCTION PROHIBITING MISREPRESENTATIONS

IT IS FURTHER 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 any Defendant-operated Web site or online service, must not materially misrepresent in any manner, expressly or by implication:

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.

III. INJUNCTION REQUIRING CONSENT FOR COLLECTION OF LOCATION INFORMATION

IT IS FURTHER ORDERED that Defendant and Defendant's officers, agents, employees, and attorneys who receive actual notice of this Order, whether acting directly or indirectly, are permanently restrained and enjoined from collecting Location Information through Defendant's software development kit(s) for mobile applications without first confirming that:

A. The consumer has provided Affirmative Express Consent for the collection of Location Information to the mobile application that has integrated Defendant's software development kit(s);

B. The consumer has not expressed, through any applicable operating system, device, or mobile application permission or setting, that the consumer does not consent to, or revokes consent to, the collection of Location Information from such mobile application; and

C. The consumer has not expressed through any applicable operating system, device, or mobile application permission or setting, that the consumer's consent to the collection of Location Information from such mobile application is limited to a level of accuracy that is less precise than the Location Information that is to be collected or inferred by Defendant.

IV. MANDATED PRIVACY PROGRAM

IT IS FURTHER ORDERED that Defendant, and any business that Defendant controls directly, or indirectly, in connection with the Collection, maintenance, use, or Disclosure of, or provision of access to, Covered Information through an Ad Tech Service operated by Defendant, must, within sixty (60) days of issuance of this Order, establish and implement, and thereafter maintain, a comprehensive privacy program ("Privacy Program") that protects the privacy of such Covered Information. To satisfy this requirement, Defendant must, at a minimum:

A. Document in writing the content, implementation, and maintenance of the Privacy Program;

B. Provide the written program and any evaluations thereof or updates thereto to Defendant's board of directors or governing body or, if no such board or equivalent governing body exists, to a senior officer of Defendant responsible for Defendant's Privacy Program at least once every twelve (12) months;

C. Designate a qualified employee or employees to coordinate and be responsible for the Privacy Program;

D. Assess and document, at least once every twelve (12) months, internal and external risks to the privacy of Covered Information that could result in the unauthorized Collection, maintenance, use, or Disclosure of, or provision of access to, Covered Information;

E. Design, implement, maintain, and document safeguards that control for the material internal and external risks Defendant identifies to the privacy of Covered Information identified in response to sub-Provision IV.D. Each safeguard must be based on the volume and sensitivity of the Covered Information that is at risk, and the likelihood that the risk could be realized and result in the unauthorized Collection, maintenance, use,

or Disclosure of, or provision of access to, Covered Information. Such safeguards must also include:

1. Regular privacy and data security training programs for all (1) employees and (2) independent contractors providing services to the Defendant's technology team, in each case on at least an annual basis, updated to address any identified internal or external risks and safeguards implemented pursuant to this Order;
2. Policies, procedures, and technical measures to comply with COPPA and the COPPA Rule;
3. Policies, procedures, and technical measures to prevent the Collection, maintenance, use, or Disclosure of, or provision of access to, Covered Information inconsistent with Defendant's representations to consumers;
4. For those apps that Defendant manually reviews for inclusion in Defendant's app categorization database, conduct an additional review of a subset of such included apps at least once every twelve (12) months with the first additional review occurring within forty-five (45) days of entry of this Order, to determine whether any apps participating in an Ad Tech Service operated by Defendant should be removed from participating in the Ad Tech Service because they are child-directed;
5. Create a record of the child-directed apps that Defendant has banned or removed from participating in its Ad Tech Service; and
6. Provide COPPA training, at least once every twelve (12) months, with respect to the proper identification of child-directed Web sites and apps, to assist employees and independent contractors who analyze such sites and apps, including the traffic quality analysts, in performing their duties;

F. Assess, at least once every twelve (12) months, the sufficiency of any safeguards in place to address the internal and external risks to the privacy of Covered Information, and modify the Privacy Program based on the results;

G. Test and monitor the effectiveness of the safeguards at least once every twelve (12) months, and modify the Privacy Program based on the results;

H. Select and retain Service Providers capable of safeguarding Personal Information they access through or receive from Defendant, and contractually require Service Providers to implement and maintain safeguards sufficient to address the internal and external risks to the privacy of Personal Information; and

I. Evaluate and adjust the Privacy Program in light of any changes to Defendant's operations or business arrangements, new or more efficient technological or operational methods to control for the risks identified in Provision IV.D of this Order, or any other circumstances that Defendant knows or has reason to know may have an impact on the effectiveness of the Privacy Program or any of its individual safeguards. At a minimum, Defendant must evaluate the Privacy Program at least once every twelve (12) months and modify the Privacy Program based on the results.

