

**UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF ILLINOIS  
EASTERN DIVISION**

UNITED STATES OF AMERICA,

Plaintiff,

vs.

VTECH ELECTRONICS LIMITED, a  
corporation, and

VTECH ELECTRONICS NORTH  
AMERICA, LLC, a limited liability  
company,

Defendants.

**Case No : 1:18-cv-114**

**PLAINTIFF'S UNOPPOSED MOTION FOR ENTRY OF THE STIPULATED ORDER**

The United States of America respectfully requests that this Court enter the attached Stipulated Order for Permanent Injunction and Civil Penalty Judgment ("Stipulated Order"). Counsel for defendants do not oppose this motion.

Date: January 8, 2018

Respectfully submitted:

**FOR THE FEDERAL TRADE  
COMMISSION:**

MANEESHA MITHAL  
Associate Director  
Division of Privacy and Identity Protection

MARK EICHORN  
Assistant Director  
Division of Privacy and Identity Protection

JACQUELINE K. CONNOR  
Attorney  
Division of Privacy and Identity Protection  
Federal Trade Commission  
600 Pennsylvania Avenue NW  
Washington, DC 20580  
Tel: (202) 326-2844  
Fax: (202) 326-3062  
jconnor@ftc.gov

KATHERINE WHITE  
Attorney  
Division of Privacy and Identity Protection  
Federal Trade Commission  
600 Pennsylvania Avenue NW  
Washington, DC 20580  
Tel: (202) 326-2878  
Fax: (202) 326-3062  
kwhite@ftc.gov

**FOR PLAINTIFF UNITED STATES OF  
AMERICA:**

CHAD A. READLER  
Acting Assistant Attorney General  
Civil Division

JOHN R. LAUSCH, JR.  
United States Attorney  
Northern District of Illinois

ETHAN P. DAVIS  
Deputy Assistant Attorney General

GUSTAV W. EYLER  
Acting Director  
Consumer Protection Branch

ANDREW E. CLARK  
Assistant Director

/s/ Joshua D. Rothman  
JOSHUA D. ROTHMAN  
Trial Attorney  
Consumer Protection Branch  
U.S. Department of Justice  
P.O. Box 386  
Washington, DC 20044  
(202) 514-1586  
Joshua.D.Rothman@usdoj.gov

**CERTIFICATE OF SERVICE**

I hereby certify that I emailed a true and correct copy of the foregoing motion to Mr. Michael Vatis, Ms. Lydia Parnes, and Mr. Christopher Olsen, attorneys for defendants, on January 8, 2018. Mr. Vatis agreed to accept service of this document by email on behalf of defendants:

Michael Vatis  
Steptoe & Johnson LLP  
1114 Avenue of the Americas  
New York, NY 10036  
Tel: (212) 506-3927  
Fax: (212) 506-3950  
mvatis@steptoe.com

Lydia Parnes  
Wilson Sonsini Goodrich & Rosati  
1700 K Street, NW  
Fifth Floor  
Washington, DC 20006  
Tel: (202) 973-8801  
lparnes@wsgr.com

Christopher Olsen  
Wilson Sonsini Goodrich & Rosati  
1700 K Street, NW  
Fifth Floor  
Washington, DC 20006  
Tel: (202) 973-8803  
colsen@wsgr.com

/s/ Joshua D. Rothman  
JOSHUA D. ROTHMAN  
Trial Attorney

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

**UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF ILLINOIS  
EASTERN DIVISION**

UNITED STATES OF AMERICA,

Plaintiff,

vs.

VTECH ELECTRONICS LIMITED, a  
corporation, and

VTECH ELECTRONICS NORTH  
AMERICA, LLC, a limited liability  
company,

Defendants.

**Case No : 1:18-cv-144**

**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 (“Commission”), filed its Complaint for Permanent Injunction and Other Equitable Relief (“Complaint”), in this matter, pursuant to Sections 13(b), and 16(a)(1) of the Federal Trade Commission Act (“FTC Act”), 15 U.S.C. §§ 53(b), and 56(a)(1), the Children’s Online Privacy Protection Act, 15 U.S.C. §§ 6502(c) and 6505(d), and the Commission’s Children’s Online Privacy Protection Rule (“COPPA Rule”), 16 C.F.R. Part 312. Defendants have waived service of the summons and the Complaint. Plaintiff and Defendants 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.

