The Richmond Journal of Law and Technology

Volume VIII, Issue 3,

Spring 2002

Bloom v. Commonwealth: Identifying The Face Behind The Instant Message

by: Jessica Clair Cobaugh[*]

Cite As: Jessica C. Cobaugh, *Bloom v. Commonwealth: Identifying The Face Behind The Instant Message*, 8 RICH. J.L. & TECH. 17 (Spring 2002) *at* http://www.law.richmond.edu/jolt/v8i3/article17.html.

TABLE OF CONTENTS

I. Introduction

{1}"You have an instant message from Naturalbornkiller2000. Would you like to accept it?[1]" A similar message to this one flashes on computers throughout the United States and the world, inviting computer users to "chat" or "IM" with friends, family and perfect strangers alike. While the opportunity to engage in real-time conversation over the Internet provides an interesting and often

less expensive way to keep in touch with friends or to meet new people, instant messages and other Internet communications increasingly appear as a means for adults to interact inappropriately with young children.[2] The use of Internet communication for the solicitation of minors to engage in sexual activity and the availability of child pornography on the Internet has become a dominant theme in the political arena.[3] While some states have promulgated statutes specifically criminalizing the use of computers and the Internet for solicitation of minors to engage in sexual activity and child pornography,[4] other states and the federal government rely on existing laws to prosecute such activities.[5]

{2}A problem in prosecuting these crimes lies in proving the identity of the alleged child predator sending the e-mail or instant message or posting an image or message on an Internet bulletin board.[6] A case demonstrating this problem is *Bloom v. Commonwealth*, in which both the Virginia Court of Appeals and the Supreme Court of Virginia upheld the conviction of Gregory Michael Bloom, arrested after allegedly soliciting a minor for sex via an instant message conversation.[7] Bloom's convictions fell under Virginia Code section 18.2-370(5), entitled "Taking Indecent Liberties With Children," and section 18.2-29, criminalizing the solicitation of another person to participate in a felony.[8]

{3}Section 18.2-370(A)(5) states that "Any person eighteen years of age or over, who, with lascivious intent, shall knowingly and intentionally. . .entice, allure, persuade, or invite any such child [under fourteen] to enter any vehicle, room, house, or other place, for any of the purposes set forth in the preceding subdivisions of this section [shall be guilty of a Class 5 felony]."[9] The "purposes" referred to in the statute include exposing of genitals by either the adult or the child, feeling or fondling the genitals by either party and the performance of an act of sexual intercourse.[10]

{4}Bloom's conviction rested on the trial court's decision to allow the victim to testify about the content of online conversations between herself and Bloom. Those conversations linked Bloom to a specific conversation he had with an undercover police officer posing as the child-victim in which Bloom proposed the two meet to have sex.[11] The reasoning of the appellate court, which analogized Internet conversations to telephone conversations, was "not adopted" by the Virginia Supreme Court. The Supreme Court affirmed Bloom's case solely on the basis of the trial court's finding of fact.[12] Both opinions establish standards for the admission of Internet conversation into evidence that may serve as triumphs for the protection of the public against would-be child predators, but might concern anyone owning a computer or regularly participating in Internet chat.

{5}This note will explore the *Bloom* decisions[13] as they relate to the admissibility of Internet communications into evidence in a criminal prosecution. To adequately discuss this topic, there will be a brief description of how instant messaging works and the police operations that use instant messaging to catch and arrest those who attempt to solicit minors for sex. Following that discussion will be a summary of both *Bloom v. Commonwealth* decisions. Because the Virginia Court of Appeals likened Internet conversations to telephone conversations, this reasoning, and case law treating Internet conversations in this manner, will be addressed in terms of whether the telephone analogy can serve as a valid standard for admitting Internet conversations into evidence. The Virginia Supreme Court's "totality of the record" approach will also be discussed in terms of case law affording similar treatment to the use of instant messages as evidence. Finally, this note will hypothesize about the effect of the *Bloom* decisions on the future admissibility of instant messages into evidence.

II. Instant Messaging and Police Investigations

{6}Undercover police operations on the Internet frequently use "Internet Relay Chats," a computer program allowing two or more users to conduct live, typed conversations.[14] An investigator accesses the Internet through an Internet Service Provider, also known as an ISP. Well known ISPs include America Online and Compuserve, but many smaller ISPs exist, providing Internet access without verification of a customer's identification.[15] The lack of verification allows both law enforcement and the general public to obtain Internet access with a false name and address.

{7}Popular Internet relay chats, running on Microsoft Windows, create a window that "pops up" on a user's screen when he or she receives a message. The user can type text into the window, which in turn appears on the screen of the message sender.[16] Depending on the computer program and skill of the user, files, pictures and even videos may be shared almost instantaneously.[17] Users identify each other through using nicknames, which some instant message programs store so that a particular user keeps the same nickname with each use.[18]

{8}Depending on a user's purpose in maintaining an Internet account with instant messaging capability, the user's nickname may have considerable importance.[19] Limitations on what users may choose as nicknames vary according to the type of service provider providing the instant message service. Larger providers are more likely to monitor nicknames and conversations where small providers are more likely to be "user-monitored" and less restrictive.[20]

{9}Police use Internet chats to investigate child sex crimes in two ways. Either a child's parent or the child notifies the police that someone has engaged in sexual conversations with the child,[21] or someone alerts police to a particular chat room or channel. Investigators then pose as bait for patrons of that chat room who are interested in soliciting minors for sex.[22] When a parent alerts police that someone has attempted to engage a child in an inappropriate sexual conversation, investigators frequently know the target's nickname and possibly his or her email address. An investigator most often poses as the child with whom the target has been messaging or as a different young male or female user. [23]

{10}While the police investigator chats with the target, software programs identify the target's Internet service provider and Internet Protocol, or IP address.[24] IP addresses, unique to each computer connected to the Internet at a particular time, insure electronic data sent from one computer to another reaches the appropriate destination. IP addresses are also associated with a domain name or a textual representation of the IP address' series of numbers.[25] Knowing the ISP, IP address, and domain name, officers may subpoena the ISP for records.

