1 OKLA. J. L. & TECH. 12 (2004)
www.okjolt.org

Abstract

Jessica Herndon is currently pursuing a J.D. at the University of Pittsburgh School of Law. Below, Ms. Herndon sheds critical light on how Internet software is used to cyberstalk children; an issue that has not been adequately addressed by the federal government. If this type of activity were officially deemed as targeting children, Congress may be able to use the Children's Online Privacy Protection Act ("COPPA") to regulate Peer-to-Peer ("P2P") programs, such as KaZaA.

Part I of this note discusses the recent trend of downloading freeware and how this freeware raises serious concerns for the privacy of Internet users, especially when these users are children. Part II provides an overview of P2P technology, including how P2P technology works, as well as an overview of the more popular programs on the Internet. Part III explores different laws designed to protect online privacy, including COPPA which specifically addresses the privacy of children online. Part IV then exposes how P2Ps are used to cyberstalk minors, especially through the use of spyware technology. Parts V and VI, respectively, propose solutions to the problems of spyware and cyberstalking. In addition to the discussion concerning COPPA, Parts V and VI discuss new bills that, if passed by Congress, could help to remedy this serious problem.

WHO'S WATCHING THE KIDS?—THE USE OF PEER-TO-PEER PROGRAMS TO CYBERSTALK CHILDREN

Jessica Herndon

I. Introduction

The widespread use of Peer-to-Peer programs ("P2Ps") continues to rise.[1] The increase in popularity of P2Ps among Internet users is attributed to the ability to download free software, or "freeware." Freeware provides users with the ability to share music, movie, and book files that would otherwise cost money to obtain from a retailer. This software is so appealing to children that they are often fooled into giving out personal family information in order to obtain free movies or music.

[1] Press Release, Nielson//NetRatings, Napster Keeps Top Spot, But Other File-Sharing Sites Gain Momentum, *at* http://www.nielsen-netratings.com/pr/pr_010723.pdf (July 23, 2001) (Nielson//NetRatings is a group that measures and researches Internet activity).

Freeware sites have grown 315%, totaling more than 4300 sites since 2001.[2] This is due in part to the free games, music, movies, and books these sites make available to users. For example, KaZaA is the most popular P2P site allowing users to download free music.[3] However, downloading KaZaA software onto a computer, though free and simple, comes at a very high price. Once freeware is downloaded, such as a game or music file, it not only installs the game or song onto the hard drive, but also installs "hidden software" that "can track your surfing habits, use your Net connection to report back to a home base and deliver targeted ads to you. It also can collect your personal information and store it in databases."[4] The targeted ads feature of freeware provides companies, such as KaZaA, with the means to operate profitably by sending users tailored advertisements, enticing them to purchase whatever the targeted pop-up is advertising.[5]

Privacy advocates have criticized P2Ps for using certain technologies to track and collect data on Internet users.[6] These critics take issue with the class of people targeted. For instance, according to Larry Poneman, CEO of Privacy Council, which helps companies manage privacy issues in the course of Internet business and online transactions, "A lot of the people most likely to use this software are teenagers or college students. There's a lack of sensitivity about privacy in that age group."[7] The truth of this statement is evidenced by the reality that the Internet has

---

[2] Janet Kornblum, *Spyware Watches Where You Surf*, USA TODAY, Mar. 10, 2002, *available at* http://www.usatoday.com/life/cyber/tech/2002/03/11/stealthware.htm.
[3] *See* KaZaA, *at* http://www.kazaa.com/us/index.htm (last visited Jan. 5, 2004).
[4] Kornblum, *supra* note 2.
[5] *Id.*
[6] John Borland, *P2P Network Hidden in Kazaa Downloads*, ZDNET NEWS, Apr. 2, 2002, *at* http://zdnet.com.com/2100-1105-873416.html (last visited Jan. 5, 2004).
[7] *Id.*

become the primary communication tool among teenagers.[8] The most popular activities among teenagers include e-mailing, instant messaging, and downloading digital files.[9]

Since so many children were using the Internet and P2Ps, the Federal Trade Commission ("FTC") conducted a survey in April of 2001 to pinpoint exactly how many Internet sites targeted children. This survey analyzed how 144 sites specifically targeting children complied with the Children's Online Privacy Protection Act ("COPPA");[10] COPPA "protects children from operators of websites or online services from deceptive acts in connection with the collection and use of personal data from and about children on the Internet."[11] The FTC concluded that around ninety percent of the sites "provided a privacy policy and declared in that privacy policy whether the site collected personal information, how that personal information was used, and whether the site provided that information to third parties."[12] The survey, however, also indicated that other COPPA provisions protecting children's privacy, such as certain disclosures required in the privacy policy and compliance with the COPPA-specific notice and consent measures, had not been followed consistently.[13]

As stated above, P2Ps use privacy infringing technology to track Internet users, including children. Tracking Internet users' activities without their knowledge amounts to cyberstalking, much like a perpetrator stalks a victim. However, the difference between a real stalker and this

