

## **ESRB PRIVACY ONLINE**

### **PRINCIPLES AND GUIDELINES**

ESRB Privacy Online provides these principles and guidelines regarding the online protection of personal information for companies that participate in the ESRB Privacy Online Program. These principles and guidelines serve as the basis upon which participating companies build their own data protection policies.

ESRB Privacy Online recognizes that the online collection and use of personal information from children raises a different set of concerns than exists with adults, and thus should be subject to a more rigorous set of guidelines. As a result, all participating companies must post a privacy statement that includes a children's section. This section must inform parents of a participating company's privacy policies regarding children, as articulated in Principle 7, which governs children. Furthermore, where companies collect information from children, participation in the ESRB Privacy Online Program mandates the adoption and adherence to Principle 7, incorporating the Children's Program Information Practices Requirements, License Agreement, Privacy Statement Composer, Self-Evaluation, Onsite Audit, Sentinel Enforcement Program, Alternative Dispute Resolution, and Outside Agency Referral. If your website is directed in whole or in part to children<sup>1</sup> or your information collection practices are otherwise subject to the Children's Online Privacy Protection Act ("COPPA") Rule, you must implement the requirements of Principle 7, which shall govern over the first 6 Principles if there are any inconsistencies.<sup>2</sup>

Please note the ESRB Privacy Online Children's Program Requirements (see pages 8-12, inclusive) have been approved by the Federal Trade Commission as a safe harbor program for compliance with the Children's Online Privacy Protection Rule.

---

<sup>1</sup> A general audience website is directed in part to children if it contains an area directed to children.

<sup>2</sup> In adopting these Principles and Guidelines, participating companies operating websites or online services directed to children must assume their visitors are twelve or under. Participating companies operating websites or online services appealing mainly to adults may, on the other hand, assume their visitors are adult, unless they have actual knowledge that a visitor is a child. Participating companies operating "mixed appeal" websites, which are designed to appeal to both adults and children, should ask the age of the visitor in a neutral manner, take reasonable steps to prevent children age twelve or under from changing their age to be older, and apply the appropriate data collection and use practices. Though requests that web visitors identify their own age may, in certain cases, not yield totally accurate results, participating companies may rely on the age given.

## 1. Notice/Disclosure

**Principle: Each participating company must implement and publish a "Privacy Statement" that informs consumers about its information practices.**

### *Implementation of Notice/Disclosure Principle:*

Participating companies are required to provide a prominently displayed link to their Privacy Statement in the form of the ESRB Privacy Online Certification Seal on the first page of their website and at any point on their website where personal information is requested.<sup>3</sup>

Privacy Statements must be complete, clearly and understandably written, and must contain no unrelated, confusing, or contradictory information.

Privacy Statements must state:

- *What information is collected and by what means.* Participating companies must specify the types of personal information collected from consumers and whether the information is collected directly, by requesting the information, or passively, as through cookies or by tracking Internet Protocol addresses.
- *Who is collecting the information.* Participating companies must clearly identify who collects information on their website, including providing consumers with contact information for the participating company such as a contact name, telephone number, postal address, and email address.
- *How the personal information is used.* Participating companies must state how personal information is used, including how the information may be used by vendors, sponsors, and/or outside third parties. For example, a participating company must state in their Privacy Statements whether information is collected for customer support, registration, product fulfillment, giveaways, contests, or similar promotions.

---

<sup>3</sup>At times, these guidelines distinguish between two classes of data, personal information and demographic information. Personal information is information that can be used to identify a person as an individual, including a name, e-mail address, phone number, home address, social security number, driver's license number, etc. Personal information deserves a higher level of protection because it enables direct contact with the individual and because the individual has a greater interest in controlling this information. Demographic information is anonymous information, which may include age/date of birth, gender, geographic area, hobbies, interests, and favorites. When associated with personal information, demographic information becomes personal information.