{11}Subpoenas are often necessary because a computer user who does not maintain a permanent direct connection to the Internet the computer will not have a permanent IP address. Users without direct connections call into telephone lines owned by the ISP. ISPs, which have a multitude of IP addresses, in turn route the user to the Internet. A single IP address, therefore, may not identify a specific user, and access logs are needed to match nicknames and user accounts with exact dates and times of online encounters with police.[26]

{12}The police investigator's goal as he or she chats with a target is a face-to-face meeting between the child, who is in reality the investigator, and the target. A face-to-face meeting establishes the identity of the target and the target's true intent.[27] Michael Sheetz, a Florida law enforcement officer involved in Internet investigation, notes: "It is conceivable, and well within the range of reasonable doubt, that a person other than the genuine account holder, or telephone subscriber, could have been using the computer during the online conversations." [28] A seemingly fool-proof

means of identifying the face behind the keyboard involves obtaining a search warrant for the target's home or place of business and executing the warrant while an officer posing as the child-victim makes online contact with the target.[29]

III. *Bloom v. Commonwealth*

{13}The case against Gregory Michael Bloom began in early February, 1999, when a child's mother alerted police that an adult male was communicating with her thirteen-year-old daughter over the Internet.[30] After speaking with the police, the victim's mother went online posing as her daughter, under her daughter's nickname, "Nikki4403."[31] While online, the victim's mother received a message from a person using the nickname "Philter425." The message began, "Hi sexy. Looking forward to Friday/Saturday."[32] The victim's mother responded that she would return online to talk to "Philter425" on Friday, February 5. She then exited the instant messenger program and informed the police of the "chat date."[33]

{14}On February 5, 1999, a police officer, posing as "Nikki4403," received messages from and corresponded with "Philter425" about sexual topics.[34] "Philter425" began the conversation with "Nikki4403" by asking whether she was "ungrounded."[35] Both the Virginia Court of Appeals and Virginia Supreme Court found this question persuasive in determining that Bloom was "Philter425" because the question linked him to earlier conversations with the victim to which the victim testified at trial.[36] The police officer posing as "Nikki4403" also informed "Philter425" she could "get out tonight" and that she did not want to baby-sit his daughter, presumably a ruse the two used when the victim's mother was present. "Nikki4403" further stated that she was alone, so "it's cool," seemingly, to talk about sex. "Philter425" then suggested the two have "wild monkey sex" in addition to his performing oral sex on her.[37] The two arranged to meet at a pay phone at a particular Burger King restaurant at 10:30 p.m. that night. "Philter425" told "Nikki4403" he would arrive in a silver Toyota Tercel.[38]

{15}In this conversation, the only facts relating to the identity of "Philter425" were that he had a daughter and a silver Toyota Tercel. "Philter425" never made reference to his name, age, race, or even his sex. In addition, "Philter425"'s question as to whether "Nikki4403" was ungrounded was the only indication that "Philter425" was aware that "Nikki4403" was a minor. If the trial court had ruled against the admission of prior conversations between the victim and Philer425, the Commonwealth would have had diminished ability to demonstrate that Bloom knew he was attempting to take indecent liberties with a minor, an element required by the statute under which Bloom was convicted.[39]

{16}At the appointed time of 10:30 p.m., police officers witnessed Bloom arrive in a silver Tercel, pause near the pay phone briefly and then drive away.[40] The officer who had earlier posed as "Nikki4403" stopped Bloom and asked him if he had "been online that evening as Philter425."[41] After first denying, Bloom eventually admitted having an instant message conversation as "Philter425." While admitting to the February 5th conversation, Bloom continued to deny having sent instant messages to the victim before the night of his arrest and filed a motion *in limine* to exclude all evidence of conversations between "Nikki4403" and "Philter425."[42] Specifically, Bloom argued "there [was] no reliable evidence to suggest that he actually made the statements."[43]

{17}In response, the Commonwealth argued to the trial court that the prior conversations between "Philter425" and "Nikki4403" would be "sufficient to identify Bloom as the person making contact with [the victim] using the screen name Philter425."[44] Counsel for the Commonwealth told the trial court that the victim would testify that she began receiving instant messages from "Philter425" on nearly a daily basis after posting a profile containing her personal information on AOL in November of 1998.[45] According to the Commonwealth, the victim would also testify that during the alleged conversations, "Philter425" informed her that he was male, that his name was Greg, that he was twenty-eight years old and that he had a three-year old daughter. The Commonwealth further asserted that "Philter425" also told the victim his telephone number, which matched Bloom's home telephone number.[46]

{18}According to the Virginia Supreme Court's opinion, Bloom did not challenge the Commonwealth's summary of the victim's potential testimony, which included characteristics appearing to identify him as "Philter425."[47] The trial court, relying on the Commonwealth's "unilateral avowal. . .of testimony that could be presented [at trial]," denied Bloom's motion *in limine*, permitting the victim to testify under the party admission exception to the hearsay rule about prior conversations between "Philter425" and herself.[48] The trial court noted that whether Bloom actually made the statements was "one of the ultimate questions to be determined by the jury."[49] The jury convicted Bloom on all charges.

{19}On appeal Bloom asserted that the trial court improperly admitted the victim's testimony about the content of her conversation with "Philter425" as a party admission. Bloom reasserted his claim that no evidence established that he had actually represented himself as "Philter425" before the night of his arrest or that he had ever conversed with the victim.[50] In finding proper the trial court's decision to admit the conversations into evidence, the Virginia Court of Appeals reasoned that conversations over the Internet are analogous to telephone conversations. Telephone conversations and Internet conversations, by analogy, are admissible as party admissions "if direct or circumstantial evidence establishes the identity of the parties to the conversation."[51]

{20}The Court of Appeals stated that Bloom's admission to the conversation with the officer on the night of his arrest and remarks linking that conversation to past conversations between "Philter425" and "Nikki4403" established him as the face behind "Philter425." The court further found that personal information revealed during the conversations such as "Philter425"'s age, name, gender, phone number and daughter matched Bloom's age, name, gender, phone number and daughter.[52] Finally, the court noted, "No evidence suggested that anyone else could impersonate the defendant by appropriating his Internet identification name and use it to establish a communication link with the victim."[53] Based on these findings, the court held the trial court properly admitted the victim's testimony as party admissions.[54]

{21}The Virginia Supreme Court, in contrast to the Virginia Court of Appeals, did not feel it necessary to analogize instant message conversations to telephone conversations.[55] Instead the court stated,

> We think the record in the present case, when viewed in its totality, clearly supports the trial court's finding, for the purpose of the admissibility of evidence, that Bloom was the person who had made the statements to [the victim] via the Internet. Philter 425 revealed that his name is Greg, which is Bloom's given name. He told [the victim] that he had a three-year-old daughter, as did Bloom. He also told [the victim] that he was 28 years of age, which was Bloom's age. Moreover, Philter425 agreed to meet Nikki4403 at