V. PRIVACY ASSESSMENTS BY A THIRD PARTY

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

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

all documents relevant to each Assessment for five (5) years after completion of such Assessment; and (4) will provide such documents to the Commission within ten (10) days of receipt of a written request from a representative of the Commission. No documents may be withheld on the basis of a claim of confidentiality, proprietary or trade secrets, work product protection, attorney-client privilege, statutory exemption, or any similar claim.

B. For each Assessment, Defendant must provide the Associate Director for Enforcement for the Bureau of Consumer Protection at the Federal Trade Commission with the name, affiliation, and qualifications of the proposed Assessor, whom the Associate Director shall have the authority to approve in his or her sole discretion.

C. The reporting period for the Assessments must cover: (1) the first 180 days after the Privacy Program has been put in place for the initial Assessment; and (2) each two-year period thereafter for twenty (20) years after issuance of the Order for the biennial Assessments.

D. Each Assessment must, for the entire assessment period: (1) determine whether Defendant has implemented and maintained the Privacy Program required by Provision IV of this Order, titled Mandated Privacy Program; (2) assess the effectiveness of Defendant's implementation and maintenance of sub-Provisions IV.A-I; (3) identify any gaps or weaknesses in, or instances of material noncompliance with, the Privacy Program; (4) address the status of gaps or weaknesses in, or instances of material non-compliance with, the Privacy Program that were identified in any prior Assessment required by this Order; and (5) identify specific evidence (including but not limited to documents reviewed, sampling and testing performed, and interviews conducted) examined to make such determinations, assessments, and identifications, and explain why the

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 Commission representative in writing, Defendant must submit the initial Assessment to the Commission within ten (10) days after the Assessment has been completed 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. OpenX Technologies, Inc*." All subsequent biennial Assessments must be retained by Defendant until the Order is terminated and provided to the Associate Director for Enforcement within ten (10) days of request.

VI. COOPERATION WITH THIRD-PARTY PRIVACY ASSESSOR

IT IS FURTHER ORDERED that Defendant, whether acting directly or indirectly, in connection with any Assessment required by Provision V of this Order titled Privacy Assessments by a Third Party, must:

A. Provide or otherwise make available to the Assessor all information and material in its possession, custody, or control that is relevant to the Assessment for which there is no reasonable claim of privilege.

B. Provide or otherwise make available to the Assessor information about Defendant's network(s) and all of Defendant's IT assets so that the Assessor can determine the scope of the Assessment, and visibility to those portions of the network(s) and IT assets deemed in scope; and

C. Disclose all material facts to the Assessor, and not misrepresent in any manner, expressly or by implication, any fact material to the Assessor's: (1) determination of whether Defendant has implemented and maintained the Privacy Program required by Provision IV of this Order, titled Mandated Privacy Program; (2) assessment of the effectiveness of the implementation and maintenance of sub-Provisions IV.A-I; or (3) identification of any gaps or weaknesses in, or instances of material noncompliance with, the Privacy Program.

VII. ANNUAL CERTIFICATION

IT IS FURTHER ORDERED that Defendant must:

A. One year after the issuance date of this Order, and each year thereafter for ten (10) years after entry of the Order, provide the Commission with a certification from a senior corporate manager, or, if no such senior corporate manager exists, a senior officer of Defendant responsible for Defendant's Privacy Program that: (1) Defendant has established, implemented, and maintained the requirements of this Order; and (2) Defendant is not aware of any material noncompliance that has not been

(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. OpenX Technologies, Inc."

VIII. MONETARY JUDGMENT FOR CIVIL PENALTY

IT IS FURTHER ORDERED that:

A. Judgment in the amount of seven million five hundred thousand dollars ($7,500,000) is entered in favor of Plaintiff against Defendant, as a civil penalty.

B. Defendant is ordered to pay to Plaintiff, by making payment to the Treasurer of the United States, two million dollars ($2,000,000), which, as Defendant stipulates, its undersigned counsel holds in escrow for no purpose other than payment to Plaintiff. Such payment must be made within seven (7) days of entry of this Order by electronic fund transfer in accordance with instructions previously provided by a representative of Plaintiff. Upon such payment, the remainder of the judgment is suspended, subject to the Subsections below.

