

Complaint

IN THE MATTER OF

RETINA-X STUDIOS, LLC**AND****JAMES N. JOHNS, JR.**CONSENT ORDER, ETC. IN REGARD TO ALLEGED VIOLATIONS OF SECTION 5 OF THE FEDERAL
TRADE COMMISSION ACT AND THE CHILDREN’S ONLINE PRIVACY PROTECTION ACT*Docket No. C-4711; File No. 172 3118*
Complaint, March 26, 2020 – Decision, March 26, 2020

This consent order addresses Retina-X Studios, LLC’s, a limited liability company, and James N. Johns, Jr.’s., individually and as sole member of Retina-X Studios, LLC, violation of the Federal Trade Commission Act and the Children’s Privacy Protection Rule. The complaint alleges that Respondents’ mobile device monitoring products and services, MobileSpy, PhoneSheriff, and TeenShield, did not take any steps to ensure that purchasers would use the products and services to only monitor employees or children. The Respondents’ monitoring products and services substantially injured device users by enabling purchasers to surreptitiously stalk them and obtain sensitive personal information without authorization. The consent order requires Respondents to restrain promoting, selling, or distributing a monitoring product or service unless Respondents comply with not requiring product or service functionality to circumvent security protections implemented by the mobile device operating system or manufacturer. Respondents must obtain the express written attestation, prior to sale or distribution, from the purchaser that it will use the monitoring product and service for legitimate and lawful purposes.

Participants

For the *Commission*: Megan Cox, Jonah Fabricant, and Shameka Walker.

For the *Respondents*: Alexandra Megaris and Jami M. Vibbert, Venable LLP.

COMPLAINT

The Federal Trade Commission, having reason to believe that Retina-X Studios, LLC, a limited liability company, and James N. Johns, Jr., individually and as sole member of Retina-X Studios, LLC (collectively, “Respondents”), have violated the provisions of the Federal Trade Commission Act (“FTC Act”) and the Children’s Privacy Protection Rule (“Rule” or “COPPA Rule”), and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent Retina-X Studios, LLC (“Retina-X”) is a Florida limited liability company with its principal place of business in 731 Duval Station Road, Suite 107, Box 203, Jacksonville, Florida 32218.
2. Respondent James N. Johns, Jr. (“Johns”) is the registered agent and sole member of Retina-X. Individually or in the concert of others, he controlled or had the authority to control, or participated in that acts and practices of Retina-X, including the acts and practices alleged in this complaint. His principal office or place of business is the same as that of Retina-X.

Complaint

3. The acts and practices of Respondents alleged in this complaint have been in or affecting commerce, as “commerce” is defined in Section 4 of the FTC Act.

RESPONDENTS’ BUSINESS ACTIVITIES

4. As recently as April 2018, Respondents developed and sold various monitoring products and services, each with the means to allow a purchaser to monitor, often surreptitiously, another person’s activities on that person’s mobile device or computer (the “device user”). Respondents offered various monitoring products and services with varying capabilities and costs.

- a. **MobileSpy:** Respondents’ MobileSpy mobile device monitoring product and service (“MobileSpy”) was marketed as a product to monitor children or employees. MobileSpy first became available in 2007, and Respondents sold more than 5,700 MobileSpy licenses. Once installed, MobileSpy captured and logged, among other things, the following: text messages; messages sent and received on various messaging services; call history; keys pressed; GPS locations; photos; contact list; screenshots; and browser history. MobileSpy’s premium version also permitted monitoring consumers, from a remote online dashboard, to view the monitored mobile device’s screen in real time.
- b. **PhoneSheriff:** Respondents’ PhoneSheriff mobile device monitoring product and service (“PhoneSheriff”) was marketed as a product to monitor children. PhoneSheriff first became available in 2011, and Respondents sold more than 4,600 PhoneSheriff licenses. Once installed, PhoneSheriff captured and logged, among other things, the following: GPS locations; text messages; messages sent and received on various messaging services; call history; photos; contact list; browser history; notes; music files; calendar entries; applications installed; mobile usage summaries; email history; and screenshots of any activity using the Snapchat application.
- c. **TeenShield:** Respondents’ TeenShield mobile device monitoring product and service (“TeenShield”) was marketed as a product to monitor children. TeenShield first became available in 2015, and Respondents sold more than 5,000 TeenShield licenses. As part of the TeenShield for iOS registration process, Respondents collected dates of birth of users being monitored. From February 2016 to October 2017, Respondents collected approximately 950 dates of birth, and about a third of those were for children under the age of 13. Once installed, TeenShield captured and logged, among other things, the following: GPS locations; text messages; messages sent and received on various messaging services; call history; photos; contact list; browser history; and email history.

Complaint

5. Purchasers were often required to jailbreak or root (i.e., actions to bypass various restrictions implemented by the operating system on and/or the manufacturer of mobile devices) the device user's mobile device prior to installing Respondents' monitoring products and services. Jailbreaking or rooting a mobile device can expose a mobile device to various security vulnerabilities and likely invalidates any warranty that a mobile device manufacturer or carrier provides.

6. All of Respondents' monitoring products and services required that the purchaser have physical access to the device user's mobile device or computer to install the monitoring products and services. Once Respondents' monitoring products and services were installed, the purchaser did not need physical access to the mobile device or computer, and could remotely monitor the device user's activities from an online dashboard.

7. By default, Respondents' monitoring products and services disclosed to the device user that they were being monitored (e.g., an icon on a monitored mobile device). However, purchasers could turn off this feature so that the monitoring products and services could run surreptitiously, meaning that the device user was unaware that he or she was being monitored. Respondents provided purchasers with instructions on how to remove the icon that would confirm that monitoring products and services were installed on a particular mobile device.

8. Device users surreptitiously monitored by Respondents' monitoring products and services could not uninstall or remove Respondents' monitoring products and services because they did not know that they were being monitored. Even if a device user suspected that they were being surreptitiously monitored, they had no way of knowing that Respondents' monitoring products and services were being used on their phone by the purchaser.

9. Despite stating in their terms of services that their monitoring products and services were to be used for monitoring employees or children, Respondents did not take any steps to ensure that purchasers would use Respondents' monitoring products and services for such purposes.

10. Moreover, the purported use of the monitoring products and services for employment or child-monitoring purposes is a pretext. Employers or parents would not typically jailbreak or root phones to install Respondents' monitoring products and services, particularly when many other monitoring products are available in the marketplace that do not require jailbreaking or rooting.

INJURY

11. Respondents' monitoring products and services substantially injured device users by enabling purchasers to surreptitiously stalk them. Stalkers and abusers use mobile device monitoring software to obtain victims' sensitive personal information without authorization and surreptitiously monitor victims' physical movements and online activities. Stalkers and abusers then use the information obtained via monitoring to perpetuate stalking and abusive behaviors, which cause mental and emotional abuse, financial and social harm, and physical harm, including death.

Complaint

12. Furthermore, victims of stalking experience financial loss both directly and indirectly. Directly, stalkers and abusers can use the information obtained through monitoring products and services to take over a victim's financial accounts, and redirect any (or all) funds to the abuser. Furthermore, victims suffer financial loss in the form of lost warranty coverage resulting from jailbreaking/rooting a mobile device and the purchase of a new mobile device to ensure that they are no longer subject to surreptitious monitoring. Indirectly, victims experience financial loss through the costs associated with therapy or counseling, and moving away from an abuser.

13. Even after stalking or domestic abuse ends, victims continue to experience substantial harms, including injury in the form of depression, anxiety, and safety fears.

14. The sale of Respondents' surreptitious monitoring products and services also substantially injured device users by undermining the mobile device security features provided by their operating system or manufacturer. Installation of Respondents' monitoring products and services required the purchaser to jailbreak or root a user's mobile device by bypassing various restrictions implemented by a mobile device operating system and/or manufacturer. Such jailbreaking or rooting may expose a mobile device to various security vulnerabilities, in part because a jailbroken/rooted phone may not receive security updates. With surreptitious monitoring products and services, these mobile device security risks are compounded by the fact that the device user is unaware that their mobile device has been jailbroken or rooted, and thus does not know that they should implement heightened safeguards to protect the security of their mobile device.

15. These harms were not reasonably avoidable by consumers, as users had no way to know that their mobile devices were being surreptitiously tracked using Respondents' monitoring products and services.

16. These harms are not outweighed by countervailing benefits to consumers or competition.

RESPONDENTS' DATA SECURITY PRACTICES

17. Even assuming Respondents believed that their monitoring products and services were being used for legitimate purposes, including the monitoring of children and employees, Respondents did not take steps to secure the personal information collected from purchasers and device users being monitored. As a result, the personal information collected from purchasers and device users was at risk of unauthorized disclosure and use.

18. Respondents outsourced most of their product development and maintenance to a service provider. The service provider developed Respondents' monitoring mobile applications, developed Respondents' websites (after 2005), managed Respondents' servers, managed Respondents' payment processing through a third party, provided marketing support for Respondents' monitoring products and services (until 2012), and ran customer support for Respondents' monitoring products and services (until 2016).

Complaint

19. Respondents used a third party cloud storage provider to store photos collected from mobile devices being monitored using PhoneSheriff or TeenShield.

20. Respondents engaged in a number of practices that, taken together, failed to provide reasonable data security to protect the personal information collected from consumers. Among other things, Respondents failed to:

- a. Adopt, implement, or maintain written information security standards, policies, procedures or practices;
- b. Conduct security testing of mobile applications that could be exploited to gain unauthorized access to consumers' sensitive personal information for well-known and reasonably foreseeable vulnerabilities;
- c. Contractually require their service providers to adopt and implement information security standards, policies, procedures or practices;
- d. Perform adequate oversight of service providers; and
- e. Adopt and implement written information security standards, policies, procedures, or practices that would apply to the oversight of their service providers.

21. In February 2017, a hacker found unencrypted credentials in the TeenShield Android Package Kit ("APK") for Respondents' cloud storage account. The hacker logged into this account, and once there, the hacker found a screenshot that included the username and password for Respondents' server. The hacker then used those server credentials to log into Respondents' server, where the hacker accessed data collected through the PhoneSheriff and TeenShield monitoring products and services. The data accessed included, among other things, login usernames, encrypted login passwords, text messages, GPS locations, contact lists, apps installed, browser history, and photos. The hacker erased the entire database.

22. Respondents only became aware that they had been breached two months later, in April 2017, when a journalist contacted Respondents. The hacker had contacted the journalist, and provided evidence to the journalist that the hacker had obtained users' data from Respondents.

23. One year later, in February 2018, a hacker again found the credentials for Respondents' cloud storage account, this time in the PhoneSheriff APK. This time, the account credentials were "obfuscated," according to terminology used by Respondents, but the hacker was nevertheless able to decrypt the credentials and access Respondents' cloud storage account.

Complaint

24. The hacker was able to access photos collected by mobile devices being monitored using PhoneSheriff and TeenShield. The hacker erased Respondents' cloud storage account, deleting all photos contained therein.

25. MobileSpy, PhoneSheriff and TeenShield have not been available for purchase since April 2018. However, Respondents' websites for each of these monitoring products and services remain online.

RESPONDENTS' DATA SECURITY REPRESENTATIONS

26. Since April 2007 Respondents' privacy policy for Mobile Spy has stated (*see* Exhibit A):

"It is company policy that our customer databases remain confidential and private...Your private information is safe with us."

27. Since April 2011 Respondents' privacy policy for PhoneSheriff has stated (*see* Exhibit B):

"It is company policy that our customer databases remain confidential and private...Your private information is safe with us."

28. Since December 2015 Respondents' privacy policy for TeenShield has stated (*see* Exhibit C):

"It is company policy that our customer databases remain confidential and private...Your private information is safe with us."

RESPONDENTS ARE SUBJECT TO THE COPPA RULE

29. The COPPA Rule applies to any operator of a commercial Web site or online service that has actual knowledge that it collects, uses, and/or discloses personal information from children. As described above, in Paragraph 4(c), Respondents collected user dates of birth during the TeenShield registration process, many of which indicated that the monitored user was a child under the age of 13. As a result, Respondents had actual knowledge that the TeenShield product was collecting, using, and/or disclosing personal information from children.

30. The COPPA Rule defines "personal information" to include, among other things, a first and last name; a home or other physical address including street name and name of a city or town; online contact information (i.e., an email address or other substantially similar identifier that permits direct contact with a person online, such as an instant messaging user identifiers, screen name, or user name); a persistent identifier such as an IP address that can be used to recognize a user over time and across different Web sites or online services; a photograph, video, or audio file where such file contains a child's image or voice; or information concerning the child or parents of that child that the operator collects online from the child and combines with an identifier described in this definition. Through TeenShield, Respondents collected personal information as

Complaint

defined in the Rule, including the content of text messages and emails, email addresses or user names for a child that could be used to contact the child, and photographs and audio files containing a child's image or voice. Respondents also collected information from the child concerning the child that was combined with other identifiers, such as the name or photograph of the child.

31. Among other things, the Rule requires that an operator with actual knowledge, like Respondents as operators of TeenShield, meet specific requirements prior to collecting online, using, or disclosing personal information from children, including but not limited to, establishing and maintaining reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.

VIOLATIONS OF THE FTC ACT**COUNT I – UNFAIRNESS**

32. As described in Paragraphs 4 to 16, Respondents sold monitoring products and services that required circumventing certain security protections implemented by the Mobile Device operating system or manufacturer, and did so without taking reasonable steps to ensure that the monitoring products and services will be used only for legitimate and lawful purposes by the purchaser. Respondents' actions cause or are likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition. This practice is an unfair act or practice.

COUNT II – DECEPTION (MOBILESPY)

33. As described in Paragraph 26, Respondents have represented, directly or indirectly, expressly or by implication, that consumers' personal information collected through the MobileSpy mobile device monitoring product and service, and stored in Respondents' databases, remains confidential, private, and safe.

34. In fact, as set forth in Paragraphs 20 through 24, consumers' personal information collected through the MobileSpy mobile device monitoring product and service, and stored in Respondents' databases, was not confidential, private, and safe. Therefore, the representations set forth in Paragraph 33 are false and misleading.

COUNT III – DECEPTION (PHONESHERIFF)

35. As described in Paragraph 27, Respondents have represented, directly or indirectly, expressly or by implication, that consumers' personal information collected through the PhoneSheriff mobile device monitoring product and service, and stored in Respondents' databases, remains confidential, private, and safe.

36. In fact, as set forth in Paragraphs 20 through 24, consumers' personal information collected through the PhoneSheriff mobile device monitoring product and service, and stored in Respondents' databases, was not confidential, private, and safe. Therefore, the representations set forth in Paragraph 35 are false and misleading.