- 1 2. The Complaint charges that Defendants participated in deceptive acts or practices in  
2 violation of Section 5 of the FTC Act, 15 U.S.C. § 45, in the making of a deceptive  
3 statement relating to their collection, storage, and transmittal of covered information.  
4 The Complaint further charges that Defendants violated the COPPA Rule by failing to  
5 post a privacy policy for their Kid Connect online service providing clear,  
6 understandable, and complete notice of their information practices; failing to provide  
7 direct notice of their information practices to parents; failing to obtain verifiable parental  
8 consent prior to collecting, using, and/or disclosing personal information from children;  
9 and failing to establish and maintain reasonable procedures to protect the confidentiality,  
10 security, and integrity of personal information collected from children.  
11
- 12 3. Defendants neither admit nor deny any of the allegations in this Complaint, except as  
13 specifically stated in this Order. Only for purposes of this action, Defendants admit the  
14 facts necessary to establish jurisdiction.  
15
- 16 4. Defendants waive any claim they may have under the Equal Access to Justice Act, 28  
17 U.S.C. § 2412, concerning the prosecution of this action through the date of this Order,  
18 and agree to bear their own costs and attorney fees.  
19
- 20 5. Defendants and Plaintiff waive all rights to appeal or otherwise challenge or contest the  
21 validity of this Order.

## 22 **DEFINITIONS**

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

- 24 A. “Child” means an individual under the age of 13.  
25  
26  
27  
28

1 B. “Collects” or “collection” means, for the purposes of Parts I and VIII of this Order only,  
2 the gathering of any personal information from a child by any means, including but not  
3 limited to:

- 4 1. Requesting, prompting, or encouraging a child to submit personal information  
5 online;
- 6 2. Enabling a child to make personal information publicly available in identifiable  
7 form; or
- 8 3. Passive tracking of a child online.

9  
10 C. “Covered information” means: (1) registration information, and (2) personal information  
11 collected from a child.

12 D. “Defendants” means VTech Electronics Limited and VTech Electronics North America,  
13 LLC, and their successors and assigns, to the extent any of these entities market products  
14 or services to consumers in the United States.

15 E. “Disclose” or disclosure” means, with respect to personal information:

- 16 1. The release of personal information collected by an operator from a child in  
17 identifiable form for any purpose, except where an operator provides such  
18 information to a person who provides support for the internal operations of the  
19 Web site or online service; and
  - 20 2. Making personal information collected by an operator from a child publicly  
21 available in identifiable form by any means, including but not limited to a public  
22 posting through the Internet, or through a personal home page or screen posted on  
23 a Web site or online service; a pen pal service; an electronic mail service; a  
24 message board; or a chat room.
- 25  
26  
27  
28

1 F. “Internet” means collectively the myriad of computer and telecommunication facilities,  
2 including equipment and operating software, which comprises the interconnected world-  
3 wide network of networks that employ the Transmission Control Protocol/Internet  
4 Protocol, or any predecessor or successor protocols to such protocol, to communicate  
5 information of all kinds by wire, radio, or other methods of transmission.  
6

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

- 10 1. Receives notice of the operator’s personal information collection, use, and  
11 disclosure practices; and
- 12 2. Authorizes any collection, use, and/or disclosure of the personal information.  
13

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

18 I. “Operator” means any person who operates a Web site located on the Internet or an  
19 online service and who collects or maintains personal information from or about the users  
20 of or visitors to such Web site or online service, or on whose behalf such information is  
21 collected or maintained, or offers products or services for sale through the Web site or  
22 online service, where such Web site or online service is operated for commercial  
23 purposes involving commerce among the several States, or with one or more foreign  
24 nations; in any territory of the United States or in the District of Columbia, or between  
25  
26  
27  
28

1 any such territory and another such territory or any State or foreign nation; or between  
2 the District of Columbia and any State, territory, or foreign nation.

3 J. "Parent" includes a legal guardian.

4 K. "Person" means any individual, partnership, corporation, trust, estate, cooperative,  
5 association, or other entity.