---

[8] Michael Pastore, *Internet Key to Communication Among Youth*, CYBERATLAS, Jan. 25, 2002, *at* http://cyberatlas.internet.com/big_picture/demographics/article/0,,5901_961881,00.html (last visited Jan. 5, 2004).
[9] *Id.*
[10] FED. TRADE COMM'N, STAFF REPORT ON PROTECTING CHILDREN'S PRIVACY UNDER COPPA: A SURVEY ON COMPLIANCE 1 (2002), Apr. 2002, *available at* http://www.ftc.gov/os/2002/04/coppasurvey.pdf [hereinafter SURVEY ON COMPLIANCE].
[11] Michael Yang, *What's Yours Is Mine: Protection and Security in a Digital World*, MD. B.J., Nov./Dec. 2003, at 24, 28. *See* 15 U.S.C § 6502 (2000). "Congress enacted COPAA in 1998 to limit the collection of personally identifiable information from youngsters without their parents' consent." SURVEY ON COMPLIANCE, *supra* note 10, at i.
[12] SURVEY ON COMPLIANCE, *supra* note 10, at 15.
[13] *Id.*

type of electronic stalker is that the latter studies its victims' movements for commercial purposes in order to send user-specific ads to them, learning their personal information in the process. To prevent this abuse of the Internet, Congress should pass new legislation specifically aimed at privacy protection on the Internet in connection with cyberstalking and spyware usage. Over the past three years, various bills have been proposed in Congress that indirectly address cyberstalking and the use of spyware, but no bills have been passed. Recently, legislators proposed several bills directly addressing these issues, proving that Congress realizes privacy dangers exist and is finally attempting to address these issues. In addition to promulgating new legislation, COPPA must be utilized to carry out enforcement rules against those P2Ps that fail to implement proper safeguards when collecting information from children.

II. Background of Peer-to-Peer Programs

The P2P revolution began with Napster. Napster, a P2P file sharing business, allowed users to trade and share free music files over the Internet.[14] Napster gave its members access to freeware called MusicShare, which allowed members to connect to Napster's servers.[15] Once connected, MusicShare scanned MP3 files, highly compressed digital audio files used for the storage and distribution of digital music,[16] on the computers connected to the Napster site and added those file names to the directory of available titles on Napster's server index.[17] When a user sent a song request to the Napster server, the server searched the hard drives of other users who were online to find the request or selection.[18] If the server found the selection, Napster then

---

[14] Joseph A. Sifferd, *The Peer-to-Peer Revolution: A Post-Napster Analysis of the Rapidly Developing File-Sharing Technology*, 4 VAND. J. ENT. L. & PRAC. 92, 93 (2002).
[15] *Id.*
[16] *MP3 Definition*, MP3 PALACE, *at* http://www.mp3haven.com/mp3palace/m3.htm (last visited Jan. 5, 2004); *Definitions*, TECH TARGET, *at* http://whatis.techtarget.com/definition/0,,sid9_gci212600,00.html (last visited Jan. 5, 2003) (MP3 stands for MPEG-1 Audio Layer-3).
[17] *Id.*
[18] Sifferd, *supra* note 14, at 93.

linked the searching computer with the computer that was holding the file (i.e., the host) so that the file could be downloaded directly from the host's personal computer to the requesting user's computer.[19] However, this process ended when the Ninth Circuit found that Napster violated copyright laws and terminated its file sharing service.[20]

Today, there are approximately 176 brands of file-sharing software.[21] KaZaA, the most popular P2P, had been downloaded 143 million times as of November 2002, and allows the sharing of music, movies, software, books, and images.[22] KaZaA allows individuals to directly connect to other individuals without the need for a central server in order to search for and download files.[23] KaZaA had over 8.4 million visitors to its website during August, 2002, a 148% increase in traffic since the beginning of that year.[24]

KaZaA, powered by the Fast-Track network, produces quick search results and downloads by simultaneously pulling pieces of a file from several sources in order to speed up the transfer.[25] Additionally, KaZaA allows users to search the Internet, create shared playlists, and rate files according to quality and completeness.[26] KaZaA did integrate anti-virus protection, which scans shared folders for viruses,[27] but viruses still spread using the P2P. Furthermore, KaZaA has a password protected content filter limiting the files that minors can

---

[19] *Id.*
[20] A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001); Sifferd, *supra* note 14, at 94.
[21] Sifferd, *supra* note 14, at 104.
[22] *Id.*
[23] Joris Evers, *KaZaA Temporarily Stops File Swapping*, CNN.COM, Jan. 18, 2002, *at* http://www.cnn.com/2002/TECH/internet/01/18/kazaa.halt.idg/ (last visited Jan. 5, 2004).
[24] Nielsen//NetRatings, *Internet Users Flock to Music Websites*, *cited in* NUA INTERNET SURVEYS, Oct. 11, 2002, *at* http://www.nua.ie/surveys/index.cgi?f=VS&art_id=905358441&rel=true.
[25] Sifferd, *supra* note 14, at 106.
[26] *Products*, KaZaA Media Desktop Website, *at* http://www.kazaa.com/us/products/index.htm (last visited Jan. 5, 2004).
[27] *Id.*

download.[28] However, not all content filters are 100% reliable because content that the filter fails to recognize as "obscene" or improper can slip through and reach the child.

III. Statutes Protecting the Privacy of Child Internet Users

Congress has enacted several statutes attempting to protect peoples' privacy interests during Internet use, including the privacy interests of children. The first statute, the Electronic Communications Privacy Act of 1986 ("ECPA"), or the Wiretap Act, prohibits the intentional interception, use, or disclosure of any wire, oral, or electronic communication.[29] Under this Act, it is lawful for a person to intercept these types of communications if that person is a party to the communication or if one of the parties to the communication has previously consented to the interception, unless the communication is intercepted for the purpose of committing a tort or crime.[30] Punishments for violating this Act include fines or imprisonment of up to five years.[31]

The Stored Information Act, also under the ECPA, prohibits people from intentionally accessing, without authorization, "a facility through which an electronic information service is provided."[32] It also prohibits people from intentionally exceeding authorization to that facility and obtaining, altering, or preventing access to an electronic communication while it is in electronic storage.[33] This Act does not apply to conduct that is authorized "by the person or entity providing an electronic communications service," nor does it apply to "a user of that service with respect to a communication of or intended for that user."[34] The statute aims to prevent hackers from obtaining, altering, or destroying certain stored electronic

