PrivacyStudio.com
The Art of Information Management

THE PRIVACY CASE BOOK:

A Global Survey of Privacy and Security Enforcement Actions with Recommendations for Reducing Risks

CHAPTER 6
E-Commerce and Online Activities

Margaret P. Eisenhauer, Esq., CIPP
Privacy and Information Management Services – Margaret P. Eisenhauer, P.C.

Chapter Six
E-COMMERCE AND ONLINE ACTIVITIES

Many of the theories of liability applied to online activities have been discussed in the previous chapters. For example, deceptive trade practices cases have been brought as a result of corporate failure to live up to privacy promises made in posted website privacy notices. However, companies face particular risks associated with certain types of online behavior, such as delivery of content protection software and adware or the interaction with children online.

For companies in Europe, the e-Privacy Directive (discussed in Chapter 5) also imposes controls over the use of cookies on websites. In particular, it requires transparency of the use of cookies. Companies must clearly display the terms under which they use cookies on their websites.

User-Installed Software

Companies concerned about protecting their intellectual property often rely on technology to prevent inappropriate copying of their content. These companies may require users to accept installation of digital rights management software to restrict use of content.

Other companies seek to capture information about users or to deliver content to users, such as advertising. These companies may encourage users to install software, perhaps to receive some type of free application, such as a screen saver, weather program or game.

United States trade practices laws require that the companies inform users about the software they are installing. Companies must also ensure that technology not create security vulnerabilities for the users. Additionally, to the extent that the technology gathers personal information, it must do so in a way that is not deceptive.

THE SONY BMG CASES (2006- 2007)[124]

Respondent: Sony BMG Music Entertainment, Inc. (Certain other parties, depending on the action)

Regulators: Case 1: Attorneys General of the States of Alabama, Alaska, Arizona, Arkansas, Connecticut, Delaware, Florida, Idaho, Illinois, Indiana, Iowa, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Mississippi, Montana, Nebraska, Nevada, New Jersey, New Mexico, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Dakota, Tennessee, Vermont, Virginia, Washington, West Virginia, Wisconsin and Wyoming and by the Attorney General for the District of Columbia (collectively, "the States") (Settlement Date: December 2006)

Case 2: Texas State Attorney General (December 2006)

Case 3: Federal Trade Commission (June 2007)

Sony BMG was also sued in a number of private class action lawsuits in the US and Canada. Most of the US lawsuits were consolidated in the US District Court for the Southern District of New York and settled in December 2006 (the "New York Settlement"). The Canadian class actions were settled in September 2006.

Basis for Complaints:
Case 1: Violation of the various States' consumer protection and trade practices statutes, *e.g.,* Alabama Deceptive Trade Practices Act, Alaska Unfair Trade Practices and Consumer Protection Act

Case 2: Violations of the Texas Consumer Protection Against Spyware Act and the Texas Deceptive Trade Practices-Consumer Protection Act

Case 3: Unfair Trade Practices, Violation of Section 5 of the FTC Act

Facts and Allegations: Respondent distributes music compact discs ("CDs"). Sony BMG sold approximately 17.1 million music CDs to consumers that contained "MediaMax" and "Extended Copy Protection" (or XCP) digital rights management ("DRM") software. When the CDs were played on consumers' computers, the DRM software was subsequently downloaded and installed on the computers.

The various complaints and private lawsuits alleged that the DRM software was installed without appropriate notice to or consent of the users. Additionally the DRM software installed a potentially dangerous rootkit that rendered the computers vulnerable to malicious software and other security threats. In addition, the rootkit hid its existence from the Windows Operating System and in the process created a vulnerability that could allow third parties to access and gain full control over a consumer's computer.

The various complaints also alleged that Sony did not appropriately notify users that the DRM software restricted the number of CD copies that can be made, limited the devices on which the music can be played, and contained technology that, undisclosed to consumers, monitors their listening habits to send marketing messages.

Finally, the complaints alleged that Sony made the DRM software difficult to locate and remove from users' computers.

