

## CYBERSPACE<sup>1</sup>: THE FINAL FRONTIER, FOR REGULATION?

*At the heart of the First Amendment lies the principle that each person should decide for him or herself the ideas and beliefs deserving of expression, consideration, and adherence. Our political system and cultural life rest upon this ideal.<sup>2</sup>*

### I. INTRODUCTION

The rapid growth of the Internet<sup>3</sup> has provided the opportunity for millions of people from around the world to communicate with each other almost instantaneously. While this emerging technology is making it easier for people to share ideas, it is also raising novel legal issues. This new technology will still confront and answer century old questions concerning governmental interference and regulation of speech and other communications.

The First Amendment and the fundamental principles of democracy favor the free flow of ideas.<sup>4</sup> The emerging technology of the Internet, with its ability to transmit nearly any kind of information anywhere, to anyone with a computer and modem, raises the issue that information should truly be "free flowing" and without restrictions. More specifically, policy makers continue to debate whether a person using the Internet has the same First Amendment protections while posting and receiving anonymous messages as persons who communicate through conventional media. Proponents for anonymity argue that the First Amendment commands that persons be allowed to share and receive information that otherwise may be harmful or embarrassing to the sender.<sup>5</sup> Conversely, opponents argue that a person's ability to post anonymous messages on the Internet is harmful because it allows "cyber-criminals" to shield themselves from accountability and responsibility in posting illegal or abusive messages.<sup>6</sup>

This article will discuss the concept of anonymity on the Internet and argue for its protection. Part II provides background information on the Internet and illustrates the prominence the Internet has in today's global society.<sup>7</sup> Part III discusses the concept of anonymity and its importance in our daily communications and how these principles necessarily extend to online communication.<sup>8</sup> Part IV outlines the purported justifications for regulating Internet content,<sup>9</sup> which is followed by Part V discussing current and attempted regulations of the Internet. This article then argues for the full protection of online anonymous speech as mandated by fundamental principles of "free speech," the traditions of our right to remain anonymous, and our notions of privacy. Finally, Part VII concludes by maintaining that self regulation of the Internet is preferable to intrusive governmental regulation.

### II. HISTORY AND ORIGINS OF THE "NET"

The Internet or "Net" is "a loose collection of millions of computers at sites throughout the world sharing information and files."<sup>10</sup> Various computers connect together to create a system and, in turn, numerous systems form a network.<sup>11</sup> Thousands upon thousands of local networks then connect, with communication software managing the

communications between them.<sup>12</sup> This comes together to form what the everyday computer-user has come to know as the Internet.

The Internet's humble beginnings trace back to the cold war period of the 1960s.<sup>13</sup> Technology was thought to be the key to winning the Cold War and the fields of science and computers grew dramatically from the perception of fear existing at the time.<sup>14</sup> By the end of the 1960s, the Department of Defense (DOD) created the Advanced Research Project Agency Network (ARPANET) to connect the DOD's computers.<sup>15</sup> Shortly after ARPANET, the government encouraged the development of other networks mainly from academic and scientific communities.<sup>16</sup> Thus, what started as a research and investigative tool for the government quickly transformed into a network of networks and the "Internet" was born.

"To fully appreciate the legal complexities of regulating the Internet, one must first understand the magnitude of the Internet."<sup>17</sup> The Internet is growing at an astounding rate<sup>18</sup> with an estimated 10 percent increase in users every month.<sup>19</sup> This translates to roughly one million new users per month.<sup>20</sup> With such an explosive growth rate and potential,<sup>21</sup> the Internet's unregulated and free flowing nature has been compared to the Wild West.<sup>22</sup> The recent attempts of regulation of the Internet have come about largely because of the previously unrestricted nature of this medium and what some fear as having a high potential for abuse.<sup>23</sup>

The Internet is not owned or controlled by any one group or person.<sup>24</sup> If the government were to attempt regulation of the Internet, the FCC would likely be the body to assert such control, but has yet to indicate any willingness to do so.<sup>25</sup> This is probably because of the inherent difficulty in such a task.<sup>26</sup> The reluctance in attempted regulation is due to the Internet's decentralization.<sup>27</sup> The widespread and immediate transfer of information may make regulation simply unworkable and practically unenforceable.