- *Whether personal information is shared, rented or sold to third parties.* Participating companies must state: (i) whether personal information is shared, rented or sold to third parties; (ii) the general purposes for which the information is used; and (iii) whether the third parties have agreed to maintain the confidentiality, security, and integrity of the personal information they obtain from the participating company.
- *A statement of the organization's commitment to data security.* Participating companies must state how they protect consumers' data and, if the company shares personal information with third parties, how the third parties protect personal information they receive from the participating company.
- *What choices consumers are offered to customize the collection and use of their personal information.* Participating companies must disclose in their Privacy Statements the choices available to consumers regarding how their personal information is collected and used.
- *What opportunities are offered for consumers to access their personal information.* Participating companies must disclose how they allow a consumer to review, correct, or remove their personal information.
- *What the organization's information practices are with regard to children.* Participating companies must state whether they collect information from children and, if so, how.
- *What steps the organization takes to ensure data quality.* For example, allowing consumers to have access to their personal information for purposes of verification and correction.
- *The consequences, if any, of an individual's refusal to provide information.* For instance, participating companies must disclose whether they require consumers to submit personal information, such as an email address, before giving consumers access to an activity on the company's website.
- *How consumers can ask questions or file complaints.* Participating companies must indicate in their Privacy Statements where to address questions or complaints. Privacy Statements must state the contact information for both the company and ESRB Privacy Online.

Participating companies should teach consumers to make informed choices about how they allow their personal information to be used as they participate in the electronic marketplace. Participating companies may perform this consumer education themselves, through the trade association, or industry public service campaigns, or through ESRB's Privacy Online Program educational services.

## 2. Choice

**Principle: Participating companies must give consumers the choice to exercise reasonable control over the collection and use of their personal information.**

### *Implementation of Choice Principle:*

Consumers must be notified of their right to choose how their personal information is handled and provided with simple, easily understood and readily available mechanisms to exercise such choice over the collection and use of their personal information. Such mechanisms may include opt-in, opt-out, or other equally effective approaches. An opt-in mechanism requires a participating company to obtain authorization from the consumer before collecting personal information from that consumer, or before using it in a particular manner. An opt-out mechanism offers the consumer an opportunity to control certain uses of personal information collected by a participating company.

The scope of choice that is reasonable, and the mechanism that is therefore appropriate, may vary according a number of factors, including:

- *The sensitivity of the data.* For instance, sensitive personal information requires a greater level of consumer choice than mere demographic information.
- *The necessity of the collection or use of personal information for completing a transaction initiated by the consumer.* The less necessary the information is to a transaction, the more available choices consumers should have regarding its collection and use.
- *Whether the use contemplated for the personal information is a secondary use<sup>4</sup> or third party distribution.* If a participating company wishes to use personal information for a purpose other than that for which they collected it, a consumer must be given choices as to how that personal information is handled.
- *The burden created by offering choices.* For instance, participating companies are not required to provide choices that would be financially burdensome.
- *The requirements of state, federal, or other applicable laws.* For instance, some laws may require a company to retain certain information about its customers.

---

<sup>4</sup> Secondary use is use for purposes not directly related to the purpose for which the information was collected.

- *Whether the personal information is collected from a child.* Where a participating company wishes to collect or use the personal information of a child, participating companies must comply with Principle 7, *Children's Program Requirements*.

### 3. Limiting Collection and Retention of Personal Information

**Principle:** Participating companies must limit the collection and retention of personal information to that which is needed for valid business reasons, and any such information must be obtained by lawful and fair means.

*Implementation of Limitation Principle:*

Even if a participating company has a valid business reason to collect personal information from a consumer, it must only collect that personal information which is needed for such valid business reason. Participating companies must periodically reevaluate whether a valid business reason continues to exist for collection or retention of certain personal information, and if the valid business reason ceases to exist or ceases to require the collection or retention of certain personal information, participating companies must limit their collection and retention practices accordingly.

### 4. Data Integrity/Security

**Principle:** Participating companies creating, maintaining, using or disseminating records of personal information must take reasonable measures to assure its reliability and should take reasonable precautions to protect it from loss, misuse, or alteration.

*Implementation of Data Integrity/Security Principle:*

Ensuring that personal information is reliable means that it is accurate, complete, and timely. Reasonable measures to assure the reliability of personal information may include, among other things, using only reputable sources of data, cross-referencing data against multiple sources, providing consumer access to personal information for purposes of verification and correction, and destroying untimely personal information or converting it to anonymous form.