6  
7 L. "Personal information" means individually identifiable information about an individual  
8 collected online from a child, including:

- 9 1. A first and last name;
- 10 2. A home or other physical address including street name and name of a city or  
11 town;
- 12 3. Online contact information as defined in 16 C.F.R. § 312.2;
- 13 4. A screen or user name where it functions in the same manner as online contact  
14 information, as defined in 16 C.F.R. § 312.2;
- 15 5. A telephone number;
- 16 6. A Social Security number;
- 17 7. A persistent identifier that can be used to recognize a user over time and across  
18 different Web sites or online services. Such persistent identifier includes, but is  
19 not limited to, a customer number held in a cookie, an Internet Protocol (IP)  
20 address, a processor or device serial number, or unique device identifier;
- 21 8. A photograph, video, or audio file where such file contains a child's image or  
22 voice;
- 23 9. Geolocation information sufficient to identify street name and name of a city or  
24 town; or  
25  
26  
27  
28

1           10. Information concerning the child or the parents of that child that the operator  
2           collects online from the child and combines with an identifier described in this  
3           section.

4  
5 M. “Registration information” means information collected by Defendants from individual  
6 consumers in the course of registering to use Defendants’ products or services, including:

- 7           1. A first and last name;
- 8           2. A home or other physical address including street name and name of a city or  
9           town;
- 10          3. Online contact information;
- 11          4. A telephone number;
- 12          5. A Social Security number;
- 13          6. Authentication credentials, such as a username and password;
- 14          7. Photo, video, or audio files; and
- 15          8. The name, date of birth, and any personal information relating to a child.

16  
17 N. “Support for the internal operations of the Web site or online service” means:

- 18          1. Those activities necessary to:
  - 19               a. Maintain or analyze the functioning of the Web site or online service;
  - 20               b. Perform network communications;
  - 21               c. Authenticate users of, or personalize the content on, the Web site or online  
22               service;
  - 23               d. Serve contextual advertising on the Web site or online service or cap the  
24               frequency of advertising;
  - 25               e. Protect the security or integrity of the user, Web site, or online service;
  - 26
  - 27
  - 28

1 f. Ensure legal or regulatory compliance; or

2 g. Fulfill a request of a child as permitted by 16 C.F.R. §§ 312.5(c)(3)

3 and (4);

- 4 2. So long as the information collected for the activities listed in paragraphs (1)(a)-  
5 (g) of this definition is not used or disclosed to contact a specific individual,  
6 including through behavioral advertising, to amass a profile on a specific  
7 individual, or for any other purpose.  
8

9 O. “Web site or online service directed to children” means a commercial Web site or online  
10 service, or portion thereof, that is targeted to children.

- 11 1. In determining whether a Web site or online service, or a portion thereof, is  
12 directed to children, the Commission will consider its subject matter, visual  
13 content, use of animated characters or child-oriented activities and incentives,  
14 music or other audio content, age of models, presence of child celebrities or  
15 celebrities who appeal to children, language or other characteristics of the Web  
16 site or online service, as well as whether advertising promoting or appearing on  
17 the Web site or online service is directed to children. The Commission will also  
18 consider competent and reliable empirical evidence regarding audience  
19 composition, and evidence regarding the intended audience.  
20  
21 2. A Web site or online service shall be deemed directed to children when it has  
22 actual knowledge that it is collecting personal information directly from users of  
23 another Web site or online service directed to children.  
24  
25  
26  
27  
28



- 1 A. Failing to make reasonable efforts, taking into account available technology, to ensure  
2 that a parent of a child receives direct notice of Defendants' practices with regard to the  
3 collection, use, or disclosure of personal information, including notice of any material  
4 change in the collection, use, or disclosure practices to which the parent has previously  
5 consented;  
6
- 7 B. Failing to post a prominent and clearly labeled link to an online notice of its information  
8 practices with regard to children, if any, on the home or landing page or screen of its Web  
9 site or online service, *and* at each area of the Web site or online service where personal  
10 information is collected;  
11
- 12 C. Failing to obtain verifiable parental consent before any collection, use, or disclosure of  
13 personal information, including consent to any material change in the collection, use, or  
14 disclosure practices to which the parent has previously consented; and
- 15 D. Failing to establish and maintain reasonable procedures to protect the confidentiality,  
16 security, and integrity of personal information.