> a designated place, and Bloom appeared at that place and admitted to [the investigating officer] that he had, in fact, communicated with Nikki4403 via the Internet that evening.[56]

The court concluded that the trial court was entitled to rely on the Commonwealth's proffer of the content of "Philter425"'s conversations with "Nikki4403" prior to the night of Bloom's arrest because the Commonwealth's avowal "was not challenged by Bloom when the motion *in limine* was argued or a trial."[57] Therefore, the court stated, "The Commonwealth was not required to prove these facts at trial to establish the admissibility of the statements."[58]

IV. Toward a Standard of Admissibility: The Virginia Court of Appeals' Telephone Analogy

{22}The opinion of the Virginia Supreme Court, while "not adopting" the telephone analogy used by the Virginia Court of Appeals, does not explicitly reject the reasoning either. In fact, the court stated that the Court of Appeals' decision "rests upon proper principles of law."[59] Because the Virginia Supreme Court's decision is ambiguous in this regard, it is helpful to analyze the Court of Appeals' reasoning in determining the effect *Bloom* may have on the future admissibility of Internet conversations into evidence as party admissions or for other purposes.

{23}As the Virginia Court of Appeals stated, courts traditionally admit telephone calls where the conversation appears relevant to the fact or facts in issue.[60] American Jurisprudence 2d provides:

> Admissibility of telephone conversations is governed by the same rules of evidence which govern the admission of oral statements made in face-to-face conversations, except that the party against whom the conversation is sought to be used must ordinarily be identified. If, however, evidence of what was said in a conversation, if made face to face, would be inadmissible as hearsay, proof of it as a telephone conversation is likewise inadmissible.[61]

{24}Black's Law Dictionary defines hearsay as "testimony that is given by a witness who relates not what he or she knows personally, but what others have said, and that is therefore dependent on the credibility of someone other than the witness."[62] Hearsay statements are generally inadmissible at trial because the person actually making the statement proffered as evidence has not taken an oath to tell the truth, is not personally present in the courtroom, and therefore, cannot undergo cross-examination by the defendant. A multitude of exceptions to the general rule of inadmissibility exist, though, including "party admissions." A statement made by a party that disfavors him a trial, although not necessarily disfavoring him at the time he made the statement, may be admitted as evidence through the testimony of a witness to the party's statement.

{25}The *Bloom* court cited *Snead v. Commonwealth* for the proposition that direct and circumstantial evidence may establish the identity of the parties to the conversation.[63] The *Snead* Court, quoting *Armes v. Commonwealth*, stated "identification is proved by direct of circumstantial evidence somewhere in the development of the case. The mere statement of his identity by the party calling is not in itself sufficient proof of such identity, in the absence of corroborating circumstances so as to render the conversation admissible."[64]

{26}A court's decision to admit a telephone conversation into evidence lies in the totality of the circumstances identifying a participant in the conversation. [65] One factor considered by courts in identifying the participant is the content of the conversation. A conversation revealing circumstances likely only to be known by the person to be identified and the person called serves as a convincing step towards a court's admission of a telephone conversation.[66] If the unidentified party admits to the conversation, invites the person called to call, or exhibits conduct showing a discernible pattern, courts are likely to admit the conversation into evidence. Finally, courts also consider a telephone company's records, subsequent acts relating to the substance of the conversation, and other various circumstances the court deems convincing.[67]

{27}*Snead* and *Armes* demonstrate the amount of circumstantial evidence needed to prove the identity of a telephone caller. In *Snead*, the state attempted to prove the defendant participated in a gambling operation. During a search of a house suspected to accommodate the gambling operation, someone called and identified himself as the defendant, "Leonard Snead."[68] Based on the alleged call, a deed indicating Snead co-owned the house in 1978, and utility bills found in the house addressed to Snead, the trial court convicted Snead of feloniously operating a gambling enterprise.[69]

{28}The Virginia Court of Appeals rejected the Commonwealth's argument that the caller's identity was established because he identified himself as "Leonard Snead," actually intended to reach the number dialed, and demanded to know to whom he was speaking. The court stated, "The corroborating facts offered by the Commonwealth are simply too tenuous to establish the circumstantial evidence necessary to establish the identity of the caller."[70] The Virginia Court of Appeals reversed Snead's conviction.

{29}In contrast to *Snead*, the *Armes* decision found sufficient circumstantial evidence to prove the defendant attempted to convince a witness to kill her lover's wife for $10,000.[71] Armes contacted the witness, her son-in-law's brother, knowing he needed money. Identifying herself as "Linda," she called the witness several times to determine his interest in killing her lover's wife.[72] Following that call by "Linda," the witness contacted the police who monitored "Linda's" subsequent calls. The court found the fact that "Linda" knew that the witness needed money and knew his home and office telephone numbers significant.[73] The court also noted that in one of "Linda's" conversations with the witness she arranged to have "Jack," her lover, give the witness $2,000 as a down payment for killing his wife. The fact that "Jack" showed up at the meeting and, after being arrested, admitted to being Armes' lover helped convince the trial and appellate court that Armes and "Linda" were the same person.[74]

{30}Using *Snead* and *Armes* as bases for Virginia's standard for the type of circumstantial evidence necessary to establish the identity of a telephone caller or, as in the *Bloom* case, the sender of an instant message, courts have given very little weight to the name a caller might use on the telephone or computer. Instead, courts seek to establish that the caller knew certain classified facts and acted in some way consistent with his or her calls before they will admit telephone conversations into evidence. In Bloom's case, apparently the victim's recent "grounding" was the only "classified fact" known by "Philter425."

{31}Bloom's case lies somewhat between *Snead* and *Armes*. "Philter425"'s description of himself as a twenty-eight-year old male named Greg with a three-year old daughter appears similar to Snead's identification of himself, an approach the Virginia Supreme Court rejected. Just as police officers in *Snead* could not independently verify that the caller was in fact Snead or was simply

pretending to be Snead, the Commonwealth had no way to independently verify that "Philter425" was in fact a twenty-eight-year old man named Greg, or, instead, Greg's roommate pretending to be Greg.[75] However, as in *Armes*, "Philter425"'s question regarding the victim's being grounded can be viewed as a "classified fact" and Bloom acted consistently with "Philter425"'s agreement to meet "Nikki4403." Because the establishment of Bloom's identity as "Philter425" could fall under either decision cited by the Virginia Court of Appeals, the viability of the Virginia Court of Appeals' telephone analogy appears uncertain.