Despite this decentralization, there is currently some control on the Internet. The most direct control comes from the Internet Society ("Society").<sup>28</sup> This organization is an international body of volunteers which acts as an advisor regarding emerging issues and concerns on the Internet.<sup>29</sup> As a voluntary, advisory organization the Society cannot effectively deal with the important legal issues applicable to the Internet.<sup>30</sup> Instead, the Society deals with technical advances and how to ensure continued growth of the Internet.<sup>31</sup> Many members of the Internet community, who are themselves Society members, may resist any type of self-regulation, fearing that this may be perceived as a form of self-censorship which is contrary to the basic ideals upon which the Internet was founded.<sup>32</sup> Moreover, many Internet users feel this lack of direct control is the ultimate value of the Internet and they view it as a pure form of democracy, where people trade ideas freely and information is equally available to everyone.<sup>33</sup>

Unfortunately, this free exchange of ideas and information invites those who may want to take advantage of such access such as computer thieves, terrorists, con artists, pedophiles, and pornographers.<sup>34</sup> Therefore, it may be argued that the new opportunities available to

the cyber-criminal provide the needed and compelling justifications for regulation of the Internet, including mandating user identification.<sup>35</sup>

### III. ANONYMITY ON THE INTERNET

The ability to remain anonymous in our everyday life is a valuable and protected concept.<sup>36</sup> Our judicial system has recognized the importance of anonymity in litigation allowing the use of pseudonyms to shield plaintiff's identities in cases dealing with sensitive issues.<sup>37</sup>

Everyone possesses the ability to communicate anonymously in everyday interaction. People may send mail and make phone calls without revealing their identity, or voice their opinions in letters to the editors which do not have to be signed.<sup>38</sup> This ability to remain anonymous dictates the way many of us choose to communicate, even if this influence is indirect or unconscious. While the morality and social significance of anonymity could be debated endlessly,<sup>39</sup> it is useful to examine anonymity's place online and exactly how it is achieved on the Internet.

In communicating on the Internet, many users subscribe to a Usenet newsgroup.<sup>40</sup> Each Usenet newsgroup hosts an ongoing discussion on a particular subject.<sup>41</sup> Once a user has subscribed to a newsgroup it is possible for that user to post messages to the group and read messages that other subscribers have posted.<sup>42</sup> Ordinarily, when a message is posted to the Usenet, the e-mail message will have information which allows the Internet to transfer the message successfully to a particular newsgroup.<sup>43</sup> The message will ordinarily identify the place of origin and the sender.<sup>44</sup> Thus, even with the use of a pseudonym, the message usually contains the e-mail address, making it quite easy to trace the message back to a particular person or computer. This is mainly a convenience aspect allowing for easy exchange among group members who engage in regular conversations. However, the means are now available to ensure greater anonymity on the Internet.<sup>45</sup>

One easy way to maintain anonymity is with the use of a pseudonym. This enables the sender to remain semi-anonymous with the ultimate identity being known only to the system operator.<sup>46</sup> A second and increasingly more popular way to remain anonymous is through the use of a remailer service.<sup>47</sup> A remailer allows the sender to first e-mail messages to a service provider, thereafter, the remailer strips all identifying information from the message.<sup>48</sup> The message is then sent to its intended destination, with the recipient being unable to identify from whom or where it came.<sup>49</sup>

A sender may still be traceable with the use of a single remailer service.<sup>50</sup> However, if a sender utilizes various remailers, sending a single message through a series of remailers, the sender remains almost completely untraceable.<sup>51</sup> Therefore, if the sender is determined to remain anonymous, he or she has the technology and resources available to do so. Thus, the remailer serves as a valuable tool to ensure free speech takes place on the Internet.<sup>52</sup>