Complaint

COUNT IV- DECEPTION (TEENSHIELD)

37. As described in Paragraph 28, Respondents have represented, directly or indirectly, expressly or by implication, that consumers' personal information collected through the TeenShield mobile device monitoring product and service, and stored in Respondents' databases, remains confidential, private, and safe.

38. In fact, as set forth in Paragraphs 20 through 24, consumers' personal information collected through the TeenShield mobile device monitoring product and service, and stored in Respondents' databases, was not confidential, private, and safe. Therefore, the representations as described in Paragraph 37 are false and misleading.

VIOLATION OF THE COPPA RULE**COUNT V – COPPA (TEENSHIELD)**

39. Respondents collected personal information from children under the age of 13 through the TeenShield product, which Respondents operated and had actual knowledge that children were being monitored using these online services.

40. In numerous instances, in connection with the acts and practices described above, Respondents collected, used, and/or disclosed personal information from children in violation of the Rule, including by failing to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children, in violation of Section 312.8 of the Rule, 16 C.F.R. § 312.8.

41. Respondents' acts or practices, as described in Paragraph 40 above, violated the COPPA Rule, 16 C.F.R. Part 312.

42. Pursuant to Section 1303(c) of COPPA, 15 U.S.C. § 6502(c), and Section 18(d)(3) of the FTC Act, 15 U.S.C. § 57a(d)(3), a violation of the Rule constitutes an unfair or deceptive act or practice in or affecting commerce, in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

43. The acts and practices of Respondents as alleged in this complaint constitute unfair or deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

THEREFORE, the Federal Trade Commission this twenty-sixth day of March, 2020, has issued this Complaint against Respondents.

By the Commission.

Complaint

Exhibit A

EXHIBIT A

Mobile Spy's Privacy and

www.mobile-spy.com/legal.html

MOBILE SPY
SMARTPHONE MONITORING SOFTWARE

Smartphone & Tablet Monitoring
Child and Employee Monitoring Software

HOME FEATURES PURCHASE COMPATIBILITY AFFILIATES SUPPORT LOGIN

Policies
Legal Policies for Mobile Spy

LIVE DEMO
How It Works Purchase

iPhone ANDROID BlackBerry ...more

All users of Mobile Spy are required to accept all the terms and conditions outlined on this page along with the **User Legal Agreement** when creating your account and upon purchase.

LEGAL POLICIES

PRIVACY POLICY

It is company policy that our customer databases remain confidential and private. We have not, will not, and won't ever sell names to "spammers" or other parties who would like to use our databases to advertise or solicit their products or services. Mobile Spy does not collect any information from your phone other than the information required for the product's successful operation. Your private information is safe with us.

COOKIES

Mobile-Spy.com uses cookies provided by third parties which allows us to deliver customized marketing to our visitors based on their site usage and avoid delivering irrelevant marketing to visitors.

- ✓ **Google Analytics:** allows us to understand how people interact with the Site, and help us to optimize Site performance, usability and users' experience.
- ✓ **Google Adwords:** allow us to deliver targeted information to users who look for our Service.
- ✓ **Retargeter:** used to deliver relevant and targeted ads to visitors of our Site by Google, across various Internet web sites.
- ✓ **FastSpring:** allows us to track which affiliate referred a visitor.

Controlling cookies: You can opt out of cookies at Google Ads Preferences Manager.

AUTOMATIC LICENSE RENEWAL

Help

Complaint

EXHIBIT A

The screenshot shows a web browser window with the address bar displaying "www.mobile-spy.com/legal.html". The website has a dark header with the "MOBILE SPY" logo and the tagline "SMARTPHONE MONITORING SOFTWARE". To the right of the logo, the text "Smartphone & Tablet Monitoring" is displayed, followed by "Child and Employee Monitoring Software" in smaller text. A navigation menu includes links for HOME, FEATURES, PURCHASE, COMPATIBILITY, AFFILIATES, SUPPORT, and LOGIN. The main content area is white and contains several sections of text, each preceded by a checkmark icon. The sections are: "AUTOMATIC LICENSE RENEWAL", "CANCELING YOUR AUTOMATIC LICENSE RENEWAL", "REFUND POLICY", and "ALLOWED USES POLICY". The "ALLOWED USES POLICY" section lists specific rules for monitoring children. A "Help" button is visible in the bottom right corner of the page.

Mobile Spy's Privacy and X

www.mobile-spy.com/legal.html

MOBILE SPY
SMARTPHONE MONITORING SOFTWARE

Smartphone & Tablet Monitoring
Child and Employee Monitoring Software

HOME FEATURES PURCHASE COMPATIBILITY AFFILIATES SUPPORT LOGIN

AUTOMATIC LICENSE RENEWAL
At the point where you made your Mobile Spy purchase and selected Automatic Renewal, you hereby agree that you will be automatically billed upon the end of your license interval that you selected:

- ✓ **Quarterly: every three (3) months**
- ✓ **Semi-Annually: every six (6) months**
- ✓ **Annually: every twelve (12) months**

If at any time, you can cancel your license plan. When this occurs, your automatic billing license plan will be terminated and your Mobile Spy account will be disabled effective immediately. Please be aware that once you enter a new license plan billing cycle, refunds will not be given for that new time period.

CANCELING YOUR AUTOMATIC LICENSE RENEWAL
To cancel your automatic license plan renewal, please contact Retina-X Studios by either submitting a support ticket at the at the Retina-X Studios Helpdesk or by chatting live with a support agent on the [support page](#).

Please be aware that when you cancel your automatic license plan renewal, your Mobile Spy account will be disabled at that time from further use. It is recommended once you cancel your billing license plan to remove Mobile Spy from all devices associated with your account.

REFUND POLICY
As with all competitors, we do not issue refunds for simply changing your mind. If you experience technical issues with our software, we will work with you to resolve these issues in a timely manner. If these issues cannot be resolved in a timely manner, a refund of the purchase price will be issued if the software is proven defective. We reserve the right to refund an order and discontinue support and service if you are threatening us or we determine you are using the service for disallowed purposes.

ALLOWED USES POLICY
Mobile Spy is designed only to be used to monitor your underage child or employee. Retina-X Studios defines each as:

- ✓ **Child: Your own legal child that is under the legal age of 18 (as defined by US law). The child must be monitored using a compatible phone that you own. You cannot monitor a child if you hold one of the following relationships:**
 - ✓ **Brother / Sister**
 - ✓ **Step-Brother / Step-Sister**
 - ✓ **Step-Father / Step-Mother**

Help

Complaint

EXHIBIT A

The screenshot shows a web browser window with the address bar displaying "www.mobile-spy.com/legal.html". The website has a dark header with the "MOBILE SPY" logo and the tagline "SMARTPHONE MONITORING SOFTWARE". To the right of the logo, navigation links include "HOME", "FEATURES", "PURCHASE", "COMPATIBILITY", "AFFILIATES", "SUPPORT", and "LOGIN". Further right, the text "Smartphone & Tablet Monitoring" is displayed, followed by "Child and Employee Monitoring Software".

The main content area lists monitoring capabilities with checkmarks:

- ✓ Step-Father / Step-Mother
- ✓ Aunt / Uncle Cousin / Nephew
- ✓ Grandfather / Grandmother
- ✓ Great-Grandfather / Great-Grandmother
- ✓ **Employee: Your employee at a company you own OR an employee at the same company as you and you have managerial responsibilities for. The employee must be monitored using a compatible phone owned by the company and issued to the employee under your company's policies regarding company phones. The employee must give consent and be notified they are being monitored before monitoring can begin.**

Below the list, a paragraph states: "Mobile Spy cannot be used to monitor any other individuals (such as a spouse, friend, significant other, parolee, probationer, etc.). This would violate the terms you agreed to at the point of purchase and be subject to immediate termination without reimbursement."

OTHER POLICIES

You agree that you will comply fully with all relevant export laws and regulations applicable to you, including, without limitation, the U.S. Export Administration Regulations if you are a resident of the United States (collectively referred herein as "Export Controls"). Without limiting the generality of the foregoing, you will not, and you will require your representatives not to, export, direct or transfer the Software, or any direct product thereof, to any destination, person or entity restricted or prohibited by the Export Controls.

If you are entering into this Agreement on behalf of any agency or instrumentality of the United States Government, the Software is "commercial computer software" and "commercial computer software documentation" and pursuant to FAR 12.212 or DFARS 227.7202, and their successors, as applicable, use, reproduction, and disclosure of the Software are governed by the terms of this Agreement.

You agree that you will not (1) intercept, examine or otherwise observe any proprietary communications protocol used by the Software, whether through the use of a network analyzer, sniffer or other program or device; or (2) use any type of virus, clock, timer, counter, worm, bot, spider, software lock, drop dead device, Trojan-horse, routing, trap door, time bomb or any other codes, instructions or third-party software that is designed to provide a means of surreptitious or unauthorized access to, or distort, delete, damage or disassemble, the Software.

You must be at least 18 years of age to purchase any of our products. You agree that you will not allow any other party to register your account, install or use the software or account login. The account email registered to the account must match the account email used during purchase.

In the bottom right corner, there is a "Help" button with a question mark icon.

Complaint

EXHIBIT A

The screenshot shows a web browser window with the address bar displaying "www.mobile-spy.com/segas.html". The website header features the "MOBILE SPY" logo and navigation links: HOME, FEATURES, PURCHASE, COMPATIBILITY, AFFILIATES, SUPPORT, and LOGIN. The main content area contains the following text:

account must match the account email used during purchase.

Customers are made aware by the documentation on this web site that, as the owner of the phone to be monitored, unrestricted physical access to the phone to be monitored is required. Unrestricted physical access is defined as:

- ✓ **Customer has access to the device while the device is in their hands.**
- ✓ **Customer has all passwords, pass codes, lock screen codes, etc. to unlock the device to gain access.**

If a customer purchases this software and does not have unrestricted physical access to the phone to be monitored, refunds will not be issued due to this situation.

As it pertains to jailbreaking an iPhone and/or iPad, Retina-X Studios is not responsible for this process or assisting in this process as it is not a Retina-X Studios product or service. The **Compatibility** page on this web site clearly outlines that all iPhones and/or iPads must be jailbroken prior to installation and also, at the point of purchase, the customer agrees to this requirement. It is the customer's responsibility to jailbreak their iPhone or iPad on their own prior to purchasing the software. Refunds will not be issued to any customer who is either unable or unwilling to jailbreak their iPhone and/or iPad.

Also, refunds will not be given for any incompatibility issues. Incompatibility situations would include:

- ✓ **The phone to be monitored is running an operating system version that is not supported outlined on this web site's Compatibility page.**
- ✓ **A customer chooses (at their own discretion) to upgrade the phone they wish to monitor and the new desired phone to be monitored is running an operating system version that is not supported outlined on this web site's Compatibility page.**
- ✓ **The customer's underage child / employee upgrades the operating system version on their phone (irrespective to the owner's wishes) to an operating system version that is not supported outlined on this web site's Compatibility page.**

The **Compatibility** page in this web site outlines all of the compatible operating systems and versions the program supports so that proposed customers thinking of purchasing Mobile Spy will know which phone models and operating system versions are compatible prior to purchase.

Refunds are not issued if your child or employee performs a complete reset of the device that will, in turn, remove all installed software from the device including this monitoring software. If your child/employee performs a device

A "Help" button is visible in the bottom right corner of the page.

Complaint

EXHIBIT A

The screenshot shows a web browser window with the address bar displaying "www.mobile-spy.com/legal.html". The website has a dark header with the "MOBILE SPY" logo and the tagline "SMARTPHONE MONITORING SOFTWARE". To the right of the logo is a navigation menu with links: HOME, FEATURES, PURCHASE, COMPATIBILITY, AFFILIATES, SUPPORT, and LOGIN. Further right, the text "Smartphone & Tablet Monitoring" is displayed, with "Child and Employee Monitoring Software" underneath it.

The main content area contains several paragraphs of text:

- A paragraph stating that all installed software from the device including this monitoring software, if your child/employee performs a device reset, it is your responsibility to gain access to the device to reinstall our software in order to continue to monitor that individual's activities. As stated previously, it is your responsibility to alert your underage child or employee using a company-issued device that you are monitoring their activities.
- A paragraph stating that any customer who claims that their purchase was made in error or submitted fraudulent information will forfeit their right to any refund and will be held liable for all charges for the transaction. Our web site has built-in safeguards to prevent one-click purchasing by mistake. Also, if you feel someone has made the purchase using your information, Retina-X Studios requests you contact your bank to submit a fraudulent charge alert so that the bank can contact the appropriate parties to have it resolved.
- A paragraph stating that please be aware that once you enter a new license plan billing cycle, refunds will not be given for that new time period. If you wish not to renew, please contact us well in advance of the renewal date so that the account can be de-activated and no new charges will incur. It is the customer's responsibility to keep information on their license plan periods.
- A paragraph stating that as it pertains to the program's icon, the icon and notifications cannot be hidden or disabled. The program is not a hidden program but instead a monitoring software meant for legitimate monitoring by parents or employers. Refunds will not be given regarding these safeguards.
- A paragraph stating that please be aware that all refunds result in immediate discontinuation of services and support.
- A paragraph stating that all sales are final.

Below these paragraphs are two sections:

- TRIAL**: The price after the trial period is 49.97 USD. If you do not want to continue using this product/service, you can cancel the new subscription purchase before the trial ends and you will not be charged (we will email you 5 days before the trial ends to remind you). Otherwise, you will automatically be charged 49.97 USD to continue using the product/service without interruption.
- DISCLAIMER**: All our products are distributed and licensed on an "as is" basis and no warranties or guarantees of any kind are promised by Mobile Spy as to their performance, reliability or suitability to any given task. In no event shall Mobile Spy be liable for any loss of data or ANY DAMAGES OF ANY KIND, financial, physical, emotional or other, which might arise from its use.

At the bottom of the page, there is a paragraph about federal and state offenses related to installing monitoring software, followed by a "Help" button in the bottom right corner.

Complaint

EXHIBIT A

The screenshot shows a web browser window with the address bar displaying "www.mobile-spy.com/legal.html". The website has a dark header with the "MOBILE SPY" logo and the tagline "SMARTPHONE MONITORING SOFTWARE". Navigation links include HOME, FEATURES, PURCHASE, COMPATIBILITY, AFFILIATES, SUPPORT, and LOGIN. The main content area is titled "Smartphone & Tablet Monitoring" and "Child and Employee Monitoring Software".

governs the use of some types of software, it is responsibility of the user to follow such laws.