Reasonable precautions to protect data may include, among other things, limiting access to such data to those employees performing a legitimate business function; technical security measures, such as encryption or passwords, to prevent unauthorized access; and the storage of data on secure servers or computers inaccessible by modem. Participating companies must take reasonable steps to assure that third parties to whom they transfer such

information are aware of these security practices, and that the third parties also take reasonable precautions to protect transferred information participating companies must obtain information, including name, address, tax identification number, telephone number and samples of material to be distributed, from third parties that buy, rent, or purchase personal information from the participating company.

## 5. Data Access

**Principle: Consumers must have the opportunity for reasonable, appropriate access to personal information about them that a participating company holds, and must be able to correct, amend, or request the removal of that information when necessary.**

### *Implementation of Access Principle:*

When consumers are offered the opportunity to access the personal information a participating company holds about them, such access must be meaningful. To be meaningful, access must encompass timely and inexpensive access to personal information, a simple means for contesting inaccurate or incomplete personal information, the means by which corrections and/or consumer objections can be logged and sent to all recipients of the personal information, and the ability of a consumer to request the removal of their personal information. Prior to giving a consumer access to their personal information, participating companies must reasonably ensure, in the light of the available technology, that the person requesting to access the information is the person about whom the information pertains.

The reasonableness and appropriateness of access and correction will depend on a variety of factors. These factors include the burden (e.g., cost) that providing access will place on a participating company; the nature of the information collected, including whether it is stored online or offline; the number of locations in which it is stored; the nature of the enterprise; the ways in which the information is to be used; preservation of information security; and whether the personal information is collected from a child.

## 6. Enforcement/Accountability

**Principle: Participating companies must implement effective and affordable mechanisms that ensure compliance with their information privacy policies and provide appropriate means of recourse for consumers.**

### *Implementation of Enforcement Principle:*

Participating companies must create and implement internal processes for ensuring that they comply with the privacy practices they have adopted. Participating companies must train personnel, who are in a position to collect personal information from or about consumers, to adhere to the stated privacy practices. Participating companies must assign specific personnel the responsibility for monitoring compliance with privacy practices. Participating companies must create a system of incentives and/or sanctions to encourage adherence to privacy policies.

Participating companies must also provide verification that the assertions they make about their privacy practices are true and that privacy practices have been implemented as represented. The nature and the extent of verification depends upon the kind of personal information with which a company deals — companies collecting and using highly sensitive personal information may be held to a higher standard of verification.<sup>5</sup> To this end, all participating companies must on a regular basis review their record of compliance with privacy practices. However, where the personal information collected and used is highly sensitive, verification may necessitate that the participating company hire an outside auditor to review the compliance record.

Each participating company must also create and implement internal processes affording consumers appropriate means of recourse for claimed failures by that participating company to adhere to its stated privacy practices. Appropriate means of recourse include, at a minimum, institutional mechanisms to ensure that consumers have a simple, effective way to have their concerns addressed. For example, a participating company must appoint identifiable, accessible, and responsive personnel to whom consumers can initially bring a grievance. Such personnel must be given the authority to investigate the grievance and complete this investigation in a timely manner. Such personnel must be required to submit a written response to the aggrieved consumer that details the results of the investigation, and should be given incentives to respond to consumers in a timely manner. If the participating company has not adhered to its privacy practices, consumers must be offered a remedy for the violation. Such a remedy must be

---

<sup>5</sup> In this instance, the sensitivity of the personal information varies based on the type of personal information, and whether it can be tied to an identifiable person. For example, credit card information or other financial information that can be tied to an individual would be considered highly sensitive, while that individual's name without any accompanying information would be considered less sensitive.

appropriate under the circumstances of the case and may include the righting of the wrong (e.g. correction of any misinformation, cessation of further collection of personal information from that consumer, or destruction of improperly collected personal information) or compensation for any harm caused.