Outcome: As part of the New York Settlements, Sony BMG agreed to strong restrictions on its use of DRM software going forward. Under this agreement Sony BMG agreed that if it manufactured any CDs with any DRM software from the settlement date through December 31, 2007, it will:

(1) Ensure that the DRM software operates in a manner ensuring that no software will be installed on the hard disk drive of a user's computer unless and until the user has agreed to such installation by accepting an End User License Agreement ("EULA") or by otherwise affirmatively consenting to such installation.

(2) Ensure that an uninstaller for such DRM software is made readily available to consumers, without their needing to provide personal information, either on the CD, through a link on the CD's user interface, or by such other comparable method as is generally used in the software industry.

(3) Ensure that the functionality of any updates and/or material changes in functionality of the DRM software is adequately disclosed.

(4) Ensure that any EULA associated with the DRM software accurately describes the nature and function of the software, and does so in easily understandable language.

(5) Show any EULA associated with the DRM software in advance of its use to an independent third party (the "EULA Reviewer") to be designated jointly by Sony BMG and Plaintiffs' Class Counsel, and receive comments on the proposed EULA from the EULA Reviewer. Sony BMG shall consider, but will not be required to adopt, the comments of the EULA Reviewer. However, to the extent that Sony BMG determines not to accept the EULA Reviewer's comments, the EULA Reviewer will not be required to keep such non-accepted comments confidential.

(6) Provide any DRM software to at least one qualified, independent third party, and obtain an opinion from that third party that the installation and use of the software would create no confirmed security vulnerabilities.

(7) Ensure that, with respect to CDs with DRM software, Sony BMG will, if such CDs are played on computers with active connections to the Internet and the CDs cause the computer to make a connection to the Internet, make a record only of the associated album title, artist, IP address from which the connection was made, and certain non-personally identifiable information; provided, however, that the foregoing shall not preclude Sony BMG from obtaining personally-identifiable information from the user upon consent.

(8) Include, on any Sony BMG CD containing any DRM software, a written disclosure, in plain language and type size, and at a location reasonably calculated to provide appropriate pre-sale notice to consumers, that the CD contains such DRM software and a brief description of such DRM software, and, unless such connection is only made upon the user's prior informed, affirmative consent, that the CD seeks to connect to a Sony BMG (or a contractor's) server.

(9) If the Sony BMG personnel responsible for DRM software are made aware of a suspected security vulnerability, either by virtue of their weekly monitoring of a designated email address or other designated means of communication, or otherwise, it will take the following steps:

(a) Sony BMG will ensure that, within no more than five (5) business days after having received such notice, the circumstances of the suspected security vulnerability are communicated to the security expert for evaluation and testing.

(b) If the security expert determines that the suspected security vulnerability is a confirmed security vulnerability (which determination will be made as soon as practicable), within five (5) business days after the vulnerability is confirmed Sony BMG will, to the extent practicable and where appropriate, notify at least two major computer security providers (*e.g.,* Symantec and Microsoft) of the confirmed security vulnerability.

(c) As soon as practicable, and, in any event, within thirty (30) days after the determination that there is a confirmed security vulnerability, Sony BMG will cause to be developed and released an update to the DRM software that corrects the confirmed security vulnerability. The thirty (30)-day period may be extended for good cause if an update is under development, and Sony BMG believes that an update will be able to be released within a reasonable time.

(d) When Sony BMG releases such an update, it will, to the extent practicable, notify at least two major computer security providers (*e.g.,* Symantec and Microsoft) of the update. The update shall remain continuously available on or through Sony BMG's website throughout the Injunctive Period.

(e) When Sony BMG releases such an update, it will also notify Plaintiffs' Class Counsel.

(f) If, after the period specified above in subparagraph (c), Sony BMG determines that it cannot effectively address the confirmed security vulnerability through means of an update, it will notify Plaintiffs' Class Counsel, and will meet and confer with Plaintiffs' Class Counsel on an appropriate course of action. Sony BMG will take such action as it deems appropriate. If Plaintiffs' Class Counsel does not believe that the actions taken by Sony

BMG are appropriate, it may seek relief from the Court, pursuant to the Court's continuing jurisdiction over matters related to this Settlement Agreement.