#### IV. PURPORTED JUSTIFICATIONS FOR REGULATING INTERNET CONTENT

The extraordinarily fast development of the Internet is providing vast communication and commercial opportunities.<sup>53</sup> Today, the areas of the law receiving the most attention on the Internet are intellectual property issues, including trademarks, copyrights, patents, trade secrets, and licensing.<sup>54</sup> Other "traditional" legal issues are also emerging, including personal jurisdiction issues,<sup>55</sup> bank and consumer fraud,<sup>56</sup> attorney advertising on the Internet,<sup>57</sup> and a multitude of others issues<sup>58</sup> as they intersect with the Internet. While these issues are legitimate areas for concern, a small group of other crimes have emerged as the rallying cry for mandatory user identification on the Internet, such as crimes involving pornography, pedophilia, and hate crimes.<sup>59</sup>

The major disadvantage or cost to society of online anonymity is its elimination of accountability. Anonymity becomes a shield for a cyber-criminal to hide behind in evading detection of immoral or illegal activity.<sup>60</sup> In recently discussing the problem with anonymity Justice Scalia commented, "It facilitates wrong by eliminating accountability, which is ordinarily the very purpose of anonymity."<sup>61</sup>

Another major disadvantage to online anonymity is the cost of attempted enforcement of criminal violations of statutes which regulate such anonymous communications on the Internet.<sup>62</sup> This may cause lawmakers to ultimately shift liability and accountability to the Internet provider or system operator instead of the individual user.<sup>63</sup> However, the ultimate cost would be borne by the entire Internet customer base as system operators would pass their costs on to customers.<sup>64</sup>

The ability to easily access and download pornographic images via the Internet has been used as one of the central arguments in favor of user identification.<sup>65</sup> The protection of society from obscene and indecent material is well established<sup>66</sup> and must still be confronted head-on in the computer medium. This pornography debate will continue to be a prominent justification for government interference.<sup>67</sup> There is a great deal of pornographic material available on the Internet, as it has been estimated that "more than eighty-three percent of all images stored in Usenet newsgroups are pornographic and nearly fifty percent of all downloads from commercial bulletin boards depict child pornography, incest, torture, or mutilation."<sup>68</sup> However, the ability to regulate pornographic materials on the Internet based on the traditional "community standards"<sup>69</sup> analysis may prove unworkable. The Internet has created a "global community," where the standard of one community may be unacceptable in a constituent community located thousands of miles away.<sup>70</sup>

The strongest justification for government interference involving pornography involves material directed at children. The majority of pornographic material on the Internet is supposedly available only on adult bulletin boards, which require users to reveal their identity to providers of such material.<sup>71</sup> There is little, if any, debate that child pornography via the Internet can not be regulated.<sup>72</sup> However, the real issue is not whether such "adult" material may come into the hands of children, because, in fact, it is documented that children may access such material rather easily.<sup>73</sup> The real danger is

when adult pedophiles deceptively utilize their computers to communicate with children in public chat rooms,<sup>74</sup> which raises the danger of adults luring the children from their homes into real face-to-face meetings.<sup>75</sup> Such fears seem to be more real than imagined, which provides a significant justification for some sort of regulation to protect children.<sup>76</sup>

The Internet can also be utilized to advance the ideas of racial or ethnic discrimination and hate.<sup>77</sup> These types of groups now have a global outlet for their rage and hate filled messages. Further, the Internet can be used on a much more personal and terrifying level to prey and stalk individuals.<sup>78</sup> The online pervert or psychopath has an ultimate weapon in the form of a personal computer and a phone line to harass or threaten their victims while remaining safely at home, hiding behind the anonymous protection of the Internet.<sup>79</sup> Therefore, with the increased use of computers and the Internet in the participation of such crimes, the perception for the need for regulation has also increased resulting in both state and federal legislation attempting to regulate the Internet.<sup>80</sup>

## V. CURRENT REGULATIONS GOVERNING THE INTERNET

### A. State Legislation

A few states have recently passed laws which basically prohibit online anonymity. Connecticut passed a statute which prohibits anyone from addressing another with the "intent to harass, annoy, or alarm" the other by communicating via a computer Network.<sup>81</sup> However, the Act does not define what is "annoying, harassing, or alarming." The argument can always be made that any anonymous message is "alarming" depending on the subject of the message and the sensitivity and discretion of the judge. Thus, the statute suffers from being overly broad and vague in this respect.