17 A copy of the Children's Online Privacy Protection Rule, 16 C.F.R. Part 312, is attached  
18 hereto as appendix A.

19 **II. MONETARY JUDGEMENT FOR CIVIL PENALTY**

20 IT IS FURTHER ORDERED that:

- 21
- 22 A. Judgement in the amount of six hundred fifty thousand dollars (\$650,000) is entered in  
23 favor of Plaintiff against Defendants, jointly and severally, as a civil penalty.
- 24 B. Defendants are ordered to pay to Plaintiff, by making payment to the Treasurer of the  
25 United States, six hundred fifty thousand dollars (\$650,000), which, as Defendants  
26 stipulate, their undersigned counsel holds in escrow for no purpose other than payment to  
27  
28

1 Plaintiff. Such payment must be made within 7 days of entry of this Order by electronic  
2 fund transfer in accordance with instructions previously provided by a representative of  
3 Plaintiff.

4 **III. ADDITIONAL MONETARY PROVISIONS**

5 IT IS FURTHER ORDERED that:

- 6
- 7 A. Defendants relinquish dominion and all legal and equitable right, title, and interest in all  
8 assets transferred pursuant to this Order and may not seek the return of any assets.
- 9 B. The facts alleged in the Complaint will be taken as true, without further proof, in any  
10 subsequent civil litigation by or on behalf of the Commission in a proceeding to enforce  
11 its rights to any payment or monetary judgement pursuant to this Order.
- 12 C. The facts alleged in the Complaint establish all elements necessary to sustain an action by  
13 the Commission pursuant to Section 523(a)(2)(A) of the Bankruptcy Code, 11 U.S.C. §  
14 523(a)(2)(A), and this Order will have collateral estoppel effect for such purposes.
- 15 D. Defendants acknowledge that their Taxpayer Identification Numbers, which Defendants  
16 must submit to the Commission, may be used for collecting and reporting on any  
17 delinquent amount arising out of this Order, in accordance with 31 U.S.C. §7701.
- 18

19 **IV. INJUNCTION REGARDING MISREPRESENTING DATA SECURITY AND**  
20 **PRIVACY PRACTICES**

21 IT IS FURTHER ORDERED that Defendants, Defendants' officers, agents, employees,  
22 and attorneys, and all other persons in active concert or participation with any of them who  
23 receive actual notice of this Order, whether acting directly or indirectly, are permanently  
24 restrained and enjoined from misrepresenting, expressly or by implication, the extent to  
25  
26  
27  
28

1 which they maintain and protect the privacy, confidentiality, security, or integrity of covered  
2 information, including Defendants' collection, use, disclosure, and deletion practices.

3 **V. COMPREHENSIVE DATA SECURITY PROGRAM REQUIREMENT**

4 IT IS FURTHER ORDERED that Defendant must, no later than the date of service of  
5 this Order, establish and implement, and thereafter maintain, a comprehensive information  
6 security program that is reasonably designed to protect the security, confidentiality, and  
7 integrity of personal information collected directly or indirectly by Defendants. The content,  
8 implementation and maintenance of the program must be fully documented in writing. The  
9 program must contain administrative, technical, and physical safeguards appropriate to  
10 Defendants' size and complexity, the nature and scope of Defendants' activities, and the  
11 sensitivity of the personal information, including:  
12

- 13 A. The designation of an employee or employees to coordinate and be responsible for the  
14 information security program;  
15  
16 B. The identification of internal and external risks to the security, confidentiality, or  
17 integrity of personal information that could result in the unauthorized disclosure, misuse,  
18 loss, alteration, destruction, or other compromise of such information, and assessment of  
19 the sufficiency of any safeguards in place to control these risks. At a minimum, this risk  
20 assessment must include consideration of risks in each area of relevant operation,  
21 including: (1) employee training and management; (2) information systems, such as  
22 network and software design, information processing, storage, transmission, and disposal;  
23 and (3) prevention, detection, and response to attacks, intrusions, or other systems  
24 failures;  
25  
26  
27  
28

- 1 C. The design and implementation of reasonable safeguards to control these risks, and  
2 regular testing or monitoring of the effectiveness of the safeguards' key controls,  
3 systems, and procedures;  
4  
5 D. The development and use of reasonable steps to select and retain service providers  
6 capable of appropriately safeguarding personal information they receive from  
7 Defendants, and requiring service providers, by contract, to implement and maintain  
8 appropriate safeguards; and  
9  
10 E. The evaluation and adjustment of the information security program in light of the results  
11 of the testing and monitoring required by sub-provision C, any changes to Defendants'  
12 operations or business arrangements, or any other circumstances that Defendants know or  
13 have reason to know may have an impact on the effectiveness of the information security  
14 program.