---

[28] *The Guide*, KaZaA Media Desktop Website, *at* http://www.kazaa.com/us/help/guide_searching.htm (last visited Jan. 5, 2004).
[29] 18 U.S.C. § 2511(1) (2000).
[30] *Id.*
[31] *Id.* § 2511(4).
[32] *Id.* § 2701(a).
[33] *Id.*
[34] *Id.* § 2701(c).

communications.[35] However, accessing electronically stored data is the primary action which constitutes a serious violation of this statute.[36] Punishments for violating the Act include fines or imprisonment for one to ten years, depending on the severity of the violation.[37]

The most significant statute protecting children's online privacy interests is the Children's Online Privacy Act ("COPPA").[38] COPPA requires that sites post a complete privacy policy, directly notify parents of the site's information collection practices, and obtain verifiable parental consent before the site collects children's information or shares this information with third parties.[39] The Federal Trade Commission ("FTC") enforces COPPA[40] and applies it to operators of commercial websites and online services[41] directed at children under the age of thirteen.[42] COPPA also applies to any general website that intentionally collects personal information from a child.[43]

More specifically, COPPA targets websites that collect individually identifiable information about children including their full names, addresses, e-mail addresses, or phone numbers.[44] It also covers other types of individually identifiable information, such as hobbies, interests, and information gathered through cookies[45] or other types of tracking devices.[46] A cookie is information a website places on a visiting user's hard drive so that the site can

---

[35] *In re* Pharmatrak, Inc. Privacy Litig., 220 F. Supp. 2d 4 (D. Mass. 2002).
[36] *In re* Intuit Privacy Litig., 138 F. Supp. 2d 1272, 1276 (C.D. Cal. 2001).
[37] 18 U.S.C. § 2701(b) (2000).
[38] *See* 15 U.S.C. § 6502 (2000).
[39] *Id.* § 6502(b).
[40] *Id.* § 6505(a).
[41] *Id.* § 6502(a)(1).
[42] *Id.* § 6501(1).
[43] *Id.* § 6502(a)(1).
[44] FED. TRADE COMM'N, HOW TO COMPLY WITH THE CHILDREN'S ONLINE PRIVACY PROTECTION RULE, Nov. 1999, *available at* http://www.ftc.gov/bcp/conline/pubs/buspubs/coppa.htm [hereinafter FED. TRADE COMM'N].
[45] *Cookies*, SearchSecurity.com, *at* http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci211838,00.html (last modified Dec. 12, 2003).
[46] FED. TRADE COMM'N, *supra* note 44.

remember something about the user at a later time. Typically, it records a user's preferences when visiting a particular site.[47]

In order to comply with COPPA, the operator must post a link to a notice explaining its information obtaining practices on the home page of its site and at each area where it collects personal information from children.[48] The notice must be clear and understandable.[49] It must also state the contact information of the operators, the kinds of information collected from children, how it is collected, how it will be used, and whether the operator discloses this information to third parties.[50]

Under COPPA, the operator must notify a parent that it wants to collect personal information from the child, obtain the parent's consent to collect this information, inform the parent of how this information will be used or disclosed, and inform the parent how he or she can give consent.[51] Under a sliding scale approach to parental consent, the acceptible method of obtaining consent will vary based on how the operator intends to use the personal information.[52] For example, use of the information for the user's internal purposes requires a less rigorous method of obtaining parental consent.[53] Under the less rigorous method, "[o]perators may use *email* to get parental consent for all internal uses of personal information, such as marketing to a child based on" that child's preferences.[54] On the other hand, if the information is disclosed to

---

[47] *Cookies*, SearchSecurity.com, *at* http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci211838,00.html (last modified Dec. 12, 2003).
[48] FED. TRADE COMM'N, *supra* note 44.
[49] *Id.*
[50] *Id.*
[51] *Id.*
[52] *Id.*
[53] *Id.*
[54] *Id.*

third parties, a more reliable method of consent is required, such as obtaining a signed release form from the parent or obtaining the parent's consent over the phone.[55]

The FTC has the power to enforce and punish COPPA violators.[56] It does so by imposing civil penalties and enforcing injunctions against such violators.[57] For example, American Popcorn Company paid $10,000 in civil penalties to settle with the FTC on charges that the company violated COPPA[58] by collecting personal information from children using its website without first obtaining parental consent.[59] The settlement barred American Popcorn Company "from future violations of the COPPA Rule and from misrepresenting its policies about collecting, disclosing, or using children's personal information."[60]

A recent case involved the National Research Center for College and University Admissions ("Research Center") and its practice of obtaining survey information from children.[61] In that case, students provided information to the Research Center and other companies upon the belief that only colleges and universities would use the information.[62] However, the companies sold the students' data to direct marketers and other commercial entities.[63] The consent agreements between the FTC and the Research Center barred any disclosure of information "previously collected for any non-educational related marketing purpose."[64] The agreements also barred further "misrepresentations about how personally

---

[55] *Id.*
[56] 15 U.S.C. § 6505(a) (2000).
[57] FED. TRADE COMM'N, *supra* note 44.
[58] Press Release, Fed. Trade Comm'n, Popcorn Company Settles FTC Privacy Violation Charges (Feb. 14, 2002) *available at* http://www.ftc.gov/opa/2002/02/popcorn.htm.
[59] *Id.*
[60] *Id.*
[61] Press Release, Fed. Trade Comm'n, High School Student Survey Companies Settle FTC Charges (Oct. 2, 2002) *available at* http://www.ftc.gov/opa/2002/10/student1r.htm.
[62] *Id.*
[63] *Id.*
[64] *Id.*

identifiable information is collected or will be used or disclosed."[65] Furthermore, "the agreements contain[ed] record-keeping provisions allowing the FTC to monitor compliance with the order."[66] These are just a few examples of how the FTC enforces COPPA.