AGREEMENT
By installing, running, or using Mobile Spy you agree to the above Policies. In addition you agree that you will follow the Mobile Spy Policies at all times when using Mobile Spy. Failure to comply with our policies will result in the account being terminated without warning.

SOFTWARE END USER LICENSE AGREEMENT (EULA)
The smartphone/tablet software, artwork, music, and other components included in this product (collectively referred to herein as the "Software") are the copyrighted property of Retina-X Studios, LLC and its licensors (collectively referred to as "REX"). The Software is licensed (not sold) to you, and REX owns all copyright, trade secret, patent and other proprietary rights in the Software. You may use the Software on a single smartphone. You may not: (1) copy (other than once for back-up purposes), distribute, rent, lease or sublicense all or any portion of the Software; (2) modify or prepare derivative works of the Software; (3) transmit the Software over a network, by telephone or electronically using any means, except in the course of your network multi player play of the Software over authorized networks; (4) reverse engineer, decompile or disassemble the Software. You may transfer the Software, but only if the recipient agrees to accept the terms and conditions of this Agreement. If you transfer the Software, you must transfer all components and documentation and erase any copies residing on computer equipment. Your license is automatically terminated if you transfer the Software.

You expressly acknowledge and agree that use of the Software is at your sole risk. Except for the limited ninety (90) day warranty on the media set forth below, it is the user's responsibility to stop programs which might block Mobile Spy on the phone, should this situation arise. Due to the fact that the software is a digital good and registration information can not be reclaimed, we do not give refunds for simply changing your mind. All sales are final. License period starts at time of purchase. Logs older than thirty days are subject to automatic deletion.

REX warrants to the original consumer purchaser that the digital media furnished in this product will be free from defects in materials and workmanship under normal use for a period of ninety (90) days from the date of purchase (as evidenced by your receipt). If the digital media furnished in this product proves to be defective, and provided that the original consumer purchaser returns the media to REX in accordance with the instructions in this paragraph, REX will replace the defective digital media free of charge to the consumer purchaser, if the digital media proves to be defective within the ninety (90) day period following the date of purchase.

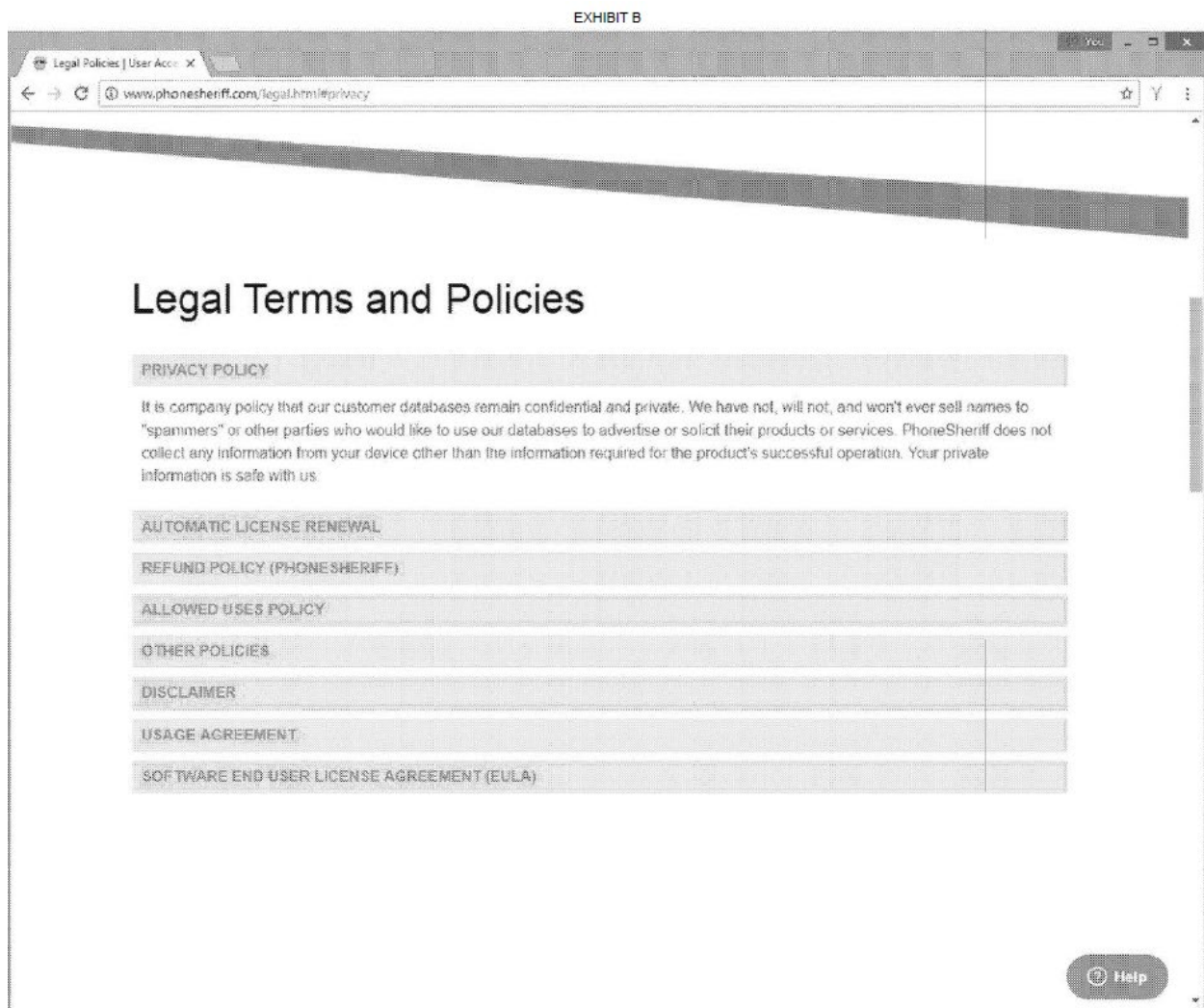
Terms are subject to change at any time.
© 2002-2015 Retina-X Studios, LLC. All rights reserved.

DEVICE REQUIREMENTS
Any compatible Android, iPhone or BlackBerry based smartphone or tablet including many models by Apple, Samsung, HTC, more

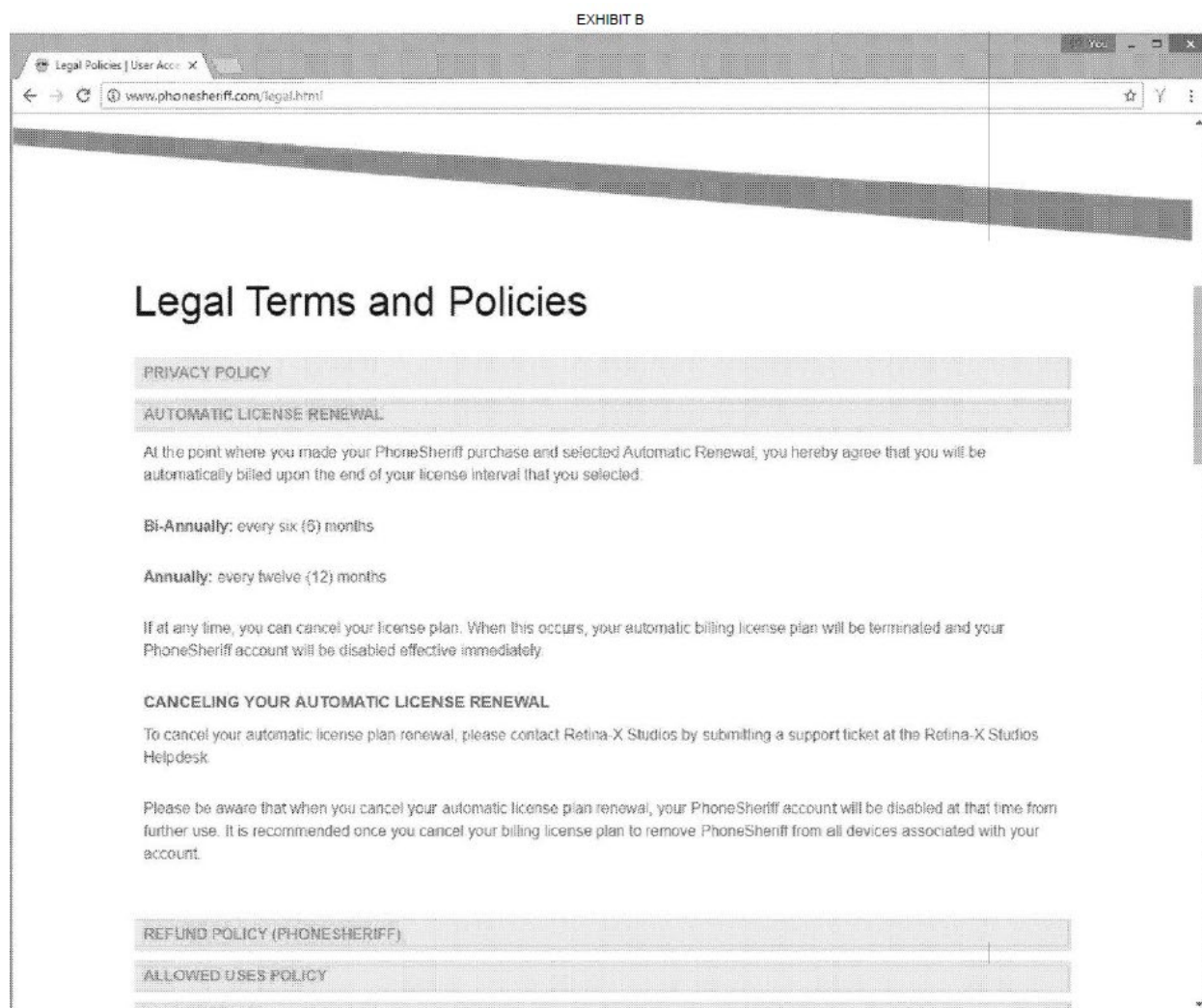
3 Months
\$49.97

Help

Complaint

Exhibit B

Complaint



Complaint

EXHIBIT B

Legal Policies | User Account X

www.phonesheriff.com/legal.html

Legal Terms and Policies

PRIVACY POLICY

AUTOMATIC LICENSE RENEWAL

REFUND POLICY (PHONE SHERIFF)

If any issues cannot be resolved in a timely manner, a refund of the purchase price will be issued if the software is proven defective. Any other refund or returned order (except where not allowed) is subject to a 10% payment processing fee. We reserve the right to refund an order and discontinue support and service if you are threatening us or we determine you are using the service for disallowed purposes. Customers are made aware by the documentation on this website that, as the owner of the device to be monitored, unrestricted physical access to the device to be monitored is required. Unrestricted physical access is defined as:

- Customer has access to the device while the device is in their hands.
- Customer has all passwords, pass codes, lock screen codes, etc. to unlock the device to gain access.

If a customer purchases this software and does not have unrestricted physical access to the device to be monitored, refunds will not be issued due to this situation.

As it pertains to jailbreaking an iPhone and/or iPad, Retina-X Studios is not responsible for this process or assisting in this process as it is not a Retina-X Studios product or service. The Compatibility page on this website clearly outlines that all iPhones and/or iPads must be jailbroken prior to installation and also, at the point of purchase, the customer agrees to this requirement. It is the customer's responsibility to jailbreak their iPhone or iPad on their own prior to purchasing the software. Refunds will not be issued to any customer who is either unable or unwilling to jailbreak their iPhone and/or iPad.

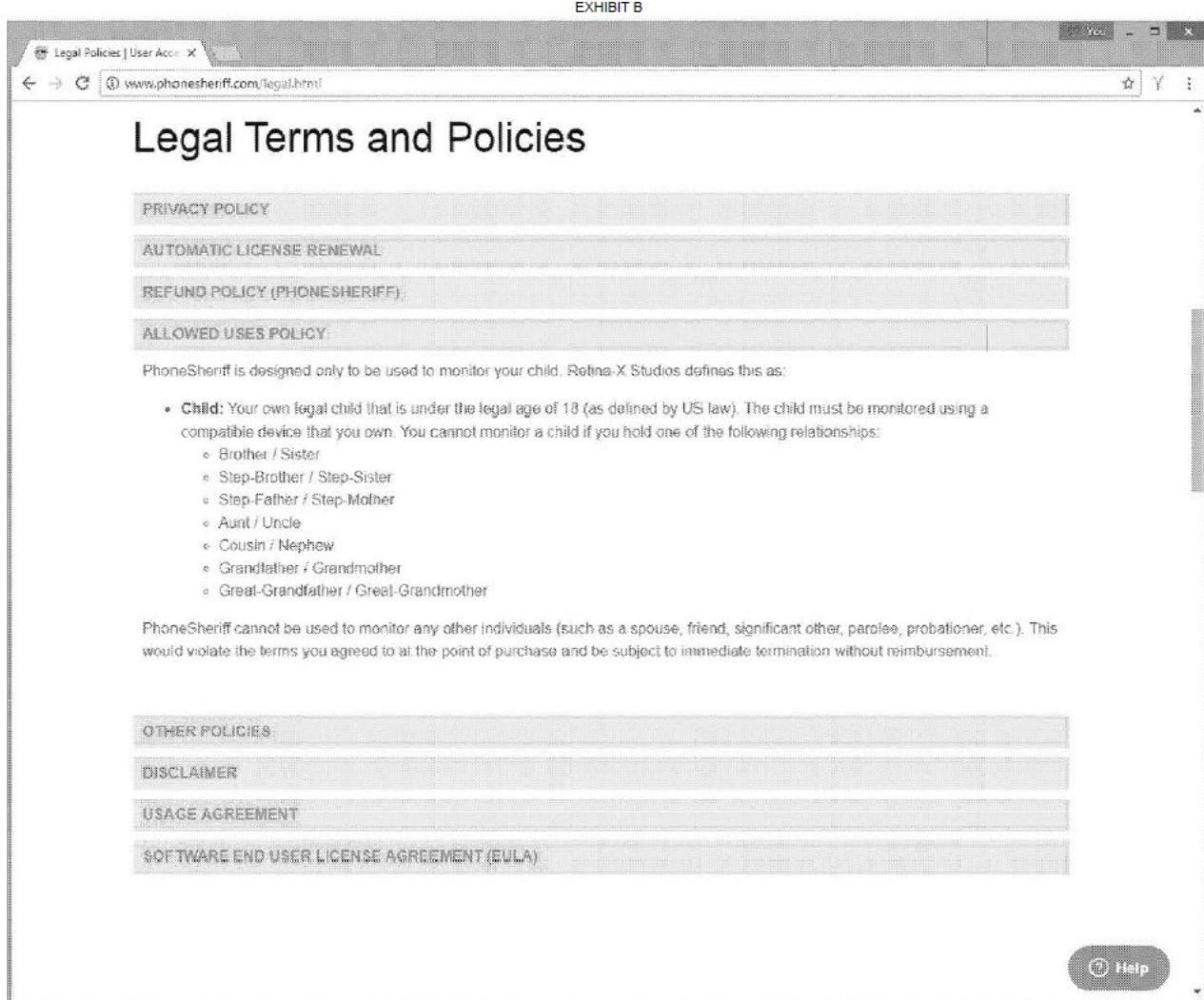
Also, refunds will not be given for any incompatibility issues. Incompatibility situations would include:

- The device to be monitored is running an operating system version that is not supported outlined on this website's Compatibility page.
- A customer chooses (at their own discretion) to upgrade the device they wish to monitor and the new desired device to be monitored is running an operating system version that is not supported outlined on this website's Compatibility page.
- The customer's underage child upgrades the operating system version on the device (irrespective to the owner's wishes) to an operating system version that is not supported outlined on this website's Compatibility page.

