

**Before the  
Federal Trade Commission  
Washington, DC**

In the Matter of )  
 )  
Echometrix, Inc. )  
 )  
----- )

**Complaint, Request for Investigation, Injunction, and Other Relief**

I. Introduction

1. This complaint details practices within the “parental control” software industry and “market- intelligence research industry” that cause consumer harm and that constitute unfair and deceptive trade practices. Parental control software provides parents with the opportunity to monitor and control their children’s online activity. Several companies promote “parental control” technologies as tools to protect children’s Internet activity. One company, Echometrix, Inc., advertises its “Sentry Parental Control Software” as providing “total family protection,” enabling parents to “block and filter web sites” accessible to their children and “set time limits” for children’s internet use.<sup>1</sup> However, Echometrix surreptitiously collects information concerning children’s online behavior, uses the information to “customize the advertising content [children] see,” and transfers information concerning children’s browsing and online chats to marketers.<sup>2</sup> The behavior is unfair, deceptive, and violates the Children’s Online Privacy Protection Act.

2. The Electronic Privacy Information Center (EPIC) has identified several practices that constitute unfair or deceptive trade practices in the marketing of parental control software. Echometrix fails to disclose how information is collected and used in violation of the Federal Trade Commission Act. 15 U.S.C. § 45(a). Secondly, Echometrix engages in practices that violate the Children’s Online Privacy Protection Act, such as failing to provide disclosure practices for information collected from children and obtaining “verifiable parental consent for the collection, use, or disclosure of personal information from children.” 15 U.S.C. §§ 6501-6506.

3. These business practices deceive the purchasers of the product - parents are unaware that the company collects information about their children and discloses it to third parties. Further,

---

<sup>1</sup> Sentry Parental Controls, <http://www.sentryparentalcontrols.com>.

<sup>2</sup> Sentry Parental Controls – Privacy Policy, <http://www.sentryparentalcontrols.com/Support/Policies/Privacy.aspx>; Echometrix Products – The Pulse, <http://www.echometrix.com/Products/Default.aspx>.

these business practices create a new risk of harm to children, whose personal information would not be disclosed to third parties but for the availability of these products in the marketplace.

4. In this complaint EPIC details the practices of Echometrix, Inc. in the parental control software market and market-intelligence research arena. Internet searches reveal several other companies offering similar products. It appears that these companies are tied together in affiliate relationships, as some of these operators offer similarly named products and affiliate marketing opportunities.<sup>3</sup> Collusion in these activities magnifies the risk to children.

5. EPIC requests that the Commission investigate the company named herein, determine the extent of threat to consumer privacy and safety, seek appropriate injunctive and compensatory relief, and further investigate other operators and practices in this market.

## II. Parties

6. The Electronic Privacy Information Center (EPIC) is a not for profit research center based in Washington, D.C. Founded in 1994, EPIC focuses on the protection of privacy and the First Amendment. Among its other activities, EPIC first brought the Commission's attention to the privacy risks of online advertising.<sup>4</sup> EPIC initiated the complaint to the FTC regarding Microsoft Passport.<sup>5</sup> The Commission subsequently required Microsoft to implement a comprehensive information security program for Passport and similar services.<sup>6</sup> EPIC also filed a complaint with the FTC regarding the marketing of amateur spyware,<sup>7</sup> which resulted in the issuance of a permanent injunction barring sales of CyberSpy's "stalker spyware," over-the-counter surveillance technology sold for individuals to spy on other individuals.<sup>8</sup>

---

<sup>3</sup> See, e.g., Sentry Affiliate Program, <http://www.sentryparentalcontrols.com/Company/Affiliates.aspx> (last visited Sep. 25, 2009).

<sup>4</sup> *In the Matter of DoubleClick*, Complaint and Request for Injunction, Request for Investigation and for Other Relief, before the Federal Trade Commission (Feb. 10, 2000), available at [http://epic.org/privacy/internet/ftc/DCLK\\_complaint.pdf](http://epic.org/privacy/internet/ftc/DCLK_complaint.pdf).

<sup>5</sup> *In the Matter of Microsoft Corporation*, Complaint and Request for Injunction, Request for Investigation and for Other Relief, before the Federal Trade Commission (July 26, 2001), available at [http://epic.org/privacy/consumer/MS\\_complaint.pdf](http://epic.org/privacy/consumer/MS_complaint.pdf).

