Vanderbilt Journal of Entertainment & Technology Law

Volume 4
Issue 2 *Issue 2 - 2002*

Article 6

2002

From Subway Stations to the Information Superhighway: Compliance Strategies for Musicians to Avoid the Worldwide Entanglement of Privacy Laws

Yvenne M. King

From Subway Stations to the Information Superhighway:

Compliance Strategies for Musicians to Avoid the Worldwide Entanglement of Privacy Laws

Yvenne M. King

Music

I. Introduction

Living the "big city" life has always been exciting and inspiring for me, but using public transportation on subways like New York City's MTA system often means rushing through the underground walkways, stairs and escalators, peering anxiously down the dark tunnel for the glimmer of an oncoming train, straining to hear the approaching churn of engines and wheels, and vying for a spot near the opening door to get a seat for the ride. Once in awhile, however, my underground journey is suddenly—and pleasantly—interrupted by a violinist's rendition of a Beethoven symphony or the syncopated beats from a homemade drum set made of paint buckets, pots and an oven rack. My harried schedule is momentarily forgotten as the musicians take me back to my own days of music, especially my flute solos of Bach and Mozart in Boston's Park Street subway station. For me, like many other aspiring musicians, whether rock or classical, performing on subway platforms was another way to create an audience outside of gigs at recital halls or clubs while waiting for that elusive record deal. Over the years, however, many musicians have migrated from underground subway stations to the information superhighway of the Internet. And websites have become the subway platforms of the digital age. *U2* has one.[1] So does *Matchbox Twenty*.[2] The classical pianist John Bell Young even has one.[3]

The advent of the Internet (and the World Wide Web) provides both signed and unsigned musicians[4] the opportunity to directly reach their fans around the world through the inexpensive, yet creative and flexible, vehicle of a website. The Internet offers musicians not only a way to develop a more global fan base, but also the opportunity to engineer (to a greater extent) their own success and retain greater percentages of revenues from sales of albums and merchandise.[5]

For example, the success of Russell Crowe's band, *30 Odd Foot of Grunts*, has been attributed to the Internet.[6] Because of the band's announcement on their website, tickets for one performance were sold out before ads were even placed in traditional media.[7] Chesney Hawkes, a singer who gained popularity during the early 90s, recognized the Internet as a great opportunity to reach out to his fans, and thus re-launched his career with a new single and a website.[8] Jessica Harp, a 19-year-old singer based in Kansas City, sold her self-produced album to fans worldwide, including some in Singapore.[9] Artists of all music genres, even classical, can benefit from online mass marketing opportunities. *The Chiara String Quartet*, formed at Julliard, books performances of Debussy, Haydn and Beethoven, and provides audio clips of performances through its website.[10] Aaron Rosand, the 74-year-old violin virtuoso who launched his website[11] in 1998, admits to his lack of interest in computers, but recognizes the important role of technology in a classical musician's career: "The Internet is opening up an entirely new world for classical musicians, especially recording artists. It's responsible for a tremendous resurgence of interest in recordings."[12]

With all the advantages of the Internet, however, come legal and business risks that musicians must face in order to fully reap the benefits of this equalized playing field. For example, a website that invites fans to add their e-mail addresses to the band's mailing list is subject to various state, federal and foreign privacy regulations protecting personally identifiable information ("personal information"), including e-mail addresses.[13] Some laws govern communications with or among consumers (i.e. among music fans or between fans and musicians) on Internet bulletin boards or chat rooms. Other laws affecting the ownership, use and infringement of creative works (i.e., intellectual property) are implicated when websites provide content and information, such as bios or photos of musicians, band names and logos, press coverage about the artists, lyrics or liner notes to albums, or audio/video clips of performances. In addition, musicians promoting a band or selling CD's or T-shirts online are engaged in commercial activities, and are thus regulated by various laws not necessarily specific to the Internet, such as the Federal Trade Commission Act, the Fair Credit Reporting Act, and the Uniform Commercial Code.

The legal implications and business consequences for musicians operating websites generally fall into two areas of concern. First, musicians should be concerned about liability for third-party claims arising from violations of applicable laws and regulations. Second, musicians should be concerned about the loss of intellectual property rights for failure to fully protect such rights under relevant laws. Like any business with an online presence, musicians should proactively address these concerns to minimize their risk of liability and maximize potential revenues.

In light of the fact that operating a website raises many complex legal issues covering numerous areas of law, this Article focuses on one area that musicians, as website owners, should address: their potential liability for third-party claims based upon violation of consumer privacy laws.[14] This Article first discusses the importance for musician website operators of protecting consumers' privacy rights. Second, it addresses the need to establish a "global privacy compliance plan" to limit musicians' legal liabilities. Finally, it explains how musicians can go about creating such a plan by developing "minimum guidelines" and "privacy practices."

II. Protection of Consumer Privacy Rights and Limiting Legal Liability

The issue of consumers' privacy rights, including the protection of personal information, is not new. The rapid advancement of technology, however, has made it an even greater concern.[15] As methods of collecting, using and disseminating personal information are becoming more sophisticated and diverse, governmental bodies around the world have responded with numerous legislative initiatives.[16]

Attorneys advising their musician clients on compliance with privacy laws are often met with questions like, "We're a rock band not a conglomerate like AOL or Yahoo! We're also not world-renowned artists like Madonna or Sarah Brightman. So, why do we need to worry about complying with privacy laws?" Regardless of size or fame, website owners face the same liability risk because the law does not distinguish between a Fortune 500 company and an individual operating a website. Thus, it is important for musicians—whether they are part of a rock band or simply a solo jazz pianist—to remember that they operate like any small business. While musicians' sites may not top the Federal Trade Commission's ("FTC") target list of potential privacy violators, the risk of liability is *real* and increasingly imminent. This is because governmental bodies and watchdog groups are increasingly pressuring companies to be more accountable for their privacy-related activities through enforcement actions.[17] Highly publicized privacy cases include, for example, the FTC's actions against GeoCities, Inc.[18] and DoubleClick.[19]

THE advent of the Internet (and the World Wide Web) provides both signed and unsigned musicians the opportunity to directly reach their fans around the world through the inexpensive, yet creative and flexible, vehicle of a website.