If the consumer is not satisfied with the resolution, participating companies must provide consumers with a mechanism to appeal initial decisions to higher management levels. Lastly, if the consumer is still unsatisfied regarding the resolution of a grievance, the consumer must be referred to ESRB Privacy Online's Alternative Dispute Resolution Officer.

## 7. Children's Program Requirements

**Principle: Participating companies that collect personal information from children must comply with these Children's Program Requirements.**

### *Implementation of Children's Program Requirements:*

Participating companies that operate websites directed in whole or in part to children 12 years old and under that collect information from children, or that have actual knowledge they collect information from children 12 years old and under, must comply with the requirements contained in the Children's Online Privacy Protection Rule (16 C.F.R. Part 312) ("Rule") implementing the Children's Online Privacy Protection Act (15 U.S.C. 6501 et seq.) ("COPPA"). In addition, participating companies must adopt and adhere to the following Children's Program Requirements.

Where there is a conflict between a provision under this Principle and the foregoing Principles, Principle 7 governs the collection, use, and disclosure practices regarding children's information.

### **CHILDREN'S PROGRAM INFORMATION PRACTICES REQUIREMENTS**

#### **A. Privacy Statement and Seal**

Participating companies that operate websites directed to children must prominently post the ESRB Privacy Online Children's Certification Seal ("Children's Seal") on the homepage of such websites and at each area where they collect personal information from children on such websites ("information entry points"). Participating companies who operate general audience websites that have separate children's areas must prominently post the Children's Seal on the homepage of the children's area and at any information entry points of the children's area.

The Children's Seal must link to the section of the participating company's privacy statement setting forth its information practices regarding children.

Participating companies' privacy statements must be clear and understandable, and should not include any unrelated, contradictory, or confusing information. Privacy statements must include:

*1. Contact Information.* Participating companies must always list the complete contact information for the participating company — including a contact name, telephone number, postal address, and email address. In addition, participating companies must also either: (i) list the complete contact information for every person, organization, or company collecting information through the participating company's website; or (ii) agree to respond to all privacy inquiries, as long as the names of all persons, organizations, or companies collecting or maintaining

personal information through the participating company's website are also listed in the participating company's Privacy Statement.

*2. Collection of Personal Information.* Participating companies must include the types of personal information collected and whether the information is collected directly or passively.

*3. Use of Personal Information.* Participating companies must indicate how children's personal information is used, including but not limited to whether it is used for fulfillment of a requested transaction, record keeping, marketing products or services back to the child, or publicly disclosing personal information in a chat room, bulletin board, or other online forum.

*4. Third-Party Disclosure and Parental Choice.* Participating companies must indicate whether personal information is disclosed to third parties. If participating companies disclose personal information to third-parties, participating companies must: (i) describe the types of business in which such third-parties are engaged and the general purposes for which such information is used; (ii) indicate whether the third parties have agreed to maintain the confidentiality, security, and integrity of the personal information they obtain from the participating company; (iii) state that the parent has the option to consent to the collection and use of their child's personal information without consenting to the disclosure of that information to third-parties; and (iv) describe the procedures for parents to prevent the disclosure of their child's information to third parties.

*5. Limiting Information Collection.* Participating companies must state that they are prohibited from conditioning a child's participation in an activity on the child's disclosing more personal information than is reasonably necessary to participate in such activity.

*6. Parental Access.* Participating companies must state that parents may view and remove their child's personal information, and refuse to permit the further collection or use of their child's personal information. Participating companies must also describe the procedures for exercising parental access for any purpose, including to prevent the disclosure of their child's information to third parties.

## **B. Direct Notice to Parents to Obtain Prior Verifiable Parental Consent**

Participating companies must make reasonable efforts, taking into account available technology, to ensure that a parent receives notice of the participating company's information practices, including notice of any material change in the collection, use, or disclosure practices to which the parent has previously consented. With certain exceptions, participating companies must provide notice to parents and obtain prior verifiable parental consent before collecting any personal information from a child. For exceptions to these requirements, see *Section D* below.