COPPA does include a provision allowing industry groups to submit self-regulatory guidelines to the FTC.[67] If the FTC approves the guidelines, compliance provides a safe harbor from COPPA enforcement.[68] The Children's Advertising Review Unit ("CARU") of the Council of Better Business Bureaus, ESRB Privacy Online (a division of the Entertainment Software Rating Board), and TRUSTe have all been approved under the FTC safe harbor program.[69]

Through COPPA, the government has attempted some regulation in order to protect children's online privacy, but the FTC has also asserted authority by challenging Internet practices that may be deceptive and unfair. The FTC has authority under section 5 of COPPA to examine information practices that may be deceptive or misleading.[70] The FTC views a practice as deceptive if it misleads consumers and affects consumers' behavior about a product or service.[71] Unfair practices occur when a substantial injury is caused by a P2P, the injury is not outweighed by any benefits, and the injury is not reasonably avoidable.[72] For example, an injury occurs when a site collects personal information from a child and discloses that information to third parties without giving parents adequate notice and a chance to limit the use of that information.[73] The four necessary elements of protecting consumer privacy include giving

---

[65] *Id.*
[66] *Id.*
[67] 15 U.S.C. § 6503(a)-(b) (2000).
[68] *Id.*
[69] FED. TRADE COMM'N, SAFE HARBOR PROGRAM, *available at* http://www.ftc.gov/privacy/safeharbor/shp.htm (last modified Apr. 17, 2003).
[70] FED. TRADE COMM'N, *supra* note 44.
[71] *Id.*
[72] *Id.*
[73] *Id.*

consumers notice "about how personal information collected online is used," giving consumers choices "about whether and how their personal information is used," granting security of personal information, and giving consumers access "to their own personal information to ensure accuracy."[74] The FTC has "declared that consumers should have an effective mechanism to enforce these fair information principals" and in many cases, "the FTC has brought enforcement actions against Web site operators based on suspect data collection practices."[75]

Finally, state attorney generals may bring civil actions if they believe that residents of their state have been threatened or affected by a person violating COPPA.[76] The states may enjoin the practices, enforce compliance with the regulations, obtain damages and restitution on behalf of state residents, or obtain other relief the court considers appropriate.[77] Thus, a state may exercise its police powers to protect the interests of its minor citizens. Furthermore, deferring this power to the local state level, in addition to the FTC policing this matter, ensures that violators are not overlooked.

IV. Cyberstalking Children Through The Use of P2Ps

Cyberstalking, a fairly new occurrence, consists of persistent and threatening behavior or unwanted advances directed at another using the Internet or other electronic communications.[78] Now that the use of computers and online services has become commonplace, more people use the Internet, making online communicators vulnerable to abuse by stalkers. Cyberstalkers target their victims through e-mail, chat rooms, discussion forums, and message boards.[79] It also includes the sending of threatening or obscene e-mails and viruses, online verbal abuse,

---

[74] Nicole A. Wong, *Online Content Liability Issues*, 711 PLI/PAT 813, 846 (2002).
[75] *Id.*
[76] 15 U.S.C. § 6504(a) (2000).
[77] *Id.*
[78] Trudy M. Gregorie, *Cyberstalking: Dangers on the Information Superhighway*, Nat'l Ctr. for Victims of Crime Website, *available at* http://www.ncvc.org/src/help/cyberstalking.html#N_1_ (last visited Jan. 5, 2004).
[79] *Id.*

harassment in live chat rooms or bulletins,[80] and electronic identity theft. Cyberstalkers can be very dangerous when they take their behaviors offline.[81] Some cyberstalking situations do become offline stalking realities. As a result, victims may experience abusive phone calls, vandalism, threatening mail, trespassing, and physical assault.[82]

As of December 2002, an estimated seventy-two percent of Americans had used the Internet sometime in the previous month.[83] Out of "an estimated 24 million children now online, one out of five [had] been solicited for sex" in 1999.[84] Also, the Internet provides a forum for pedophiles to meet children via the Internet, establish relationships, and eventually make person-to-person contact with children in order to engage in criminal sexual activities.[85] Pedophiles commonly contact children through e-mail, instant messaging, and chat rooms.[86]

The number of children using P2P technologies exacerbates the problems associated with cyberstalking. For example, P2Ps can be used to target children for cyberstalking activities by sending obscene pictures to them via file sharing. File sharing through P2Ps allows users to exchange their files with other P2P users, and has become very popular among teenagers. For example, twenty-three percent of teenagers have traded music via a file sharing application, such as KaZaA.[87] Since, P2P services allow the distribution and sharing of pornography files and

---

[80] *Id.*
[81] *Cyberstalking and Online Harassment*, CyberAngels, *at* http://www.cyberangels.com/stalking/index.html (last visited Jan. 5, 2004).
[82] Gregorie, *supra* note 78.
[83] Ipsos-Reid, *Internet Use Climbing in Most Markets*, *cited in* NUA INTERNET SURVEYS, *at* http://www.nua.ie/surveys/index.cgi?f=VS&art_id=905358657&rel=true (Dec. 11, 2002).
[84] Congressional Study, Jun. 8, 2000, *cited in* Agent Spy: Realtime PC Surveillance, *at* http://www.agent-spy.com/statistics.htm (last visited Jan. 5, 2004).
[85] Donna Rice Hughes, *Sexual Predators Online*, ProtectKids.com, *at* http://www.protectkids.com/dangers/onlinepred.htm (2001).
[86] *Id.*
[87] Robyn Greenspan, *Users Do More Than Surf*, CYBERATLAS, *at* http://cyberatlas.internet.com/big_picture/applications/article/0,,1301_1562221,00.html (Dec. 31, 2002).