Additionally, in its other agreements with the Regulators, Sony BMG further agreed:

(1) Sony BMG's product packaging shall clearly and prominently disclose details about any software bundled with CDs (*i.e*. that it will install on consumers' computers, limit the number of copies that can be made, limit the transfer of files to certain Windows or Sony format devices, and that declining to install it will prevent consumers from accessing or listening to the audio files on their computer).

(2) Sony BMG shall not install any DRM software on consumers' computers without: (a) properly disclosing on the computer screen the information required above; (b) clearly and prominently disclosing on the consumers' computer screen that declining to install the DRM software will prevent them from accessing or listening to their audio files on computers; and (c) obtaining consumers' assent to install the software by clicking a clearly labeled button/link.

(3) Sony BMG shall not use any information it collected from the Internet about its consumers for marketing purposes or to deliver marketing messages. It shall destroy all such data within three days of receipt.

(4) Prior to transmitting consumer information via the internet Sony BMG shall (a) clearly and prominently disclose on the computer screen that this information will be transmitted back to Sony BMG, and (b) obtain the consumer's assent to transmit the information.

(5) Sony BMG shall not install any DRM software that prevents consumers from easily locating and/or removing the software and shall provide a reasonable and effective means to uninstall the software.

(6) Sony BMG shall:

- For a period of two years after the order, provide, free of charge, a program and patch that uninstalls XCP and MediaMax software and removes the associated security vulnerability;

- For a period of two years after the order, post a notice on its website containing information about the uninstall programs and security patch; and

- For a period of 12 months after the order, continue purchasing Internet browser premium keywords to give consumers notice of the security vulnerability associated with the DRM software and the steps to take to protect their computers.

(7) Sony BMG shall extend for 180 days the exchange and compensation program outlined in [the New York Settlement agreement]. It shall also post notices on its website about the extended program and about the repair reimbursement program (see Fine Imposed section below).

Fines Imposed:
Pay up to $150 in consumer redress to each affected consumer to repair damage to their computers caused by Sony BMG's software, as provided in the New York Court settlement.

Case 1: $4,250,000 to the States

Case 2: $750,000 to the State of Texas

(No additional fine imposed by the FTC)

THE DIRECTREVENUE CASE (JUNE 2007)

Respondent: DirectRevenue, LLC

Regulator: Federal Trade Commission

Basis for Complaint: Unfair Trade Practices, Violation of Section 5 of the FTC Act

Facts and Allegations: Respondent is a large software distributor that conducts business principally out of New York. DirectRevenue developed, downloaded and installed advertising-supported software ("adware") to consumers' computers, both directly and through affiliates. The consumers were often unaware of the adware installation, as it was frequently bundled together with other free or paid software programs.

This adware tracked and stored information regarding consumers' internet usage, and then used that information to personalize and display pop-up and other advertisements directly on consumers' computers. DirectRevenue also made it very difficult for consumers to locate and remove the adware by using names that resemble core system software or programs, keeping it off the add/remove programs utility, and other practices.

In light of the activities listed above, the FTC complaint alleged that DirectRevenue violated the FTC Act by:

- Deceptively failing to disclose adware bundled together with other software;
- Unfairly installing adware on consumers' computers; and
- Using unfair uninstall practices related to the adware it had installed.

The FTC classified this conduct as deceptive and unfair under Section 5(a) of the FTC Act as the violations caused substantial injury to consumers.