Direct notice to parents sent to obtain prior verifiable parental consent must contain:

- 1. Privacy Statement Information.* Participating companies must include all of the information that is required under *Section A*, above.
- 2. Intent to Collect Information.* Participating companies must state that they wish to collect personal information from the parent's child.
- 3. Parental Permission Required.* Participating companies must state that they are required to obtain the parent's permission to collect the personal information of the child. Participating companies must also describe the procedures by which a parent may give such permission.

### **C. Prior Verifiable Parental Consent**

In most cases, participating companies must obtain prior verifiable parental consent before collecting, using, or disclosing a child's personal information. Participating companies must also obtain prior verifiable parental consent to any material change in the collection, use, or disclosure practices to which the parent has previously consented. Though none of these mechanisms for securing parental consent are foolproof, they provide sufficiently high assurance that consent has been provided by the parent.

*Mechanisms for Verifiable Parental Consent.* Reasonable measures must be taken, in light of the available technology, to ensure that the person providing consent is the child's parent. Acceptable mechanisms for obtaining verifiable parental consent include: (i) providing a consent form to be signed by the parent and returned to the participating company by mail or fax;(ii) requiring a parent to use a credit card in connection with a transaction;(iii) having a parent call a toll-free telephone number staffed by trained personnel;(iv) using an electronic (digital) signature; or (v) using e-mail accompanied by a PIN or password obtained through one of the verification methods described above. Acceptable methods for authenticating the identity of the individual over the telephone may include asking a series of questions that only a parent of the child would have knowledge of (e.g., parent's name, mailing address, email address, child's name, child's email address, etc.).

Until April 21, 2002, methods to obtain prior verifiable parental consent where participating companies' use of information is internal and there is no disclosure to third parties or the public, may also include use of 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 after receiving consent; or obtaining a postal address or telephone number from the parent and confirming the parent's consent by letter or telephone call. Participating companies that use such methods must provide notice that the parent can revoke any consent given in response to the earlier email.

## **D. Exceptions to Prior Verifiable Parental Consent**

Although prior verifiable parental consent is required before most collection, use, or disclosure of a child's personal information, in a few exceptions a participating company may be permitted to collect a child's or parent's name or online contact information (i.e. email address) before obtaining parental consent. As detailed below, in some cases, the participating company must send the parent a direct notice of its information practices containing specific statements about the information collection and use.

*1. Obtaining Consent.* Participating companies may collect the name or online contact information of a parent or child to be used for the sole purpose of obtaining parental consent — so long as the participating company deletes such information from its records if the company has not obtained parental consent after a reasonable time from the date of information collection. To obtain parental consent, participating companies must provide parents with a direct notice that includes all information set forth in *Section B*, above, and must explain that the participating company has collected the name or online contact information of a parent or child in order to provide notice to and obtain consent from the parent. The participating company must not use such information to recontact the child or the parent, or for any other purpose.

*2. One-Time Request.* Participating companies may collect a child's online contact information for the sole purpose of responding directly, on a one-time-basis, to a specific request from the child — so long as such information is not used to recontact the child or for any other purpose, and is subsequently deleted from the participating company's records. Under this exception, participating companies do not need to provide direct notice to parents.

*3. Repeated Requests.* Participating companies may collect a child's online contact information to be used to respond directly, more than once, to a specific request from the child — so long as such information is not used for any other purpose. In such cases, the participating company must make reasonable efforts, taking into consideration available technology, to give direct notice to parents, which must: (i) include all Privacy Statement Information (see *Section A*, above); (ii) explain to parents that the participating company has collected the child's email address, or other online contact information, in order to respond to the child's request; (iii) explain that the child's request will require more than one contact with the child; (iv) explain that the parent may refuse to permit further contact with the child and may require the company to delete the child's information; (v) explain how a parent can refuse to permit further contact and information collection from the child; and (vi) explain that if the parent does not respond, the company may use the information for the purposes stated in the direct notice. This direct notice to parents must be sent immediately after the participating company's initial response to the child and before making any additional response.