In the United Sates, a website operator's violation of consumer privacy rights (often by breaching its own privacy policy) is commonly deemed an unfair or deceptive trade practice under the Federal Trade Commission Act. The FTC has full authority to bring enforcement actions and impose civil penalties for such violations.[20] For example, the FTC recently charged three website operators with violating the Children's Online Privacy Protection Act of 1998 ("COPPA") when they collected personal information from children under the age of 13 through their websites.[21] The website operators were required to pay $100,000 in civil penalties, establish privacy policies and procedures in accordance with COPPA and delete all personal information collected from children under the age of 13 after the date COPPA became effective.[22] The European Union ("EU") adopted the "Directive 95/46/EC"[23] in 1998 ("EU Privacy Directive") to regulate data collection by the 15 member states.[24] Violations of the EU Privacy Directive can result in monetary fines, as well as the blocking of the flow of data to and from websites and affected EU users. Other countries, such as Canada, Hong Kong and Japan, also recently passed privacy regulations that include civil and monetary penalties for non-compliance.[25]

III. A Global Privacy Compliance Plan

Establishing preventative measures and compliance procedures can help avoid wasting time and money spent responding to actions for privacy law violations or remedying non-complaince. In addition, if a musician's site, at minimum, collects e-mail addresses or sells CDs online, failing to comply with privacy laws not only increases the musician's legal liability, but also negatively impacts her public relations and promotional efforts.[26]

Compliance with privacy laws can be an overwhelming task given the quantity and complexity of applicable regulations. In the United States alone, the protection of

consumers' privacy is governed by a patchwork of state and federal laws and regulations, as well as by non-governmental industry self-regulatory measures.[27] For example, the U.S. Constitution, tort laws, and specific federal privacy and Internet-specific laws[28] all protect consumers' privacy interests to varying degrees.

Privacy laws with force outside the United States also affect websites operated by musicians. Consider, for example, the case of the *Misfits*. The band is popular throughout the U.S. as well as abroad. As the band's reputation has grown over the years, more and more fans around the world frequent the *Misfits*' website.[29] Because each country regulates privacy rights on an individual basis, the *Misfits*' site must consequently comply with the privacy laws of every country in the world!

The varying levels of protection offered by different countries further complicates efforts to comply with the large number of privacy laws. For example, COPPA requires businesses to obtain "verifiable consent" from the parent of any child under the age of 13 whose personal information is collected by a website.[30] By contrast, the EU Privacy Directive does not specifically protect children under the age of 13. Rather, it prohibits the collection of an individual's "sensitive information," such as information regarding her religious beliefs, health or sex life, without her "explicit consent."[31]

Musicians, however, can meet these legal challenges by establishing a strategic plan to comply, on a global basis, with the intricate network of state, federal and foreign privacy laws. The remainder of this Article discusses the implementation of a global privacy compliance plan, which consists of establishing minimum guidelines and developing privacy practices.

For purposes of this Article, developing a global privacy compliance plan will be based on a website containing one or more of the following features: (1) a list of upcoming performances; (2) bios and photos of the musicians; (3) liner notes and lyrics from albums; (4) press releases, reviews of performances and albums, and other articles about the musicians; (5) a basic fan e-mail list or a fan club to join through membership registration; (6) a bulletin board for fans to communicate with each other; (7) an online store for fans to purchase albums, posters, T-shirts and other related merchandise; (8) a venue for fans to download audio/video clips of selected songs; and (9) links to websites of fellow musicians, relevant music organizations or entertainment sites.[32]

IV. Minimum Guidelines

A global privacy compliance plan should be based on the regulations of the country (or countries) with the most stringent privacy requirements. If the website complies with the laws of the country having the highest privacy standards, then it will naturally follow that the site also meets the applicable laws of all other countries having the same or lower standards. Such standards, referred to herein as minimum guidelines, serve as a guide for the policies and procedures to be developed in a compliance plan. For example, the EU Privacy Directive is currently considered to have enacted the most stringent privacy regulations. Therefore, a site owner should incorporate this Directive into the minimum guidelines. To structure the minimum guidelines in an easily accessible format, each requirement of the EU Privacy Directive should be broken down into a list of compliance requirements (i.e., a checklist), including consequences for non-compliance and steps for enforcement. For example, Article 10 of the EU Privacy Directive requires specific information to be disclosed to users when data is collected from them.[33] Each requirement, such as the identity of the "controller" and purposes of the "processing for which the data are intended," should be listed as discrete bullet points in the minimum guidelines.[34]

WITH all the advantages of the Internet, however, come legal and business risks that musicians must face in order to fully reap the benefits of this equalized playing field.

In addition, the minimum guidelines may consist of more than one body of law. This makes sense because one jurisdiction may have the highest standard of protection in one area while another has stringent requirements regarding a different issue. For example, COPPA's regulations should be incorporated into the minimum guidelines because the U.S. currently imposes the highest privacy standards regarding the personal information

of children. COPPA governs all websites that are either directed to children under the age of 13 or knowingly collect personal information from children (i.e., collect the age of the users along with other personally identifiable information).[35] Even if a website does not actually know it is collecting information from children under the age of 13 (i.e., it does not ask users to reveal their age when submitting their e-mail addresses), it is wise to comply with COPPA for the obvious reason that websites can appeal to, and be accessed over the Internet by, people of all ages.

In determining which privacy laws are relevant when establishing minimum guidelines, the site owner should first identify the countries in which the musician's current fans reside, as well as the countries from which new fans may come. These countries should then be prioritized according to the location in which the largest number of fans (or potential fans) reside. The countries of the EU can be considered one country for purposes of this analysis.[36] Except for musicians with global fan bases, the top five countries from this list will probably provide a sufficient frame of reference to determine the relevant privacy laws. The privacy laws of each jurisdiction should be examined in detail, and the regulations with the most stringent requirements should be incorporated into the minimum guidelines. For purposes of this Article, the relevant laws for the minimum guidelines will be limited to the EU Privacy Directive and COPPA.

V. Privacy Practices

The privacy practices section of a compliance plan should be based on initial set-up tasks that will serve as a foundation upon which the site owner can build by periodically updating its privacy policies and procedures. These tasks involve: (1) assessing the site's data collection practices and creating a data collection practices chart; (2) drafting privacy-related legal documents to be posted on the site; and (3) establishing procedures for monitoring and maintaining compliance. Each of these tasks is discussed in detail below.

Prior to creating the actual comliance plan, however, it is helpful to understand the basic rationale behind the laws seeking to protect consumers' privacy rights. The United States and Europe have similar policy objectives which can be articulated as five basic principles: (1) openness, in the sense that consumers are informed of the personal data collection practices of the sites they visit; (2) disclosure, meaning that there must be a way for consumers to find out what information about them is being recorded and used; (3) secondary usage, meaning that information collected for one purpose cannot be used for another without the consent of the data subjects (i.e. the users); (4) correction, meaning that individuals must have the ability to correct or amend erroneous information about them; and (5) security, in the sense that organizations creating, maintaining, using or disseminating records of personally identifiable information must assure the reliability of the data for the intended use and take precautions against possible misuse.[37]

A. Assessment of Data Collection Practices and Creation of Data Chart

The initial task of determining whether a site meets the minimum guidelines can be accomplished by creating a data collection practices chart (or data chart) that (a) lists *all* the types of information, whether personally identifiable or anonymous, flowing through the site, and (b) describes how such information is collected, used, disclosed and transmitted by the site.