violent materials,[88] this practice could lead to unintentional downloading of such material by minors. For example, an innocent search for a particular file may turn up obscene material that is saved under a harmless name.[89]

Perhaps the most alarming problem with P2Ps is that unauthorized access to computer files is possible and can easily provide a potential pedophile with everything that person needs to know in order to track down a child, or at least make online contact with that child.[90] This problem is aggravated by the fact that not all operating systems and software applications are secure enough to prevent users from gaining access to someone's entire computer.[91] This activity and the file sharing of pornography with minors are properly labeled cyberstalking because they are considered harassing or harmful behaviors, particularly if the user labels obscene material using a harmless name for the purpose of offending an unsuspecting user.

Another major problem occurring with P2Ps is the use of spyware. Spyware is "[s]oftware that tracks a user's Web behavior or personal information without the user's knowledge and shares this data with third parties, such as advertisers."[92] Often, spyware installation occurs without the computer user realizing it;[93] in other words, this type of software collects a user's Web data without consent. The term spyware is also applied to "information gathering software that installs itself as part of another program" (also referred to as "adware").[94]

---

[88] *File Sharing*, Be Safe Online, *at* http://www.besafeonline.org/English/file_sharing.htm (2002).
[89] *Id.*
[90] *Id.*
[91] *Id.*
[92] Robertson Barrett, *Glossary of Spyware and Technology Terms*, CONSUMER WEBWATCH, *at* http://www.consumerwebwatch.org/news/articles/spyware_glossary.htm#spyware (Oct. 21, 2002).
[93] Thomas R. Temin, *Utility Cleans Your System of Spyware; LavaSoft's Ad-Aware 5.83 Desktop Utility; Evaluation*, 21 GOV'T COMPUTER NEWS 47 (2002), *available at* LEXIS, Legal News Publications.
[94] Barret, *supra* note 92.

Recently, "spyware has proliferated in vast new advertising networks."[95] Individually targeted adware arose when freeware producers began accepting advertising to make money on the distribution of their free software.[96] In order to ensure that these advertisements reach users who download the freeware, freeware producers "began to bundle advertising within their wares."[97] Adware occasionally includes a code that tracks users' Internet activity and reports this information to third parties so that these third parties can aim certain advertisements at the users.[98] Essentially, this constitutes a form of spyware because these users are completely unaware that their movements are being tracked.[99] The P2Ps bundle this spyware with freeware, often stating so in their "boilerplate" policy.[100] Some "privacy experts say millions of eager teens and…adult Internet users download the programs just to locate a game or MP3 music file, miss the terse disclosures and…are surprised when they receive a stream of advertisements."[101] Spyware has been around for years, but this form of spyware, secretly "piggybacking" on freeware, poses great risks for Internet users and their privacy interests.

The rise of spyware causes various problems.[102] For instance, it degrades the performance of a user's computer. The applications use Random Access Memory ("RAM") and their accumulation slows down a user's system.[103] Many of these P2P, with bundled spyware,

---

[95] Robertson Barrett, *Spyware Everywhere: Free Software Is the Lure, Online Surveillance Is the Reality*, CONSUMER WEBWATCH, *at* http://www.consumerwebwatch.org/news/articles/spyware.htm (Oct. 21, 2002).
[96] Mike Tuck, *Adware and Under-Wear – The Definitive Guide*, SITEPOINT, *at* http://www.ecommercebase.com/article.php?aid=888&pid=0 (Sept. 30, 2002).
[97] *Id*.
[98] *Adware*, SearchWebServices.com, Apr. 14, 2001, *at* http://searchwebservices.techtarget.com/sDefinition/0,,sid26_gci521293,00.html (last visited Jan. 5, 2004).
[99] *Id.*
[100] Barrett, *supra* note 92.
[101] *Id*.
[102] Evan Hansen et al., *Your PC's Enemy Within*, CNET NEWS, *at* http://news.com.com/2009-1023-937457.html?tag=dl (June 26, 2002).
[103] Temin, *supra* note 93.

"downloads caused system crashes, driver overwrites, and other significant PC problems."[104] Furthermore, spyware "bombards you with marketing pitches."[105] These insistent pop-up advertisements are very annoying and distracting. Worst of all, some of these advertisements disable the user's back button and close box or replicates windows faster than the user can close them.[106] Another significant problem involves tracking Internet users and gaining access to a user's personal information. These programs can also "tie up network bandwidth" and potentially "compromise security."[107] Finally, once installed, spyware can be difficult to uninstall.[108] Even if the P2P is successfully uninstalled, the bundled spyware may still exist on the computer.[109] Therefore, users and family members who use the computer are essentially "broadcasting their online behavior or personal information to unfamiliar third parties and thus become long-term targets of constant, focused promotions."[110] Also, since spyware runs the entire time the user is online, hackers may be able to get into a user's computer through this "back door."[111]

V. Solutions to Problems Concerning Spyware

The Wiretap Act does not aid opponents of spyware programs because courts are reluctant to find that a tort or crime has been committed in violation of the Act.[112] Therefore, online privacy protection statutes must be passed or formed to create a cause of action. Plaintiffs may have a claim under the Stored Communications Act, although courts disagree on whether a