<sup>6</sup> *In the Matter of Microsoft Corporation*, File No. 012 3240, Docket No. C-4069 (Aug. 2002), available at <http://www.ftc.gov/os/caselist/0123240/0123240.shtm>. See also Fed. Trade Comm'n, "Microsoft Settles FTC Charges Alleging False Security and Privacy Promises" (Aug. 2002) ("The proposed consent order prohibits any misrepresentation of information practices in connection with Passport and other similar services. It also requires Microsoft to implement and maintain a comprehensive information security program. In addition, Microsoft must have its security program certified as meeting or exceeding the standards in the consent order by an independent professional every two years."), available at <http://www.ftc.gov/opa/2002/08/microst.shtm>.

<sup>7</sup> *In the Matter of AwarenessTech.com, et al.*, Complaint and Request for Injunction, Request for Investigation and for Other relief, before the Federal Trade Commission, available at [http://epic.org/privacy/dv/spy\\_software.pdf](http://epic.org/privacy/dv/spy_software.pdf).

<sup>8</sup> *FTC v. Cyberspy Software*, No. 6:08-cv-1872 (D. Fla. Nov. 6, 2008) (unpublished order), available at <http://ftc.gov/os/caselist/0823160/081106cyberspytro.pdf>.

7. Echometrix, Inc., formerly SearchHelp Inc., develops software that allegedly provides parents with “real-time online protection of their children.” Echometrix brands include FamilySafe Parental Control products ([www.familysafesolutions.net](http://www.familysafesolutions.net)) and Sentry Parental Control products ([www.sentryparentalcontrol.com](http://www.sentryparentalcontrol.com)). Echometrix also offers technology to corporations seeking to analyze children’s online behavior. The technology is called PULSE, a software engine that reads and analyzes digital content extracted from online conversations and activity of teenagers and children in real time. The software is available through subscription at Echometrix’s website.<sup>9</sup> The domain name is registered to William Bozsnyak of EchoMetrix, Inc., 6800 Jericho Tpke, Suite 208E, Syosset, NY 11791. The corporate address listed on the website is also 6800 Jericho Tpke., Suite 208E, Syosset, NY 11791.

8. The following facts are the result of an EPIC investigation of the complained company. We describe the company’s representation of its products, including suggested uses and technical abilities. We note two main practices: the failure to fully disclose how information is being collected and used and the failure to adequately warn consumers of the dangers of using or misusing these products.

### III. Factual Background

#### **Echometrix**

9. Echometrix, formerly SearchHelp, Inc., is an information-services company, which produces the FamilySafe and Sentry Parental Controls technologies. Echometrix provides a link on its webpage<sup>10</sup> to the Sentry Family Protection Products webpage.<sup>11</sup> The marketing promotes illegal surveillance, fails to disclose how information is being collected and used, fails to disclose how information of children is being collected and used, and fails to adequately warn consumers or the software licensees of the dangers of using or misusing these products. Below is a screenshot of a portion of the Products homepage:<sup>12</sup>



<sup>9</sup> [http://echometrix.com/Products/Pulse\\_Features.aspx/](http://echometrix.com/Products/Pulse_Features.aspx/).

<sup>10</sup> <http://www.echometrix.com/Products/Default.aspx> (last visited Sep. 25, 2009).

<sup>11</sup> [www.sentryparentalcontrols.com](http://www.sentryparentalcontrols.com) (last visited Sep. 25, 2009).

<sup>12</sup> <http://www.echometrix.com/Products/Default.aspx>.

10. Echometrix also creates and markets a product called PULSE, which is described as “a proprietary software engine that reads digital content from multiple sources across the web, including: instant messages (“IM”), blogs, social environment communities, forums, and chat rooms.” PULSE analyzes the data and provides market research intelligence to firms.<sup>13</sup> Echometrix licenses the PULSE software for a fee. A screenshot of the advertisement, as displayed on the Echometrix website, is displayed below:



#### PRODUCTS | THE PULSE



IF TEENS ARE RELEVANT TO YOUR BUSINESS, YOU NEED PULSE!

PULSE is a proprietary software engine that reads digital content from multiple sources across the web, including: instant messages (“IM”), blogs, social environment communities, forums, and chat rooms. PULSE analyzes the sentiment, and delivers the unsolicited raw conversations in real time. Pulse is the most real market research available!