C. The Plaintiff's agreement to the suspension of part of the judgment is expressly premised upon the truthfulness, accuracy, and completeness of Defendant's sworn financial statements and related documents (collectively, "Financial Attestations") submitted to the Commission,

including:

1. The April 16, 2021 letter from Defendant's counsel, Julia Tama, to Plaintiff's counsel, Sarah Choi and Kevin Moriarty;
2. The documentation enclosed as exhibits to the April 16, 2021 letter from Defendant's counsel, Julia Tama, to Plaintiff's counsel, Sarah Choi and Kevin Moriarty;
3. The April 30, 2021 e-mail from Defendant's counsel, Carter Greenbaum and attachments thereto; and
4. The May 25, 2021 e-mail from Defendant's counsel and attachments thereto.

D. The suspension of the judgment will be lifted as to Defendant if, upon motion by Plaintiff, the Court finds that Defendant failed to disclose any material asset, materially misstated the value of any asset, or made any other material misstatement or omission in the Financial Attestations.

E. If the suspension of the judgment is lifted, the judgment becomes immediately due as to Defendant in the amount specified in Subsection A of this Section (which the parties stipulate only for purposes of this Section represents the amount of civil penalty for the violations alleged in the Complaint), less any payment previously made pursuant to this Section, plus interest computed from the date of entry of this Order.

IX. ADDITIONAL MONETARY PROVISIONS

IT IS FURTHER ORDERED that:

A. Defendant relinquishes dominion and all legal and equitable right, title, and interest in all assets transferred pursuant to this Order and may not seek the return of any assets.

B. The facts alleged in the Complaint will be taken as true, without further proof, in any subsequent civil litigation by or on behalf of the Commission, including in a proceeding to enforce its rights to any

payment or monetary judgment pursuant to this Order.

C. Defendant acknowledges that its Taxpayer Identification Number(s), which Defendant must submit to the Commission, may be used for collecting and reporting on any delinquent amount arising out of this Order, in accordance with 31 U.S.C. § 7701.

X. DATA DELETION

IT IS FURTHER ORDERED that Defendant, within ninety (90) days of entry of this Order, shall delete all Ad Request Data collected prior to the entry of this Order, including any sample of the Ad Request Data used for internal analytics.

XI. NOTICE TO DEMAND-SIDE PARTNERS

IT IS FURTHER ORDERED that:

A. Defendant, within thirty (30) days of entry of this Order, shall transmit the notice attached hereto as Exhibit A ("Notice") by email to all of OpenX's demand-side partners.

B. Defendant, within thirty-five (35) days of entry of this Order, shall provide the Commission with a certification, signed by OpenX's Chief Executive Officer on behalf of OpenX, that OpenX has transmitted the Notice to all of OpenX's demand-side partners.

XII. ORDER ACKNOWLEDGMENTS

IT IS FURTHER ORDERED that Defendant obtains acknowledgments of receipt of this Order:

A. Defendant, within seven (7) days of entry of this Order, must submit to the Commission an acknowledgment of receipt of this Order sworn under penalty of perjury.

B. For ten (10) years after entry of this Order, Defendant must deliver a copy of this Order to: (1) all principals, officers, directors, and LLC managers and members; (2) all employees having managerial

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

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

XIII. COMPLIANCE REPORTING

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

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

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."

XIV. RECORDKEEPING

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.

XV. COMPLIANCE MONITORING

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.

B. For matters concerning this Order, the Commission and Plaintiff are authorized to communicate directly with Defendant. Defendant must permit representatives of the Commission and Plaintiff to interview any employee or other Person affiliated with Defendant who has agreed to such an interview. The Person interviewed may have counsel present.

C. The Commission and Plaintiff may use all other lawful means, including posing, through its representatives, as consumers, suppliers, or other individuals or entities, to Defendant or any individual or entity affiliated with Defendant, without the necessity of identification or prior notice. Nothing in this Order limits the Commission's lawful use of compulsory process, pursuant to Sections 9 and 20 of the FTC Act, 15 U.S.C. §§ 49, 57b-1.

XVI. RETENTION OF JURISDICTION

IT IS FURTHER ORDERED that this Court retains jurisdiction of this matter for purposes of construction, modification, and enforcement of this Order.

SO ORDERED this ___ day of _____, 2021.