15 **VI. DATA SECURITY PROGRAM ASSESSMENT REQUIREMENT**

16 IT IS FURTHER ORDERED that, in connection with compliance with the Provision of  
17 this Order titled Comprehensive Data Security Program Requirement, Defendants must  
18 obtain initial and biennial assessments ("Assessments"):

- 19 A. The Assessments must be obtained from a qualified, objective, independent third-party  
20 professional, who uses procedures and standards generally accepted in the profession. A  
21 professional qualified to prepare such Assessments must be: an individual qualified as a  
22 Certified Information System Security Professional (CISSP) or as a Certified Information  
23 Systems Auditor (CISA); an individual holding Global Information Assurance  
24 Certification (GIAC) from the SANS Institute; or a qualified individual or entity  
25  
26  
27  
28

1 approved by the Associate Director for Enforcement, Bureau of Consumer Protection,  
2 Federal Trade Commission.

3 B. The reporting period for the Assessments must cover: (1) the first 180 days after the  
4 issuance date of the Order for the initial Assessment, and (2) each 2-year period  
5 thereafter for 20 years after issuance of the Order for the biennial Assessments.  
6

7 C. Each Assessment must:

- 8 a. Set forth the specific administrative, technical, and physical safeguards that  
9 Defendants have implemented and maintained during the reporting period;  
10 b. Explain how such safeguards are appropriate to Defendants' size and complexity,  
11 the nature and scope of Defendants' activities, and the sensitivity of the personal  
12 information collected;  
13 c. Explain how the safeguards that have been implemented meet or exceed the  
14 protections required by the Provision of this Order titled Comprehensive Data  
15 Security Program Requirement; and  
16 d. Certify that the security program is operating with sufficient effectiveness to  
17 provide reasonable assurance that the security, confidentiality, and integrity of  
18 personal information is protected and has so operated throughout the reporting  
19 period.  
20  
21

22 D. Each Assessment must be completed within 60 days after the end of the reporting period  
23 to which the Assessment applies. Defendants must submit the initial Assessment to the  
24 Commission within 10 days after the Assessment has been completed. Defendants must  
25 retain all subsequent biennial Assessments, at least until the Order terminates.  
26  
27  
28

1 Defendants must submit any biennial Assessments to the Commission within 10 days of a  
2 request from a representative of the Commission.

3 **VII. ORDER ACKNOWLEDGMENTS**

4 IT IS FURTHER ORDERED that Defendants obtain acknowledgments of receipt of this  
5 Order:

- 6
- 7 A. Each Defendant, within 7 days of entry of this Order, must submit to the Commission an  
8 acknowledgment of receipt of this Order sworn under penalty of perjury.
- 9 B. For five (5) years after entry of this Order, Defendants must deliver a copy of this Order  
10 to: (1) all principals, officers, directors, and managers and members; (2) all employees,  
11 agents, and representatives having management responsibilities related to subject matter  
12 covered by this Order; and (3) any business entity resulting from any change in structure  
13 as set forth in the Part titled Compliance Reporting. Delivery must occur within seven  
14 (7) days of entry of this Order for current personnel. For all others, delivery must occur  
15 before they assume their responsibilities.
- 16
- 17 C. From each individual or entity to which a Defendant delivered a copy of this Order, that  
18 Defendant must obtain, within 30 days, a signed and dated acknowledgment of receipt of  
19 this Order.
- 20

21 **VIII. COMPLIANCE REPORTING**

22 IT IS FURTHER ORDERED that Defendants make timely submissions to the  
23 Commission:

- 24 A. One year after entry of this Order, each Defendant must submit a compliance report,  
25 sworn under penalty of perjury. Each Defendant must:
- 26
- 27
- 28