V. Standards Set By Other Courts: The Internet Conversation to Telephone Conversation Analogy

{32}The Virginia Court of Appeals is not the first court to analogize Internet conversations to telephone conversations for the purpose of accepting their content as evidence against defendants in cases involving child pornography or sexual advances toward minors.[76] However, cases analogizing Internet conversations in this way have not done so for the purpose of establishing the identity of a message sender in order to avoid the hearsay rule.

{33}In *Reno v. ACLU*, the Supreme Court analogized the availability of obscenity on the Internet to that available through a telephone "dial-a-porn" service.[77] In this case, the Court addressed the constitutionality of the Communications Decency Act of 1996, which in part criminalized the "knowing" transmission of "obscene or indecent" messages to any recipient under eighteen years of age.[78] The Government urged the Court to find the act constitutional under its precedents, including *Ginsburg v. New York*, upholding a ban on the sale of obscene material to minors under seventeen, [79] *FCC v. Pacifica*, upholding restriction on broadcasting a monologue with so called "Filthy Words,"[80] and *Renton v. Playtime Theaters, Inc.*, upholding a zoning ordinance that prevented adult theaters from locating in residential neighborhoods.[81]

{34}The Court rejected the Government's contention that the Communications Decency Act mirrored the laws upheld in *Ginsberg*, *Pacifica* and *Renton*.[82] Instead, the Court found that the Internet lacked the "history of extensive government regulation of the broadcast medium. . .the scarcity of available frequencies at its inception. . . and its 'invasive' nature."[83] Characterizing the Internet as a "non-invasive" means of communication, the Court relied on its decision in *Sable Communications of California, Inc. v. FCC*,[84] striking down a blanket prohibition on indecent telephone messages, to find the Communications Decency Act of 1996 unconstitutional.[85]

{35}Specifically, the Court noted, "users seldom encounter content 'by accident.'"[86] Persuaded by findings of the lower court "that almost all sexually explicit images are preceded by warnings as to the content," and that the lower court had "cited testimony that 'odds are slim' that a user would come across a sexually explicit sight by accident,"[87] the Court likened the use of the Internet to obtain sexually explicit material to the "dial-it medium" which "requires the listener to take affirmative steps to receive the communication."[88] The Court concluded that accessing the Internet, like "[p]lacing a telephone call . . . is not the same as turning on a radio and being taken by surprise by an indecent message," and therefore the Internet could not be regulated as stringently as broadcast media.[89]

{36}In *United States v. Maxwell*,[90] a case similar to *Bloom* dealing with the distribution of child pornography, the Court of Appeals for the Armed Forces analogized Internet communications to telephone messages. The court found that Internet users have an expectation of privacy in their online communications similar to the expectation of privacy they would have in their telephone conversations.[91] The defendant in *Maxwell* argued to suppress evidence uncovered as a result of search warrant for AOL's computers and later his personal computer.[92] A magistrate issued the warrant for AOL based on a consumer complaint that child pornography was being distributed via AOL.[93] The consumer filing the complaint listed the defendant's screen name, "REDDE1," as one of many screen names he knew to participate in the distribution of child pornography.[94] Based on the search of AOL, a second warrant was issued for the defendant's computer.[95]

{37}Describing chat rooms, the court stated, "These conversations are not maintained by AOL, but software is provided to the user to record his or her log of the messages that transpire. This form of communication is most akin to a telephone party line."[96] Describing instant messages, the court stated that in allowing a user to send messages to another user who happens to be online at the same time, an instant message conversation "is most like a telephone conversation."[97]

{38}In ultimately determining that Internet users have the same expectation of privacy in their Internet conversations as they would in telephone conversations, the court stated:

> [T]he technology used to communicate via e-mail is extraordinarily analogous to a telephone conversation. Indeed, e-mail is transmitted from one computer to another via telephone communication, either hard line or satellite. We have recognized that "telephone conversations are protected by the Fourth Amendment if there is a reasonable expectation of privacy."[98]

{39}Despite this finding, the court noted that users of instant messaging systems run the risk of one of the users saving the conversation to a disk as was the case in *Maxwell*. Such an action, said the court "would be much like clandestinely recording one's telephone conversation."[99]

{40}Quoting language from the Supreme Court's decision in *Hoffa v. United States*,[100] the *Maxwell* court found that the defendant had no Fourth Amendment protection from the consumer who had alerted authorities. The court stated that "there is no protection under the Fourth Amendment for 'a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it.'"[101] "Thus, [the court concluded] any of the material or information seized and turned over to the FBI or to other police agencies by [the consumer] was 'fair game' for introduction into evidence and for use in procuring a search warrant."[102]

{41}Though Maxwell never challenged the Government's assertion that it was he who received and distributed pornography under the screen name "REDDE1," the defendant in *United States v. Lamb*,[103] a case citing *Maxwell* with approval, did make such a challenge in pre-trial motions.[104] Lamb was arrested under the Federal Bureau of Investigation's "Innocent Images" operation, designed to curb the flow of child pornography over the Internet.[105] Screen names registered to "Lamb," "Josh6979" and "JoMil5," were associated with the transmission of over 100 child pornography images over eight months.[106] The defendant objected to a magistrate's issuance of a search warrant for his home based in part on the content of messages accompanying the image

transmissions on the grounds that "the sender's identity [was] unknown."[107] In contrast to the *Bloom* trial court, the *Lamb* court preserved the question of the sender's identity for trial, stating that "[t]he messages were allegedly attached to the images originating from the person using defendant's screen name and account number; whether defendant is the sender is a question that will presumably be answered at trial."[108]

{42}With similar reasoning to the *Maxwell* court's, the Superior Court of Massachusetts suppressed evidence in the trial of Robert Accetta.[109] Accetta, like Bloom, allegedly roused suspicion in the victim's father when he addressed an instant message to the boy's nickname from his own nickname, "ShavedMA," while the victim's father was using the victim's computer.[110] The court held that statements intercepted by the victim's father without police intervention could be used against Accetta as well as any evidence seized on the basis of those statements. However, statements made while the police intervened without a warrant were suppressed.[111]

{43}Again, the question of whether "ShavedMA" was in fact the defendant was never raised. Identification of Accetta as "ShavedMA" resulted from an explicit message "ShavedMA" sent the victim's father (believing him to be the victim) referring to a previous sexual encounter between the defendant and the victim.[112] With that information, the father surveyed the boy's room and found a piece of paper with the defendant's name and phone number. Through the phone number, police identified the defendant and obtained a search warrant for his home.[113] Though the court never specifically discusses the issue, it is possible that the victim could actually identify Accetta by sight from the above-referenced sexual encounter, something the victim in *Bloom* could not do.