[104] Tom Mainelli, *Are You Flirting With Disasterware?*, CNN.COM, *at* http://www.cnn.com/2002/TECH/ptech/05/16/disaster.ware.idg/index.html (May 16, 2002).
[105] *Id*.
[106] Gregg Keizer, *It's An Ad, Ad, Ad, Ad World*, PCWORLD, May 2002, *available at* http://www.pcworld.com/resource/printable/article/0,aid,86929,00.asp (last visited Jan. 5, 2004).
[107] Mainelli, *supra* note 104.
[108] *Id*.
[109] Barrett, *supra* note 92.
[110] *Id*.
[111] *Id*.
[112] *See In re* Pharmatrak, Inc., 220 F. Supp. 2d 4, 12 (D. Mass. 2002); *In re* Intuit, 138 F. Supp. 2d at 1272, 1277-79 (C.D. Cal. 2001).

claim exists.[113] Some courts argue that any access to electronically stored data amounts to a violation of the Act,[114] while others hold that computers are not facilities providing electronic communication services under the Act. Instead, these courts find that computers are just means of providing consumers with access to the Internet.[115]

COPPA could be used as an aid in eliminating and preventing the invasion of privacy from spyware. Operators of general audience websites with knowledge that they collect personal information from children under the age of thirteen must comply with COPPA.[116] In order to establish a COPPA violation, three elements must be proven by the FTC. First, the site is targeted at children under the age of thirteen years old. Many minors use KaZaA and other P2P software. Since file sharing sites attract large numbers of teenagers,[117] KaZaA and other P2P software programs should fall squarely within COPPA. For example, "[m]ore than a third of the visitors to…[KaZaA]…are Gen[eration] Y surfers . . . while that group normally comprises only 12.6 percent of the active Web audience."[118] Therefore, it would be difficult for these P2Ps to deny having the knowledge that information is being collected from minors. However, mere knowledge that information is being collected from minors may not necessarily amount to an act of "targeting" minors.

The second element of COPPA deals with the collection of children's personal information. Companies collect children's personal information from the computers these children use by utilizing tracking software and cookies, which the P2Ps knowingly place on computers with the downloaded freeware. The operator's knowledge must exist in order for a

---

[113] *See In re* Pharmatrak, 220 F. Supp. 2d at 13; *In re Intuit*, 138 F. Supp. 2d at 1277.
[114] *See In re* Pharmatrak, 220 F. Supp. 2d at 13.
[115] *See In re* Intuit, 138 F. Supp. 2d at 1276.
[116] FED. TRADE COMM'N, *supra* note 44.
[117] Nielson//NetRatings, *supra* note 1.
[118] *Id.*

COPPA violation to occur. However, with statistics showing the amount of children using P2P software, KaZaA and other P2Ps most certainly possess some knowledge that children use their software.

Finally, the FTC must prove that the websites offering P2P software are operators. In deciding who is an operator, "the FTC will consider who owns and controls the information; who pays for the collection and maintenance of the information; what the pre-existing contractual relationships are in connection with the information; and what role the Web site plays in collecting or maintaining the information."[119] Although the P2P software, not the website, bundles in spyware programs, children must utilize the website to gain access to the P2P software. Additionally, every time a user opens a freeware program, it takes the user to the P2P website, which shows a strong connection between the software and the website. One could argue that marketers creating spyware control and pay for the collection of information, since these marketers pay P2P websites to bundle spyware programs with freeware. However, this argument is unlikely to prevail because P2Ps contract with the companies wanting spyware bundled with freeware. Thus, P2P website operators play a major role in allowing the collection and distribution of personal information. For these reasons, the FTC can easily find P2P websites to be found in violation of COPPA. Therefore, it is possible that the people in control of websites with bundled spyware could be considered operators of general audience websites with knowledge that they collect personal information from children.

If the FTC finds a site to be in violation of COPPA, it will bring enforcement actions and impose civil penalties against the P2P.[120] In order to comply with COPPA, a site must post a privacy policy on its homepage, provide notice to parents about the site's collection of

[119] FED. TRADE COMM'N, *supra* note 44.
[120] *Id.*

information, obtain parental consent before collecting this information, and provide parents with the right to refuse the disclosure of that information to third parties.[121] Although tracking software is automatically installed on computers by downloading the software, and not necessarily through viewing the website, these COPPA requirements may still apply. For example, the notice requirement would apply by requiring the P2P to boldly position an explanation of the P2P's methods of obtaining information on its site. The notice could also be placed in the user agreement that the user must read before installation of the software. Therefore, people who download and install the software would know exactly what programs they are downloading, how these programs will affect the user's computer, and how these programs use and obtain personal information. In addition, these P2Ps could verify that the people downloading their software are over thirteen years old by getting parents' verifiable consent before installation takes place. If a parent agrees to allow P2P software on the computer, then the parent also agrees to allow tracking spyware to be installed as well.

COPPA can also be used to notify parents of the software on their computers and the functions of these programs. It could promote more parental control over the use of their children's private information online. Though COPPA may help protect the privacy of children under the age of thirteen, it does not eliminate all privacy problems. Many bills have been proposed by Congress to protect peoples' privacy while on the Internet. The FTC can pursue companies violating their own privacy policies, but "it's powerless to do anything about

[121] FED. TRADE COMM'N, DRAFTING A COPPA-COMPLIANT PRIVACY POLICY, *available at* http://www.ftc.gov/bcp/conline/edcams/coppa/index.html (last visited Jan. 5, 2004).

companies that collect data."[122] Mozelle Thompson, FTC commissioner, stated, "[T]he only way to change things is through 'baseline privacy legislation.'"[123]