_____

UNITED STATES DISTRICT JUDGE

SO STIPULATED AND AGREED:

FOR PLAINTIFF UNITED STATES OF AMERICA:

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 5th 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

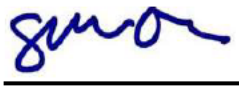
Dated: December 15, 2021

FOR THE FEDERAL TRADE COMMISSION:

ALDEN F. ABBOTT
General Counsel

KRISTIN COHEN
Acting Associate Director
Division of Privacy and Identity Protection

MARK EICHORN
Assistant Director
Division of Privacy and Identity Protection



Dated: December 14, 2021

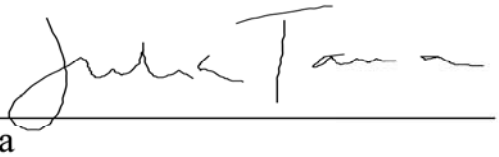
SARAH CHOI
Attorney
Division of Privacy and Identity Protection
Federal Trade Commission
600 Pennsylvania Avenue NW
Mail Stop CC-8232
Washington, DC 20580
(202) 326-2212
schoi@ftc.gov



Dated: December 14, 2021

KEVIN H. MORIARTY
Attorney
Division of Privacy and Identity Protection
Federal Trade Commission
600 Pennsylvania Avenue NW
Mail Stop CC-8232
Washington, DC 20580
(202) 326-2949
kmoriarty@ftc.gov

FOR DEFENDANT:



Date: June 15, 2021

Julia K. Tama
Venable LLP
600 Massachusetts Avenue, NW
Washington, D.C. 20001
Tel: 202-344-4000
Email: Jktama@venable.com
Counsel for OpenX Technologies, Inc.

DEFENDANT:

Joshua Metzger

Date: 06/15/21

General Counsel
OpenX Technologies, Inc.

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.

Appendix A

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.

§ 312.2 Definitions.

Child means an individual under the age of 13.

Collects or *collection* means the gathering of any personal information from a child by any means, including but not limited to:

(1) Requesting, prompting, or encouraging a child to submit personal information online;

(2) Enabling a child to make personal information publicly available in identifiable form. An operator shall not be considered to have collected personal information under this paragraph if it takes reasonable measures to delete all or virtually all personal information from a child's postings before they are made public and also to delete such information from its records; or

(3) Passive tracking of a child online.

Commission means the Federal Trade Commission.

Delete means to remove personal information such that it is not maintained in retrievable form and cannot be retrieved in the normal course of business.

Disclose or disclosure means, with respect to personal information:

(1) The release of personal information collected by an operator from a child in identifiable form for any purpose, except where an operator provides such information to a person who provides support for the internal operations of the Web site or online service; and

(2) Making personal information collected by an operator from a child publicly available in identifiable form by any means, including but not limited to a public posting through the Internet, or through a personal home page or screen posted on a Web site or online service; a pen pal service; an electronic mail service; a message board; or a chat room.

Federal agency means an agency, as that term is defined in Section 551(1) of title 5, United States Code.

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

Obtaining verifiable consent means making any reasonable effort (taking into consideration available technology) to ensure that before personal information is collected from a child, a parent of the child:

(1) Receives notice of the operator's personal information collection, use, and disclosure practices; and

(2) Authorizes any collection, use, and/or disclosure of the personal information.

Online contact information means an email address or any other substantially similar identifier that permits direct contact with a person online, including but not limited to, an instant messaging user identifier, a voice over internet protocol (VOIP) identifier, or a video chat user identifier.

Operator means 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 the users of or visitors to such Web site or online service, or on whose behalf such information is collected or maintained, or offers products or services for sale through that Web site or online service, where such Web site or online service is operated for commercial purposes involving commerce among the several States or with 1 or more foreign nations; in any territory of the United States or in the District of Columbia, or between any such territory and another such territory or any State or foreign nation; or between the District of Columbia and any State, territory, or foreign nation. This definition does not include any nonprofit entity that would otherwise be exempt from coverage under Section 5 of the Federal Trade Commission Act (15 U.S.C. 45). Personal information is *collected or maintained on behalf of* an operator when:

(1) It is collected or maintained by an agent or service provider of the operator; or

(2) The operator benefits by allowing another person to collect personal information directly from users of such Web site or online service.

Parent includes a legal guardian.

Person means any individual, partnership, corporation, trust, estate, cooperative, association, or other entity.

Personal information 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 as defined in this section;

(4) A screen or user name where it functions in the same manner as online contact information, as defined in this section;

(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 Internet Protocol (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 identifier described in this definition.

Release of personal information means the sharing, selling, renting, or transfer of personal information to any third party.

Support for the internal operations of the Web site or online service means:

(1) Those activities necessary to:

(i) Maintain or analyze the functioning of the Web site or online service;

(ii) Perform network communications;

(iii) Authenticate users of, or personalize the content on, the Web site or online service;

(iv) Serve contextual advertising on the Web site or online service or cap the frequency of advertising;

(v) Protect the security or integrity of the user, Web site, or online service;

(vi) Ensure legal or regulatory compliance; or

(vii) Fulfill a request of a child as permitted by § 312.5(c)(3) and (4);

(2) So long as The information collected for the activities listed in paragraphs (1)(i)–(vii) of this definition is not used or disclosed to contact a specific individual, including through behavioral advertising, to amass a

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

Third party 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.