VI. "The Record Viewed In Its Totality" Standard of Admissibility

{44}The only cases resembling the Virginia Supreme Court's "totality of the record" standard come from the Second District Appellate Court of Illinois. The most notable of these cases is *Illinois v. Patterson*.[114] Although in *Patterson*, the defendant's specific intent to commit aggravated criminal sexual abuse, not his identity, was at issue; the defendant did put forth evidence questioning the ability of prosecutors to establish the Internet child-predator's identity.

{45}Police arrested Patterson after an undercover officer posing online as a fifteen-year-old boy named Rob received sexually explicit instant messages from a person using the name "Boysneeded."[115] As in *Bloom*, the undercover officer arranged to meet "Boysneeded" at a local McDonalds.[116] In the course of the instant message conversation, "Boysneeded" expressed concern "about this here [sic] about men going to meet young men and then they get arrested."[117] "Boysneeded" also informed the police officer he would arrive at the McDonalds in a blue Jeep Grand Cherokee wearing jeans and a Chicago sweatshirt.[118]

{46}When the defendant came to the McDonalds, he did not find his fifteen-year-old date there. As he proceeded back to his blue Jeep Grand Cherokee to leave, police officers blocked him into his parking space and asked him why he was there. The defendant answered that he had come to meet "Rob," a fifteen-year-old boy. Defendant also stated that he believed fifteen was the age of consent, but admitted to his prior statements concerning being arrested for meeting young men.[119]

{47}At trial, the defendant moved to suppress evidence of his statements to "Rob" and to the officer at the McDonalds on the grounds that he had been interrogated in police custody for the purposes of *Miranda v. Arizona*. The trial court denied defendant's motion to suppress.[120] The trial court found the evidence sufficient to convict the defendant of attempted aggravated criminal sexual abuse despite evidence tending to call into question both the identity of the defendant and the victim. The first of that evidence was the testimony of the defendant's roommate that "approximately 100 other people in addition to the defendant and himself" had access to the defendant's computer.[121] This evidence would also suggest that other people had access to the defendant's screen names.

{48}The defendant then testified in his own behalf, stating that he frequently visited chat rooms with homosexual themes, that he had met around 100 people face-to-face conversing on the Internet, that about fifty of those people had misrepresented themselves in some way, that he had a number of screen names and profiles, including "Boysneeded," and, finally, that he began speaking with "Rob" because of his profile. He testified that he could not be sure of Rob's actual age, which was listed as fifteen in his online profile, because of the frequency of misrepresentations by participants in Internet chats.[122]

{49}In affirming the defendant's conviction, the court stated:

> [T]he defendant arrived at the agreed-upon place, at the agreed-upon time, wearing the clothing he informed [Rob] he would be wearing and driving the car he informed [Rob] he would be driving. [W]hen [officers] approached defendant, defendant admitted that he was waiting for a fifteen year-old boy named Rob. Viewing this evidence in the light most favorable to the prosecution results in the conclusion that the State provided sufficient evidence of the defendant's specific intent to commit aggravated criminal sexual criminal abuse.[123]

{50}The *Patterson* court's language closely parallels the Virginia Supreme Court's language in its decision to uphold Bloom's conviction. While the decision in both of these cases appears to be based on sound reasoning because both defendants admitted their illicit rendezvous, a defendant's denial could make the admissibility of out of court Internet statements more difficult.

VII. Analysis of the Two *Bloom* Standards and The Future Admissibility of Internet Conversations

{51}Both the telephone analogy used by the Virginia Court of Appeals and the "totality of the record" approach used by the Virginia Supreme Court create unsatisfying standards for the admission of Internet conversations when those conversations are used to prove the identity of one of the parties. The fantastical nature of the Internet makes establishing the identity of an Internet message sender inherently more problematic than establishing the identity of a telephone caller. However, simply reviewing facts as set forth by the prosecution, as did the *Bloom* trial court and Virginia Supreme Court, appears to completely lack reliability.

{52}In *Reno*, the Supreme Court acknowledged the problem of determining the identity of Internet users and, based in part on that observation, condemned the Communications Decency Act of 1996. The Court, quoting the lower court's finding of facts, stated:

> [T]here "is no effective way to determine the identity or age of a user who is accessing material through e-mail or chat rooms. An e-mail address provides no authoritative information about the addressee, who may use an e-mail 'alias' or an anonymous remailer ... For these reasons, there is no reliable way in many instances for a sender to know if the recipient is an adult or a minor.[124]

{53}As demonstrated by the *Patterson* case discussed above, Internet conversations increase the opportunity for disguise and mistaken identity because participants on both sides of the conversation may be engaged in fantasy or role-play. As a result, it becomes increasingly difficult to establish through evidence that a real pedophile has engaged in illicit conversation with a real child. Although the Court of Appeals in *Bloom* noted that no evidence demonstrated anyone had tried to impersonate Gregory Michael Bloom,[125] one wonders what effect such evidence would have had on the court's standard of determining the reliability of the Internet conversation and its admission into evidence. Similarly, it would have been more difficult for the Virginia Supreme Court to affirm Bloom's conviction based on the "totality of the record" if Bloom had presented such evidence.

{54}Had Bloom not admitted to having the instant message conversation with the officer posing as "Nikki4403," the trial court would not have had enough evidence to establish Bloom's identity as "Philter425." Both appellate courts relied heavily on Bloom's question, "Are you ungrounded now?," to establish "internal links between the earlier and later conversations support[ing] the inference that "Philter425" was the same person both times."[126] Had Bloom not asked that question, the trial court would have had to admit the conversations based solely on the fact that the personal description given by "Philter425" matched Bloom. While no one can argue with presenting as much evidence as possible against someone who would sexually abuse a child, both the "telephone analogy" and "totality of the record" approach present the possibility that innocent instant message users could find themselves defending charges stemming from conversations they never had.