Outcome: The FTC entered into a consent decree with DirectRevenue, ordering:

DirectRevenue shall establish, implement and maintain a comprehensive program that is reasonably designed to ensure that its affiliates obtain express consent before installing DirectRevenue's programs or applications onto consumers' computers. This program shall include:

(1) Obtaining contact information from prospective participants in any affiliate program;

(2) Providing potential affiliates with a copy of the order and written notice that violation of the order will result in immediate termination of the affiliate program account. In addition, a signed and dated statement shall be obtained acknowledging receipt of and agreement to comply with order;

(3) Requiring each affiliate program to provide identifying information of its sub-affiliates, employees, agents, sub-contractors or anyone else whose work corresponds to the subject matter of this order. In addition, each person listed above shall receive a copy of the order and shall provide a signed and dated statement acknowledging receipt of and agreement to comply with the order;

(4) Establishing, implementing and maintaining a functioning email address or other Internet-based mechanism to report consumers' complaints (regarding the practices of DirectRevenue or of its affiliates), and clearly and prominently disclosing that mechanism on DirectRevenue's websites. In addition, DirectRevenue shall associate complaints with the appropriate software, application, website, good or service (or with the

appropriate affiliate program when applicable) and respond to complaints in a timely manner via email or other Internet-based mechanism;

(5) Investigating promptly and completely the complaints received in order to determine if any participant affiliate is engaging in acts or practices that violate the order;

(6) Terminating any affiliate that has violated this order, and immediately ceasing to display advertisements or send any communications to the consumers who received software through the violations of the affiliate; and

(7) Identifying clearly and prominently the program causing the display of any advertisement, along with providing a hyperlink to a webpage that gives clear and prominent instructions for uninstalling the software or application and accessing DirectRevenue's complaint mechanism.

DirectRevenue shall not send advertisements or other communications through any program or application it installed on consumers' computers prior to October 1, 2005. Within 30 days of the order, DirectRevenue may send up to 3 notices to these consumers' computers advising them that they will no longer receive advertising or communication from DirectRevenue and further advising them as to how they may either authorize DirectRevenue to continue sending advertisements or how they may remove the programs or applications from their computers. DirectRevenue shall not:

(1) Install, publish or otherwise distribute any software script, code, program, or other content that exploits security vulnerabilities on any computer operating system, web browser, or other application in order to download or install any software script, code, program or content onto any computer;

(2) Download or install any software program or application without express consent to do so; or

(3) Install any program or application unless it provides consumers with reasonable and effective means to uninstall the same.

Maintenance of Relevant Documents: For a period of five years from the order, DirectRevenue shall maintain and provide upon request a print or electronic copy of any document that contradicts, qualifies, or calls into question DirectRevenue's compliance with the order.

Delivery of Order: DirectRevenue shall deliver a copy of the order to all current and future principals, officers, directors, and managers and to all current and future employees, agents and representatives who have responsibility over the subject matter of the order within 30 days. The order shall be delivered to new employees within 30 days of assuming responsibilities with DirectRevenue.

Reporting: DirectRevenue shall notify the FTC at least 30 days prior to any corporate change (or proposed change) that may affect compliance with the order. Within 60 days after service of the order and when required by the FTC, DirectRevenue shall file a report setting forth its compliance with the order. It shall also cooperate with the FTC after written notice and appear, or cause officers, employees, representatives or agents to appear for interviews, conferences, discovery, review of documents, testimony, deposition or any other matter or proceeding relevant to the subject of the order.

Fine Imposed: $1,500,000

The New York Attorney General addressed DirectReveunue's conduct by bringing enforcement actions against companies that engaged DirectRevenue as an adware marketing partner.

THE INTERNET ADVERTISERS CASES (JANUARY 2007)[125]

Respondents: Cingular Wireless LLC, Travelocity.com LP, Priceline.com Incorporated

Regulator: New York Attorney General

Basis for Complaint: Violation of NY General Business Law – deceptive trade practices

Facts and Allegations: As described in the DirectRevenue case summary above, DirectRevenue developed, downloaded and installed advertising-supported software ("adware") to consumers' computers. The adware then delivered a steady stream of advertisements for DirectRevenue's customers to the consumers when they surfed the Internet. The consumers were often unaware of the adware installation, as it was frequently bundled together with other free or paid software programs.