Similarly, a Pennsylvania statute makes it illegal to "program, possess, or use a device which can be used to conceal or assist another to conceal...the existence or place of origin or of destination of any telecommunication."<sup>82</sup> Also, a Georgia statute makes it unlawful for any person or organization to "knowingly transmit any data through a computer network...if such data uses any individual name...to falsely identify the person."<sup>83</sup>

### B. Attempted Federal Regulation

The most chilling example of overbroad regulation to date governing the Internet came with the federal Communications Decency Act of 1996 (CDA) portions of which, similar to the state statutes, prohibited anonymous messages intended to annoy or harass the recipient.<sup>84</sup> The constitutionality of the Act was immediately challenged after it was signed by the president, and portions of the law were eventually declared unconstitutional.<sup>85</sup>

The CDA's key provisions were primarily concerned with minors and their access to "indecent" or "offensive" material.<sup>86</sup> However, a main provision of the Act did directly prohibit anonymity as well.<sup>87</sup> The District Court<sup>88</sup> in *ACLU v. Reno* held that the CDA was unconstitutional as it violated the First and Fifth Amendments as there is no effective

way to determine the identity or age of a user who is accessing this type of "indecent" or "obscene" on-line material.<sup>89</sup>

Further, the Supreme Court recently upheld the District Court's decision that Congress did violate the First Amendment with its attempts at Internet Regulation via the CDA,<sup>90</sup> as the statute was an attempt to regulate content.<sup>91</sup> Justice Stevens writing for the Court stated:

We are persuaded that the CDA lacks the precision that the First Amendment requires when a state regulates the content of speech. In order to deny minors access to potentially harmful speech, the CDA effectively suppresses a large amount of speech that adults have a constitutional right to receive and to address to one another.<sup>92</sup>

The Court concluded that such vagueness and sweeping breadth would impermissibly chill protected speech and that the statute was therefore unconstitutional.<sup>93</sup>

The District and Supreme Court decisions recognized the value that should be afforded to online anonymity. The District Court stated "[a]nonymity is important to Internet users who seek to access sensitive information, such as users of the Critical Path AIDS Project's Web site, the users, particularly gay youth, of Queer Resources Directory, and users of Stop Prisoner Rape."<sup>94</sup> Such anonymity and lack of direct governmental control or censorship enhances the value of the Internet as the most effective form of communication.<sup>95</sup>

The Supreme Court's decision is a landmark on the emerging intersection between the Internet and our civil liberties.<sup>96</sup> For the first time, the Court emphasized the uniqueness of the Internet as a distinct medium and signaled how future restrictions of similar content based on-line communications would be held to the highest level of review.<sup>97</sup> Thus, the Court has seemingly clarified its position with respect to the Internet, giving some concrete positions on how cyberspace will in fact be regulated in the future.<sup>98</sup>

## VI. PROTECTING ONLINE ANONYMOUS SPEECH

### A. Fundamental Principles of "Free Speech"

The First Amendment states that, "Congress shall make no law abridging the freedom of speech, or of the press, or the right to peacefully assemble, and petition the government for a redress of grievances."<sup>99</sup> Our government, society and every citizen has come to view these protections as mandating the widest and most far reaching means of communication possible.<sup>100</sup>

As the Internet provides for the greatest and quickest dissemination of information ever imagined,<sup>101</sup> this new form of communication must be given the same protections valued by our founding fathers.<sup>102</sup> The Internet, while still in its infancy, stands to be the biggest tool for changing society and the way we think about virtually every social and political issue.<sup>103</sup> In fact, in recently describing the Internet, Bill Gates, CEO and co-founder of

Microsoft Corporation, commented, "It's a phenomenon. It's a gold rush. It's a mania. It's beyond anything I've ever experienced."<sup>104</sup> The protections of the First Amendment must necessarily extend to this revolutionary "phenomenon" in order to ensure every citizen of his or her individual rights<sup>105</sup> and to foster the growth and improvement of our government and society.<sup>106</sup>