{55}People familiar with AOL's instant message program might note that the users of the program can activate a feature that loads the program as the computer starts up or logs on to the Internet. Password protection is often ineffective because people instruct their computers to "save password" to keep them from having to reenter it before each use. These features make it possible that an unsuspecting user of a public computer, perhaps at a public library, could activate his or her instant message account and inadvertently trigger the mechanisms for password save and automatic load. The next person using the computer, who may fantasize about sex with young children, could seize the unsuspecting library user's account and identification.

{56}That scenarios such as this possibly call into question the standard used by the Virginia Court of Appeals that "a statement of [a party's] identity by the party called [or calling], standing alone, is not generally regarded as sufficient proof of such identity unless it is corroborated by other circumstances."[127] This standard is especially problematic when the "other circumstances" corroborating identity come from the calling or messaging party's description of himself with no opportunity for independent verification of that description. Conversely, in not analogizing instant message conversations to telephone conversations, the Virginia Supreme Court's standard allows for the possibility that prosecutorial proffers, rather than hard evidence, will convict those accused of using the Internet for illegal purposes.

{57}To illustrate problems with the Virginia Supreme Court's decision, picture an instant message user commandeering the nickname "Prez2001." He states that his name is George and that he lives on Pennsylvania Avenue in Washington D.C. with his wife Laura. It certainly appears the user has identified himself as President Bush. This becomes a problem when "Prez2001" contacts "Rachel-12," a twelve-year-old girl, for sex.[128] If the President were arrested, it is hard to imagine any trial court admitting such conversations into evidence against the against him merely because details such as name, address and spouse matched the defendant. However, under current Virginia precedent, a prosecutorial proffer that certain details from conversations between "Prez2001" and "Rachel-12" would establish "Prez2001"'s identity, such conversations could be admitted. On appeal, when viewed in the light most favorable to the Commonwealth, in addition to perhaps and admission by the President that in fact used the screen name "Prez2001," it is possible the Supreme Court of Virginia could uphold the Presidents conviction based on the facts listed above.

VIII. Conclusion

{58}Because communication via the Internet has become so widely accepted and even preferred in some situations, many people do not fully understand the possible ramifications of those conversations. While Internet users may generally worry that their credit card numbers might end up in the hands of a hacker, or that their website preferences might place them on another junk email list, *Bloom v. Commonwealth* suggests that instant message users in particular should actually know or at least be familiar with the identity of the people with whom they are chatting. Although the "what-if" scenarios proposed in this note may seem alarmist, *Bloom* suggests a no tolerance policy for users whose nicknames and profiles turn up in child sexual abuse investigations. After *Bloom*, users receiving messages like the one stated at the beginning of this note should think seriously about answering "No."

ENDNOTES

[*]. Jessica Cobaugh holds an undergraduate degree from Duke University and expects to graduate with her Juris Doctor from the University of Richmond T.C. Williams School of Law in May, 2002. Ms. Cobaugh, a Senior Staff member of the *Richmond Journal of Law and Technology*, plans to return to her native North Carolina to practice.

[1]. This exact message presented itself on the author's screen during her first semester of law school. The message came from a classmate who no longer uses the nickname, "Naturalbornkiller2000."

[2]. *See* Michael W. Sheetz, *CyberPredators: Police Internet Investigations Under Florida Statute 847.0135*, 54 U. MIAMI L. REV. 405 (2000). In his fifteen-year experience as a Florida law enforcement officer, the author participated in many Internet "sting" operations designed to catch pedophiles soliciting children for sex or looking for child pornography. *Id*. at 406. He states, "It has been my experience as an investigator that when using a female sounding name and a youthful persona, so many requests for private chat occur within five minutes that immediate response to all would be impossible." *Id*. at 411.

[3]. *See Bill Seeks to Crack Down on Child Sex Solicitations on Internet*, ASSOCIATED PRESS POL. SERV., Mar. 27, 1997, *available at* 1997 WL 2512012; *Legislation Being Drafted to Stop On-line Sexual Predators*, ASSOCIATED PRESS POL. SERV., Mar. 24, 1998, *available at* 1998 WL 7399054.

[4]. *See* FLA. STAT. ANN. § 847.0135 (West 2000 & Supp. 2002). The short title of this act is "The Computer Pornography and Child Exploitation Prevention Act of 1986." Subsection three of the act specifically prohibits the use of computer online services for the purpose of soliciting a child to commit a sexual act. *Id.*

[5]. *See* 18 U.S.C. § 2423(b) (2001) (prescribing interstate travel with the intent to engage in a sexual act with a minor). *See also* VA. CODE ANN. § 18.2-370 (Michie 1996 & Supp. 2001).

[6]. *See, e.g.*, United States v. Lamb, 945 F. Supp. 441, 467 (N.D.N.Y. 1996)(search warrant for defendant's home, computer, and AOL account granted although identity of sender of e-mails containing child pornography unknown); United States v. Maxwell, 45 M.J. 406, 420 (C.A.A.F. 1996)(typographic error on warrant authorized search of incorrect screen name); Illinois v. Patterson, 734 N.E.2d 462, 466 (Ill. App. Ct. 2000)(conviction affirmed despite testimony by defendant's roommate that approximately 100 people had used computers in addition to defendant).

[7]. *See* Bloom v. Commonwealth, 542 S.E.2d 18, 18-20 (Va. Ct. App. 2001), *aff'd on other grounds*, 554 S.E.2d 84, 87-88 (Va. 2001)

[8]. *See* VA. CODE ANN. §§ 18.2-370, 18.2-29 (Michie 1996 & Supp. 2001).

[9]. VA. CODE ANN. § 18.2-370(A)(5).

[10]. *Id.* § 18.2-370(A)(1),(3),(4).

[11]. *See* Bloom v. Commonwealth, 542 S.E.2d 18, 20 (Va. Ct. App. 2001).

[12]. *See* Bloom v. Commonwealth, 554 S.E.2d 84, 88 n. 2 (Va. 2001). Although the Virginia Supreme Court's decision will be discussed in detail later in this note, the only portion of the opinion addressing the Virginia Court of Appeals ruling states:

> While we affirm the judgment of the Court of Appeals and conclude that its decision rests upon proper principles of law, we do not adopt its observation that "[c]onversations over the Internet are analogous to telephone conversations." (citation omitted). For example, in telephone conversations, unlike communications via the Internet, the participants have the opportunity for voice recognition.