**4. Protecting Child Safety.** Participating companies may collect a child's name and online contact information to the extent reasonably necessary to protect the safety of a child participant on the website where the participating company has used reasonable efforts in an attempt to provide notice to the parent — so long as such information is used for the sole purpose of protecting the child's safety, not used to re-contact the child or for any other purpose, and not disclosed on the website. In such cases, the participating company must make reasonable efforts, taking into consideration available technology, to give direct notice to parents, which must: (i) include all Privacy Statement Information (see *Section A*, above); (ii) explain that the participating company has collected the child's email address, or other online contact information, to protect the safety of the child participating on the website; (iii) explain that the parent may refuse to permit further contact with the child and may require the company to delete the child's information; (iv) explain how a parent can refuse to permit further contact and information collection from the child; and (v) explain that if the parent does not respond, the company may use the information for the purposes stated in the direct notice.

**5. Protecting Others.** Participating companies may collect a child's name and online contact information to protect the security or integrity of its website, to take precautions against liability, to respond to judicial process, or to provide information to law enforcement agencies or investigations on matters related to public safety — so long as such information is not used for any other purpose. Under this exception, participating companies do not need to provide direct notice to parents.

## **E. Parental Access**

Participating companies must provide parents access to their child's personal information. Such access must include: (i) a description of the types of information collected from children by the participating company, such as name, address, telephone number, and hobbies; (ii) the opportunity to prevent the participating company from further using or collecting online information about their child in the future; and (iii) the opportunity to direct the participating company to delete the child's personal information from the company's records. Reasonable measures must be taken, in light of the available technology, to ensure that the person requesting access is the child's parent. Acceptable verification mechanisms include: (i) providing a request form to be signed by the parent and returned to the participating company by mail or fax; (ii) requiring a parent to use a credit card in connection with a transaction; (iii) having a parent call a toll-free telephone number staffed by trained personnel; (iv) using an electronic (digital) signature; or (v) using e-mail accompanied by a PIN or password obtained through one of the verification methods described above.

## **F. Limiting Information Collection**

Participating companies are prohibited from conditioning a child's participation in an activity on the child's disclosing more personal information than is reasonably

necessary to participate in such activity.

## **G. Data Integrity and Security**

Participating companies must establish and maintain reasonable procedures, taking into account available technology, to protect the confidentiality, security, and integrity of personal information collected from children.

### **LICENSE AGREEMENT**

Participating companies must execute and be bound by the ESRB Privacy Online License Agreement. As part of this Agreement and as a material obligation, participating companies must agree to comply at all times with all aspects of the ESRB Privacy Online program. Failure to comply with any of the Principles and Guidelines could be interpreted by ESRB Privacy Online as a material breach of the Agreement and constitute a trademark infringement and a dilution of the goodwill and reputation attaching to our mark.

### **PRIVACY STATEMENT COMPOSER**

ESRB Privacy Online offers services to assist companies in creating or modifying privacy statements. These services include: (i) an online privacy statement composition program called the ESRB Privacy Statement Composer; and, (ii) a Privacy Policy & Statement Creation Assistance Team. If a participating company does not have a privacy statement, the Composer helps a company create their first draft. This draft can subsequently be customized to meet a particular business model and unique privacy practices. A team of attorneys is available to work one-on-one with companies to ensure that privacy policies and statements contain collection and use practices that adhere to all of ESRB's requirements while meeting the parameters of most existing business models.

### **SELF-EVALUATION**

Participating companies should complete the Self-Evaluation form in preparation for the Onsite Audit. This form helps participating companies assess and define their information collection and use policies. Preparing for the Onsite Audit allows participating companies to maximize the benefits of the Onsite Audit and to ensure that all aspects of the ESRB Privacy Online Program are being met.

## **ONSITE AUDIT**

Prior to certification, and at annual intervals thereafter, participating companies must submit to an ESRB Privacy Online Onsite Audit. Each Onsite Audit is conducted by a staff attorney who is trained in the area of privacy law. Through these onsite audits, ESRB Privacy Online determines whether a company's privacy statement is an accurate representation of its internal and external information practices. The Onsite Audit also provides ESRB Privacy Online with the opportunity to ensure that a company's information practices meet all of our program's requirements and such requirements are maintained on a consistent basis. ESRB Privacy Online does not grant or renew a certification without first conducting an Onsite Audit and certifying that a company meets the program's criteria.