The Compatibility page in this website outlines all of the compatible operating systems and versions the program supports so that proposed customers thinking of purchasing the PhoneSheriff software will know which device models and operating system versions are compatible prior to purchase.

Help

Complaint



Complaint

EXHIBIT B

Legal Policies | User Account X

www.phonesheriff.com/legal.html

Legal Terms and Policies

- PRIVACY POLICY
- AUTOMATIC LICENSE RENEWAL
- REFUND POLICY (PHONESHERIFF)
- ALLOWED USES POLICY
- OTHER POLICIES

You agree that you will comply fully with all relevant export laws and regulations applicable to you, including, without limitation, the U.S. Export Administration Regulations if you are a resident of the United States (collectively referred herein as 'Export Controls'). Without limiting the generality of the foregoing, you will not, and you will require your representatives not to, export, direct or transfer the Software, or any direct product thereof, to any destination, person or entity restricted or prohibited by the Export Controls.

If you are entering into this Agreement on behalf of any agency or instrumentality of the United States Government, the Software is 'commercial computer software' and 'commercial computer software documentation' and pursuant to FAR 12.212 or DFARS 227.7202, and their successors, as applicable, use, reproduction, and disclosure of the Software are governed by the terms of this Agreement.

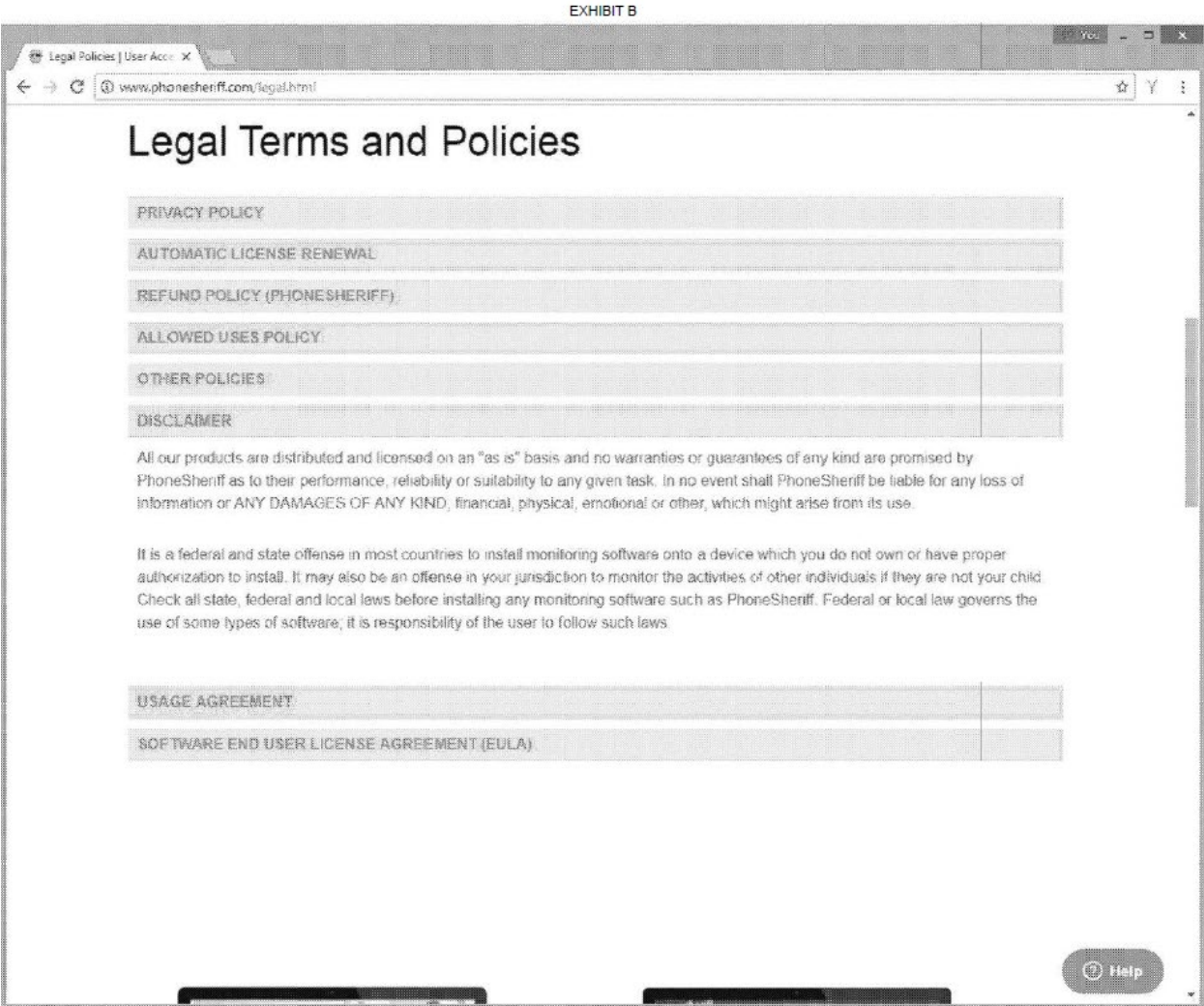
You agree that you will not (1) intercept, examine or otherwise observe any proprietary communications protocol used by the Software, whether through the use of a network analyzer, sniffer or other program or device; or (2) use any type of virus, clock, timer, counter, worm, bot, spider, software lock, drop dead device, Trojan-horse routing, trap door, time bomb or any other codes, instructions or third-party software that is designed to provide a means of surreptitious or unauthorized access to, or distort, delete, damage or disassemble, the Software.

You must be at least 18 years of age to purchase any of our products. You agree that you will not allow any other party to register your account, install or use the software or account login. The account email registered to the account must match the account email used during purchase.

- DISCLAIMER
- USAGE AGREEMENT
- SOFTWARE END USER LICENSE AGREEMENT (EULA)

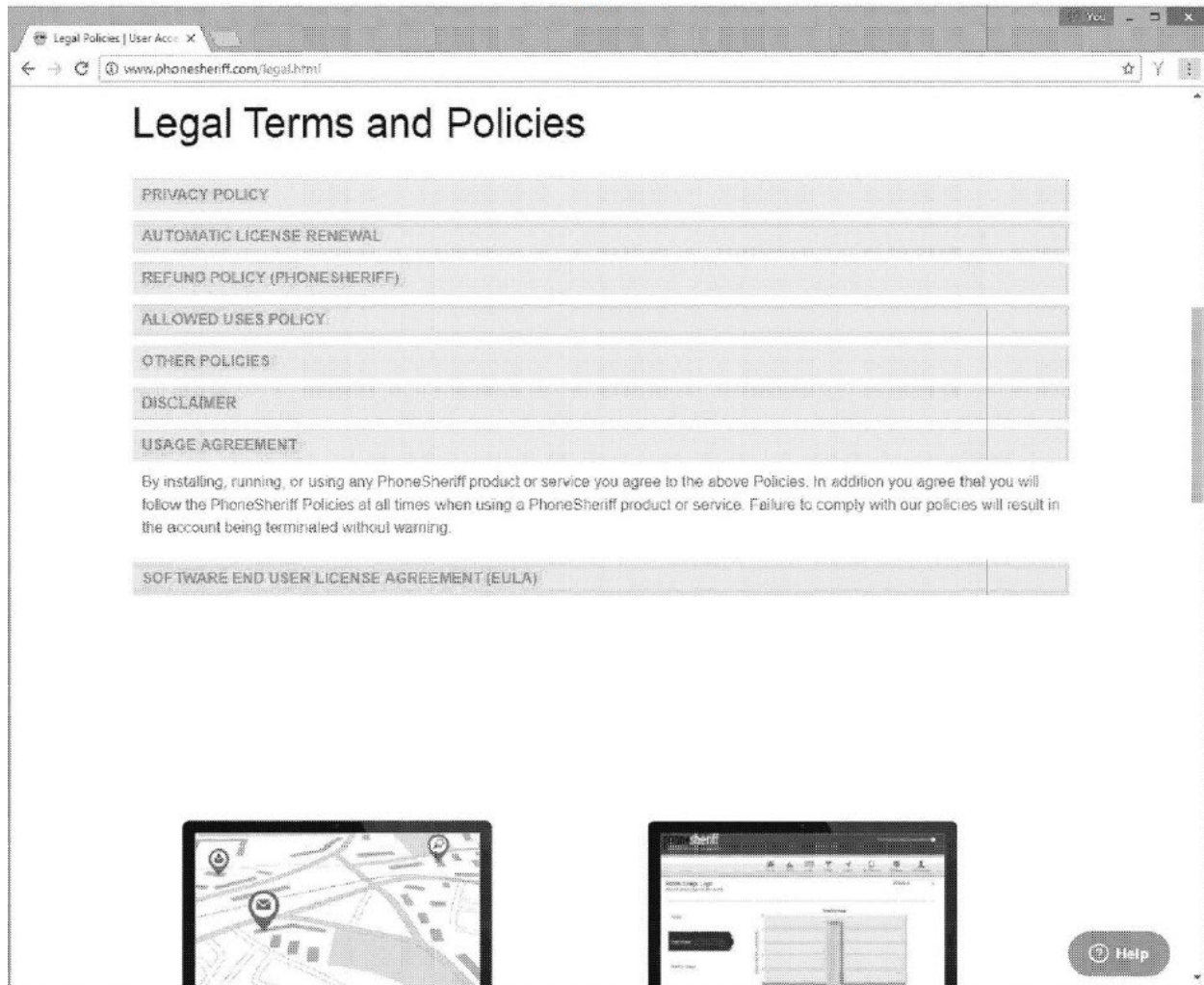
Help

Complaint

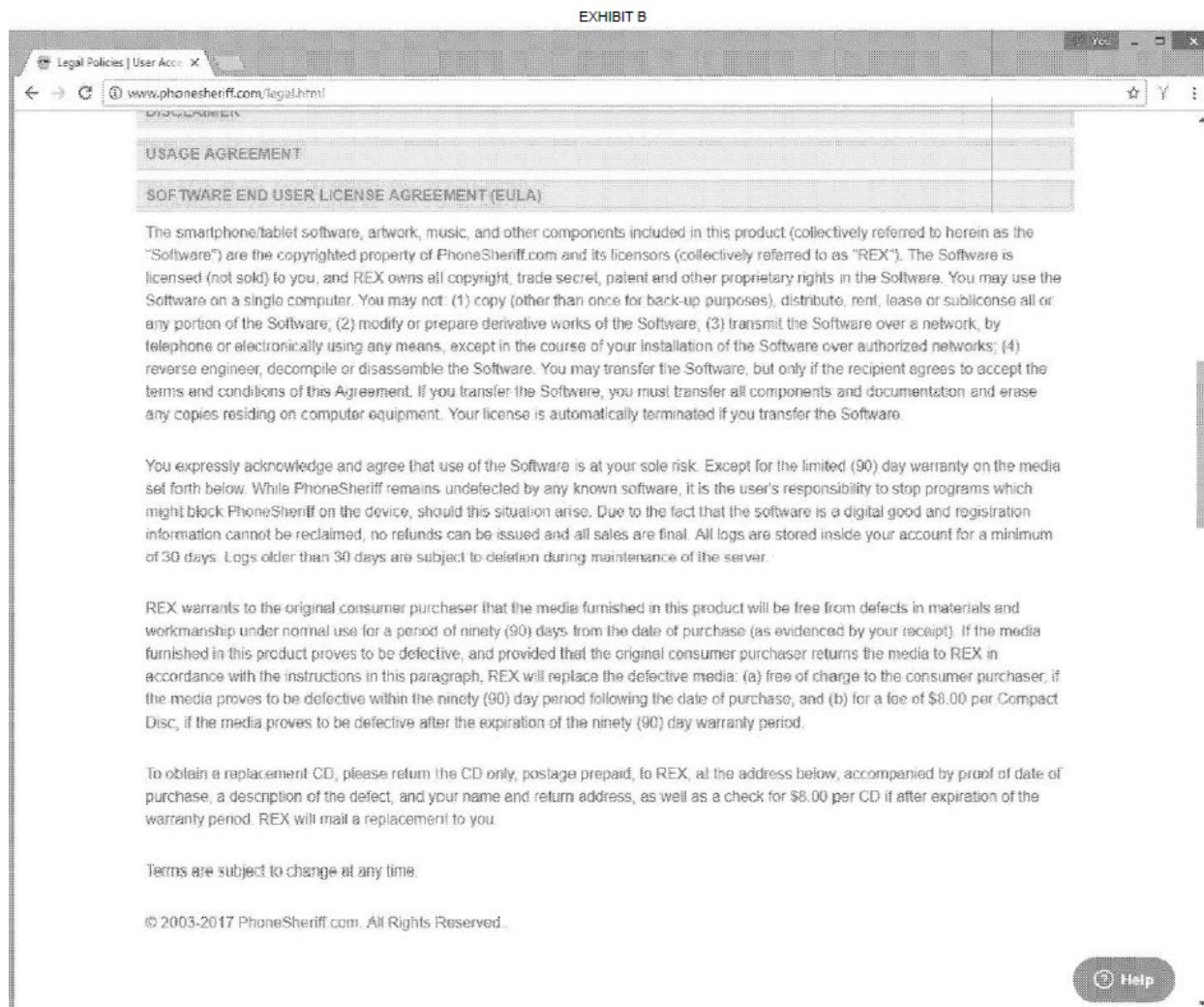


Complaint

EXHIBIT B



Complaint



Complaint

Exhibit C

EXHIBIT C



Legal | TeenShield Mobile

www.teenshield.com/legal.html

Home Features Support Blog Sign In

Legal Policies

End User License Agreement, Terms of Use and Privacy Policy.