11. PULSE is geared towards gathering information from the teenage demographic for marketing purposes. PULSE is proud to “reveal[] the truth driving the \$240 billion teen market.” PULSE contextualizes the information gathered from instant message conversations, blogs, and chat rooms and analyzes it in real time to “identify[], evaluate[], and graphically display[] a wide spectrum of analytic information relating to the type, tone, grade, frequency of communications, impressions, needs, desires, hopes, dreams and wants of this teen audience who live on the Web.” Below is a screenshot<sup>14</sup>:

<sup>13</sup> *Id.*

<sup>14</sup> *Id.*

PULSE reveals the truth driving the \$240 Billion teen market.

PULSE is based on the best of breed technology available in today's market. It's the first real-time web based sentiment analytics tool that specializes exclusively on teen data.

Every single minute PULSE is aggregating the web's social media outlets such as chat and chat rooms, blogs, forums, instant messaging, and web sites to extract meaningful user generated content from your target audience, the teens!

PULSE contextualizes the aggregated content and provides instantaneous customized summaries in real time of the teen market. The PULSE identifies, evaluates, and graphically displays a wide spectrum of analytic information relating to the type, tone, grade, frequency of communications, impressions, needs, desires, hopes, dreams and wants of this teen audience who live on the Web.

12. Under a section titled “What makes PULSE useful for you?,” the website lists the features of the product:

- ONLY PULSE has access to get inside privileged IM chats making it an accurate predictor of the teen mindset.
- Unbiased, unfiltered conversations and content.
- PULSE gives immediate, unique information about what teens are saying in their own words.
- PULSE reveals what teens think - about a product, a brand, a trend, a movie, a TV show, a retailer, and current events.

A screen shot of the “What makes PULSE useful for you?” section of the webpage is displayed below:<sup>15</sup>

**What makes PULSE useful for you?**

Pulse's collective intelligence can give you predictive insight into teen consumer intent, helping you as marketer use your resources better and adapt in real time to the markets YOU serve. PULSE can change the way you think and:

- ONLY PULSE has access to get inside privileged IM chats making it an accurate predictor of the teen mindset.
- Unbiased, unfiltered conversations and content.
- PULSE gives immediate, unique information about what teens are saying in their own words.
- Pulse reveals what teens think - about a product, a brand, a trend, a movie, a TV show, a retailer, and current events.

13. According to the company, PULSE allows users to view information, sorted by different demographics, including age, gender, and geographic location. A screenshot of this feature, as described on the “PULSE FEATURES” webpage is reproduced below<sup>16</sup>:

- View different perspectives including age, gender, region, key influencers, brand strength, brand image.

<sup>15</sup> <http://echometrix.com/Products/Default.aspx> (last visited Sep. 25, 2009).

<sup>16</sup> [http://echometrix.com/Products/Pulse\\_Features.aspx](http://echometrix.com/Products/Pulse_Features.aspx) (last visited Sep. 25, 2009).

14. According to the company, PULSE offers users the opportunity to determine how many conversations are taking place on the internet, and *where* on the web these conversations are occurring. A screenshot of this feature, as described on the “PULSE FEATURES” webpage is reproduced below<sup>17</sup>:

- Instant view of how many conversations are taking place and where on the web they came from.

15. According to the company, Echometrix sells access to this PULSE software to corporations and marketing firms interested in compiling data about teenagers online via its website. Below is a screenshot of the pricing plan on the “PULSE FEATURES” webpage:<sup>18</sup>

PRICING:

[48 Hour Access \\$250](#)

[1 Month Subscription \\$2,500](#)

[Annual Subscription \\$20,000](#)

**Developers Terminal \$60,000 Annual license billed monthly (Comming Soon!)**



---

<sup>17</sup> *Id.*

<sup>18</sup> *Id.*

16. The Echometrix website has a short privacy policy displayed on its webpage, which asserts that it is in full compliance with COPPA. The policy alleges that the company “NEVER has and NEVER will collect, distribute *or* sell personal information as defined by COPPA.” Further, according to Echometrix, “under no circumstances does Pulse identify nor expose *in any way* the source of any digital content.” A screenshot of the entire privacy policy is reproduced below.<sup>19</sup>

### EchoMetrix | PRIVACY POLICY

---

Echometrix has a long-standing policy of strict adherence to the laws, policies and guiding principles defined in COPPA (The Child On-Line Privacy Act). The company NEVER has and NEVER will collect, distribute or sell personal information as defined by COPPA.