The respondents were clients of DirectRevenue LLC; they engaged DirectReveue to deliver ads for their websites and services to Internet users who had downloaded the DirectRevenue software. The Attorney General alleged that the respondents each knew that consumers downloaded the adware without full notice and consent. The Attorney General further alleged that, by using DirectRevenue's adware to advertise their products and services on the Internet, the respondents engaged in a deceptive business practice, in violation of New York law.

Outcome: Each of the respondents voluntarily entered into an Assurance of Discontinuance Agreement with the AG to settle the claims. Each agreement requires the respondent, if it uses adware in the future to:

(1) Require its adware marketing partners to agree in writing to:

- Provide consumers with full disclosure of (i) the name of each company delivering its advertisements through adware, (ii) the name of the adware programs, and (iii) the name of all software bundled with the adware programs;
- Brand each advertisement with a prominently and easily identifiable brand name or icon, and use the branding consistent with each advertisement attributable to the brand;
- On each screen and dialog box (without having to scroll down) where adware or bundled software is offered, provide a description of the adware's functions, identify all information monitored, stored and/or distributed by the adware program and obtain consumer consent to both download and run the adware;
- Provide a conspicuous entry in the Add/Remove Programs facility in the consumer's operating system that identifies the adware brand and provider, and does not require consumers to download any additional applications to complete the uninstallation; and
- For all consumers who previously downloaded the adware, provide notice that meets the requirements above and obtain consent to continue serving ads to these consumers.

(2) Implement a due diligence program with respect to adware advertising, with such due diligence performed at inception of a relationship and quarterly thereafter, whereby the respondent shall:

- Ask its adware marketing partners to provide the names of all programs used by the companies to deliver its advertisements;
- Download each of the identified adware programs at a sampling of three websites obtained through independent Internet research;

- Verify that the adware programs comply with the Assurance and company policy; and
- Cease using any adware program that violates this assurance or company policy.

(3) Within 30 days and annually for the next three years, provide a certified letter or affidavit to the Attorney General's office setting forth its compliance with the terms.

Fine Imposed: $35,000 against Priceline.com,

$30,000 against Travelocity

$35,000 against Cingular Wireless

The agreements in these cases strongly suggest that companies who seek to use digital rights management software, adware or other tools should take steps to ensure transparency of any process that installs software or otherwise changes a user's computer state. The functionality of the software must be clearly disclosed as well. Transparency should be obtained by including information on the company websites, on product packaging, and in clearly-written end user agreements that are presented to users in a conspicuous manner prior to installation.

Consumer protection and fair trade practices laws likely also require companies to:

- Obtain consent to DRM software or adware installation or computer state changes. If the software collects personal information, companies obtain specific consent for this data collection as well;
- Provide a readily-available, uninstaller for installed software free of charge; and
- Take appropriate and reasonable steps to ensure that the software does not create any security vulnerabilities for the users. If vulnerabilities are later discovered, take immediate and appropriate steps to protect users from possible threat (such as notifying security companies) and the users.

Social Networking Sites

Significant concerns have been raised by regulators about privacy and consumer protection in the context of social networking websites. While the Children's Online Privacy Protection Act **of 2000 (COPPA)** restricts the ability of commercial website operators in the United States to collect personal information of children under thirteen years of age,[126] teens have passionately embraced social networking and have shown little discretion in the posting of personal information. As a result of high-

profile cases of pedophiles accessing teen profiles, contacting the teens and abusing them, the state attorneys general began investigating the major social networking website operators. Similar attention is apparently being given to these sites by other data protection authorities, such as the French CNIL.

THE FACEBOOK CASE (OCTOBER 2007)[127]

Respondent: Facebook Inc., dba as Facebook.com

Regulator: New York Attorney General

Basis for Complaint: Violation of NY General Business Law – deceptive trade practices

Facts and Allegations: Facebook is a social networking website that allows individuals (including teenagers) to create a free profile, post personal information and pictures, and link to friends' profiles.