An assessment of the site's data collection practices provides both short- and long-term benefits. Initially, the data chart helps determine whether the site complies with the applicable privacy laws, as established under the minimum guidelines, and what practices need to be instituted or adjusted to meet the guidelines. The data chart also aids in the drafting of requisite privacy-related legal documents to accurately reflect the site's privacy policies and procedures. Once a compliance plan is developed, the data chart then serves as a useful tool for continuously tracking what the site is doing—whether and how new types of information are being collected, whether new laws affect the site's operation, and how the policies and procedures should be revised in accordance with new practices and laws.

1. Identifying the Types of Information Collected

The first step in developing a useful data collection practices chart is to list each type of information that the website collects from its users, and identify whether each type of information is considered "personal informa-

tion" or "anonymous information" (as defined below). This requires an initial analysis of the legal definitions of personal information and "use" of such information under the EU Privacy Directive and COPPA.[38]

The EU Privacy Directive defines personal information as "personal data," which includes any information relating to an identified or identifiable natural person.[39] An "identifiable person" is one who can be identified, directly *or indirectly*, by reference to an identification number or by one or more factors specific to physical, physiological, mental, economic, cultural or social identity.[40] Further, the EU Privacy Directive treats sensitive information as "special categories of data" that cannot be used without an individual's "explicit consent."[41] Sensitive information consists of personal data pertaining to a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life.[42]

Under COPPA, personal information, referred to as "individually identifiable information," means any information that enables a party to identify or contact a child.[43] This definition includes a child's (1) first and last name, (2) home or other physical address, (3) e-mail address or other online contact information (e.g., user ID, screen name or other identifier that permits *direct contact with a person online*), (4) phone number, (5) social security number, (6) "persistent identifier" (e.g., customer number held in a cookie or another identifier *associated with individually identifiable information*), and (7) last name or photograph associated with other information permitting physical or online contact.[44] In addition, personal information under COPPA includes "hobbies, interests and other data collected through cookies and various tracking mechanisms, provided that such information is connected to *individually identifiable information*."[45]

Based on the definitions above, any information that does not individually identify a person is considered anonymous information. One method of collecting anonymous information consists of stripping away personally identifiable features of personal information that has been collected and aggregating it. For example, a website might ask users joining a fan club to submit their names, e-mail addresses and ages. A person's age, in this case, would be deemed personal information unless the name and e-mail address were stripped away from the user's age. The site could then use such data stripped of its personally identifying features to analyze the age groups of fans to whom the music appeals, or share the aggregated data with third parties without the users' consent. Other methods of collecting anonymous information are accomplished through tracking mechanisms, such as website log files, Java, JavaScript, VB Script and cookies. Information stored in cookies, however, can contain either personal or anonymous information.[46] The site owner should, therefore, be certain about what information is being collected through tracking mechanisms so that users can be accurately informed of the types of information the site is collecting about them.

ALTHOUGH privacy advocates strongly favor the use of opt-in controls, most websites use variations of the opt-out mechanism for marketing purposes. For example, a website often pre-sets a default choice so that a user must uncheck a box to have her e-mail address taken off a list for future communications about products and services.

Using the legal definitions of personal information under the EU Privacy Directive and COPPA, the site owner should determine whether each piece of information collected is deemed personal or anonymous information, and itemize all of them in the data chart. The site owner should also compile a separate list of the types of anonymous information collected by the site for tracking purposes, as well as for future assessments of and adjustments to the musician's business and marketing strategies.

2. Identifying the Uses of Collected Information

The second step in developing an effective data chart is to describe how and when each piece of information is collected and used by the website. For example, a website might collect e-mail addresses for the purpose

of e-mailing newsletters to fans about the musician's and upcoming gigs. Or the site might offer a fan club membership by asking a user to submit her name, e-mail address, user name and password through a registration form. And, obviously, a website will collect a user's name, address and credit card information when she purchases a CD or merchandise online. A site may even collect users' opinions on songs or their age, gender and hobbies as part of a contest or promotional giveaway.[47]

Step two includes a legal analysis similar to that required in step one to determine what "use" of personal information means under the EU Privacy Directive and COPPA. The EU Privacy Directive defines the use of personal information as the "processing of personal data" which includes "any operation or set of operations which is performed upon personal data, *whether or not by automatic means*, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction."[48]

COPPA describes the use of personal information as the act of using, collecting or disclosing personal information. Collecting personal information is defined as "the gathering of any personal information from children by any means."[49] This includes (a) asking children to submit personal information online, (b) enabling children to make their personal information publicly available through a chat room, message board or other means, except where the individually identifiable information is not connected with the disclosed information, and (c) tracking or using any "identifying code linked to an individual, such as a cookie."[50] Disclosing personal information refers to when a site owner releases information about a child in an identifiable form for any purpose, including sharing, selling, renting or providing such information to third parties, or making the information publicly available by any means (e.g., posting the information to a personal home page, e-mail service, message board, or chat room).[51]

COPPA governs all data collection practices through any means, whether accomplished "directly or passively."[52] The EU Privacy Directive similarly covers every type of data collection practice, whether done "automatically" or not.[53] Because both regulations, through their use of expansive language, cover online and offline activities, site owners should evaluate and track *all* information they collect—whether personal or anonymous—and *all* uses to which they put it in order to develop an effective global privacy compliance plan.

3. Obtaining Consent

The third step is to determine whether the site obtains a user's consent when collecting and using each type of personal information. Providing users the ability to consent to the collection and use of their personal information can be accomplished through either an opt-in or opt-out mechanism. Users are given the choice of opting-in where the site obtains their affirmative consent *prior to* collecting and using their personal information. By contrast, an opt-out mechanism is deployed once the collection has already taken place. The user's consent is deemed given unless she specifically objects to the collection and use of certain personal information. An example of an opt-out mechanism at work is where a site gives a user the chance to be taken off (through affirmative action on the user's part) a list that is shared with third parties. Although privacy advocates strongly favor the use of opt-in controls, most websites use variations of the opt-out mechanism for marketing purposes. For example, a website often pre-sets a default choice so that a user must un-check a box to have her e-mail address taken off a list for future communications about products and services. In recognition of the conflicting interests of businesses and consumers, legislatures have generally required that users be given "clear and conspicuous" notice of how their personal information is used, as well as the choice to object to such uses through a "readily available" opt-out mechanism.[54]

4. Sharing Information with Third Parties

The fourth step involves determining whether each piece of information collected through the website is shared with third parties, how third parties use the information, the third parties' obligations to abide by the site's privacy policies and procedures, and when and how a user's consent is obtained. Attention should be paid to, for example, whether a third party is obligated by a written contract to adopt the same privacy standards as those used by the website.