Echometrix's entire line of FamilySafe Parental Controls products, are designed to facilitate and enable Internet use while monitoring and protecting children from potentially dangerous web-sites, or persons on the Internet. The company DOES NOT and never has collected, distributed nor sold personal information, of any type, to anyone.

Echometrix's PULSE is a proprietary software engine that reads digital content from multiple sources across the web, analyzes and reveals the sentiment embedded in the digital conversations. Under no circumstances does Pulse identify nor expose in any way the source of any digital content.

17. Nowhere on the Echometrix website did EPIC find a disclaimer that warns users of the legal consequences of misusing the software or of illegal surveillance, nor was there any information regarding how the data collected from children is actually used.

### Sentry Parental Controls

18. Sentry Parental Controls markets the “webwatcher” software via their website<sup>20</sup>. The marketing fails to fully disclose to parents how information of their children is collected and used, and fails to adequately warn consumers of the dangers of using these products.

19. The software’s ability to block and filter websites, record IM conversations, and receive *real-time alerts* is detailed in their advertisements lining the top and sides of each webpage. A screenshot of an advertisement for the Total Family Protection package, which promotes the software’s automatic “stealth mode” setting, is reproduced below:<sup>21</sup>

---

<sup>19</sup> <http://echometrix.com/Products/docs/OnlinePrivacyPolicy.doc> (last visited Sep. 25, 2009) (emphases added).

<sup>20</sup> [www.sentryparentalcontrols.com](http://www.sentryparentalcontrols.com) (last visited Sep. 25, 2009).

<sup>21</sup> <http://www.sentryparentalcontrols.com/products/TotalProtection.aspx> (last visited Sep. 25, 2009).

**SENTRY PARENTAL CONTROLS**  
Total Family Protection

**STEALTH MODE** **BEST OVERALL VALUE!**

**Advanced Monitoring Software for Parents!**

- ✓ Block & Filter Websites
- ✓ Record IM Conversations
- ✓ Control Their Computer Remotely!
- ✓ receive Real-Time Alerts
- ✓ Set Time Limits.
- ✓ Works on Vista and XP!

**FREE TRIAL** **Only \$3.99/mo** **BUY NOW**

20. Sentry’s privacy policy is virtually inaccessible – it is displayed only after clicking the SUPPORT heading, then the POLICIES link, and finally PRIVACY POLICY. The privacy policy allows parents to “delete” their child’s account, but admits that all of the child’s information may not be deleted from Sentry’s records. A screenshot of the YOUR ABILITY TO EDIT AND DELETE YOUR ACCOUNT INFORMATION AND PREFERENCES – CHILDREN section of the privacy policy is captured below.<sup>22</sup>

### Children

- Parents can review, edit, and delete information relating to their child's SearchHelp account using tools offered in the products' Control Panel.
- If a parent chooses not to allow us to further collect or use a child's information, parents enrolled in SearchHelp can delete their child's account by signing into that child's account and then using the Control Panel. However, information might possibly remain in our archived records after your account has been deleted.

21. Sentry’s privacy policy also includes information on how information is collected and used. The policy explains that SearchHelp “receives and records information on our server logs from your child’s browser and chat clients, including IP address, SearchHelp cookie information, and the page requested,” using the information “to customize the advertising and content you see, fulfill your requests for products and services, improve our services, contact you, conduct research, and provide anonymous reporting for internal and external clients.”<sup>23</sup> A screenshot of the INFORMATION COLLECTION AND USE – GENERAL section is produced below:

<sup>22</sup> <http://www.sentryparentalcontrols.com/Support/Policies/Privacy.aspx> (last visited Sep. 25, 2009).