- 1           1. Identify the primary physical, postal, and email address and telephone number, as  
2           designated points of contact, which representatives of the Commission and  
3           Plaintiff may use to communicate with Defendant;
- 4           2. Identify all of that Defendant's businesses by all of their names, telephone  
5           numbers, and physical, postal, email, and Internet addresses;
- 6           3. Describe the activities of each business, including the goods and services offered,  
7           the means of advertising, marketing, and sales, and involvement of any other  
8           Defendant;
- 9           4. Describe in detail whether and how that Defendant is in compliance with each  
10          section of this Order;
- 11          5. Provide a copy of each different version of any privacy notice posted on each  
12          Web site or online service operated by that Defendant that is directed to children  
13          or otherwise communicated to parents of children from whom that Defendant  
14          collects personal information;
- 15          6. Provide a statement setting forth in detail any methods used to obtain verifiable  
16          parental consent prior to any collection, use, and/or disclosure of personal  
17          information or the methods used to avoid collecting, using, and/or disclosing  
18          personal information;
- 19          7. Provide a statement setting forth in detail the means provided for parents to  
20          review any personal information collected and to refuse to permit its further use  
21          or maintenance;
- 22          8. Provide a statement setting forth in detail the procedures used to protect the  
23          confidentiality, security, and integrity of personal information collected; and  
24  
25  
26  
27  
28

1           9. Provide a copy of each Order Acknowledgment obtained pursuant to this Order,  
2           unless previously submitted to the Commission.

3           B. For ten (10) years after entry of this Order, each Defendant must submit a compliance  
4           notice, sworn under penalty of perjury, within 14 days of any change in: (a) any  
5           designated point of contact; or (b) the structure of any Defendant or any entity that  
6           Defendant has any ownership interest in or controls directly or indirectly that may affect  
7           compliance obligations arising under this Order including: creation, merger, sale, or  
8           dissolution of the entity or any subsidiary, parent, or affiliate that engages in any acts or  
9           practices subject to this Order.

10           C. Each Defendant must submit to the Commission notice of the filing of any bankruptcy  
11           petition, insolvency proceeding, or similar proceeding by or against such Defendant  
12           within 14 days of its filing.

13           D. Any submission to the Commission required by this Order to be sworn under penalty of  
14           perjury must be true and accurate and comply with 28 U.S.C. § 1746, such as by  
15           concluding: “I declare under penalty of perjury under the laws of the United States of  
16           America that the foregoing is true and correct. Executed on: \_\_\_\_\_” and supplying the  
17           date, signatory’s full name, title (if applicable), and signature.

18           E. Unless otherwise directed by a Commission representative in writing, all submissions to  
19           the Commission pursuant to this Order must be emailed to [Debrief@ftc.gov](mailto:Debrief@ftc.gov) or sent by  
20           overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement,  
21           Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue  
22           NW, Washington, DC 20580. The subject line must begin: United States v. VTech  
23           Electronics Limited.  
24  
25  
26  
27  
28

**IX. RECORDKEEPING**

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

- A. All records necessary to demonstrate full compliance with each provision of this Order, including all submissions to the Commission;
- B. Copies of all consumer complaints relating to Defendants' collection of covered information, and any response; and
- C. A copy of each materially different form, page, or screen created, maintained, or otherwise provided by Defendants through which covered information is collected, and a copy of each materially different document containing any representation regarding collection, use, and disclosure practices pertaining to covered information. Each webpage copy shall be accompanied by the URL of the webpage where the material was posted online. Electronic copies shall include all text and graphics files, audio scripts, and other computer files used in presenting information on the Internet.

**X. COMPLIANCE MONITORING**

IT IS FURTHER ORDERED that, for the purpose of monitoring Defendants; compliance with this Order:

- A. Within fourteen (14) days of receipt of a written request from a representative of the Commission or Plaintiff, each 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

1 procedure prescribed by Federal Rules of Civil Procedure 29, 30 (including telephonic  
2 depositions), 31, 33, 34, 36, 45, and 69.

3 B. For matters concerning this Order, the Commission and Plaintiff are authorized to  
4 communicate directly with each Defendant. Defendants must permit representatives of  
5 the Commission and Plaintiff to interview any employee or other person affiliated with  
6 Defendants who has agreed to such an interview. The person interviewed may have  
7 counsel present.  
8

9 C. The Commission and Plaintiff may use all other lawful means, including posing, through  
10 its representatives as consumers, suppliers, or other individuals or entities, to Defendants  
11 or any individual or entity affiliated with Defendants, without the necessity of  
12 identification or prior notice. Nothing in this Order limits the Commission's lawful use  
13 of compulsory process, pursuant to Sections 9 and 20 of the FTC Act, 15 U.S.C. §§ 49,  
14 57b-1.  
15

16 **XI. RETENTION OF JURISDICTION**

17 IT IS FURTHER ORDERED that this Court retains jurisdiction of this matter for  
18 purposes of construction, modification, and enforcement of this Order.  
19