Web site or online service directed to children 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 definition, but that does not target children as its primary audience, shall not be deemed directed to children if it:

(i) Does not collect personal information from any visitor prior to collecting age information; and

(ii) Prevents the collection, use, or disclosure of personal information from visitors who identify themselves as under age 13 without first complying with the notice and parental consent provisions of this part.

(4) A Web site or online service shall not be deemed directed to children solely because it refers or links to a commercial Web site or online service directed to children by using information location tools, including a directory, index, reference, pointer, or hypertext link.

§ 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.

General requirements. It shall be unlawful for any operator of a Web site or online service directed to children, or any operator that has actual knowledge that it is collecting or maintaining personal information from a child, to collect personal information from a child in a manner that violates the regulations prescribed under this part. Generally, under this part, an operator must:

(a) Provide notice on the Web site or online service of what information it collects from children, how it uses such information, and its disclosure practices for such information (§ 312.4(b));

(b) Obtain verifiable parental consent prior to any collection, use, and/or disclosure of personal information from children (§ 312.5);

(c) Provide a reasonable means for a parent to review the personal information collected from a child and to refuse to permit its further use or maintenance (§ 312.6);

(d) Not condition a child's participation in a game, the offering of a prize, or another activity on the child disclosing more personal information than is reasonably necessary to participate in such activity (§ 312.7); and

(e) Establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children (§ 312.8).

§ 312.4 Notice.

(a) *General principles of notice.* It shall be the obligation of the operator to provide notice and obtain verifiable parental consent prior to collecting, using, or disclosing personal information from children. Such notice must be clearly and understandably written, complete, and must contain no unrelated, confusing, or contradictory materials.

(b) *Direct notice to the parent.* An operator must make reasonable efforts, taking into account available technology, to ensure that a parent of a child receives direct notice of the operator's practices with regard to the collection, use, or disclosure of personal information from children, including notice of any material change in the collection, use, or disclosure practices to which the parent has previously consented.

(c) *Content of the direct notice to the parent*—(1) *Content of the direct notice to the parent under § 312.5(c)(1) (Notice to Obtain Parent's Affirmative Consent to the Collection, Use, or Disclosure of a Child's Personal Information).* This direct notice shall set forth:

(i) That the operator has collected the parent's online contact information from the child, and, if such is the case, the name of the child or the parent, in order to obtain the parent's consent;

(ii) That the parent's consent is required for the collection, use, or disclosure of such information, and that the operator will not collect, use, or disclose any personal information from the child if the parent does not provide such consent;

(iii) The additional items of personal information the operator intends to collect from the child, or the potential opportunities for the disclosure of personal information, should the parent provide consent;

(iv) A hyperlink to the operator's online notice of its information practices required under paragraph (d) of this section;

(v) The means by which the parent can provide verifiable consent to the collection, use, and disclosure of the information; and

(vi) That if the parent does not provide consent within a reasonable time from the date the direct notice was sent, the operator will delete the parent's online contact information from its records.

(2) *Content of the direct notice to the parent under § 312.5(c)(2) (Voluntary Notice to Parent of a Child's Online Activities Not Involving the Collection, Use or Disclosure of Personal Information).* Where an operator chooses to notify a parent of a child's participation in a Web site or online service, and where such site or service does not collect any personal information other than the parent's online contact information, the direct notice shall set forth:

(i) That the operator has collected the parent's online contact information from the child in order to provide notice to, and subsequently update the parent about, a child's participation in a Web site or online service that does not otherwise collect, use, or disclose children's personal information;

(ii) That the parent's online contact information will not be used or disclosed for any other purpose;

(iii) That the parent may refuse to permit the child's participation in the Web site or online service and may require the deletion of the parent's online contact information, and how the parent can do so; and

(iv) A hyperlink to the operator's online notice of its information

practices required under paragraph (d) of this section.

(3) *Content of the direct notice to the parent under § 312.5(c)(4) (Notice to a Parent of Operator's Intent to Communicate with the Child Multiple Times).* This direct notice shall set forth:

(i) That the operator has collected the child's online contact information from the child in order to provide multiple online communications to the child;

(ii) That the operator has collected the parent's online contact information from the child in order to notify the parent that the child has registered to receive multiple online communications from the operator;

(iii) That the online contact information collected from the child will not be used for any other purpose, disclosed, or combined with any other information collected from the child;

(iv) That the parent may refuse to permit further contact with the child and require the deletion of the parent's and child's online contact information, and how the parent can do so;

(v) That if the parent fails to respond to this direct notice, the operator may use the online contact information collected from the child for the purpose stated in the direct notice; and

(vi) A hyperlink to the operator's online notice of its information practices required under paragraph (d) of this section.