5. Use of Children's Personal information

Step five requires determining whether the site collects children's personal information. If the website directly or indirectly collects a user's age, the site owner should integrate COPPA's parental notice and parental consent requirements into its compliance plan. The data chart should describe when and how a child's personal information is collected, what it is used for, when and how the parent is notified, how and when parental consent is obtained, and how the parent can delete or revise such information.

B. Drafting Globally Compliant Legal Documents for Privacy Issues

After conducting an assessment of the site's data collection practices and creating the data chart, the site owner can use the data chart to draft privacy-related legal documents. The first of these documents is the privacy policy, which informs users of the site's information collection practices. The second document that needs to be drafted is the terms of use agreement, which sets forth the responsibilities, obligations and liabilities of parties involved in the use and operation of the website. The data collection practices chart ensures that the site's written policies and procedures are consistent with its actual data collection practices, while the minimum guidelines facilitate the incorporation of the privacy regulations (e.g., the EU Privacy Directive and COPPA) into the substance of these documents.

1. Privacy Policy

The privacy policy should describe how the website collects and uses personal information both internally and with third parties. This document should also inform users about the accuracy of the personal information the site collects, how users can access it and the security measures deployed to protect it.

Because musicians typically cater to a diverse audience, the language in a privacy policy should be "clearly and understandably written, be complete, and ... contain no unrelated, confusing, or contradictory materials."[55] In other words, leave out the legalese, and use clear, specific and concise sentences. Here are some practice tips: (1) begin with an introduction of the purpose or mission of the website; (2) organize text into small sections; (3) use headings and bullet points; (4) provide definitions for Internet or technology-related terms that are used in the privacy policy; and (5) include specific examples throughout the document to illustrate the site's actual practices. Pursuant to the minimum guidelines, the privacy policy should address the following major issues in the order suggested below.

a. Types of Information Collected

This section describes the types of information collected by the site and should be organized into two subsections: personal information and anonymous information. Although personal information is the central focus of privacy regulations, consumer-friendly business judgment counsels that a website should disclose how it collects and uses both personal and anonymous information. Each subsection should define the type of information it addresses, as well as provide a description (including examples) of how, why and when each piece of information is collected.

b. Consent to the Collection of Personal information

This section should explain whether, how and when the website either obtains a user's consent or gives a user a choice regarding the collection and use of her personal information. The site owner should always inform users if their personal information is going to be used for a purpose different from what was originally intended or previously authorized, and give them the opportunity to opt out of the new use.[56] For example, a user purchases a CD through the site and her e-mail address is initially collected for the site owner to e-mail her a confirmation of the order. If the site owner wishes to subsequently e-mail that user a list of upcoming performances, then the site owner should notify the user of the new use and obtain her consent prior to the new use. The practice and procedure for handling new uses of personal information should be explained in the privacy policy, as well as recorded in the data collection practices chart.

As a corollary to providing users with choice and consent, this section should disclose any possible consequences that users face by refusing to submit, or restricting the site's use of, certain information. For

example, if a user does not want to indicate her preferences for certain merchandise when signing up for a fan club, the website should inform the user that she will consequently not be eligible for an upcoming promotional giveaway of that merchandise.

As discussed above, if the website collects any sensitive information, this section should explain when and how the site collects and uses such information and how users can object to its collection and use. In addition, there are circumstances under which the site owner is not required to obtain consent for using personal information. These circumstances are explained elsewhere[57] in the privacy policy, but should be noted here as well.

c. Sharing Information with Third Parties

The privacy policy should inform users, in a clear and conspicuous manner, whether, why, how and when personal information is shared with third parties. [58] It should also inform them about how their consent to such sharing is secured.[59] This section should also describe the types of third parties involved and the businesses in which they are engaged.[60] Further, the site owner should outline the obligations of third parties regarding their use of personal and/or sensitive information, explain any possible consequences that users face by withholding consent, and refer users to the section on exceptions to obtaining consent.[61]

d. Children's Personal Information

To effectively comply with COPPA's detailed standards and procedures designed to protect children, the privacy policy should contain a separate section on how, when, why and what personal information from children under the age of 13 is collected and used by the website.

Subsection one can summarize the site owner's wish to involve parents in a child's online activities, and explain the available options related to the collection and use of children's personal information. This introduction should also include a statement of the general rule that the collection and use of any child's personal information by either the website or a third party requires the website to (1) notify the child's parent, and (2) obtain the parent's "verifiable consent" *prior to* any collection and use.[62] Two other statements should also be provided in subsection one. The first is a statement to the effect that notice will be given to parents and their verifiable consent obtained before the site changes its previously disclosed data collection practices. Secondly, the site should state that it "cannot condition a child's participation in an activity on the disclosure of more personal information than is reasonably necessary to participate in such activity."[63]

Subsection two should detail the types of children's personal information that the site collects. The language of this subsection should be drafted in the same manner as the above section describing personal and anonymous information,[64] except that the language here should specifically refer to children under the age of 13. If the site owner shares the personal information of children with third parties, subsection three should describe this in the same way as explained in the section discussing sharing personal information with third parties.[65] Subsections four, five and six should explain the site's procedures for providing notice to parents and obtaining their verifiable consent, as well as the possible exceptions to those requirements.[66]

The seventh subsection should discuss how and when parents can review, revise and/or delete any of their children's personal information that has been collected and used. This subsection should also disclose any possible consequences if a parent refuses to submit, or restricts the site's use of, certain personal information, such as the child's inability to use the site's services entirely or access certain areas of the site.[67]

e. Exceptions to Obtaining Users' Consent

Certain circumstances will require the site owner to disclose personal information regardless of the user's consent or objection. Disclosure may be required under laws and regulations, court orders, instructions from governmental agencies or law enforcement authorities, as well as in connection with a suspected violation of the privacy policy, the terms of use agreement, or any other rules and regulations established by the site owner. The site owner should explain these exceptions to its usual data collection practices.

f. Data Security

Pursuant to the minimum guidelines, the site owner should undertake technological and non-technological measures to protect its users' personal information from being lost, destroyed, altered, misused, accessed or disclosed without authorization. This section should explain the site owner's efforts to secure such data.

g. Data Integrity and Access

Similar to data security measures, the site owner must use adequate technological and non-technological systems to ensure that all personal information is collected and used only for intended purposes, and that the data is reliable, accurate, complete and current for such purposes. This means that the website should give users an opportunity to access, review, delete and correct any personal information submitted to the site. The privacy policy should explain how users may review and access their data, and whether or how users receive confirmation of changes made to their personal information.[68]