[13]. Both opinions affirming Bloom's conviction will be discussed because while not accepting the Court of Appeals' analogy, the Virginia Supreme Court did not appear to specifically reject the Court of Appeals' ruling. Moreover, a survey of cases dealing with the admissibility of e-mail and instant messages demonstrates that federal and state courts have analogized those forms of communications to telephone conversations. *See, e.g.*, Reno v. ACLU, 521 U.S. 844 (1997); United States v. Lamb, 945 F. Supp. 441, 452 n.7 (N.D.N.Y. 1996); United States v. Maxwell, 45 M.J. 406, 411 (C.A.A.F. 1996); Massachusetts v. Accetta, No. 99-725, 1999 Mass. LEXIS 414, at *8 (Mass. 1999).

[14]. Sheetz, *supra* note 2, at 409-10.

[15]. *Id.* at 409.

[16]. *Id.* at 410.

[17]. *Id.*

[18]. *See id.* America Online's Instant Messenger stores nicknames and password protects a user's "buddy list" to prevent other users from posing as the person behind that nickname. America On Line also keeps track of nicknames already in use and prevents two users from having the same nickname.

[19]. *Id.* Sheetz recalled two nicknames, "HARD4U" and "Bi-Fem-Amanda," as examples of nicknames he came across during his law enforcement tenure. *Id*.

[20]. *Id.* at 411.

[21]. This was the case in *Bloom*, 542 S.E.2d 18 (Va. Ct. App. 2001), and *Accetta*, No. 99-275, 1999 Mass. LEXIS 414 (Mass. 1999).

[22]. Sheetz, supra note 20, at 411. This was the case in *Lamb*, 945 F. Supp. 441 (N.D.N.Y. 1996), *Patterson*, 734 N.E.2d 462 (Ill. App. Ct. 2000), and *Illinois v. Scott*, 740 N.E.2d 1201 (Ill. App. Ct. 2000).

[23]. Sheetz, *id.*

[24]. *Id.* at 412.

[25]. *Id*. at 412-13. An example is Microsoft.com.

[26]. Sheetz, *id.* at 413.

[27]. *Id.* at 414–15.

[28]. *Id.*

[29]. *Id.*

[30]. *See* Bloom v. Commonwealth, 542 S.E.2d 18, 19-20 (Va. Ct. App. 2001). *See also* Bloom v. Commonwealth, 554 S.E.2d 84, 85 (Va. 2001). The Virginia Supreme Court's description of the facts in Bloom's case are slightly more descriptive than those provided by the Court of Appeals.

[31]. Bloom, 554 S.E.2d at 85

[32]. *Id.*

[33]. *Id.*

[34]. *See id* at 85–86. The conversation is reproduced in full within the Virginia Supreme Court opinion.

[35]. *Id.* at 85.

[36]. *See* Bloom, 554 S.E.2d at 85, 87; Bloom, 542 S.E.2d at 20.

[37]. *See* Bloom, 554 S.E.2d at 85.

[38]. *Id.*

[39]. *See* VA. CODE ANN. §18.2-370(A)(5) (Michie Supp. 2000).

[40]. *Id.* Bloom, 554 S.E.2d at 86.

[41]. *Id.*

[42]. *Id.*

[43]. *Id.*

[44]. *Id.* at 87.

[45]. *Id.* In her profile, the victim described herself as a fifteen-year old girl, although in reality she was only thirteen. She further stated that she was five foot eight inches tall with brown hair and brown eyes and that "she was sexy." *Id.* at 85.

[46]. *Bloom*, 554 S.E.2d at 86 (Va. 2001).

[47]. *Id.* at 87. Possible challenges coming to the mind of the author include the fact that the victim apparently never met "Philter425" and therefore could not testify as to whether the description given by "Philter425" matched the person she knew to be "Philter425." There is also no evidence that the victim ever called or received telephone calls from Bloom in which he identified himself as "Philter425." Finally, introduction of evidence that other people could have accessed the "Philter425" nickname (if any such evidence existed) may have swayed the trial judge against allowing the victim's testimony.

[48]. *Id.* at 87-88

[49]. *Id.* at 87.

[50]. *See* Bloom, 542 S.E.2d at 20 (Va. Ct. App. 2001).

[51]. *Id.*

[52]. *Id.* at 21

[53]. *Id.*

[54]. *See id.* The court addressed other challenges by Bloom to the sufficiency of the evidence to prove he was over eighteen, he made an attempt, he enticed allured, persuaded or invited the victim, he intended to commit sodomy, or he had lascivious intent. Those challenges, all dismissed by the court, are outside the scope of this casenote.

[55]. *See* 554 S.E. 2d at 88, n. 2 (Va. 2001).

[56]. *Id.* at 87.

[57]. *Id.* at 88.

[58]. *Id.*

[59]. Bloom, 554 S.E.2d at 88 n. 2 (Va. 2001).

[60]. *See* 29 AM. JUR. 2d *Evidence* § 577 (1994).

[61]. *Id.*

[62]. BLACK'S LAW DICTIONARY 726 (7th ed. 1999).

[63]. *See* Bloom, 542 S.E.2d at 20.

[64]. Snead v. Commonwealth, 358 S.E.2d. 750, 753 (Va. Ct. App. 1987) (quoting Armes v. Commonwealth, 349 S.E.2d. 150, 152 (Va. Ct. App. 1986)).

[65]. 79 A.L.R.3d 79 § 2 (1977). Summary and comment.

[66]. *See id.*

[67]. *See id*.

[68]. *See Snead*, 358 S.E.2d 750, 752.

[69]. *See id.* at 753.

[70]. *Id.*

[71]. *See* Armes v. Commonwealth, 349 S.E.2d 150 (Va. Ct. App. 1986).

[72]. *See id* at 151-52.

[73]. *See id*.

[74]. *See id.* at 153.

[75]. The possibility of roommates using each other's screen names and having similar interests in pedophilia is discussed further in *Illinois v. Patterson*, 734 N.W.2d 462 (Ill. App. Ct. 2000).

[76]. *See* Reno v. ACLU, 521 U.S. 844 (1997); United States v. Maxwell, 45 M.J. 406 (C.A.A.F. 1996); Massachusetts v. Accetta, No. 99-725, 1999 Mass. LEXIS 414 (Mass. 1999).

[77]. *See* Reno, *supra* note 76.

[78]. *See id.*

[79]. Ginsberg v. New York, 390 U.S. 629 (1968).