<sup>23</sup> <http://www.sentryparentalcontrols.com/Support/Policies/Privacy.aspx>



## Information Collection and Use

### General

- SearchHelp collects personal information when you register with SearchHelp, when you or your child uses SearchHelp products or services, when you visit SearchHelp pages or the pages of certain SearchHelp partners, and when you enter promotions or sweepstakes. SearchHelp may combine information about you that we have with information we obtain from business partners or other companies.
- When you register we may ask for information such as your name, email address, birth date, gender, ZIP code, occupation, industry, and personal interests. When you register with SearchHelp and sign in to our services, you and your child are not anonymous to us.
- SearchHelp collects information about your transactions with us and with some of our business partners, including information about your use of products and services that we offer.
- SearchHelp automatically receives and records information on our server logs from your child's browser and chat clients, including IP address, SearchHelp cookie information, and the page requested.
- SearchHelp uses information for the following general purposes: to customize the advertising and content you see, fulfill your requests for products and services, improve our services, contact you, conduct research, and provide anonymous reporting for internal and external clients.

### FamilySafe Solutions

23. FamilySafe Solutions markets the “webwatcher” software via their websites.<sup>24</sup> The marketing fails to disclose how information is being collected and used and fails to warn consumers of the dangers of using this product.

24. The familysafesolutions.net webpage has no privacy policy that describes how information is collected and used.

## IV. Legal Analysis

### **The FTC's Section 5 Authority**

25. The provider of this parental control software and market-intelligence technology is engaging in unfair and deceptive acts and practices, and empowers the FTC to enforce this prohibition.<sup>25</sup> Such practices are prohibited by the FTC Act, and the Commission is empowered to enforce the Act's prohibitions. These powers are described in FTC Policy Statements on Deception and Unfairness.

---

<sup>24</sup> <http://www.familysafesolutions.net>;

[https://www.sentryparentalcontrols.com/content/order5\\_Intermark/Default.aspx#](https://www.sentryparentalcontrols.com/content/order5_Intermark/Default.aspx#) (last visited Sep. 25, 2009).

<sup>25</sup> 15 U.S.C. § 45.

26. A trade practice is unfair if it “causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.”<sup>26</sup>

27. The injury must be “substantial.”<sup>27</sup> Typically, this involves monetary harm, but may also include “unwarranted health and safety risks.”<sup>28</sup> Emotional harm and other “more subjective types of harm” generally do not make a practice unfair.<sup>29</sup> Secondly, the injury “must not be outweighed by an offsetting consumer or competitive benefits that the sales practice also produces.”<sup>30</sup> Thus the FTC will not find a practice unfair “unless it is injurious in its net effects.”<sup>31</sup> Finally, “the injury must be one which consumers could not reasonably have avoided.”<sup>32</sup> This factor is an effort to ensure that consumer-decision making still governs the market by limiting the FTC to act in situations where seller behavior “unreasonably creates or takes advantage of an obstacle to the free exercise of consumer decisionmaking.”<sup>33</sup> Sellers may not withhold from consumers important price or performance information, engage in coercion, or unduly influence highly susceptible classes of consumers.<sup>34</sup>

28. The FTC will also look at “whether the conduct violates public policy as it has been established by statute, common law, industry practice, or otherwise.”<sup>35</sup> Public policy is used to “test the validity and strength of the evidence of consumer injury, or, less often, it may be cited for a dispositive legislative or judicial determination that such injury is present.”<sup>36</sup>

---

<sup>26</sup> *Id.* at § 45(n). *See, e.g.*, Fed. Trade Comm’n v. Seismic Entertainment Productions, Inc., Civ. No. 1:04-CV-00377 (Nov. 21, 2006) (finding that unauthorized changes to users’ computers that affected the functionality of the computers as a result of Seismic’s anti-spyware software constituted a “substantial injury without countervailing benefits.”).

<sup>27</sup> Fed. Trade Comm’n FTC Policy Statement on Unfairness, (Dec. 17, 1980), *available at* <http://www.ftc.gov/bcp/policystmt/ad-unfair.htm> [*hereinafter* FTC Unfairness Policy].

<sup>28</sup> *Id.* *See, e.g.*, Fed. Trade Comm’n v. Information Search, Inc., Civ. No. 1:06-cv-01099 (Mar. 9, 2007) (“The invasion of privacy and security resulting from obtaining and selling confidential customer phone records without the consumers’ authorization causes substantial harm to consumers and the public, including, but not limited to, endangering the health and safety of consumers.”).