A user's right to access her personal information is not absolute. Rather, it is determined by balancing the user's legitimate interest in maintaining the integrity of her personal information against the site owner's interest in remaining free of burdensome or fraudulent requests. Accordingly, the site owner may deny a user access if (1) the data is publicly available (provided that the information collected by the site is not combined with information not publicly available), or (2) the site owner did not receive sufficient information to confirm the user's identity.[69] The site owner must respond to a user's request for access to or correction of her data within a reasonable time period, but does not have to fulfill the request if it is unreasonably expensive and burdensome.[70] Consequently, the site owner may incorporate into the compliance plan (and disclose in the privacy policy) a practice by which a user is charged a reasonable fee for data access requests. Requests for access by users may also be limited to a reasonable number within a given time period.[71] And, as is recommended in the section discussing exceptions to obtaining users' consent, this section should fully describe all circumstances under which the site owner may deny a user access to her data.[72]

h. Enforcement

As part of the global privacy compliance plan, the site owner should establish procedures to investigate and resolve complaints and disputes and enforce the site's rules and regulations. This section should include a general statement informing users that such procedures have been established, and explain how users can submit a complaint to the contact person (defined below) for any alleged violation(s) of their privacy rights as set forth in the privacy policy and terms of use agreement.

i. Contact Person

As part of the enforcement procedures, the site owner should appoint an authorized representative (i.e., a contact person) to respond to users' questions, concerns and complaints about access to the website, the use of the site's services and products, and related policies and procedures, including parents' inquiries regarding the use of children's personal information. The privacy policy should list the contact person's name, title or position in the site owner's company, address, phone number and e-mail address.[73]

j. Changes to the Privacy Policy and Information Practices

As musicians' businesses develop and circumstances change, they may find it necessary to change their sites' information or data collection practices. Site owners may also need to change their data collection practices in order to comply with new or revised laws. This section should explain how a website plans to inform users of changes to the privacy policy and its information practices. The site owner should reserve the right to amend the privacy policy at any time while assuring users that any changes will be disclosed in the privacy policy located on the site. Users should also be given the opportunity to opt-out of any new uses of their personal information. In addition, the date on which the privacy policy was last updated should be posted at or near the beginning of this document in a clear and conspicuous manner.

k. Users' Acceptance of Terms

Although not required, it is customary to include a closing paragraph that discusses users' acceptance of the

terms of the privacy policy. This section should make clear that by accessing the site, the user acknowedges that she has read and accepts the terms of the privacy policy, the terms of use agreement and all other rules and regulations imposed by the website. This section should further state that users' acceptance of all such terms is legally binding.

2. Terms of Use Agreement

The second legal document to be created as part of the global privacy compliance plan is the terms of use agreement between the site and its users. This agreement contains provisions similar to those found in a "shrink-wrap" license agreement.[74] The privacy-related portion of the terms of use agreement outlines a user's duties and obligations to other users, third parties and the site owner when accessing the site and using any services or products offered on it.[75] Generally, this section describes prohibited conduct, and offers guidelines on and specific examples of how the user can protect herself while online.[76] Some websites, such as Disney's, even create a separate section of "user rules" or "safety tips."[77] Further, the site owner should reserve the right to (1) determine, in its sole discretion, whether any user conduct or information provided by such user is objectionable or otherwise inappropriate, and (2) prevent or terminate a user's access to the site or its password-protected areas for any objectionable or inappropriate conduct. These rights should be expressly reserved in order for the site to maintain some flexibility in determining how to protect its users and itself from various types of inappropriate online behavior.

VI. Practical Tips for Maintaining a Global Privacy Compliance Plan

The last step in creating a global privacy compliance plan is to establish technical and non-technical procedures to help maintain and update the site's privacy compliance on an ongoing basis. The following provides some practical suggestions that should be incorporated into any compliance plan.

A. Placement of Links and Notices

To minimize the complexity of the legal documents posted on the site, links should be used generously so that users can quickly access cross-referenced subject areas and pertinent parts of the documents. For example, links should be provided whenever the privacy policy or terms of use agreement is referenced. Similarly, links should be provided to forms and procedures referenced in the policy's discussion of notice and verifiable consent practices. A table of contents should also be used in the privacy policy so that users can go directly to particular subsections. Furthermore, pages where users can revise their personal information should be linked to discussions in the policy of how users can access, review and modify their personal information. And, if the information of the contact person is located at the end of the privacy policy, a link should be placed on the first page with a heading, such as "For questions, contact our Privacy Officer." Both Yahoo! and Nick.com incorporate these types of practices into their online privacy policies. Yahoo! provides numerous links so that users do not have to wade through a long legal document,[78] and Nick.com uses links to its forms regarding COPPA procedures.[79]

Once the privacy policy and terms of use agreement are drafted, it is important to plan the placement and location of the links to these documents on the site. These links should be clearly labeled as information regarding the site's policies and procedures, and placed in close proximity to each area on the site where personal information is requested.[80] Although many websites place document links at the bottom of their webpages, and often in a small font size, in the spirit of fair information practices, such links should be clear and conspicuous, in a visible font, and located ideally at the top or in side menu bars of the webpage. For example, the privacy policy link on Disney's website[81] is located at the bottom of the page, but in a large, boldfaced font. Other privacy policy links, although appearing in a small-sized font, can be effective if they are underlined, in a boldfaced font, and on the initial viewing screen.[82] Moreover, links to the privacy policy and terms of use agreement should be placed on every webpage of the site, and in the same location on each page.

In addition to keeping users informed of when the privacy policy was last updated, the site owner should record, in the data collection practices chart, all such dates to track when it began collecting and using a particular type of personal information. This enables the site owner to recall when consent was obtained

regarding the use of each piece of personal information, and thus ensure compliance with consent requirements if the personal information is used for new purposes. For example, if a website collects a user's mailing address through her online purchase of a CD, and the musician subsequently wishes to mail that user a flyer about a future tour, COPPA and the EU Privacy Directive require prior consent from the user for this new use.

When obtaining user consent, the site owner should err on the conservative side by assuming that consent has not been obtained when it receives no response from a user about the use of certain personal information. If the non-response pertains to children's personal information, the site owner should not re-contact the child for any purposes (except where COPPA permits re-contact) and delete that personal information from the site's records after a reasonable period of time has passed. The time period should be recorded in the data chart for tracking and maintenance purposes. Also, it should be kept in mind that this type of limited use should be strictly applied to any sensitive information that is collected.

From an administrative perspective, it is wise for site owners to place the notice and consent forms for parents, regarding requests for use of children's personal information, in one document so that they receive notice concerning and can respond to such requests at the same time. This can help the site owner track compliance with COPPA and control access to the site by children under the age of 13.[83] Another means of controlling access to the site by children is to create pop-up windows asking users if they are under the age of 13. If a user answers affirmatively, then the system could prompt the user through the parental notice and consent process. Although it is possible that users do not disclose their real ages, using such a mechanism could help limit the site owner's liability by showing that good faith measures were adopted to protect children under the age of 13. Further, although no law currently addresses online privacy issues for children between the ages of 13 and 18, the site owner may wish to consider creating some policies specifically addressing this age group. At a minimum, a privacy policy should provide a general statement regarding the protection of users under the age of 18.[84]

B. Training Staff and Assigning Privacy-Related Tasks

Adequately training staff members and assigning them privacy-related responsibilities is essential to maintaining an effective global privacy compliance plan. Persons working for the site owner, whether as employees or independent contractors, should be familiar with the compliance plan so that everyone involved—whether in marketing, sales, technology, legal or operations—can follow and apply the policies and procedures in a uniform and consistent manner.