An example of baseline privacy legislation is the Online Personal Privacy Act ("OPPA"), which would protect the online privacy of individuals using the Internet.[124] OPPA reflects Congress' finding that "privacy is a personal and fundamental right worthy of protection through appropriate legislation."[125] The findings of Congress also reflect that existing laws and forms of Internet self-regulation "provide minimal privacy protection," despite the fact that most individuals "have a significant interest in their personal information."[126] OPPA addressed how polls consistently reflect individual Internet users' concerns about the "lack of control over their personal information."[127] Market research also finds that "billions of dollars in e-commerce are lost" because people fear the "lack of privacy protection" and tend to "give false information about themselves to protect their privacy."[128] OPPA would impose notice and consent requirements on Internet Service Providers ("ISP"), operators of commercial websites, or online service providers who "collect personally identifiable information."[129] Disclosures of a sensitive nature, such as financial or medical information, require the "user's affirmative consent" before the collection, disclosure, or use of this information occurs.[130] Additionally, "Nonsensitive Personally Identifiable Information…[requires] robust notice to the user, in addition to clear and conspicuous notice."[131] The operator or provider must also give "the user an opportunity to

---

[122] Kornblum, *supra* note 2.
[123] *Id.*
[124] *See* Online Personal Privacy Act, S. 2201, 107th Cong. (2002).
[125] *Id.* § 3(1).
[126] *Id.* §§ 3(2), 3(5)-(6).
[127] *Id.* § 3(11).
[128] *Id.* §§ 3(12), 3(13).
[129] *Id.* § 102(a).
[130] *Id.* § 102(b).
[131] *Id.* § 102(c).

decline consent for such collection" and use of personally identifiable information.[132] Furthermore, OPPA would create both private and public causes of action for violations of the Act.[133]

OPPA proves that Congress is aware of the privacy problems relating to the Internet. Although the Act could eliminate some problems associated with spyware, it probably would not eliminate all of them. For instance, the required notice and consent requirements apply to operators. This could help warn people of the dangers of installing freeware with bundled spyware once downloaded from websites. However, the notice would not prevent spyware from affecting the computer once a person installed the software. Although warnings may help, they will not substantially eliminate the problem. In addition, the sections of OPPA requiring notices on websites that collect sensitive and nonsensitive information could be difficult to enforce in a spyware scenario. This occurs because after installation, the software collects data without the user's knowledge. This particular part of the statute may not be feasible in dealing with spyware, unless software manufacturers create a pop-up warning, which informs users every time personal information will be collected and sent.

Another proposed statute, the Consumer Privacy Protection Act ("CPPA") of 2002, would help consumers to protect personal information. For example, CPPA would require clear and concise privacy notices to consumers if a site planned on using information "unrelated to the transaction."[134] CPPA would also require data collection organizations to establish clear and concise privacy policies with respect to the collection, sale, or use of personal information.[135] It would give consumers the opportunity to limit the "sale or disclosure" of their personal

---

[132] *Id.*
[133] *Id.* §§ 203, 204.
[134] Consumer Privacy Protection Act of 2002, H.R. 4678, 107th Cong. § 101(a)(1) (2002).
[135] *Id.* § 102.

information as well as encourage self-regulatory programs.[136] Finally, the data collection organizations would be required to "implement an information security policy…in order to prevent an unauthorized disclosure or release of such information" to a third party.[137] The CPPA would not provide a private cause of action, but it would be enforceable by the FTC.[138]

Although CPPA does not directly relate to spyware, it could be a solution to some of the spyware problems. CPPA solutions are similar to those of the Online Privacy Protection Act because the P2P software distributors would be required to place privacy notices on their websites and explain the consequences of downloading and installing these programs. CPPA would also require P2P software distributors, such as KaZaA, to allow people to opt out of downloading software which contains spyware in order to give users the ability to limit the collection of personal information.

The Spyware Control and Privacy Protection Act ("SCPPA") dealt with software that is publicly available and possesses a "capability to collect information about the user" and discloses that information to third parties.[139] The Act, introduced to the Senate in 2001, never passed. It would have required that this type of software must not only give clear notice that it has such capability, but it must also describe "the information subject to collection" and give clear electronic "instructions on how to disable such capability without" altering software performance.[140] SCPPA would have solved many spyware problems because it specifically dealt with spyware installed on computers as a result of downloading freeware. This bill would have directly done what the other two bills mentioned above could only do indirectly. It would have

---

[136] *Id.* §§ 103(a)(1), 106.
[137] *Id.* § 105(a)(1).
[138] *Id.* §§ 107, 108.
[139] Spyware Control and Privacy Protection Act, S. 197, 107th Cong. § 2(a)(1) (2001).
[140] *Id.* §§ 2(a)(1)(A), (C).

required software distributors who bundle spyware with their programs to give clear notice about whether the software contains bundled spyware and what exactly the spyware will do once installed on the computer.

Currently, if a user does not want to deal with the problem of having spyware on their computer, the user's only option is to refrain from downloading and installing P2P programs. However, SCPPA would have required instructions on disabling the spyware, while allowing the user to continue his or her use of the P2P software. This important aspect would have given users the choice of allowing the spyware on their computers. Currently, if a user eliminates the spyware from the computer, P2P programs cease functioning properly and the user must reinstall the P2P along with the bundled spyware. Thus, the bill would have eliminated this cycle by allowing the use of P2Ps without the attached and unwanted spyware. The bill would have also demanded full disclosure to users informing them of what they have downloaded. Users' understanding and knowledge of the programs they download and install is a main step in the prevention of privacy invasions. This type of full disclosure can educate users how to become more alert Internet users.