20 **SO ORDERED this \_\_\_\_\_ day of \_\_\_\_\_, 2018.**  
21  
22  
23

24 \_\_\_\_\_  
25 UNITED STATES DISTRICT JUDGE  
26  
27  
28

1 **SO STIPULATED AND AGREED:**

2  
3 **FOR PLAINTIFF UNITED STATES OF AMERICA**

4 CHAD A. READLER  
5 Acting Assistant Attorney General  
6 Civil Division

7 JOHN R. LAUSCH, JR.  
8 United States Attorney  
9 Northern District of Illinois

10 ETHAN P. DAVIS  
11 Deputy Assistant Attorney General

12 GUSTAV W. EYLER  
13 Acting Director  
14 Consumer Protection Branch

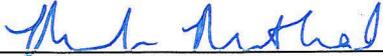
15 ANDREW E. CLARK  
16 Assistant Director

17 

18 JOSHUA D. ROTHMAN  
19 Trial Attorney  
20 Consumer Protection Branch  
21 U.S. Department of Justice  
22 P.O. Box 386  
23 Washington, DC 20044  
24 (202) 514-1586  
25 Joshua.D.Rothman@usdoj.gov  
26  
27  
28

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

**FOR THE FEDERAL TRADE COMMISSION**



MANEESHA MITHAL  
Associate Director  
Division of Privacy and Identity Protection



MARK EICHORN  
Assistant Director  
Division of Privacy and Identity Protection



JACQUELINE K. CONNOR  
Attorney  
Division of Privacy and Identity Protection  
Federal Trade Commission  
600 Pennsylvania Avenue NW  
Washington, DC 20580  
Tel: (202) 326-2844  
Fax: (202) 326-3062  
jconnor@ftc.gov



KATHERINE WHITE  
Attorney  
Division of Privacy and Identity Protection  
Federal Trade Commission  
600 Pennsylvania Avenue NW  
Washington, DC 20580  
Tel: (202) 326-2878  
Fax: (202) 326-3062  
kwhite@ftc.gov

1 **FOR DEFENDANTS**

2 

Date: 10/24/2017

3 MICHAEL VATIS

4 Steptoe & Johnson LLP  
5 1114 Avenue of the Americas  
6 New York, NY 10036  
7 Tel: (212) 506-3927  
8 Fax: (212) 506-3950  
9 mvatis@steptoe.com

10 *Counsel for VTech Electronics Limited and VTech Electronics North America, LLC*

11 

Date: 10/24/2017

12 LYDIA PARNES

13 Wilson Sonsini Goodrich & Rosati  
14 1700 K Street, NW  
15 Fifth Floor  
16 Washington, DC 20006  
17 Tel: (202) 973-8801  
18 lparnes@wsgr.com

19 *Counsel for VTech Electronics Limited and VTech Electronics North America, LLC*

20 

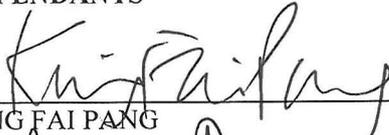
Date: 10/24/17

21 CHRISTOPHER N. OLSEN

22 Wilson Sonsini Goodrich & Rosati  
23 1700 K Street, NW  
24 Fifth Floor  
25 Washington, DC 20006  
26 Tel: (202) 973-8803  
27 colsen@wsgr.com

28 *Counsel for VTech Electronics Limited and VTech Electronics North America, LLC*

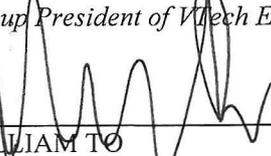
**DEFENDANTS**

21 

Date: 10/20/17

22 KING FAI PANG

23 *Group President of VTech Electronics Limited*

24 

Date: 10/20/17

25 WILLIAM TO

26 *President of VTech Electronics North America, LLC*

27  
28

**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.

**§ 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.

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.<sup>401</sup> 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.<sup>402</sup> 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]." <sup>403</sup>

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 <sup>404</sup> 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." <sup>405</sup>

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

<sup>403</sup> 15 U.S.C. 6502(a)(1).

<sup>404</sup> If the third-party plug-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.

<sup>405</sup> 16 CFR 312.2 (Definitions).

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." <sup>406</sup> 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." <sup>407</sup> 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**

<sup>406</sup> 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).

<sup>407</sup> *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.")

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