> FOR example, musicians who have many fans in Europe, or under 13 years of age, should seriously consider certification with programs such as TRUSTe or BBBOnLine or instituting the safe harbor procedures provided by COPPA or the EU Privacy Directive.

Persons should be designated to monitor activity on the site as well as the site's functionality. For example, someone should be responsible for regularly checking the site's content for accuracy and currency, such as news about upcoming gigs, availability of CDs or merchandise and reviews of albums and performances. Publication of false or out-of-date material can lead to legal claims and diminish the overall integrity of the site, as well as negatively affect the musicians' reputation among their fans and industry professionals. A person should be responsible for monitoring all incoming e-mails and user activities in chat rooms or on bulletin boards to track possible infringing activities or inappropriate or criminal behavior. Another staff person should regularly monitor and test the site, its interactive components and related systems, in order to maintain the security and integrity of all data. For example, measures should be undertaken to ensure that users are actually receiving notice of and the opportunity to opt in or out of the site's collection and use of their personal information. The website owner should also designate a person to update the data collection practices chart, on at least a quarterly basis, as to what the site is doing—whether and how new types of information are being col-

lected, whether new laws affect the site's operation, and how the policies and procedures should be revised in accordance with new practices and laws.

C. Third-Party Written Agreements

Compliance with applicable privacy laws requires not only setting privacy standards, but also holding business partners, associates and any third party having access to any personal or anonymous information collected by the site to those same privacy practices. Accordingly, the global privacy compliance plan should include procedures for the site owner to execute written agreements with any third party so that it can limit its risk of liability for third-party actions and better protect the personal information of its users.

These agreements should specifically obligate third parties to adopt all privacy policies and procedures (including the requisite legal documents) used by the website during the *entire* period that the third party receives and/or uses any information regarding the site's users. As a less favored alternative, the site owner could require third parties to incorporate privacy policies and procedures with at least the same level of privacy protection as that used by the website.[85] These written agreements should also outline third parties' privacy obligations in terms of both technological and non-technological practices, such as using high-quality, industry-standard systems to keep data secure and appointing qualified staff to handle privacy and other website issues.

D. Self-Regulation

Site owners can further minimize their liability by incorporating into their compliance plans information practices recommended by industry associations supporting self-regulatory initiatives (e.g., Online Privacy Alliance, Direct Marketing Association, and Network Advertisers Initiative) or by joining online privacy seal programs. Seal programs, designed and implemented by widely recognized third parties, such as TRUSTe or BBB*OnLine*, are known to the public as independent organizations that help establish industry standards for protecting consumers' privacy interests. These types of programs certify websites that comply with their standards and allow those sites to display the programs' seal of approval. In addition, the EU Privacy Directive and COPPA offer website operators the opportunity to self-certify compliance with the laws' requirements and, consequently, qualify for safe harbor treatment (i.e., the websites are deemed to be in compliance with the regulations).[86]

Participation in seal programs and safe harbor programs, or adopting recommended data collection practices, are not legally required, but are administratively straightforward to implement and can help promote good public relations. Many small businesses, however, often choose not to participate because of the time and fees that some programs require. The decision to undertake one or more of these self-regulatory measures requires each website to balance the business, legal, marketing and financial advantages and disadvantages involved. For example, musicians who have many fans in Europe, or under 13 years of age, should seriously consider certification with programs such as TRUSTe[87] or BBB*OnLine*[88] or instituting the safe harbor procedures provided by COPPA or the EU Privacy Directive.[89]

E. Emergency Backup Plans

It is important to have emergency backup or disaster recovery plans in order to continuously provide fans access to the website, minimize interruptions such as system downtimes or losses of data and limit liability for third-party claims. The site owner should first designate a staff person to oversee and handle the resolution of system problems. The site owner should also create a chart showing which service providers the site's staff should contact when problems arise (including names, phone numbers, etc.) and describing each service provider's responsibilities, such as fixing downed servers, checking and cleaning systems affected by viruses or recovering lost or damaged data. This chart, essentially a written disaster recovery plan, should also include the response times and levels of support (in accordance with written service agreements) expected of each service provider. In other words, when addressing disaster recovery procedures, a site owner should have in place (and periodically review) service agreements (e.g., for ISP, ASP or maintenance services) that outline the extent and scope of the duties and obligations of its various service providers.

Being prepared to implement disaster recovery procedures also requires an analysis of how the site and its data are affected if one of its service providers

breaches a service agreement or becomes financially insolvent. The site owner should thus know whether and how the data and other intellectual property connected to the site is accessible and should set up procedures to transfer the data and related services to a replacement service provider when necessary.

VII. Conclusion

Through the use of websites, the Internet opens new doors for signed and unsigned musicians. With this opportunity, however, come challenges. Important among those is designing and implementing a global privacy compliance plan to address the complex entanglement of state, federal and foreign privacy laws. With this compliance tool in hand, musicians can take greater control of their music and careers—on a global basis. JELP

Yvenne M. King counsels all types of arts and technology-related professionals on arts and entertainment, intellectual property, Internet, technology and corporate law matters. J.D. George Washington University, B.S. University of Virginia. The author would like to especially thank Paul Werner for all of his help, and Shareen Rafique and Shahed Hasan for presenting me with the opportunity to write for JELP. Much appreciation to Harold Bell for the support, advice and encouragement over the years. Special thanks to my best friend, Kay Haas, for the many English-writing and life lessons, and to my parents and sister for sharing love and life.

Notes

1. *See* U2.com, *at* http://www.u2.com (last visited Mar. 13, 2002).

2. *See* Official Matchbox Twenty Website, *at* http://www.matchboxtwenty.com (last visited Mar. 18, 2002).

3. *See* John Bell Young Website, *at* http://www.johnbellyoung.com (last visited Mar. 18, 2002).

4. For purposes of this Article, musician(s) means a solo musician or group of musicians of any musical style, such as rock, pop, classical, or jazz.

5. *See* Ed Christman, *Web Promotions Help Push Matchbox Twenty Set to Success*, BILLBOARD, July 29, 2000, at 53, *available at* 2000 WL 24844722; Paul Talacko, *A Sound Marketing Idea for Web-Wise Musicians: Music on the Internet*, FIN. TIMES (London), July 11, 2001, at 14.