<sup>29</sup> *Id.*

<sup>30</sup> *Id.*

<sup>31</sup> *Id.*

<sup>32</sup> *Id.*

<sup>33</sup> *Id.*

<sup>34</sup> *Id.*

<sup>35</sup> *Id.*

<sup>36</sup> *Id.*

29. The FTC will make a finding of deception if there has been a “representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer’s detriment.”<sup>37</sup>

30. First, there must be a representation, omission, or practice that is likely to mislead the consumer.<sup>38</sup> The relevant inquiry for this factor is not whether the act or practice actually misled the consumer, but rather whether it is *likely* to mislead.<sup>39</sup> Second, the act or practice must be considered from the perspective of a reasonable consumer.<sup>40</sup> “The test is whether the consumer’s interpretation or reaction is reasonable.”<sup>41</sup> The FTC will look at the totality of the act or practice and ask questions such as “how clear is the representation? How conspicuous is any qualifying information? How important is the omitted information? Do other sources for the omitted information exist? How familiar is the public with the product or service?”<sup>42</sup>

31. Finally, the representation, omission, or practice must be material.<sup>43</sup> Essentially, the information must be important to consumers. The relevant question is whether consumers would have chosen another product if the deception had not occurred.<sup>44</sup> Express claims will be presumed material.<sup>45</sup> Materiality is presumed for claims and omissions involving “health, safety, or other areas with which the reasonable consumer would be concerned.”<sup>46</sup> The harms of this parental control software and market-intelligence research software are within the scope of the FTC’s authority to enforce COPPA, and its purveyors should face FTC action for violations of Section 5 of the FTC Act.

### **The FTC’s COPPA Authority**

32. The FTC has the authority to enforce the Children’s Online Privacy Protection Act (COPPA).<sup>47</sup> The FTC has used this enforcement authority to prosecute fourteen COPPA

---

<sup>37</sup> Fed. Trade Comm’n, FTC Policy Statement on Deception, (Oct. 14, 1983), *available at* <http://www.ftc.gov/bcp/policystmt/addecept.htm> [*hereinafter* FTC Deception Policy].

<sup>38</sup> *Id. See, e.g.*, Fed Trade Comm’n v. Pantron I Corp., 33 F.3d 1088 (9th Cir. 1994) (holding that Pantron’s representation to consumers that a product was effective at reducing hair loss was materially misleading, because according to studies, the success of the product could only be attributed to a placebo effect, rather than on scientific grounds).

<sup>39</sup> *Id.*

<sup>40</sup> *Id.*

<sup>41</sup> *Id.*

<sup>42</sup> *Id.*

<sup>43</sup> *Id.*

<sup>44</sup> *Id.*

<sup>45</sup> Thompson Medical Co., 104 F.T.C. 648, 816 (1984).

<sup>46</sup> *Id.*

<sup>47</sup> Fed. Trade Comm’n, Brief Overview of FTC’s Investigative and Law Enforcement Authority, *available at* <http://www.ftc.gov/ogc/brfovrwv.shtm>.

violators.<sup>48</sup> Although many FTC COPPA violation cases usually concern violations of website operators, the FTC has successfully challenged the “information collection practices of [one] online service in connection with a *software* product.”<sup>49</sup> The harms of this parental control software and market-intelligence research software are within the scope of the FTC’s authority to enforce COPPA, and its purveyors should face FTC action for violations of COPPA.

### **The Harm of Online Data Collection Involving Children**

33. The harm from Echometrix’s online data collection is experienced by the millions of children and teenagers in the United States who are not aware they are being monitored. The harm is also experienced by parents who unwittingly subject their children’s private information to third parties for marketing purposes. The deployer of the software is also harmed – in this case, a licensor of the PULSE software who is exposed to legal risks by using the software as advertised. Parental control software, if used for its narrow purposes as advertised, is not inherently deceptive. However, risks come with the company’s failure to disclose their practices concerning information collection, disclosure, and use.

34. The FTC Act and COPPA regulate the collection and disclosure of data online. Several internet websites and software companies have been prosecuted by the FTC and have been subject to civil penalties for failing to provide clear privacy policies and for selling marketing data about consumers to third parties. The creators of the BonziBUDDY software product were fined \$75,000 for failing to fully disclose their information collection practices with regards to children, and failing to obtain verifiable parental consent for the collection of such data. In that case, the information was collected from children, but not disclosed to third parties. In 2008, the FTC fined social networking website Xanga.com \$1 million for collecting information from children under 13 and failing to disclose its information gathering and disclosure practices.