(4) *Content of the direct notice to the parent required under § 312.5(c)(5) (Notice to a Parent In Order to Protect a Child's Safety).* This direct notice shall set forth:

(i) That the operator has collected the name and the online contact information of the child and the parent in order to protect the safety of a child;

(ii) That the information will not be used or disclosed for any purpose unrelated to the child's safety;

(iii) That the parent may refuse to permit the use, and require the deletion, of the information collected, and how the parent can do so;

(iv) That if the parent fails to respond to this direct notice, the operator may use the information for the purpose stated in the direct notice; and

(v) A hyperlink to the operator's online notice of its information practices required under paragraph (d) of this section.

(d) *Notice on the Web site or online service.* In addition to the direct notice to the parent, an operator must post a prominent and clearly labeled link to an online notice of its information practices with regard to children on the home or landing page or screen of its Web site or online service, *and,* at each area of the Web site or online service where personal information is collected from children. The link must be in close proximity to the requests for information in each such area. An operator of a general audience Web site or online service that has a separate children's area must post a link to a notice of its information practices with regard to children on the home or landing page or screen of the children's area. To be complete, the online notice of the Web site or online service's information practices must state the following:

(1) The name, address, telephone number, and email address of all operators collecting or maintaining personal information from children through the Web site or online service. *Provided that:* The operators of a Web site or online service may list the name, address, phone number, and email address of one operator who will respond to all inquiries from parents concerning the operators' privacy policies and use of children's information, as long as the names of all the operators collecting or maintaining personal information from children through the Web site or online service are also listed in the notice;

(2) A description of what information the operator collects from children, including whether the Web site or online service enables a child to make personal information publicly available; how the operator uses such information; and, the operator's disclosure practices for such information; and

(3) That the parent can review or have deleted the child's personal information, and refuse to permit further collection or use of the child's information, and state the procedures for doing so.

§ 312.5 Parental consent.

(a) *General requirements.* (1) An operator is required to obtain verifiable parental consent before any collection, use, or disclosure of personal information from children, including consent to any material change in the collection, use, or disclosure practices to which the parent has previously consented.

(2) An operator must give the parent the option to consent to the collection and use of the child's personal information without consenting to disclosure of his or her personal information to third parties.

(b) *Methods for verifiable parental consent.* (1) An operator must make reasonable efforts to obtain verifiable parental consent, taking into consideration available technology. Any method to obtain verifiable parental consent must be reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent. (2) Existing methods to obtain verifiable parental consent that satisfy the requirements of this paragraph include:

(i) Providing a consent form to be signed by the parent and returned to the operator by postal mail, facsimile, or electronic scan;

(ii) Requiring a parent, in connection with a monetary transaction, to use a credit card, debit card, or other online payment system that provides notification of each discrete transaction to the primary account holder;

(iii) Having a parent call a toll-free telephone number staffed by trained personnel;

(iv) Having a parent connect to trained personnel via video-conference;

(v) Verifying a parent's identity by checking a form of government-issued identification against databases of such information, where the parent's identification is deleted by the operator from its records promptly after such verification is complete; or

(vi) *Provided that,* an operator that does not ''disclose'' (as defined by § 312.2) children's personal information, may use an email coupled with additional steps to provide assurances that the person providing the consent is the parent. Such additional steps include: Sending a confirmatory email to the parent following receipt of consent, or obtaining a postal address or telephone number from the parent and confirming the parent's consent by letter or telephone call. An operator that uses this method must provide notice that the parent can revoke any consent given in response to the earlier email.

(3) *Safe harbor approval of parental consent methods.* A safe harbor program approved by the Commission under § 312.11 may approve its member operators' use of a parental consent method not currently enumerated in paragraph (b)(2) of this section where the safe harbor program determines that such parental consent method meets the requirements of paragraph (b)(1) of this section.

(c) *Exceptions to prior parental consent.* Verifiable parental consent is required prior to any collection, use, or disclosure of personal information from a child *except* as set forth in this paragraph:

(1) Where the sole purpose of collecting the name or online contact information of the parent or child is to provide notice and obtain parental consent under § 312.4(c)(1). If the operator has not obtained parental consent after a reasonable time from the date of the information collection, the

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 *Web site or online service directed to children* 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 parent.