6. PR NEWSWIRE, *On-Line Fans Decide Which Cities to be Included in 30 Odd Foot of Grunts and Frontman Russell Crowe's Summer American Tour*, June 27, 2001 (on file with author). *See generally* Gruntland.com, *at* http://www.gruntland.com (last visited Mar. 18, 2002).

7. *Newsmakers: Gotta Crowe*, PHILA. INQUIRER, June 30, 2001, at E5.

8. *Online: Working It Out: The One and Only*, GUARDIAN (London), Nov. 15, 2001, at 4, *available at* 2001 WL 30176207. *See generally* Official Chesney Hawkes Website, *at* http://www.chesneyhawkes.com (last visited Mar. 18, 2002).

9. Brittany Draffen, *Someone to Harp About*, KAN. CITY TEEN STAR, Feb. 23, 2001, *at* http://www.jessicaharp.net.

10. Nancy Beth Jackson, *Classical Musicians Applaud Web; Sites Help Lure New Audiences for Their Works*, CHI. TRIB., Jan. 21, 2002, at B3, *available at* 2002 WL 2614732. *See generally* Chiara String Quartet Website, *at* http://www.chiaraquartet.com (last visited Mar. 18, 2002).

11. *See generally* Aaron Rosand Website, *at* http://www.aaronrosand.com (last modified Jan. 16, 2002).

12. Jackson, *supra* note 10.

13. *See* discussion *infra* at V.A.1.

14. For purposes of this Article, the terms website owner(s), site owner(s) and website operator(s) refer to the musicians featured on a particular website, who are assumed to own and operate the site, and own, control and pay for the collection and maintenance of all data and creative works flowing through the site.

15. *See* Beth Givens, Testimony Before Cal. Leg. Joint Task Force on Personal Info. and Privacy, *A Review of State and Federal Privacy Laws* (Apr. 1, 1997), *at* http://www.privactrights.org/ar/jttaskap.htm; *see also* Timothy J. Muris, *Protecting Consumers' Privacy: 2002 and Beyond*, Remarks at the Privacy 2001 Conference (Oct. 4, 2001), *at* http://www.ftc.gov/speeches/muris/privisp1002.htm.

16. *See* L. Richard Fischer & Shannon K. Ryerson, *California Governor Acts of Privacy Legislation*, PRIVACY & INFO. L. REP., Dec. 2001, at 22-23; Richard Fischer and Shannon K. Ryerson, *Vermont Passes Own Stricter Financial Privacy Regulations*, PRIVACY & INFO. L. REP., Nov. 2001, at 18-19; Eric J. Sinrod, *E-Legal: Congress Looks to Control the Internet*, *at* http://www.law.com (Feb. 19, 2002).

17. *See* Muris, *supra* note 15. *See also Privacy Online: Fair Information Practices in the Electronic Marketplace: Prepared Statement of Fed. Trade Comm'n Chairman Robert Pitofsky, at* http://www.ftc.gov/os/2000/05/testimonyprivacy.htm (May 25, 2000).

18. *In re* GeoCities, Inc., FTC No. C-3849, 1999 FTC LEXIS 17 (Feb. 5, 1999).

19. *In re* DoubleClick Inc. Privacy Litig., 154 F. Supp.2d 497 (S.D.N.Y. 2001).

20. 15 U.S.C. §§ 45, 57b (1994).

21. Press Release, Fed. Trade Comm'n, FTC Announces Settlements With Websites That Collected Children's Personal Data Without Parental Permission (April 19, 2001), *at* http://www.ftc.gov/opa/2001/04/girlslife.htm.

22. *Id.*

23. Council Directive 95/46/EC, 1995 O.J. (L 281) [hereinafter EU Privacy Directive].

24. EU Privacy Directive, art. 32.

25. The Personal Information and Electronic Documents Act became effective January 1, 2001. S.C. 2000 ch. 5 (Can.). *See generally* Juliana M. Spaeth et al., *Privacy, Eh! The Impact of Canada's Personal Information Protection and Electronic Documents Act on Transnational Business*, 4 VAND. J. ENT. L. & PRAC. 29 (Winter 2002).

26. *See* Dave Steer, *Privacy Practices Help Build Trust, Get and Retain Web Customers*, ECMGT.COM, *at* http://ecmgt.com/Nov1999/feature.article.htm (Oct. 29, 1999).

27. *See generally* Dorothy Glancy, *At the Intersection of Visible and Invisible Worlds: United States Privacy Law and the Internet*, 16 SANTA CLARA L. COMPUTER & HIGH TECH. L.J. 357 (2000); Joel R. Reidenberg, *E-Commerce and Trans-Atlantic Privacy*, 38 HOUS. L. REV. 717 (2001).

28. *See, e.g.*, Fair Credit Reporting Act, 15 U.S.C. § 1861 (1994); Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-06 (Supp. V 1999); Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801-09 (Supp. V 1999); Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510-20 (1994 & Supp. V 1999).

29. Misfits.com, *at* http://www.misfits.com (last updated Mar. 6, 2002).

30. 15 U.S.C. § 6502(b) (Supp. V 1999); 16 C.F.R. § 312.5(a) (2001).

31. EU Privacy Directive, art. 8.

32. *See* Misfits.com, *at* http://www.misfits.com (last updated Mar. 6, 2002); Official Matchbox Twenty Website, *at* http://matchboxtwenty.com (last visited Mar. 18, 2002); Sarah Brightman Website, *at* http://www.sarahbrightman.co.uk (last visited Mar. 19, 2002).

33. EU Privacy Directive, art. 10.

34. *Id.*

35. 15 U.S.C. §§ 6501-02 (Supp. V 1999); 16 C.F.R. §§ 312.2-.3.

36. The fifteen Member States of the European Union are Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, Netherlands, Portugal, Spain, Sweden, and the United Kingdom. Note that the EU Privacy Directive regulates the privacy rights of all member states of the EU, but also authorizes each member state to pass legislation to set additional standards. Therefore, further analysis of any member state in which a significant fan base exists should be considered.

37. *See Privacy Online: Fair Information Practices in the Electronic Marketplace: Prepared Statement of Fed. Trade Comm'n Chairman Robert Pitofsky, at* http://www.ftc.gov/os/2000/05/testimonyprivacy.htm (May 25, 2000). *See also* U.S. Dep't of Com. Website, *Safe Harbor Overview, at* http://www.export.gov/safeharbor/sh_overview.html (last visited Mar 18, 2002); U.S. Dep't of Com. Website, *Safe Harbor Workbook, at* http://www.export.gov/safeharbor/sh_workbook.html (last visited Mar. 20, 2002) [hereinafter *Safe Harbor Workbook*]. *See also* Givens, *supra* note 15.

38. These definitions, along with any related definitions

from other applicable privacy laws, should be incorporated into the minimum guidelines.

39. EU Privacy Directive, art 2.

40. *Id.* (emphasis added).

41. *Id.* art. 8.