Despite the previously mentioned disadvantages of anonymous online communication, there are also significant advantages, the most obvious being that anonymity tends to foster increased communication among large audiences.<sup>107</sup> Those people seeking sensitive or potentially embarrassing information can receive such information easily at little, if any, socially stigmatizing costs.<sup>108</sup> Society as a whole may eventually benefit from the sharing of such delicate information.<sup>109</sup> Further, the Internet may serve as a unique tool in fighting poverty and discrimination by allowing for all segments of society to have easily obtainable access to the same information.<sup>110</sup>

More importantly, "the decision in favor of anonymity may be motivated by fear of economic or official retaliation, by concern about social ostracism, or merely by a desire to preserve as much as one's privacy as possible."<sup>111</sup> Those seeking an outlet for criticizing governments, organizations, or employers, may fear such reprisals and their voice online may be their only outlet for their concerns.<sup>112</sup> In seeking to criticize a repressive regime or government, many may find online anonymity as one of their most powerful and effective tools in today's technological age.<sup>113</sup>

## B. Historical Right to Remain Anonymous

While there is no specific enumerated right to anonymity in the Constitution,<sup>114</sup> the Supreme Court has come to recognize it as such a "right" and afford anonymity protection.<sup>115</sup> Moreover, the historical importance anonymity has played in forming our society illustrates and favors the extension of protecting online anonymity.

The "right" to anonymously voice our opinions and concerns has played a pivotal role in the formation of our country.<sup>116</sup> Virtually every important political actor at this time shielded himself with anonymity.<sup>117</sup> The Supreme Court in *Talley v. California*<sup>118</sup> recognized this importance and historical precedent stating:

Anonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind. Persecuted groups and sects from time to time throughout history have been able to criticize oppressive practices and laws either anonymously or not at all. The obnoxious press licensing law of England, which was also enforced on the Colonies was due in part to the knowledge that exposure of the names of printers, writers and distributors would lessen the circulation of literature critical of the government. The old seditious libel cases in England show the lengths to which government had to go to find out who was responsible for books that were obnoxious to the rulers. John Lilburne was whipped, pilloried and fined for refusing to answer questions designed to get evidence to convict him or someone else for the secret distribution of books in England. Two puritan ministers, John Perry and John Udal, were sentenced to death on charges

that they were responsible for writing, printing or publishing books. Before the Revolutionary War colonial patriots frequently had to conceal their authorship or distribution of literature that easily could have brought down on them prosecutions by English-controlled courts. Along about that time the Letters of Junius were written and the identity of their author is unknown to this day. Even the Federalist Papers, written in favor of the adoption of our Constitution, were published under fictitious names. It is plain that anonymity has sometimes been assumed for the most constructive purposes.<sup>119</sup>

The more recent United States Supreme Court case of *McIntyre v. Ohio Elections Commission*<sup>120</sup> reinforces the importance anonymous speech has played in our society and the willingness of the Court to extend its protection. In *McIntyre*, Margaret McIntyre distributed leaflets to persons at a public school meeting expressing her opposition to a school levy.<sup>121</sup> Mrs. McIntyre made the leaflets on her home computer and had additional copies produced by a professional printer.<sup>122</sup> She did not personally sign all the leaflets<sup>123</sup> and with her son's assistance she placed the leaflets on the windshields of cars in the school parking lot.<sup>124</sup>

Mrs. McIntyre was convicted under a Ohio statute which prohibited the distribution of election literature without the name of the person responsible for its circulation.<sup>125</sup> After a series of appeals up to and including the Ohio Supreme Court, the United States Supreme Court reversed her conviction.<sup>126</sup>

In discussing the importance of anonymity, the Court quoted from the language of Talley and noted the role of anonymity in the "progress of mankind."<sup>127</sup> The Court then went on to state, "Discussion of public issues and debate on the qualifications of candidates are integral to the operation of the system of government established by our Constitution. The First Amendment affords the broadest protection to...expression in order to assure the unfettered interchange of ideas for the bringing about of political and social changes by the people."<sup>128</sup> The *McIntyre* decision, therefore, strongly reaffirms that anonymous political speech is protected as a "core" First Amendment right.<sup>129</sup>