The NY AG alleged that Facebook made misrepresentations about its website by claiming that children on Facebook were safer from sexual predators than at most sites, and by claiming that it promptly responds to safety concerns. Facebook had also represented itself as a "trusted environment for people to interact safely" and a website invested heavily in "building safety controls."

The AG alleged that Facebook's security controls had serious deficiencies. In particular, the AG alleged that investigators, "posing as young teenagers, set up profiles on Facebook, received online sexual advances from adults within days, and found widespread pornographic and obscene content." Additionally, the AG alleged that "Facebook often failed to respond, and at other times was slow to respond to complaints lodged by the investigators - posing as parents of underage users - asking the site to take action against predators that had harassed their children."

Outcome: Facebook voluntarily entered into an Assurance of Discontinuance Agreement with the AG to settle the claims. This agreement requires Facebook to:

(1) Disclose newly implemented safety procedures on its website as specified by the agreement;

(2) Accept complaints about nudity or pornography, harassment or unwelcome contact confidentially or via an independent email to abuse@facebook.com;

(3) Respond to and begin addressing complaints about nudity or pornography, harassment or unwelcome contact within 24 hours;

(4) Retain an Independent Safety and Security Examiner (ISSE) approved by the AG for 2 years;

(5) Allow Facebook's complaint review process to be examined by the ISSE;

(6) Provide users and non-users (such as the parents and guardians of users) with easy online access to the ISSE; and

(7) Submit to the AG reports prepared by the ISSE evaluating Facebook's performance in responding to complaints.

Fine Imposed: None

THE MYSPACE CASE (JANUARY 2008)[128]

Respondent: MySpace

Regulators: 49 State Attorneys General (all states except Texas) and the AG of the District of Colombia. The multi-state group was led by North Carolina Attorney General Roy Cooper and Connecticut Attorney General Richard Blumenthal, co-chairmen of the Executive Committee consisting of Connecticut, North Carolina, Georgia, Idaho, Massachusetts, Mississippi, New Hampshire, Ohio, Pennsylvania, Virginia and the District of Columbia.

Basis for Complaint: The settlement culminated a 2 year investigation by the AGs into the use of MySpace by children and the risks presented to children by the social networking environment.

Facts and Allegations: The AGs alleged that MySpace did not have appropriate controls to verify and authenticate participants in the social networking website. They further alleged that MySpace did not taken sufficient steps to protect children from inappropriate content and adult predators on the site.

Outcome: The AGs and MySpace published a Joint Statement on Key Principles of Social Networking Sites. [129]

The AGs and MySpace reached a voluntary agreement containing the following provisions:

(1) MySpace will make web site design and functionality changes to better protect children from adult contact and content. For example, MySpace agreed to change profile settings for users under age 18, so that profiles of 14 and 15-year olds were automatically private and the profiles of 16 and 17-years were private by default.

(2) MySpace will create and lead an Internet Safety Technical Task Force, with support from the AGs, to develop age and identity verification tools for social networking sites. This Task Force will collaborate with other social networking site operators, identify verification experts, child protection groups and technology companies.

(3) MySpace will hire a contractor to create a registry of email addresses associated with children whose parents want to restrict their access to the site. MySpace will prohibit individuals using these registered email addresses from creating a profile.

(4) MySpace agreed to:
- Strengthen software identifying underage users;
- Retain a contractor to better identify and expunge inappropriate images;
- Obtain and constantly update a list of pornographic web sites and regularly sever any links between them and MySpace;
- Implement changes making it harder for adults to contact children;
- Dedicate meaningful resources to educating children and parents about on-line safety;
- Provide a way to report abuse on every page that contains content, consider adopting a common mechanism to report abuse and respond quickly to abuse reports; and
- Create a closed "high school" section for users under 18.

(5) MySpace also agreed to work to increase its educational efforts, by providing information and tools for parents, educators and children about Internet safety. It agreed to support AG efforts to improve law enforcement ability to investigate and prosecute Internet crimes.

Fine Imposed: None