42. *Id.*

43. 16 C.F.R. § 312.2 (2001) (emphasis added); *see also* Fed. Trade Comm'n Website, *How to Comply with the Children's Online Privacy Protection Rule, at* http://www.ftc.gov/bcp/conline/pubs/buspubs/coppa.htm (Nov. 1999).

44. 16 C.F.R. § 312.2 (2001) (emphasis added); *see also* Fed. Trade Comm'n Website, *How to Comply with the Children's Online Privacy Protection Rule, at* http://www.ftc.gov/bcp/conline/pubs/buspubs/coppa.htm (Nov. 1999).

45. Fed. Trade Comm'n Website, *How to Comply with the Children's Online Privacy Protection Rule, at* http://www.ftc.gov/bcp/conline/pubs/buspubs/coppa.htm (Nov. 1999) (emphasis added).

46. Center for Democracy & Tech., *CDT's Guide to Online Privacy: Getting Started: Online Tracking FAQ, at* http://www.cdt.org/privacy/guide/start/track.html (last visited Mar. 20, 2002); *See* Viktor Mayer-Schönberger, *The Cookie Concept, at* http://www.cookiecentral.com/content.phtml?area=2&id=1 (last visited Mar. 20, 2002).

47. *See, e.g.*, Dana Fuchs Band Website, *at* http://danafuchs.com/home.html (last visited Mar. 19, 2002); Lucinda Williams Website, *at* http://www.lucindawilliams.com (last visited Mar. 19, 2002); Whitney Houston Platinum Club, *at* http://www.whitneyhouston.com/ (last visited Mar. 19, 2002).

48. EU Privacy Directive, art. 2 (emphasis added).

49. 16 C.F.R. § 312.2 (2001) (emphasis added). Note, as previously mentioned, the site owner should clearly understand what information each tracking mechanism actually collects.

50. *Id.* (emphasis added). As previously mentioned, the site owner should clearly understand what information is actually collected by each tracking device.

51. *Id.* (emphasis added). Both online and offline information practices are regulated.

52. *Id.* § 312.2(b)(2)(iii).

53. EU Privacy Directive, art. 2

54. *Safe Harbor Workbook, supra* note 37.

55. § 312.

56. *See Safe Harbor Workbook, supra* note 37.

57. *See* discussion *infra* at V.B.1.e.

58. *See Safe Harbor Workbook, supra* note 37.

59. *See Safe Harbor Workbook, supra* note 37.

60. § 312.4(b)(2)(iv).

61. *See* discussion *infra* at V.B.1.e.

62. § 312.3 (emphasis added).

63. *Id.* §§ 312.4(b)(2)(v)-(c).

64. *See* discussion *supra* at V.A.1.

65. *See* discussion *supra* at V.B.1.c.

66. Both technological and non-technological measures should be undertaken to ensure that users are actually notified of each collection and use of personal information and that the site obtains users' consent when necessary. *See* § 312.4.

67. *Id.* §§ 312.6(c)-.7.

68. *See Safe Harbor Workbook, supra* note 37.

69. *See* U.S. Dep't of Com. Website, *Safe Harbor Documents, Frequently Asked Question Eight: Access, at* http://www.export.gov/safharbor/FAQ8AccessFINAL.htm (July 21, 2000) [hereinafter *FAQ Eight*].

70. *See Safe Harbor Workbook, supra* note 37; *FAQ Eight, supra* note 69.

71. *FAQ Eight, supra* note 69.

72. *FAQ Eight, supra* note 69.

73. 16 C.F.R. § 312.4(b)(2)(i) (2001); Note that if there is more than one website operator, all operators should be mentioned in the Privacy Policy; otherwise, COPPA requires a contact person representing each of the operators.

74. This document may also be called "Terms and Conditions," "Terms of Service Agreement," "User Agreement" or "Member Agreement."

75. This Article only discusses the user rules of conduct that typically appear in such a document, not other contractual issues that are also included, such as intellectual property rights, warranties, limitations of liability, indemnification and other related issues.

76. *See generally* Center for Democracy & Tech., *CDT's Guide to Online Privacy, at* http://www.cdt.org/privacy/guide/start/track.html (last visited Mar. 20, 2002); Privacy Rights Clearinghouse, *Privacy in Cyberspace: Rules of the Road for the Information Superhighway, at* http://www.privacyrights.org (revised Aug. 2000).

77. *See* Disney Online, *Internet Safety Tips, at* http://disney.go.com/legal/internet_safety.html (last visited Mar. 19, 2002).

78. Yahoo!, *Privacy Policy, at* http://privacy.yahoo.com/privacy/us/ (last visited Mar. 19, 2002).

79. *See* Nick.com, *Nick.com Privacy Policy, at* http://www.nick.com/blab/site_wide/privacy/index.jhtml (last visited Mar. 19, 2002).

80. 16 C.F.R. §§ 312.4(b)(1)(ii)-(iii) (2001).

81. *See* Disney Online, *at* http://disney.go.com/park/homepage/today/flash/index.html (last visited Mar. 19, 2002).

82. *See* Barbie Website, *at* http://www.barbie.com/ (last visited Mar. 19, 2002).

83. *See, e.g.*, Official Matchbox Twenty Website, *Registration Page, at* http://www.matchboxtwenty.com/frame-html/register.php (last visited Mar. 19, 2002). *See also* Nick.com, *Nick.com Privacy Policy, at* http://www.nick.com/blab/site_wide/privacy/index.jhtml (last visited Mar. 19, 2002).

84. *See* Barbie Website, *Privacy Policy, at* http://www.barbie.com/parents/policy.asp (last visited Mar. 19, 2002).

85. *See Safe Harbor Workbook, supra* note 37; *see generally* §§ 312.4(b)(2)(iv), .8. All written agreements should also address liability, ownership of and rights to use intellectual property, indemnification and other related issues.

86. § 312.10; U.S. Dep't of Com. Website, *Safe Harbor Documents, Frequently Asked Question Six: Self-Certification, at* http://www.export.gov/safeharbor/FAQ6SelfCertFINAL.htm (last visited Mar. 20, 2002); U.S. Dep't of Com. Website, *Safe Harbor Documents, Frequently Asked Question Seven: Verification, at* http://www.export.gov/safeharbor/Faq7verifFINAL.htm (last visited Mar. 20, 2002); *Safe Harbor Workbook, supra* note 37. *See also* U.S. Dep't of Com. Website, *Information Required for Safe Harbor Certification, at* http://www.export.gov/safeharbor/sh_registration.html (last visited Mar. 20, 2002).

87. *See generally* TRUSTe, *at* http://www.truste.org/ (last visited Mar. 19, 2002).

88. *See generally* BBB*OnLine, at* http://www.bbbonline.org/ (last visited Mar. 19, 2002).

89. § 312.10. *See also Safe Harbor Workbook, supra* note 37.