Recently, legislators attempted to confront Internet privacy issues by directly attacking the use of spyware. For example, the Software Principles Yielding Better Levels of Consumer Knowledge Act ("SPYBLOCK") would allow consumers to control the programs they download onto their computers. The Act would make it illegal to secretly install spyware onto computers without notifying computer users.[141] Under this Act, users would be informed of the type of information the software collects and the purpose of collection.[142] If users agree to install the programs onto their computers, the programs must be easily removable and the advertising

[141] Software Principles Yielding Better Levels of Consumer Knowledge Act. S. 2145, 108th Cong. § 2(a) (2004).
[142] *Id.* § 3(a).

software must inform the users about how to turn off the advertising feature.[143] There would be no private cause of action, but the FTC and state attorney generals would enforce the Act.[144] Further, this "proposed legislation follows a similar earlier effort, House Resolution 2929, introduced in July 2003…which is still being debated at the committee level…[The bill] requires explicit user consent before the installation of software and orders enforcement by the FTC."[145] Chris Hoofnagle, the associate director of the Electronic Privacy Information Center, believes that the serious problem of spyware has finally seized Congress' attention and an anti-spyware bill has a good chance of passing this session.[146]

VI. Solutions to Cyberstalking

Spyware, a form of cyberstalking, poses substantial dangers by providing collected information to third parties who may use it to target children. Many local law enforcement departments do not possess the proper training and resources for investigating cyberstalking cases.[147] Although the crime remains an elusive and multi-jurisdictional problem, "no uniform federal law exists to protect victims or to define ISP liabilities."[148] The only existing federal law touching upon this crime "imposes a $1,000 fine or five years imprisonment to anyone transmitting in interstate commerce any threat to kidnap or injure someone."[149] Since no clearly defined cyberstalking crime exists at the federal level, states have drafted their own legislation dealing with the issue.[150] Furthermore, the diversity of state laws offering different definitions,

---

[143] *Id.* § 3(c).
[144] *Id.* §§ 6, 7.
[145] Adrienne Newell, *Anti-Spyware Law Proposed*, PCWORLD, Feb. 26, 2004, *available at* http://www.pcworld.com/news/article/0%2Caid%2C114999%2C00.asp (last visited Apr. 2, 2004).
[146] *Id.*
[147] Harry A. Valetk, *Cyberstalking: Navigating a Maze of Laws*, N.Y. L.J., July 23, 2002, at 5.
[148] *Id.*
[149] 18 U.S.C. § 875(c) (2000).
[150] Valetk, *supra* note 147.

protections, and penalties fails to adequately protect victims of cyberstalking.[151] These different and conflicting statutes create confusion and deter law enforcement from becoming involved.[152] Most state statutes require direct communication with the target, while some require sending a message that the person is likely to receive.[153] In some states, cyberstalking is part of the stalking or harassment laws, while other states have separate cyberstalking statutes.[154] Most states require that threats be against the cyberstalked victim, while some states prohibit threats against anyone.[155] The statutes usually require that the cyberstalker's intent is to harass the victim.[156] As for now, since no federal standard exists, the best sources for cyberstalking guidance are the states that have promulgated legislation on this crime.

Due to the confusion arising from the varying state laws, a uniform federal law must be created to prevent cyberstalking. Since personal information has become readily available to an increasing number of people using the Internet, some state legislators are beginning to see the need to address the crime of cyberstalking, however this problem still persists. Cyberstalking allows users to cross state lines to commit their crimes via the Internet, creating jurisdictional problems. Varying state laws with different definitions, jurisdictions, standards, and punishments create confusion in applying and enforcing these statutes. Again, a uniform federal statute should be enacted to address this rising problem.

The Just Punishment for Cyberstalkers Act, introduced in 2000, never passed. This bill would have amended Title 18 of the United States Code, expanding the prohibition on stalking to

---

[151] *Id.*
[152] *Id.*
[153] *Id.*
[154] Gregorie, *supra* note 78.
[155] Valetk, *supra* note 147.
[156] *Id.*

include cyberstalking.[157] This bill would have prohibited the use of instrumentalities of interstate commerce to participate in the crime of cyberstalking.[158] It would have also made cyberstalking a federal crime and eliminated the many conflicting state statutes. However, like the other proposed bills mentioned, this one did not pass a congressional vote.

Without the aid of congressional policies, people, especially children, must learn of the dangers associated with passively surfing the Internet and must take considerable measures to prevent cyberstalking from happening to them. Safety tips when using the Internet include logging off if an online situation becomes hostile, familiarizing oneself with various ISP policies that expressly prohibit cyberstalking, and contacting law enforcement agencies if a situation places a person in fear.[159] Also, people should not share personal information in online public forums, give strangers personal information, use one's real name or nickname as a screen name or user identification, or give any information about oneself in a user profile.[160] Certain websites, such as the FTC website at www.ftc.gov, offer advice and information on privacy and protecting children from online dangers.

VII. Conclusion

The federal government has proposed several bills addressing cyberstalking and the use of spyware. However, none passed Congress. With the rise in popularity of computer use and Internet use, especially among children, Internet regulation seems even more crucial. Internet activity tends to cross state lines, making federal regulation of cyberstalking even more necessary. Furthermore, a new type of technology called spyware is being used by P2Ps to track Internet users, including children. This invades privacy and may violate COPPA. Spyware,

---

[157] *See* Just Punishment for Cyberstalkers Act of 2000, S. 2991, 106th Cong. (2000).
[158] *Id.* § 2.
[159] Valetk, *supra* note 147.
[160] *Id.*

downloaded with popular P2P freeware programs, currently exists as just another form of unregulated cyberstalking by programmers and websites. Some federal laws have addressed the issues presented in this note, but Congress has failed to enact these laws. Hopefully, Congress will formally address these pressing issues to adequately prevent children's privacy interests from being invaded before more children are abducted or harmed due to a stalker's ability to obtain and locate unsuspecting children.