As the Internet has virtually become the modern day version of the printing press in revolutionizing the ability for the "lone dissenter" to disseminate his or her ideas and opinions to all segments of society, the *McIntyre* decision necessarily extends to and protects online anonymous political speech.<sup>130</sup> Furthermore, while the same threat that anonymous speech protected us from nearly two centuries ago is not as obvious, its dangers still exist to mandate the protections of such speech today and especially online.<sup>131</sup> It was a mere forty years ago that Senator Joseph McCarthy sought to persecute communist sympathizers in his attempt to "cleanse America of it's Communist influence"<sup>132</sup> after the end of World War II.<sup>133</sup> This "Red Scare" had a profound chilling impact on society overall<sup>134</sup> and only illustrates how quickly governmental power can be abused. This potential for abuse is even more pervasive today as the government also has the ability to exploit the recent advancements in information dissemination.

More importantly, while anonymity has historically been framed in terms of political discussions, "it now appears to encompass most forms of social interactions and relations

between people."<sup>135</sup> Various forms of modern communication and interaction place a high value on the ability to stay anonymous.<sup>136</sup> Thus, the McIntyre decision provides the groundwork for extending First Amendment protections to online communications which are not purely "political" in nature.<sup>137</sup>

The equalizing effect of the Internet allows virtually all segments of society to communicate with one another.<sup>138</sup> With such new found freedoms, the sharing of instantaneous ideas will contain various viewpoints in a single e-mail message. The ability of cyber-citizens to communicate in cyber-conversations in real time<sup>139</sup> means that what might begin as a "political" message can easily translate into a "non-political" one, and vice versa. Therefore, the ability to effectively separate the content of online messages simply cannot be done. "As a practical matter, therefore, it would be exceedingly difficult, and probably impossible, to craft a ban on anonymous speech on the Internet that distinguished between political and non-political speech and yet was enforceable."<sup>140</sup>

Any attempted regulation of online anonymity, therefore, becomes an attempted regulation of content, "since all speech inherently involves choices of what to say and what to leave unsaid."<sup>141</sup> Every speaker, even those online, has the right to tailor his or her views and speech under given circumstances and this, "applies not only to expression of value, opinion, or endorsement, but equally to statements of fact the speaker would rather avoid."<sup>142</sup> Such a right necessarily encompasses the ability for the speaker to choose not to reveal his or her identity.<sup>143</sup> Selective identity revelation is an important aspect for many people in communicating.<sup>144</sup> If some people are forced into revealing their identity, they may be effectively forced to not communicate at all.

Thus, the Internet in providing the most sweeping communication revolution ever, could fall prey to this chilling effect. The exact number of those foregoing online communication all together could not easily be estimated, but the impact would certainly be felt. A significant and specific segment of society who value anonymity and feel it is required for their social interaction with others would essentially be denied basic freedom of speech rights in this new medium. This effect cannot be justified against the First Amendment for, "[a] ban on specific group voices on public affairs violates the most basic guarantee of the First Amendment--that citizens, not the government, control the content of public discussion."<sup>145</sup>

In fact, the general nature of justifications for prohibiting anonymity based on offensive, indecent, or potentially dangerous speech further illustrates the point that any anti-anonymity regulation is basically content based as the "principal inquiry in determining content neutrality . . . is whether the government has adopted a regulation of speech because of agreement or disagreement with the message it conveys."<sup>146</sup>

The government is concerned with the supposed dangers lurking online.<sup>147</sup> However, such potential danger is not enough to warrant governmental regulation.<sup>148</sup> Any attempted regulation of anonymity will be far too reaching in its scope as there is no concrete harm to redress. Further, the government cannot effectively differentiate between messages it

has a right to control<sup>149</sup> and those it merely disfavors, such as those criticizing the government or its officials, those seemingly "indecent" and those simply distasteful or hateful.<sup>150</sup>

Those seeking to post such traditional forms of protected core First Amendment speech will be effectively denied their ability to share their ideas as the cloak of anonymity is stripped away. It appears the government is simply attempting to promote an interchange of ideas on the Internet of those it feels are appropriate for this new medium. Such forms of censorship and regulation cannot be tolerated as we can not allow the government to prohibit the exchange of ideas simply because some segments of society find the exchange offensive or alarming.<sup>151</sup>

Regulation of anonymity would necessarily have to survive a strict scrutiny analysis.<sup>152</sup> While the government's contention and argument of protecting the welfare of society and particularly children from online dangers appears compelling, "It is not enough to show that the government's ends are compelling; the means must be carefully tailored to achieve those ends."<sup>153</sup> Any attempted ban on anonymity will prove to be too vague<sup>154</sup> or overbroad and it will not help to solve any specific harm in a substantial or direct way,<sup>155</sup> and thus cannot survive a strict scrutiny analysis.