TEENSHIELD END USER LICENSE AGREEMENT (EULA) AND TERMS OF USE

This TeenShield End User License Agreement (collectively referred to herein as the "Agreement") constitutes a binding agreement between you the purchaser of a TeenShield license (collectively referred to herein as the "User"), and Retina-X Studios, LLC (collectively referred to herein as "RXS"). You should read the following terms and policies carefully before installing the TeenShield application or using the TeenShield website (collectively referred to herein as the "Service"). If you do not agree to be bound by these policies, terms and conditions, you may not purchase or use the Service. The use of the Service is strictly prohibited unless you agree to be bound by the terms and conditions of this Agreement.

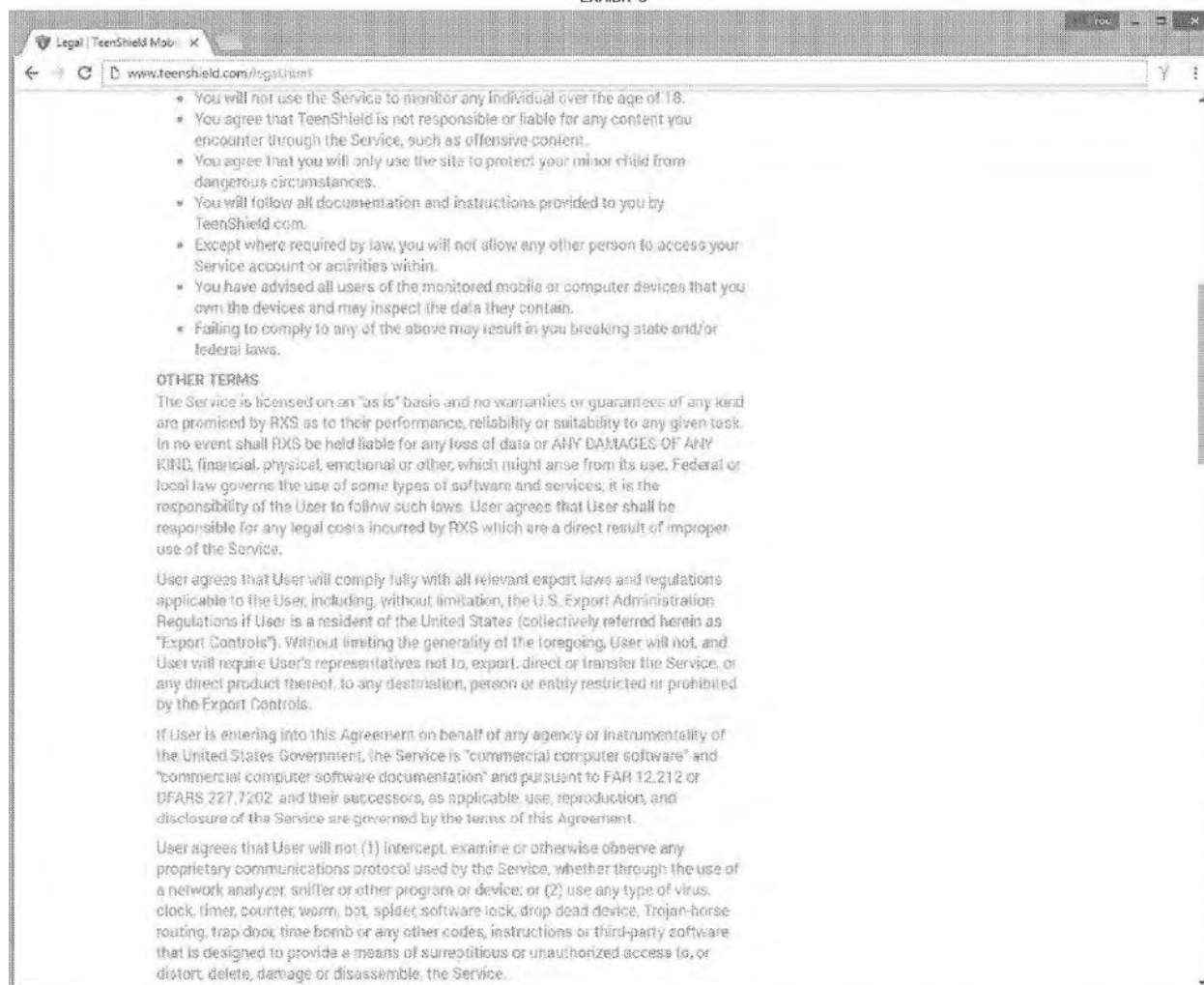
REPRESENTATION AND WARRANTIES

TeenShield provides you, as the legal guardian of one or more children under the age of 18, with the ability to view and collect various electronic activities of your children from computers or mobile devices. These activities may include but are not limited to text messages, locations, photos and activities on various applications. By purchasing and using the Service you hereby warrant, covenant, represent and certify the following:

- You will only use the Service to aid your efforts to protect your Minor Children for whom you are legal guardian.
- You will only use the Service to monitor computers or mobile devices of which you are the legal owner.
- You agree that as the guardian of your minor children you give yourself their consent to monitor activities.
- All information you provide to TeenShield is accurate and true including the age of your children.
- You will not use the Service to violate any law, rule or governmental regulation you are subject to.
- You consent to give TeenShield and its licensors access to the proper credentials needed to monitor your minor child.
- You consent to TeenShield granting you access to the activities through the password-protected Service.
- You will not use the Service to monitor any individual over the age of 18.