(b) Neither an operator nor the operator's agent shall be held liable under any Federal or State law for any disclosure made in good faith and following reasonable procedures in responding to a request for disclosure of personal information under this section.

(c) Subject to the limitations set forth in § 312.7, an operator may terminate any service provided to a child whose parent has refused, under paragraph (a)(2) of this section, to permit the operator's further use or collection of personal information from his or her child or has directed the operator to delete the child's personal information.

§ 312.7 Prohibition against conditioning a child's participation on collection of personal information.

An operator is prohibited from conditioning a child's participation in a game, the offering of a prize, or another activity on the child's disclosing more personal information than is reasonably necessary to participate in such activity.

§ 312.8 Confidentiality, security, and integrity of personal information collected from children.

The operator must establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children. The operator must also take reasonable steps to release children's personal information only to service providers and third parties who are capable of maintaining the confidentiality, security and integrity of such information, and who provide assurances that they will maintain the information in such a manner.

§ 312.9 Enforcement.

Subject to sections 6503 and 6505 of the Children's Online Privacy Protection Act of 1998, a violation of a regulation prescribed under section 6502 (a) of this Act shall be treated as a violation of a rule defining an unfair or deceptive act or practice prescribed under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)).

§ 312.10 Data retention and deletion requirements.

An operator of a Web site or online service shall retain personal information collected online from a child for only as long as is reasonably necessary to fulfill the purpose for which the information was collected. The operator must delete such information using reasonable measures to protect against unauthorized access to, or use of, the information in connection with its deletion.

§ 312.11 Safe harbor programs.

(a) *In general.* Industry groups or other persons may apply to the Commission for approval of self-regulatory program guidelines (''safe harbor programs''). The application shall be filed with the Commission's Office of the Secretary. The Commission will publish in the **Federal Register** a document seeking public comment on the application. The Commission shall issue a written determination within 180 days of the filing of the application.

(b) *Criteria for approval of self-regulatory program guidelines.* Proposed safe harbor programs must demonstrate

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) *Request for Commission approval of self-regulatory program guidelines.* 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) *Reporting and recordkeeping requirements.* 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) *Post-approval modifications to self-regulatory program guidelines.* 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) *Revocation of approval of self-regulatory program guidelines.* 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) *Operators' participation in a safe harbor program.* An operator will be deemed to be in compliance with the requirements of §§ 312.2 through 312.8, and 312.10 if that operator complies with Commission-approved safe harbor program guidelines. In considering whether to initiate an investigation or bring an enforcement action against a subject operator for violations of this part, the Commission will take into account the history of the subject operator's participation in the safe harbor program, whether the subject operator has taken action to remedy such non-compliance, and whether the operator's non-compliance resulted in any one of the disciplinary actions set forth in paragraph (b)(3).

§ 312.12 Voluntary Commission Approval Processes.

(a) *Parental consent methods.* An interested party may file a written request for Commission approval of parental consent methods not currently enumerated in § 312.5(b). To be considered for approval, a party must provide a detailed description of the proposed parental consent methods, together with an analysis of how the methods meet § 312.5(b)(1). The request shall be filed with the Commission's Office of the Secretary. The Commission will publish in the **Federal Register** a document seeking public comment on the request. The Commission shall issue a written determination within 120 days of the filing of the request; and

(b) *Support for internal operations of the Web site or online service.* An interested party may file a written request for Commission approval of additional activities to be included within the definition of support for internal operations. To be considered for approval, a party must provide a detailed justification why such activities should be deemed support for internal operations, and an analysis of their potential effects on children's online privacy. The request shall be filed with the Commission's Office of the Secretary. The Commission will publish in the **Federal Register** a document seeking public comment on the request. The Commission shall issue a written determination within 120 days of the filing of the request.

§ 312.13 Severability.

The provisions of this part are separate and severable from one another. If any provision is stayed or determined to be invalid, it is the Commission's intention that the remaining provisions shall continue in effect.

Appendix A

By direction of the Commission, Commissioner Rosch abstaining, and Commissioner Ohlhausen dissenting.

Donald S. Clark,

Secretary.

Dissenting Statement of Commissioner Maureen K. Ohlhausen

I voted against adopting the amendments to the Children's Online Privacy Protection Act (COPPA) Rule because I believe a core provision of the amendments exceeds the scope of the authority granted us by Congress in COPPA, the statute that underlies and authorizes the Rule.[401] Before I explain my concerns, I wish to commend the Commission staff for their careful consideration of the multitude of issues raised by the numerous comments in this proceeding. Much of the language of the amendments is designed to preserve flexibility for the industry while striving to protect children's privacy, a goal I support strongly. The final proposed amendments largely strike the right balance between protecting children's privacy online and avoiding undue burdens on providers of children's online content and services. The staff's great expertise in the area of children's privacy and deep understanding of the values at stake in this matter have been invaluable in my consideration of these important issues.