35. In 2005, the FTC charged Vision I Properties, LLC, under FTC Act § 5a with failure to disclose the extent of its information collection and disclosure practices online. In its privacy policy, Vision I Properties, Inc. stated, “We use the information we collect from you to process orders and to provide an enhanced shopping experience. [ ] does not sell, trade or rent personal information or shopping habits to third parties.”<sup>50</sup> However,

Vision I began renting to third parties for marketing purposes consumers’ personal information collected through shopping cart and check out pages generated by its software at merchant sites. Such personal information includes

---

<sup>48</sup> Fed. Trade Comm’n, Children’s Privacy Enforcement, *available at* [http://www.ftc.gov/privacy/privacyinitiatives/childrens\\_enf.html](http://www.ftc.gov/privacy/privacyinitiatives/childrens_enf.html).

<sup>49</sup> <http://www.ftc.gov/opa/2004/02/bonziung.shtm> (emphasis added).

<sup>50</sup> <http://www.ftc.gov/os/caselist/0423068/050310comp0423068.pdf>.

the name, address, phone number, and purchase history of nearly one million consumers. This personal information was used by third parties to send direct mail and make telemarketing calls to consumers who shopped at merchant sites using the software.<sup>51</sup>

The FTC settled the case. The settlement bars Vision I Properties' disclosure of previously collected consumer information, and forbids future collection or disclosure of such information.

36. More recently, the FTC obtained a consent order against Sears Holding Management Corporations.<sup>52</sup> The order arose from the company's use of software to collect and disclose online activity to third parties, without "adequately [informing consumers as to] the full extent of the information the software tracked."<sup>53</sup>

The FTC charged . . . that the software also monitored consumers' online secure sessions – including sessions on third parties' Web sites – and collected consumers' personal information transmitted in those sessions, such as the contents of shopping carts, online bank statements, drug prescription records, video rental records, library borrowing histories, and the sender, recipient, subject, and size for Web-based e-mails.<sup>54</sup>

The order requires that the company fully, clearly, and prominently disclose the "types of data the software will monitor, record, or transmit."<sup>55</sup> Further, the company must disclose to consumers whether and how this information will be used by third parties.<sup>56</sup>

37. Online data collection of children poses the specific danger that the information collected could fall into the wrong hands, as the sellers of the information have no true stake or interest in protecting children's privacy. Children aged 2-11 comprise approximately 16 million, nearly ten percent, of active online users.<sup>57</sup> In the past five years, the number of children using the internet has increased by eighteen percent, and the growth of children as online users "outpaces the overall growth of children in the U.S."<sup>58</sup> Today, children ages 2-11 spend more than eleven hours online daily.<sup>59</sup> One study shows that nearly eighty percent of children who use the internet

---

<sup>51</sup> *Id.*

<sup>52</sup> <http://www.ftc.gov/os/caselist/0823099/090604searsdo.pdf> (last visited Sep. 25, 2009).

<sup>53</sup> <http://www.ftc.gov/os/caselist/0823099/090604searscmpt.pdf> (last visited Sep. 25, 2009).

<sup>54</sup> *Id.*

<sup>55</sup> <http://www.ftc.gov/opa/2009/09/sears.shtm>.

<sup>56</sup> *Id.*

<sup>57</sup> Nielsen Online Data Quick Take: Kids Online (July 6, 2009), available at [http://en-us.nielsen.com/main/news/news\\_releases/2009/july/Nielsen\\_Online\\_Data\\_Quick\\_Take\\_\\_Kids\\_Online](http://en-us.nielsen.com/main/news/news_releases/2009/july/Nielsen_Online_Data_Quick_Take__Kids_Online).

<sup>58</sup> *Id.*

<sup>59</sup> *Id.*

provide sensitive information about themselves online when there is an incentive, such as a free gift, involved.<sup>60</sup>

38. Studies have revealed that seemingly innocuous information can be combined and easily re-identified, or matched with its true owner. In one study, a researcher was able to uniquely identify 87% of the U.S. population simply by using a combination of birth, gender, and zip code information from members of the public.<sup>61</sup> This poses a risk to children, when information about region, age, and gender are collected and disclosed to third parties.