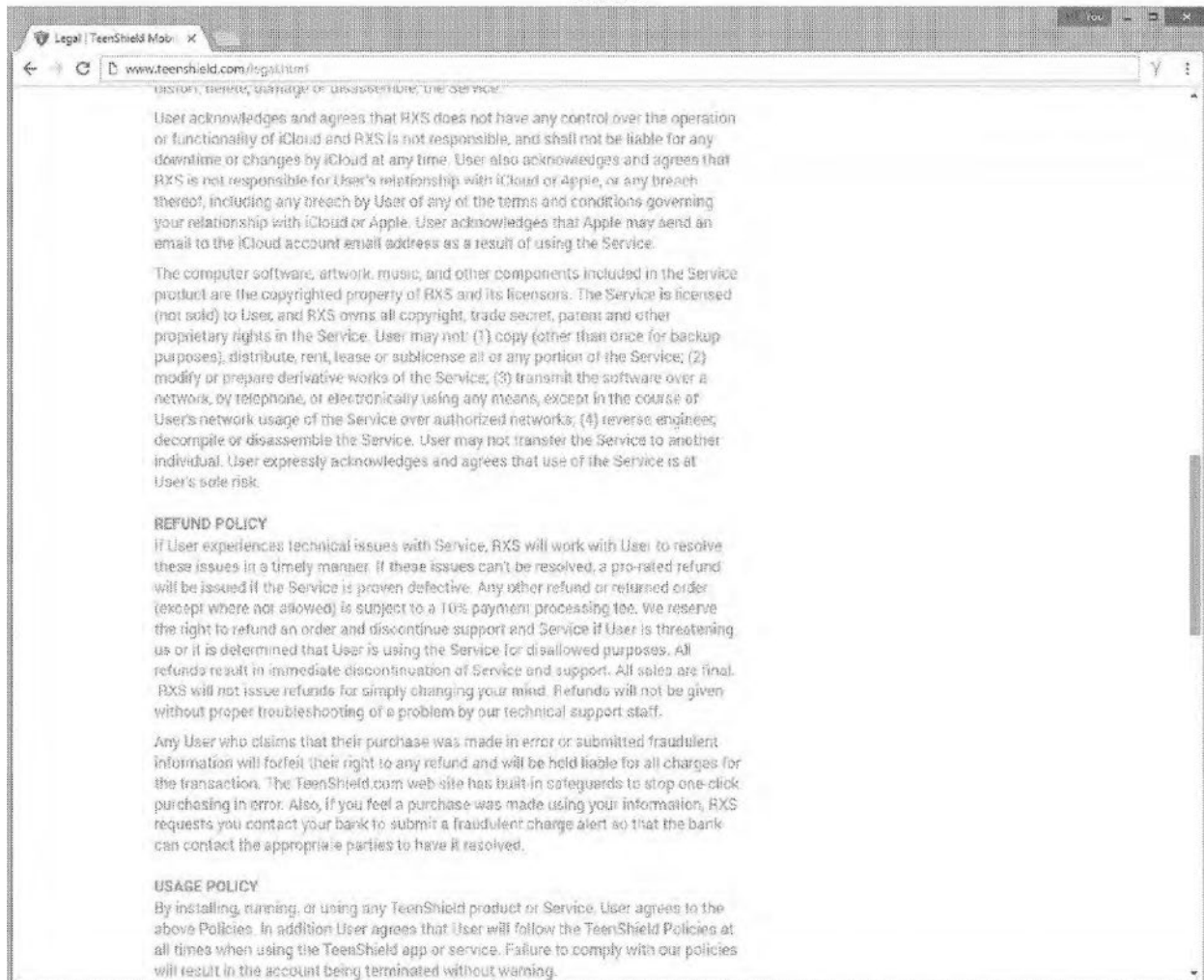
Complaint

EXHIBIT C

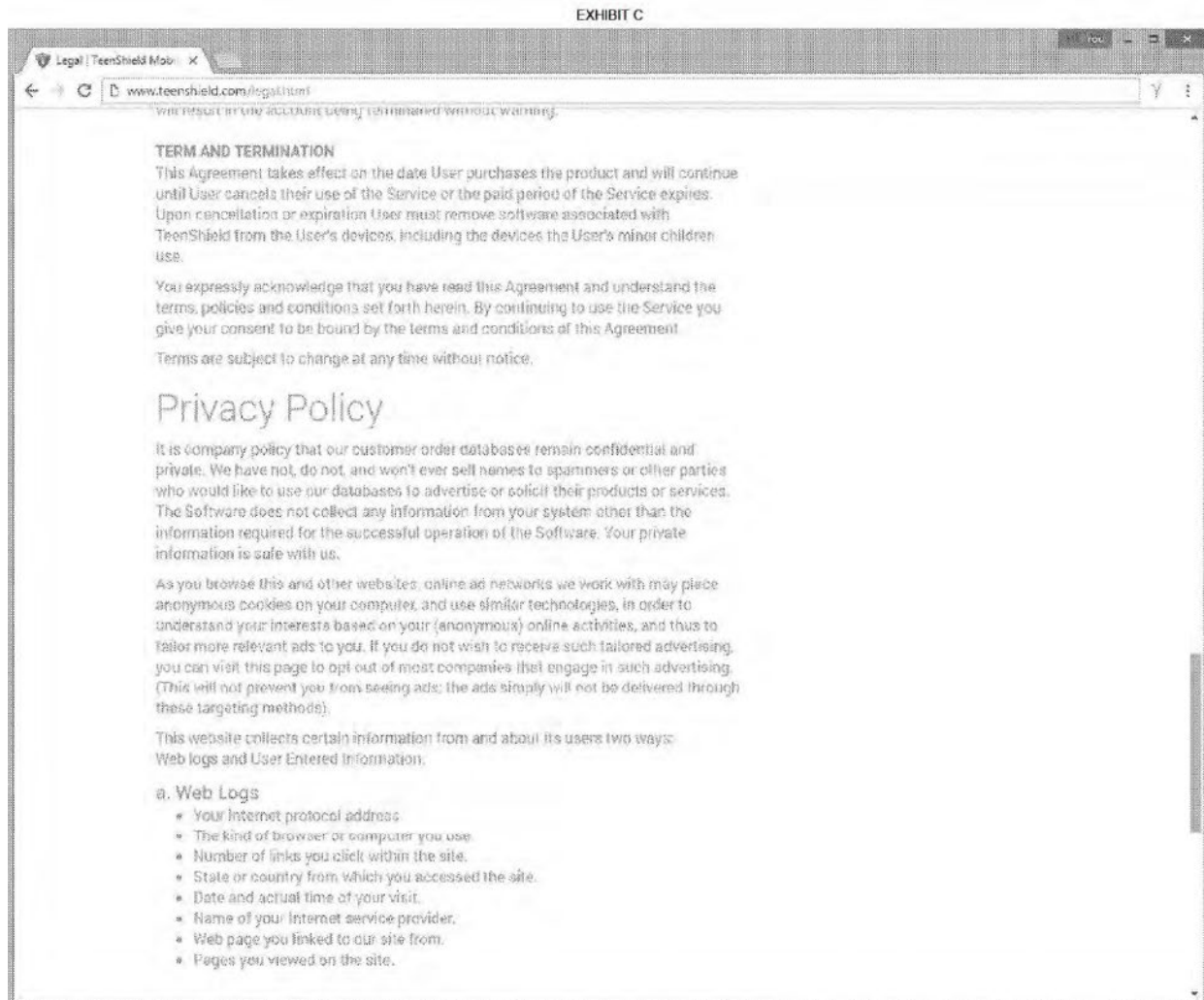


Complaint

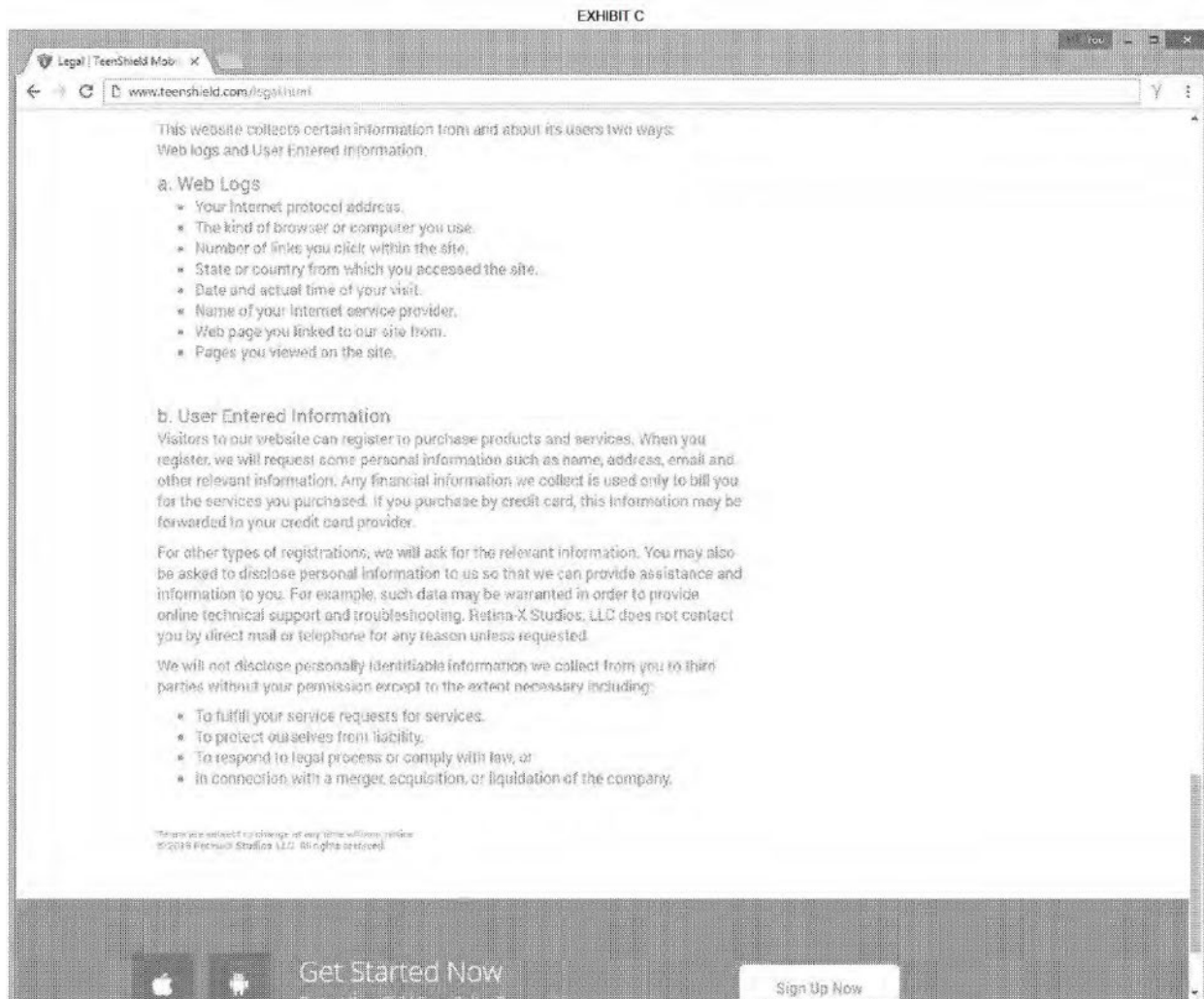
EXHIBIT C



Complaint



Complaint



Decision and Order

DECISION

The Federal Trade Commission (“Commission”) initiated an investigation of certain acts and practices of the Respondents named in the caption. The Commission’s Bureau of Consumer Protection (“BCP”) prepared and furnished to Respondents a draft Complaint. BCP proposed to present the draft Complaint to the Commission for its consideration. If issued by the Commission, the draft Complaint would charge the Respondents with violations of the Federal Trade Commission Act and the Children’s Online Privacy Protection Rule.

Respondents and BCP thereafter executed an Agreement Containing Consent Order (“Consent Agreement”). The Consent Agreement includes: 1) statements by Respondents that they neither admit nor deny any of the allegations in the Complaint, except as specifically stated in this Decision and Order, and that only for purposes of this action, they admit the facts necessary to establish jurisdiction; and 2) waivers and other provisions as required by the Commission’s Rules.

The Commission considered the matter and determined that it had reason to believe that Respondents have violated the Federal Trade Commission Act and the Children’s Online Privacy Protection Rule, and that a Complaint should issue stating its charges in that respect. The Commission accepted the executed Consent Agreement and placed it on the public record for a period of 30 days for the receipt and consideration of public comments. The Commission duly considered any comments received from interested persons pursuant to Section 2.34 of its Rules, 16 C.F.R. § 2.34. Now, in further conformity with the procedure prescribed in Rule 2.34, the Commission issues its Complaint, makes the following Findings, and issues the following Order:

Findings

1. The Respondents are:
 - a. Respondent Retina-X Studios, LLC, a Florida limited liability company with its principal place of business at 731 Duval Station Road, Suite 107, Box 203, Jacksonville, Florida 32218.
 - b. Respondent James N. Johns, Jr. the registered agent and sole member of Respondent Retina-X Studios, LLC. Individually or in concert with others, he formulates, directs, or controls the policies, acts, or practices of Retina-X Studios, LLC. His principal place of business is the same as that of Retina-X Studios, LLC.
2. The Commission has jurisdiction over the subject matter of this proceeding and over the Respondents, and the proceeding is in the public interest.

Decision and Order

ORDER**Definitions**

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

- A. “Child” or “Children” means an individual under the age of 13.
- B. “Clear(ly) and Conspicuous(ly)” means that a required disclosure is difficult to miss (i.e., easily noticeable) and easily understandable by ordinary consumers, including in all of the following ways:
 - 1. In any communication that is solely visual or solely audible, the disclosure must be made through the same means through which the communication is presented. In any communication made through both visual and audible means, such as a television advertisement, the disclosure must be presented simultaneously in both the visual and audible portions of the communication even if the representation requiring the disclosure is made in only one means.
 - 2. A visual disclosure, by its size, contrast, location, the length of time it appears, and other characteristics, must stand out from any accompanying text or other visual elements so that it is easily noticed, read, and understood.
 - 3. An audible disclosure, including by telephone or streaming video, must be delivered in a volume, speed, and cadence sufficient for ordinary consumers to easily hear and understand it.
 - 4. In any communication using an interactive electronic medium, such as the Internet or software, the disclosure must be unavoidable.
 - 5. The disclosure must use diction and syntax understandable to ordinary consumers and must appear in each language in which the representation that requires the disclosure appears.
 - 6. The disclosure must comply with these requirements in each medium through which it is received, including all electronic devices and face-to-face communications.
 - 7. The disclosure must not be contradicted or mitigated by, or inconsistent with, anything else in the communication.
 - 8. When the representation or sales practice targets a specific audience, such as Children, the elderly, or the terminally ill, “ordinary consumers” includes reasonable members of that group.

Decision and Order

- C. “Collects” or “Collection” means, for the purposes of Provision III of this Order, 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.
- D. “Covered Business” means Corporate Respondent, any business that Corporate Respondent controls, directly or indirectly, and any business that Individual Respondent controls, directly or indirectly.
- E. “Covered Incident” means any instance in which any United States federal, state, or local law or regulation requires a Covered Business or Individual Respondent to notify any U.S. federal, state, or local government entity that information collected or received, directly or indirectly, by a Covered Business from or about an individual consumer was, or is reasonably believed to have been, accessed or acquired without authorization.
- F. “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.
- G. “Internet” means collectively the myriad of computer and telecommunication facilities, including equipment and operating software, which comprises 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.
- H. “Jailbreak(ing) or Root(ing)” includes any action that bypasses a restriction by the Mobile Device manufacturer or operating system.

Decision and Order

- I. “Mobile Device” means any portable computing device that operates using a mobile operating system, including but not limited to, any smartphone, tablet, wearable, or sensor, or any periphery of any portable computing device.
- J. “Monitoring Product or Service” means any software application, program, or code that that can be installed on a user’s Mobile Device to track or monitor that user’s activities on the Mobile Device, including but not limited to, the user’s text messages, web browser history, geolocation, and photos.
- K. “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 identifier.
- L. “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 the 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.
- M. “Parent” includes a legal guardian.
- N. “Person” means any individual, partnership, corporation, trust, estate, cooperative, association, or other entity.
- O. “Personal Information” means individually identifiable information from or about an individual consumer, including:
 - 1. A first and last name;
 - 2. A home or other physical address;
 - 3. An email address;
 - 4. A telephone number;
 - 5. A Social Security number;
 - 6. A driver’s license or other government issues identification number;
 - 7. A financial account number;

Decision and Order

8. Credit or debit card information;
 9. Date of birth;
 10. Online Contact Information as defined in 16 C.F.R. § 312.2;
 11. A screen or user name where it functions in the same manner as Online Contact Information, as defined in 16 C.F.R. § 312.2;
 12. 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;
 13. A photograph, video, or audio file;
 14. Geolocation information sufficient to identify street name and name of a city or town; or
 15. Information concerning a Child or the parents of that Child that the Operator Collects online from the Child and combines with an identifier described in this section.
- P. “Respondents” means Corporate Respondent and Individual Respondent, individually, collectively, or in any combination.
1. “Corporate Respondent” means Retina-X Studios, LLC, and its successors and assigns.
 2. “Individual Respondent” means James N. Johns, Jr.
- Q. “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;

Decision and Order

- 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 16 C.F.R. §§ 312.5(c)(3) and (4).
 - 2. So long as the information Collected for the activities listed in paragraphs (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.
- R. “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, user 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, we 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 this 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:
 - a. Does not Collect Personal Information from any visitor prior to Collecting age information; and
 - b. Prevents the Collection, use, or disclosure or Personal Information from visitors who identify themselves as under age 13 without first complying with the notice and parental consent provisions of 16 C.F.R. Part 312, attached hereto as Appendix A.
 - 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

Decision and Order

to Children by using information location tools, including a directory, index, reference, pointer, or hypertext link

I. MONITORING PRODUCTS AND SERVICES

IT IS ORDERED that Respondents, and Respondents' officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, are permanently restrained and enjoined from, or assisting others in, promoting, selling, or distributing a Monitoring Product or Service unless Respondents comply with the following:

- A. **Mobile Device Security:** No Monitoring Product or Service's functionality may require circumventing security protections implemented by the Mobile Device operating system or manufacturer, such as by Jailbreaking or Rooting a Mobile Device.
- B. **Registration Attestation and Documentation:** Prior to the sale or distribution of any Monitoring Product or Service, Respondents must obtain:
 - 1. An express written attestation from the purchaser that it will use the Monitoring Product or Service for legitimate and lawful purposes by authorized users.
 - a. The express written attestation must state the legitimate and lawful purpose for which the purchaser is using the device, which may include only the following:
 - i. Parent monitoring a minor Child;
 - ii. Employer monitoring an employee who has provided express written consent to being monitored; or
 - iii. Adult monitoring another adult who has provided express written consent to being monitored;
 - b. Respondents cannot provide purchasers with written attestation language;
 - c. Respondents cannot suggest, direct, or otherwise assist, purchasers in submitting fraudulent written attestations; and
 - 2. Documentation proving that the purchaser is an authorized user on the monitored Mobile Device's service carrier account.
- C. **Icon Notice:** The Monitoring Product or Service must display an application icon, accompanied by the name of the Monitoring Product or Service adjacent to the

Decision and Order

application icon. The consumer must be able to click on the application icon to a page on which Respondents present a Clear and Conspicuous notice stating:

1. The name and material functions of the Monitoring Product or Service;
2. That the Monitoring Product or Service is running on the user's Mobile Device; and
3. Where and how the user can contact Respondents for additional information, or to resolve an issue of improper installation of the Monitoring Product or Service.

Exception to the Icon Notice Requirement:

1. Respondents may program the Monitoring Product or Service to allow the purchaser of the Monitoring Product or Service to disable the Icon Notice only if the purchaser attests, prior to installation, that the purchaser is the legal guardian or parent of a minor Child, and that the Monitoring Software or Product will be installed on a Mobile Device predominantly used by the minor Child.

II. ADDITIONAL WARNINGS AND NOTICES

IT IS FURTHER ORDERED that Respondents, and Respondents' officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, are permanently restrained and enjoined from, or assisting others in, promoting, selling, or distributing Monitoring Products or Services unless Respondents provide the purchaser with the following notices:

- A. Home Page Notice: The home page of any Internet website advertising the Monitoring Product or Service must Clearly and Conspicuously provide notice that the Monitoring Product or Service may only be used for legitimate and lawful purposes by authorized users, and that installing or using the Monitoring Product or Service for any other purpose may violate local, state, and/or federal law. The foregoing notice must be placed such that it can be viewed on the screen first seen by a potential purchaser who lands on the home page.
- B. Purchase Page Notice: Respondents may not complete the sale of a Monitoring Product or Service unless Respondents provide the purchaser with Clear and Conspicuous notice the Monitoring Product or Service may only be used for legitimate and lawful purposes by authorized users, and that installing or using the Monitoring Product or Service for any other purpose may violate local, state, and/or federal law.

Decision and Order

III. INJUNCTION CONCERNING THE COLLECTION OF PERSONAL INFORMATION

IT IS FURTHER ORDERED that Respondents, and Respondents' officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, in connection with being an operator of any Web site or online service directed to Children or of any Web site or online service with actual knowledge that it is Collecting or maintaining Personal Information from a Child, are hereby permanently restrained and enjoined from violating the Children's Privacy Protection Rule, 16 C.F.R. Part 312, including but not limited to failing to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of Personal Information from Children.

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

IV. PROHIBITION AGAINST MISREPRESENTATIONS

IT IS FURTHER ORDERED that Respondents, and Respondents' officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, in connection with any product or service, are hereby permanently restrained and enjoined from misrepresenting, expressly or by implication, the extent to which Respondents maintain and protect the privacy, security, confidentiality, or integrity of Personal Information.

V. DATA DELETION

IT IS FURTHER ORDERED that within one hundred twenty (120) days after entry of this Order, Respondents and Respondents' officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, must destroy all Personal Information collected from a Monitoring Product or Service prior to entry of this Order. Provided, however, that such Personal Information need not be destroyed, and may be disclosed, to the extent requested by a government agency or required by law, regulation, or court order, including without limitation as required by rules applicable to the safeguarding of evidence in pending litigation.