[80]. FCC v. Pacifica, 438 U.S. 726 (1978).

[81]. Renton v. Playtime Theaters, Inc., 475 U.S. 41 (1986).

[82]. *See Reno*, 521 U.S. at 864–68.

[83]. *Id.* at 868. With regard to invasiveness, a factor the Court used to liken the Internet to telephone dial-a-porn, the Court stated, "Moreover, the Internet is not as 'invasive' as radio or television." *Id.* at 869. The District Court found that "communications over the Internet do not 'invade' an individual's home or appear on one's computer screen unbidden." *Id.* It is interesting to note that instant messages often do appear on one's computer screen unbidden.

[84]. 492 U.S. 115 (1989).

[85]. *Id.* at 869–70.

[86]. *Id.* at 869.

[87]. *Id.*

[88]. *Id.* at 870.

[89]. *Id.*

[90]. 45 M.J. 406 (C.A.A.F. 1996).

[91]. *Id*. at 418.

[92]. *Id*. at 412–13, 415.

[93]. *Id*. at 412–13.

[94]. *Id.* at 413. Interestingly, because of a typo in the search warrant identifying the defendant's screen name as REDDEL, evidence linking the defendant to child pornography almost went unfound. Because the Federal Bureau of Investigation Agent in charge of the investigation had provided AOL with the original list of screen names before obtaining the warrant, the defendant was identified. *See id*. The search undertaken by AOL also proved more expansive than that prescribed in the warrant, identifying a second screen name under which the defendant contacted other armed forces members regarding his sexual orientation. *Id.* The Appellate Court ordered that information gleaned from the second screen name should have been suppressed. *See id.* at 421.

[95]. *Id.* at 414

[96]. *Id.* at 411.

[97]. *Id.*

[98]. *Id.* at 417 (citations omitted).

[99]. *Id.*

[100]. 385 U.S. 293 (1966).

[101]. *Id.* at 418. (quoting United States v. Hoffa, 385 U.S. 293, 302 (1966)).

[102]. *Id.* at 419.

[103]. 945 F. Supp. 441 (1996).

[104]. See *id*. at 451–52.

[105]. *Id.* at 445.

[106]. *Id.* at 446.

[107]. *Id.* at 463.

[108]. *Id.*

[109]. Commonwealth v. Accetta, No. 99-275, 1999 Mass. LEXIS 414 (Mass. 1999).

[110]. *Id.* at *1-2.

[111]. *Id.* at *5.

[112]. *Id.* at *2.

[113]. *Id.*

[114]. *See* People v. Patterson, 734 N.E.2d 462 (Ill. App. Ct. 2000); People v. Scott, 740 N.E.2d 1201 (Ill.App. Ct. 2000).

[115] *Patterson*, 734 N.E.2d at 464.

[116] *Id.* at 465.

[117] *Id.*

[118] *Id.*

[119] *Id.* at 466.

[120] *Id.*

[121] *Id.*

[122] *Id.* at 466-7.

[123] *Id.* at 468.

[124] *Reno*, 521 U.S. 844, 855-56.

[125] *See* Bloom, 542 S.E.2d 18, 21.

[126] *Id.* at 20-21.

[127] *Snead*, 358 S.E.2d 750, 752 (Va. Ct. App.1987), quoting Benson v. Commonwealth 58 S.E.2d 312, 315 (Va. 1950).

[128] The author certainly does not wish to imply that the President would use the Internet in this fashion but merely seeks to set forth an example delineating the problems with the Virginia Supreme Court's decision.

Related Browsing

1. http://www.timesdispatch.com/ – A 25-year-old Henrico County man was arrested on charges involving a 13-year-old Stafford County girl he allegedly got to know on the Internet. He was charged with two counts of statutory rape, two counts of contributing to the delinquency of a minor, and charges of taking indecent liberties with a minor.

2. http://www.sexcriminals.com/ – This website provides news about recent sexual offenses and law, information on reporting such offenses and links to state sex-offender registries. It also posts information on wanted fugitives.

3. http://kidmon.com/ – This website provides information to parents who want to monitor their children's access to the Internet. It also provides links to the Department of Justice and companies providing software to control children's access to the Internet.

4. http://www.chatnanny.com/ - This software company provides programs that monitor Internet chats, saves webpages for later parental viewing and log all text typed and programs run.

5. http://www.ageofconsent.com/ – This website posts international ages of consent.

6. http://www.cyberangels.org -- Cyberangels is the an online safety, education and help group. They describe themselves as a cyber-neighborhood watch and operate worldwide in cyberspace through more than 9,000 volunteers worldwide.

7. http://www.ala.org/alaorg/oif/children.html - "The Internet for Children" provides parents and children with links to websites providing information about safety on the internet.

8. http://www.wisechoice.net/ – Internet filtering program designed to filter out pornographic and hate websites and speech to insure the safety of your family.

9. http://www.fno.org/fnojun95.html – "Protecting Your Children from the Internet;" From Now On: The Educational Technology Journal.

10. http://www.securitysoft.com/new1_02/press/myinky1602.html- This website discusses software that could be used in the computers of sex offenders. The software alerts police to illicit activities.

11. http://www.prospect.org/print/V9/39/heins-m.html - This website discusses cases dealing with children, computers, and sensors.

12. http://www.cwfa.org/library/pornography/2000-08-17_ala.shtm- This website discusses neighborhood libraries and sexual predators.

13. http://www.filterreview.com/ - This website provides information for families about different kinds of filtering devices.

14. http://www.prevent-abuse-now.com/pedoweb.htm - This website gives an overview of how pedophiles can use the Internet.

15. http://www.prevent-abuse-now.com/law3a.htm - This website provides information about Internet crimes against children.

16. http://www.stopsexoffenders.com/childsafety/internetsafetyguide.shtml - This website provides an Internet safety guide for children.

17. http://crime.about.com/cs/childrenindanger2/ - This website provides links to many articles about children and abuse.

18. http://www.isoc.org/internet/issues/children/ - This website provides articles and links concerning children and the Internet.

19. http://www.pedowatch.org/pedowatch/faq.htm - This is the website of an organization called Pedowatch. This organization is run by a private investigator in Colorado, and its purpose is to prevent children from being exploited online and offline.

20. http://familyinternet.about.com/library/weekly/aa062101a.htm - This site reports the results of a survey done by the Crimes Against Children Research Center. For example, one out of five children has been solicited for sex online.