### **Echometrix's Unfair and Deceptive Practices**

39. The practice of surreptitiously collecting sensitive information from children and simultaneously disclosing this information to third parties for marketing purposes is unfair because these claims cause a substantial harm, not outweighed by any countervailing benefits, which consumers cannot reasonably avoid. In Sentry Parental Control's privacy policy, which is not readily accessible, SearchHelp, Inc. (now Echometrix) claims that information collected from children is not disclosed to third parties. However, Echometrix's other brand of products, PULSE, boasts of having access to the teenage market in real-time by capturing instant message conversations, chat room conversations, and blog posts.

40. FamilySafe Parental Control's website does not have a link to a privacy policy on its homepage, and access to the Sentry Parental Controls' privacy policy is only achieved through multiple steps. Echometrix's website provides an incomplete privacy policy, which does not fully disclose how children's information is used and offers contradictory information as to what kind of information is collected.

41. These practices are in violation of COPPA and thus are likely to cause harm. The collection and disclosure of information from children has few countervailing benefits. While this information could aid in market research and target advertising, this benefit can easily be achieved by providing an opt-in provision, which clearly states every entity who will receive the information and explains how the information will be used, or the use of marketing techniques that do not require the collection or disclosure of personally identifiable information on children. The targets of this surveillance – children – cannot reasonably avoid this harm, as they are not made aware of the surveillance by the operation of the product. Furthermore, parents cannot reasonably avoid this harm on behalf of their children, because the information collection and

---

<sup>60</sup> Joseph Turow and Lilach Nir, "The Internet and the Family 2000: The View From Parents, the View from Kids." A Report from the Annenberg Public Policy Center of the University of Pennsylvania.

<sup>61</sup> Latanya Sweeney, *Weaving Technology and Policy Together to Maintain Confidentiality*, 25 J. Law, Med., & Ethics 98, 98-99 (1997).

use practices are not clearly or fully disclosed and the business practice is so contrary to the purpose represented by the company.

42. The marketing and promotion of this parental control software is deceptive. Purchasers – parents – are likely to believe they are purchasing software that can be legitimately used for the purposes advertised. The advertised purposes include monitoring and controlling your child’s online activity, to “protect your children online while online.”<sup>62</sup> Further, Sentry Parental Control’s privacy policy states that information collected from children will not be disclosed to third parties. These representations are material. Express claims are presumed material. Claims are material if they concern safety or the concerns of a reasonable consumer. The exposure of a child’s personal and private information gathered online is of concern to reasonable consumers, and can be considered a safety concern. The purchasers are harmed when they expose their children’s information to third parties.

43. The failure to adequately warn users of the dangers of misusing the product or of the disclosure and use policy of gathered information is deceptive because it is likely to materially mislead consumers, causing injury to the victims of surveillance. An omission can be misleading if a seller does not adequately correct a false impression. Consumers of the parental control software are likely to use these products for the advertised purposes: monitoring their child’s computer. Specifically, consumers expect that the information gathered on their children will not be disclosed to a third party for any purpose, and especially not without the consent of the consumer-parent. Further, Echometrix’s failure to warn market research firms about the illegality of collecting and using children’s information, subjects children to harm.

#### V. Prayer for Investigation and Relief

44. EPIC requests that the Commission investigate Echometrix, enjoin its unfair and deceptive practices, and seek damages for aggrieved individuals.

45. EPIC requests that the Commission enjoin Echometrix from offering the software services at issue in this Complaint (including but not limited to PULSE, Sentry Parental Control Software, and FamilySafe Solutions) until the company verifiably establishes that its data collection, use, and disclosure practices comply with the FTC Act COPPA, and other applicable federal laws.

45. EPIC requests that the Commission initiate an investigation into the information collection, disclosure, and sale practices of Echometrix;

---

<sup>62</sup> <http://www.sentryparentalcontrols.com/> (last visited Sep. 25, 2009).

46. EPIC requests that the Commission order Echometrix to destroy all records collected from children in violation of the COPPA;

47. EPIC requests that the Commission provide such other relief as the Commission finds necessary to redress injury to consumers resulting from Amazon's practices as described herein.

Respectfully Submitted,

Marc Rotenberg, esq.  
EPIC Executive Director

Kimberly Nguyen  
EPIC Consumer Privacy Fellow

ELECTRONIC PRIVACY INFORMATION CENTER  
1718 Connecticut Ave., NW Suite 200  
Washington, DC 20009  
202- 483-1140 (tel)  
202-483-1248 (fax)

September 25, 2009