VI. MANDATED INFORMATION SECURITY PROGRAM

IT IS FURTHER ORDERED that each Covered Business shall not transfer, sell, share, collect, maintain, or store Personal Information unless it establishes and implements, and thereafter maintains, a comprehensive information security program ("Information Security Program") that protects the security, confidentiality, and integrity of such Personal Information. To satisfy this requirement, each Covered Business must, at a minimum:

- A. Document in writing the content, implementation, and maintenance of the Information Security Program;

Decision and Order

- B. Provide the written program and any evaluations thereof or updates thereto to its board of directors or governing body or, if no such board or equivalent governing body exists, to a senior officer responsible for its information security program at least once every twelve months and promptly after any Covered Incident;
- C. Designate a qualified employee or employees to coordinate and be responsible for the Information Security Program;
- D. Assess and document, at least once every twelve months and promptly following a Covered Incident, internal and external risks to the security, confidentiality, or integrity of Personal Information that could result in the unauthorized disclosure, misuse, loss, theft, alteration, destruction, or other compromise of such information;
- E. Design, implement, maintain, and document safeguards that control for the internal and external risks to the security, confidentiality, or integrity of Personal Information identified in response to sub-Provision VI.D. Each safeguard shall be based on the volume and sensitivity of the Personal Information that is at risk, and the likelihood that the risk could be realized and result in the unauthorized access, collection, use, alteration, destruction, or disclosure of the Personal Information. Respondents' safeguards shall also include:
 - 1. Technical measures to monitor all of Respondents' networks and all systems and assets within those networks to identify data security events, including unauthorized attempts to exfiltrate Personal Information from those networks;
 - 2. Technical measures to secure Respondents' web applications and mobile applications and address well-known and reasonably foreseeable vulnerabilities, such as cross-site scripting, structured query language injection, and other risks identified by Respondents through risk assessments and/or penetration testing;
 - 3. Data access controls for all databases storing Personal Information, including by, at a minimum, (a) requiring authentication to access them, and (b) limiting employee or service provider access to what is needed to perform that employee's job function;
 - 4. Encryption of all Personal Information on Respondents' computer networks; and
 - 5. Establishing and enforcing policies and procedures to ensure that all service providers with access to Respondents' network or access to Personal Information are adhering to Respondents' Information Security Program.

Decision and Order

- F. Assess, at least once every twelve (12) months and promptly following a Covered Incident, the sufficiency of any safeguards in place to address the risks to the security, confidentiality, or integrity of Personal Information, and modify the Information Security Program based on the results.
- G. Test and monitor the effectiveness of the safeguards at least once every twelve months and promptly following a Covered Incident, and modify the Information Security Program based on the results. Such testing shall include vulnerability testing of each of Respondents' network(s) once every four (4) months and promptly after any Covered Incident, and penetration testing of each Covered Business's network(s) at least once every twelve (12) months and promptly after any Covered Incident;
- H. Select and retain service providers capable of safeguarding Personal Information they receive from each Covered Business, and contractually require service providers to implement and maintain safeguards for Personal Information; and
- I. Evaluate and adjust the Information Security Program in light of any changes to Respondents' operations or business arrangements, a Covered Incident, or any other circumstances that Respondents know or have reason to know may have an impact on the effectiveness of the Information Security Program. At a minimum, each Covered Business must evaluate the Information Security Program at least once every twelve (12) months and modify the Information Security Program based on the results.

VII. INFORMATION SECURITY ASSESSMENTS BY A THIRD PARTY

IT IS FURTHER ORDERED that, in connection with compliance with Provision VI of this Order titled Mandated Information Security Program, Respondents 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 Information Security Program; and (3) retains all documents relevant to each Assessment for five (5) years after completion of such Assessment and 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, attorney client privilege, statutory exemption, or any similar claim.
- B. For each Assessment, Respondents shall provide the Associate Director for Enforcement for the Bureau of Consumer Protection at the Federal Trade Commission with the name and affiliation of the person selected to conduct the Assessment, which the Associate Director shall have the authority to approve in his or her sole discretion.

Decision and Order

- C. The reporting period for the Assessments must cover: (1) the first one hundred eighty (180) days after the issuance date of the Order for the initial Assessment; and (2) each 2-year period thereafter for twenty (20) years after issuance of the Order for the biennial Assessments.
- D. Each Assessment must: (1) determine whether each Covered Business has implemented and maintained the Information Security Program required by Provision VI of this Order, titled Mandated Information Security Program; (2) assess the effectiveness of each Covered Business's implementation and maintenance of sub-Provisions VI.A-I; (3) identify any gaps or weaknesses in the Information Security Program; and (4) 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 sufficient to justify the Assessor's findings. No finding of any Assessment shall rely solely on assertions or attestations by a Covered Business's management. The Assessment shall be signed by the Assessor and shall state that the Assessor conducted an independent review of the Information Security Program, and did not rely solely on assertions or attestations by a Covered Business's management.
- 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, Respondents 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, DC 20580. The subject line must begin, "In re Retina-X Studios, LLC, FTC File No. 172 3118." All subsequent biennial Assessments shall be retained by Respondents until the order is terminated and provided to the Associate Director for Enforcement within ten (10) days of request.

VIII. COOPERATION WITH THIRD PARTY INFORMATION SECURITY ASSESSOR

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

- A. 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 Respondents have implemented and maintained the Information Security Program required by Provision VI of this Order, titled Mandated Information Security Program; (2) assessment of the effectiveness of the implementation and maintenance of sub-Provisions VI.A-I; or (3) identification of any gaps or weaknesses in the Information Security Program; and

Decision and Order

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

IX. ANNUAL CERTIFICATION

IT IS FURTHER ORDERED that in connection with compliance with Provision VI of this Order titled Mandated Information Security Program, Respondents shall:

- A. One year after the issuance date of this Order, and each year thereafter, provide the Commission with a certification from a senior corporate manager, or, if no such senior corporate manager exists, a senior officer of each Covered Business responsible for each Covered Business's Information Security Program that: (1) each Covered Business has established, implemented, and maintained the requirements of this Order; (2) each Covered Business is not aware of any material noncompliance that has not been (a) corrected or (b) disclosed to the Commission; and (3) includes a brief description of any Covered Incident. 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, DC 20580. The subject line must begin, "Retina-X Studios, LLC, FTC File No. 172 3118, Docket No. C-4711."

X. COVERED INCIDENT REPORTS

IT IS FURTHER ORDERED that Respondents, for any Covered Business, within a reasonable time after the date of discovery of a Covered Incident, but in any event no later than 10 days after the date the Covered Business, or any of the Covered Business's clients, first notifies any U.S. federal, state, or local government entity of the Covered Incident, must submit a report to the Commission. The report must include, to the extent possible:

- A. The date, estimated date, or estimated date range when the Covered Incident occurred;
- B. A description of the facts relating to the Covered Incident, including the causes and scope of the Covered Incident, if known;

Decision and Order

- C. A description of each type of information that triggered the notification obligation to the U.S. federal, state, or local government entity;
- D. The number of consumers whose information triggered the notification obligation to the U.S. federal, state, or local government entity;
- E. The acts that the Covered Business has taken to date to remediate the Covered Incident and protect Personal Information from further exposure or access, and protect affected individuals from identity theft or other harm that may result from the Covered Incident; and
- F. A representative copy of each materially different notice required by U.S. federal, state, or local law or regulation and sent by the Covered Business or any of its clients to consumers or to any U.S. federal, state, or local government entity.

Unless otherwise directed by a Commission representative in writing, all Covered Incident reports 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, DC 20580. The subject line must begin, “Retina-X Studios, LLC, FTC File No. 172 3118, Docket No. C-4711.”

XI. ORDER ACKNOWLEDGMENTS

IT IS FURTHER ORDERED that Respondents obtain acknowledgments of receipt of this Order:

- A. Each Respondent, 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, the Individual Respondent, for any business that such Respondent, individually or collectively with any other Respondent, is the majority owner or controls directly or indirectly, and the Corporate Respondent, must deliver a copy a copy of this Order to: (1) all principals, officers, directors, and LLC managers and members; (2) all employees having managerial responsibilities for conduct related to the subject matter of the Order, and all agents and representatives who participate in conduct related to the subject matter of the Order; 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. For all others, delivery must occur before they assume their responsibilities.
- C. From each individual or entity to which a Respondent delivered a copy of this Order, that Respondent must obtain, within thirty (30) days, a signed and dated acknowledgment of receipt of this Order.

Decision and Order

XII. COMPLIANCE REPORT AND NOTICES

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

- A. One year after entry of this Order, each Respondent must submit a compliance report, sworn under penalty of perjury, in which:
 - 1. Each Respondent must: (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 Respondent; (b) identify all of the Respondents' businesses by all of their names, telephone numbers, and physical, postal, email, and Internet addresses; (c) describe the activities of each business, including the goods and services offered, the means of advertising, marketing, and sales, and the involvement of any other Respondent (which Individual Respondent must describe if he knows or should know due to his own involvement); (d) describe in detail whether and how that Respondent is in compliance with each Provision of this Order, including a discussion of all of the changes Respondents made to comply with the Order; and (e) provide a copy of each Order Acknowledgment obtained pursuant to this Order, unless previously submitted to the Commission.
 - 2. Additionally, the Individual Respondent must: (a) identify all telephone numbers and all physical, postal, email and Internet addresses, including all residences; (b) identify all business activities, including any business for which Individual Respondent performs services whether as an employee or otherwise and any entity in which Individual Respondent has any ownership interest; and (c) describe in detail Individual Respondent's involvement in each such business, including title, role, responsibilities, participation, authority, control, and any ownership.
- B. For 10 years after the issuance date of this Order, each Respondent must submit a compliance notice, sworn under penalty of perjury, within fourteen (14) days of any changes in the following:
 - 1. Each Respondent must report any change in: (a) any designated point of contact; or (b) the structure of Corporate Respondent or any entity that Respondent has any ownership interest in or control 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.
 - 2. Additionally, Individual Respondent must report any change in: (a) name, including aliases or fictitious name, or residence address; or (b) title or role in any business activity, including (i) any business for which Individual

Decision and Order

Respondent performs services whether as an employee or otherwise and (ii) any entity in which Individual Respondent has any ownership interest and over which Individual Respondent has direct or indirect control. For each such business activity, also identify its name, physical address, and any Internet address.

- C. Each Respondent must submit to the Commission notice of the filing of any bankruptcy petition, insolvency proceeding, or similar proceeding by or against such Respondent within fourteen (14) days of its filing.
- D. Any submission to the Commission required by this Order to 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, DC 20580. The subject line must begin: “United States v. Retina-X Studios, LLC, FTC File No. 172 3118, Docket No. C-4711.”

XIII. RECORDKEEPING

IT IS FURTHER ORDERED that Respondents must create certain records for ten (10) years after entry of this Order, and retain each such record for 5 years. Specifically, Corporate Respondent and Individual Respondent, for any business that such Respondent, individually or collectively with any other Respondent, is a majority owner or controls directly or indirectly, must create and retain the following records:

- A. Accounting records showing the revenues from all goods or services sold, the costs incurred in generating those revenues, and resulting net profit or loss;
- B. Personnel records showing, for each person providing services, whether as an employee or otherwise, that person’s: name; address; telephone numbers; job title or position; dates of service; and (if applicable) the reason for termination;
- C. Copies or records of all consumer complaints and refund requests, whether received directly or indirectly, such as through a third party, and any response;
- D. For five (5) years after the date of preparation of each Assessment required by this Order, all materials and evidence that the Assessor considered, reviewed, relied upon or examined to prepare the Assessment, whether prepared by or on behalf of Respondents, including all plans, reports, studies, reviews, audits, audit trails,

Decision and Order

policies, training materials, and assessments, and any other materials concerning Respondents' compliance with related Provisions of this Order, for the compliance period covered by such Assessment;

- E. All records necessary to demonstrate full compliance with each provision of this Order, including all submissions to the Commission; and
- F. A copy of each unique advertisement or other marketing material.

XIV. COMPLIANCE MONITORING

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

- A. Within ten (10) days of receipt of a written request from a representative of the Commission, each Respondent 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.
- B. For matters concerning this Order, representatives of the Commission are authorized to communicate directly with each Respondent. Respondents must permit representatives of the Commission to interview any employee or other person affiliated with any Respondent who has agreed to such an interview. The interviewee may have counsel present.
- C. The Commission may use all other lawful means, including posing, through its representatives as consumers, suppliers, or other individuals or entities, to Respondents or any individual or entity affiliated with Respondents, without the necessity of identification of 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.
- D. Upon written request from a representative of the Commission, any consumer reporting agency must furnish consumer reports concerning the Individual Respondent, pursuant to Section 604(2) of the Fair Credit Reporting Act, 15 U.S.C. §1681b(a)(2).

XV. ORDER EFFECTIVE DATES

IT IS FURTHER ORDERED that this Order is final and effective upon the date of its publication on the Commission's website (ftc.gov) as a final order. This Order will terminate March 26, 2040, or twenty (20) years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying settlement) in federal court alleging any violation of this Order, whichever comes later; *provided, however*, that the filing of such a complaint will not affect the duration of:

Decision and Order

- A. Any Provision in this Order that terminates in less than twenty (20) years;
- B. The Order's application to any Respondent that is not named as a defendant in such complaint; and
- C. This Order is such complaint is filed after the Order has terminated pursuant to this Provision.

Provided, further, that if such complaint is dismissed or a federal court rules that the Respondent did not violate any Provision of the Order, and the dismissal or ruling is either not appealed or upheld on appeal, then the Order will terminate according to this Provision as though the complaint had never been filed, except that the Order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

Decision and Order

Attachment A

4008 Federal Register / Vol. 78, No. 12 / Thursday, January 17, 2013 / Rules and Regulations

average firm-wide billing rate (partners and associates) in 2011 was \$403, the average partner rate was \$482, and the average associate rate was \$303.

The Commission believes it reasonable to assume that the workload among law firm partners and associates for COPPA compliance questions could be competently addressed and efficiently distributed among attorneys at varying levels of seniority, but would be weighted most heavily to more junior attorneys. Thus, assuming an apportionment of two-thirds of such work is done by associates, and one-third by partners, a weighted average tied to the average firm-wide associate and average firm-wide partner rates, respectively, in the *National Law Journal* 2011 survey would be about \$365 per hour. The Commission believes that this rate B which is very near the mean of TIA's stated range of purported hourly rates that its members typically pay to engage counsel for COPPA compliance questions B is an appropriate measure to calculate the cost of legal assistance for operators to comply with the final Rule amendments.³⁹⁶

TIA also states that the 2012 SNPRM estimate of \$42 per hour for technical support is too low, and that engaging expert technical personnel can, on average, involve hourly costs that range from \$72 to \$108.³⁹⁷ Similar to TIA's hours estimate, discussed above, the Commission believes that TIA's estimate may have been based on implementing requirements that, ultimately, the Commission has determined not to adopt. For example, technical personnel will not need to "ensure" the security procedures of third parties; operators that have been eligible to use email plus for parental consents will not be required to implement new systems to replace it. It is unclear whether TIA's estimate for technical support is based on the types of disclosure-related tasks that the final Rule amendments would actually require, other tasks that the final Rule amendments would not require, or non-disclosure tasks not covered by the PRA. Moreover, unlike its estimate for lawyer assistance, TIA's

estimates for technical labor are not accompanied by an adequate explanation of why estimates for technical support drawn from BLS statistics are not an appropriate basis for the FTC's PRA analysis. Accordingly, the Commission believes it is reasonable to retain the 2012 SNPRM estimate of \$42 per hour for technical assistance based on BLS data.