## **SENTINEL ENFORCEMENT**

The Sentinel Program is the oversight and enforcement arm of the ESRB Privacy Online program, and ensures that participating companies comply with every aspect of the ESRB Privacy Online program. The Sentinel Program is a mandatory mechanism that provides effective enforcement in three distinct ways:

### **A. Sentinel Monitoring and Verification**

Participating companies agree to submit to quarterly reviews of their information practices. The goal of these reviews is to provide effective ongoing enforcement and assure both the consumer and the participating company that a reliable safeguard exists to verify that the company's privacy policy implementation is accurate, meaningful, and effective. Monitoring reviews are unannounced and conducted by specially trained online monitors methodically moving through a participating company's website, page by page, ensuring that: (i) a functional link to the participating company's privacy statement is posted on its homepage and at all information entry points; (ii) except in the case of websites directed to children (where all visitors are presumed to be 12 and under), personal information entry points include a date of birth field to prevent accidental collection of personal information from children before obtaining prior verifiable parental consent; and (iii) the participating company complies with all aspects of the ESRB Privacy Online Program.

If an ESRB Privacy Online Monitor discovers a possible violation regarding a participating company's information practices, the Monitor flags the matter in the Monitor's Report. An ESRB Privacy Online Compliance Manager reviews these reports, and confirms that there is a possible violation. The Compliance Manager then notifies the company that an inquiry into the company's information practices is being initiated and that, depending on the determination, further action may be required. If ESRB Privacy Online determines that a violation of the Principles and Guidelines has occurred, the company is notified in writing of

the specific violations, the corrective actions that must be taken by the company to address the violations, and the consequences of failure to take such actions. Failure to take the corrective actions can result in a number of penalties including the imposition of fines, removal of the ESRB Privacy Online Certification Seal, and referral to the Federal Trade Commission (see Outside Agency Referral, below). Penalties are assessed according to the type of violations and whether such violations were inadvertent, intentional, or willful. In addition, penalties may be assessed against companies that exhibit a pattern of non-compliance.

## **B. Sentinel Spot Checks**

Participating companies agree to submit to randomly scheduled, unannounced audits of their privacy practices, known as "Spot Checks." Spot Checks involve the seeding of a participating company's database by an ESRB Privacy Online Monitor who submits fictitious consumer data at each information entry point. The website's response is then tracked and recorded to determine if the company's collection and use practices adhere to its privacy statement.

## **C. Consumer Online-Hotline**

Another effective enforcement method used by ESRB Privacy Online is the Sentinel Consumer Online-Hotline. The Sentinel Consumer Online-Hotline is a no-charge service that allows web users who have a privacy grievance or who believe that a privacy violation has taken place on a participating company's website to directly report the violation or grievance to ESRB Privacy Online. The reporting can be done swiftly and easily by filling out the Sentinel Consumer Online-Hotline form, indicating the alleged privacy violation. ESRB Privacy Online responds immediately to all consumer concerns and complaints submitted in any form.

## **ALTERNATIVE DISPUTE RESOLUTION**

Participating companies must create and implement an internal dispute resolution program, which should be designed to fairly and expeditiously resolve privacy related issues and complaints raised by either consumers or ESRB Privacy Online monitors. In addition, participating companies must submit to ESRB Privacy Online's Alternative Dispute Resolution services when consumer grievances are not effectively addressed through a company's own internal mechanisms. Participating companies are required to fully participate in any inquiry or investigation opened by ESRB Privacy Online, and are bound to abide by the final judgment of any ESRB Alternative Dispute Resolution.

## **OUTSIDE AGENCY REFERRAL**

If a participating company fails to take appropriate actions in response to a valid complaint or an ESRB Privacy Online mandate, or in any way engages in a

Entertainment Software Rating Board's Privacy Online Program  
Marc Szafran, mszafran@esrb.org, 212.759.0700

pattern of violating ESRB Privacy Online requirement's, ESRB may invoke the remedies described above and is prepared to refer such company to the Federal Trade Commission for engaging in unfair and deceptive trade practices.