In COPPA Congress defined who is an operator and thereby set the outer boundary for the statute's and the COPPA Rule's reach.[402] It is undisputed that COPPA places obligations on operators of Web sites or online services directed to children or operators with actual knowledge that they are collecting personal information from children. The statute provides, ''It is unlawful for an operator of a Web site or online service directed to children, or any operator that has actual knowledge that it is collecting personal information from a child, to collect personal information from a child in a manner that violates the regulations prescribed [by the FTC].'' [403]

The Statement of Basis and Purpose for the amendments (SBP) discusses concerns that the current COPPA Rule may not cover child-directed Web sites or services that do not themselves collect children's personal information but may incorporate third-party plug-ins that collect such information [404] for the plug-ins' use but do not collect or maintain the information for, or share it with, the child-directed site or service. To address these concerns, the amendments add a new proviso to the definition of operator in the COPPA Rule: ''Personal information is collected or maintained on behalf of an operator when: (a) it is collected or maintained by an agent or service provider of the operator; or (b) the operator benefits by allowing another person to collect personal information directly from users of such Web site or online service.'' [405]

The proposed amendments construe the term ''on whose behalf such information is collected and maintained'' to reach child-directed Web sites or services that merely derive from a third-party plug-in some kind of benefit, which may well be unrelated to the collection and use of children's information (*e.g.,* content, functionality, or advertising revenue). I find that this proviso—which would extend COPPA obligations to entities that do not collect personal information from children or have access to or control of such information collected by a third-party does not comport with the plain meaning of the statutory definition of an operator in COPPA, which covers only entities ''on whose behalf such information is collected and maintained.'' [406] In other words, I do not believe that the fact that a child-directed site or online service receives any kind of benefit from using a plug-in is equivalent to the collection of personal information by the third-party plug-in on behalf of the child-directed site or online service.

As the Supreme Court has directed, an agency ''must give effect to the unambiguously expressed intent of Congress.'' [407] Thus, regardless of the policy justifications offered, I cannot support expanding the definition of the term ''operator'' beyond the statutory parameters set by Congress in COPPA.

I therefore respectfully dissent.

[FR Doc. 2012–31341 Filed 1–16–13; 8:45 am]

BILLING CODE 6750–01–P

[401] 15 U.S.C. 6501–6506.

[402] 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 Online Privacy Protection Rule 64 FR 59888, 59891 (Nov. 3, 1999) (final rule).

[403] 15 U.S.C. 6502(a)(1).

[404] If the third-party plugs-ins are child-directed or have actual knowledge that they are collecting children's personal information they are already expressly covered by the COPPA statute. Thus, as the SBP notes, a behavioral advertising network that targets children under the age of 13 is already deemed an operator. The amendment must therefore be aimed at reaching third-party plug-ins that are either not child-directed or do not have actual knowledge that they are collecting children's personal information, which raises a question about what harm this amendment will address. For example, it appears that this same type of harm could occur through general audience Web sites and online services collecting and using visitors' personal information without knowing whether some of the data is children's personal information, which is a practice that COPPA and the amendments do not prohibit.

[405] 16 CFR 312.2 (Definitions).

[406] This expanded definition of operator reverses the Commission's previous conclusion that the appropriate test for determining an entity's status as an operator is to ''look at the entity's relationship to the data collected,'' using factors such as ''who owns and/or controls the information, who pays for its collection and maintenance, the pre-existing contractual relationships regarding collection and maintenance of the information, and the role of the Web site or online service in collecting and/or maintaining the information (*i.e.,* whether the site participates in collection or is merely a conduit through which the information flows to another entity.)'' Children's Online Privacy Protection Rule 64 FR 59888, 59893, 59891 (Nov. 3, 1999) (final rule).

[407] *Chevron* v. *Natural Resources Defense Council, Inc.,* 467 U.S. 837, 842–43 (1984) (''When a court reviews an agency's construction of the statute which it administers, it is confronted with two questions. First, always, is the question whether Congress has directly spoken to the precise question at issue. If the intent of Congress is clear, that is the end of the matter; for the court, as well as the agency, must give effect to the unambiguously expressed intent of Congress.'').

EXHIBIT A



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.

Exhibit A ("Notice")