Thus, for the 180 new operators per year not previously accounted for under the FTC's currently cleared estimates, 10,800 cumulative disclosure hours would be composed of 9,000 hours of legal assistance and 1,800 hours of technical support. Applied to hourly rates of \$365 and \$42, respectively, associated labor costs for the 180 new operators potentially subject to the proposed amendments would be \$3,360,600 (*i.e.*, \$3,285,000 for legal support plus \$75,600 for technical support).

Similarly, for the estimated 2,910 existing operators covered by the final Rule amendments, 58,200 cumulative disclosure hours would consist of 48,500 hours of legal assistance and 9,700 hours for technical support. Applied at hourly rates of \$365 and \$42, respectively, associated labor costs would total \$18,109,900 (*i.e.*, \$17,702,500 for legal support plus \$407,400 for technical support). Cumulatively, estimated labor costs for new and existing operators subject to the final Rule amendments is \$21,470,500.

(2) Reporting

The Commission staff assumes that the tasks to prepare augmented safe harbor program applications occasioned by the final Rule amendments will be performed primarily by lawyers, at a mean labor rate of \$180 an hour.³⁹⁸ Thus, applied to an assumed industry total of 120 hours per year for this task, incremental associated yearly labor costs would total \$21,600.

³⁹⁶ Based on Commission staff's experience with previously approved safe harbor programs, staff anticipates that most of the legal tasks associated with safe harbor programs will be performed by in-house counsel. *Cf.* Toy Industry Association (comment 89, 2012 SNPRM), at 19 (regional BLS statistics for lawyer wages can support estimates of the level of in-house legal support likely to be required on an ongoing basis). Moreover, no comments were received in response to the February 9, 2011 and May 31, 2011 *Federal Register* notices (76 FR at 7211 and 76 FR at 31334, respectively, available at <http://www.gpo.gov/fdsys/pkg/FR-2011-02-09/pdf/2011-2904.pdf> and <http://www.gpo.gov/fdsys/pkg/FR-2011-05-31/pdf/2011-13357.pdf>), which assumed a labor rate of \$150 per hour for lawyers or similar professionals to prepare and submit a new safe harbor application. Nor was that challenged in the comments responding to the 2011 NPRM.

The Commission staff assumes periodic reports will be prepared by compliance officers, at a labor rate of \$28 per hour.³⁹⁹ Applied to an assumed industry total of 600 hours per year for this task, associated yearly labor costs would be \$16,800.

Cumulatively, labor costs for the above-noted reporting requirements total approximately \$38,400 per year.

G. Non-Labor/Capital Costs

Because both operators and safe harbor programs will already be equipped with the computer equipment and software necessary to comply with the Rule's new notice requirements, the final Rule amendments should not impose any additional capital or other non-labor costs.⁴⁰⁰

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.

³⁹⁶ *Cf.* Civil Division of the United States Attorney's Office for the District of Columbia, United States Attorney's Office, District of Columbia, *Laffoy Matrix B 2003-2013*, available at http://www.justice.gov/usao/dc/divisions/Laffoy_Matrix_2003-2013.pdf (updated "Laffoy Matrix" for calculating "reasonable" attorneys fees in suits in which fee shifting is authorized can be evidence of prevailing market rates for litigation counsel in the Washington, DC area; rates in table range from \$245 per hour for most junior associates to \$505 per hour for most senior partners).

³⁹⁷ Toy Industry Association (comment 89, 2012 SNPRM), at 18.

³⁹⁹ See Bureau of Labor Statistics National Compensation Survey: Occupational Earnings in the United States, 2010, at Table 3, available at <http://www.bls.gov/sce/ocsp/sp/nctb1477.pdf>. This rate has not been contested.

⁴⁰⁰ NCTA commented that the Commission failed to consider costs "related to redeveloping child-directed Web sites" that operators would be "forced" to incur as a result of the proposed Rule amendments, including for "new equipment and software required by the expanded regulatory regime." NCTA (comment 113, 2011 NPRM), at 23. Similarly, TIA commented that the proposed Rule amendments would entail "increased monetary costs with respect to technology acquisition and implementation * * *." Toy Industry Association (comment 163, 2011 NPRM), at 17. These comments, however, do not specify projected costs or which Rule amendments would entail the asserted costs.

Decision and Order

Federal Register / Vol. 78, No. 12 / Thursday, January 17, 2013 / Rules and Regulations

4009

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

Decision and Order

4010 Federal Register / Vol. 78, No. 12 / Thursday, January 17, 2013 / Rules and Regulations

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

Decision and Order

Federal Register / Vol. 78, No. 12/Thursday, January 17, 2013/Rules and Regulations

4011

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

Decision and Order

4012 Federal Register / Vol. 78, No. 12 / Thursday, January 17, 2013 / Rules and Regulations

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

Decision and Order

Federal Register / Vol. 78, No. 12 / Thursday, January 17, 2013 / Rules and Regulations

4013

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.

Decision and Order

4014 Federal Register / Vol. 78, No. 12 / Thursday, January 17, 2013 / Rules and Regulations

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.⁴⁰³ 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

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.").

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 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.

⁴⁰⁵ 16 CFR 312.2 (Definitions).

Analysis to Aid Public Comment

ANALYSIS OF CONSENT ORDER TO AID PUBLIC COMMENT

The Federal Trade Commission ("Commission") has accepted, subject to final approval, an agreement containing a consent order from Retina-X Studios, LLC ("Retina-X") and individual Respondent James N. Johns, Jr. (collectively, "Respondents").

The proposed consent order ("proposed order") has been placed on the public record for thirty (30) days for receipt of comments by interested persons. Comments received during this period will become part of the public record. After thirty (30) days, the Commission again will review the agreement and the comments received, and will decide whether it should withdraw from the agreement or make final the agreement's proposed order.

From 2007 to 2018 Retina-X developed and sold various products and services, each with the means to allow a purchaser to monitor, often surreptitiously, another person's activities on that person's mobile device. James N. Johns, Jr. is the registered agent and sole member of Retina-X. Individually or in concert with others, Mr. Johns controlled or had the authority to control, or participated in the acts and practices alleged in the proposed complaint.

Respondents' mobile device monitoring products and services included MobileSpy, PhoneSheriff, and TeenShield. These monitoring products and services had varying capabilities and costs. Purchasers were often required to jailbreak or root (i.e., actions to bypass various restrictions implemented by the operating system on and/or the manufacturer of mobile devices) the device user's mobile device prior to installing Respondents' monitoring products and services. Jailbreaking or rooting a mobile device exposes a mobile device to various security vulnerabilities and likely invalidates any warranty that a mobile device manufacturer or carrier provides.

All of Respondents' monitoring products and services required that the purchaser have physical access to the device user's mobile device, and could remotely monitor the device user's activities from an online dashboard. By default, Respondents' monitoring products and services disclosed to the device user that they were being monitored (e.g., an icon on, or monitored mobile device). However, purchasers could turn off this feature so that the monitoring products and services could run surreptitiously, meaning that the device user was unaware that he or she was being monitored. Respondents provided purchasers with instructions on how to remove the icon that would confirm that monitoring products and services were installed on a particular mobile device.

Device users surreptitiously monitored by Respondents' monitoring products and services could not uninstall or remove Respondents' monitoring products and services because they did not know that they were being monitored. Device users often had no way of knowing that Respondents' monitoring products and services were being used on their phone. Respondents did not take any steps to ensure that purchasers would use Respondents' monitoring products and services for legitimate purposes, such as to monitor employees or children.

Moreover, Respondents did not take steps to secure the personal information collected from purchasers and device users being monitored. Respondents outsourced most of their product development and maintenance to a service provider. Respondents engaged in a number of practices

Analysis to Aid Public Comment

that, taken together, failed to provide reasonable data security to protect the personal information collected from consumers. As a result of these unreasonable data security practices, Respondents were breached twice.

The Commission proposed 5-count complaint alleges that Respondents violated Section 5(a) of the Federal Trade Commission Act and the Children's Online Privacy Protection Rule. The first count alleges that Respondents unfairly sold monitoring products and services that required jailbreaking or rooting, without taking reasonable steps to ensure that the monitoring products and services would only be used for legitimate and lawful purposes by the purchaser.

The second to fourth counts allege that Respondents deceived consumers about Respondents' data security practices by falsely representing that consumers' personal information collected through MobileSpy, PhoneSheriff, and TeenShield, and stored in Respondents' databases was confidential, private, and safe. The fifth count alleges that Respondents violated the Children's Online Privacy Protection Rule by failing to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children through the TeenShield product. Respondents failed to implement appropriate security procedures to protect the personal information collected from consumers, including children, such as by: (1) failing to adopt, implement, or maintain security standards, policies, procedures or practices; (2) failing to conduct security testing of mobile applications that could be exploited to gain unauthorized access to consumers' sensitive personal information for well-known and reasonably foreseeable vulnerabilities; (3) failing to contractually require their service providers to adopt and implement information security standards, policies, procedures or practices; (4) failing to perform adequate oversight of service providers; and (5) failing to adopt and implement written information security standards, policies, procedures, or practices that would apply to the oversight of their service providers.

The proposed order contains provisions designed to prevent Respondents from engaging in the same or similar acts or practices in the future.

Part I of the proposed order prohibits Respondents from selling a monitoring product unless: (1) the monitoring product does not circumvent security protections implemented by the mobile device operating system or manufacturer; (2) prior to the sale of the monitoring product, express written attestation is obtained from the purchaser that the monitoring product stating that the monitoring product will be used for legitimate and lawful purposes; and (3) documentation is obtained proving that the purchaser is an authorized user on the monitored mobile device's service carrier account. The proposed order also requires that Respondents display an application icon, including the name of the monitoring product, when the monitoring product is on the mobile device. Moreover, a clear and conspicuous notice must be presented when the application icon is clicked.

Part II of the order restrains Respondents from distributing monitoring products unless Respondents have: (1) a home page notice stating that the monitoring product may only be used for legitimate and lawful purposes by authorized users; and (2) a purchase page notice stating that the monitoring product may only be used for legitimate and lawful purposes by authorized users,

Analysis to Aid Public Comment

and that installing or using the monitoring product for any other purpose may violate local, state, and/or federal law.

Part III of the proposed order prohibits Respondents from violating the Children's Online Privacy Protection Rule. Part IV of the proposed order prohibits Respondents from misrepresenting the extent to which Respondents maintain and protect the privacy, security, confidentiality, or integrity of consumers' personal information. Part V requires that Respondents' delete all personal information collected from a monitoring product prior to entry of the proposed order within 120 days.

Part VI of the proposed order prohibits Respondents, and any business that a Respondent controls, directly, or indirectly, from transferring, selling, sharing, collecting, maintaining, or storing personal information unless Respondents establish and implement, and thereafter maintain, a comprehensive information security program that protects the security confidentiality, and integrity of such personal information. Part VII requires Respondents to obtain initial and biennial data security assessments for twenty years. Part VIII of the proposed order requires Respondents to disclose all material facts to the assessor and prohibits Respondents from misrepresenting any fact material to the assessments required by Part VII. Part IX requires Respondents to submit an annual certification from a senior corporate manager (or senior officer responsible for its information security program), that Respondents have implemented the requirements of the proposed order, are not aware of any material noncompliance that has not been corrected or disclosed to the Commission, and includes a brief description of any covered incident involving unauthorized access to or acquisition of personal information. Part X requires Respondents to submit a report to the Commission of their discovery of any covered incident.

Parts XI through XIV of the proposed order are reporting and compliance provisions, which including recordkeeping requirements and provisions requiring Respondents to provide information or documents necessary for the Commission to monitor compliance. Part XV states that the proposed order will remain in effect for 20 years, with certain exceptions.

The purpose of this analysis is to aid public comment on the proposed order. It is not intended to constitute an official interpretation of the complaint or proposed order, or to modify in any way the proposed order's terms.

Complaint

IN THE MATTER OF

**AGNATEN SE,
VETERINARY SPECIALISTS OF NORTH AMERICA, LLC,
AND
NVA PARENT INC.**

CONSENT ORDER, ETC. IN REGARD TO ALLEGED VIOLATIONS OF SECTION 5 OF THE FEDERAL
TRADE COMMISSION ACT AND SECTION 7 OF THE CLAYTON ACT

Docket No. C-4707; File No. 191 0160

Complaint, February 14, 2020 – Decision, April 9, 2020

This consent order addresses the \$5 billion acquisition by Agnaten SE of all assets of NVA Parent Inc. in violation of Section 7 of the Clayton Act and Section 5 of the Federal Trade Commission Act. The complaint alleges that the Acquisition would reduce the number of specialty providers of internal medicine, oncology, and ophthalmology service in all of the relevant markets and significantly increase concentration in each market. The Acquisition eliminates head-to-head competition between Compassion First and NVA in the provision of specialty and emergency veterinary services. The consent order requires Respondents to divest, within 10 days after the Acquisition Date, the Divestiture Clinics to MedVet and that Respondent Agnaten shall not acquire Respondent NVA until it has obtained for all the Divestiture Clinics.

Participants

For the *Commission*: *Michael R. Barnett.*

For the *Respondents*: *Matthew P. Hendrickson and Jessica N. Schneider, Skadden, Arps, Slate, Meagher & Flom LLP; Katherine A. Rocco and Muran Zhu, Kirkland & Ellis LLP.*

COMPLAINT

Pursuant to the Clayton Act and the Federal Trade Commission Act, and its authority thereunder, the Federal Trade Commission (“Commission”), having reason to believe that Respondents Agnaten SE, the owner of Veterinary Specialists of North America, LLC and Compassion-First Pet Hospitals (“Compassion First”), a corporation subject to the jurisdiction of the Commission, has agreed to acquire Respondent NVA Parent Inc. (“NVA”), a corporation subject to the jurisdiction of the Commission, in violation of Section 5 of the Federal Trade Commission Act (“FTC Act”), as amended, 15 U.S.C. § 45, that such acquisition, if consummated, would violate Section 7 of the Clayton Act, as amended, 15 U.S.C. § 18, and Section 5 of the FTC Act, as amended, 15 U.S.C. § 45, and it appearing to the Commission that a proceeding in respect thereof would be in the public interest, hereby issues its Complaint, stating its charges as follows

I. RESPONDENTS

1. Respondent Compassion First is a private corporation organized, existing, and doing business under and by virtue of the laws of Austria, with its office and principal place of business located at Rooseveltplatz 4-5/Top 10, A-1090 Vienna, Austria, with its United States