### C. Anonymity and Rights of Association and Assembly

Moreover, besides infringing on traditional free speech rights most associated with the First Amendment, a ban on online anonymity also infringes on other less obvious First Amendment and other constitutional rights.<sup>156</sup>

When we think of people gathering, we have visions of face to face meetings and communications such as town meetings or joining a particular group or affiliation which represents a particular cause we believe in. However, the Internet now allows people to engage in such meetings, become a member of a virtual community, or join such groups with such an ease as to facilitate probably more interaction and affiliation than ever before.<sup>157</sup> Nevertheless, the ability to have ones anonymity protected in joining a particular group or association is an recognized constitutional right and this right must, therefore, logically be extended online.<sup>158</sup>

The landmark decision in NAACP v. Alabama ex rel. Patterson<sup>159</sup> illustrates the fundamental protections afforded in the right to assemble or associate. In this case, the state of Alabama sought to expel the NAACP from the state for its alleged violation of a statute which required the registration of foreign corporations doing business in the state.<sup>160</sup> The state launched an investigation and the organization responded to a request in providing records of its activities but not a list of its members.<sup>161</sup>

The Court reversed a decision holding the NAACP for contempt in not revealing the membership list noting the importance of the right of privacy and association stating, "inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group

espouses dissident beliefs."<sup>162</sup> The Court has gone on to give such association and privacy rights extended protection.<sup>163</sup> This protection to privacy in association has come to include a vast array of activities and organizations we may feel are important enough for our participation.<sup>164</sup>

The ease of the Internet provides the ability and motivation for people to join a multitude of organizations they may have otherwise not. The home computer user simply has to pull-up an organization's home page and begin a dialogue. All the while the identity of the person is being protected. This ease will facilitate more and more people to join in a particular association or organization. There is no potential embarrassment or harassment in participating online, no chance your neighbor will "catch" you coming out of the group's field office or organizational meeting.

The person who uses their computer to associate with a particular group necessarily is afforded those same privacy rights.<sup>165</sup> By mandating user identification, there exists the chance that someone cyber-surfing may stumble upon the individual in an exchange with the organization. Further, a prohibition on anonymity would infringe on the rights of the organization itself in not being able to ensure the privacy of its member's identity among its own members or the public.<sup>166</sup>

Furthermore, traditional concepts of privacy are also infringed upon with a prohibition of online anonymity.<sup>167</sup> It goes against our basic notions that the government would be able to reach into our homes and have such a direct and formidable restriction on a method by which many may choose to communicate.<sup>168</sup> By prohibiting anonymity online, the State is effectively entering our castle<sup>169</sup> and telling us we cannot communicate, from the privacy of our own home, in a way we otherwise are protected in doing.<sup>170</sup>

## SELF-REGULATION AS AN EFFECTIVE ALTERNATIVE

### TO GOVERNMENT REGULATION

The government's attempt to regulate any aspect of the Internet may be unwarranted. The Internet has and will continue to regulate itself in a much more productive way than any broad attempts the legislature may take.<sup>171</sup>

The ever changing technology on the Internet means traditional concepts of law and regulation are too static and cannot effectively govern cyberspace.<sup>172</sup> Regulations that have been applied to other forms of mass-media, such as television and radio, may prove unworkable in the interactive cyberspace world. In those traditional broadcast areas, regulations have been upheld because of the unique and pervasive characteristics that television and radio have taken in society and most of our homes in allowing programs to be accessed by children with great ease.<sup>173</sup>

These concerns are not present on the Internet.<sup>174</sup> This medium, while pervasive in some regards, is uniquely interactive.<sup>175</sup> Users must actively seek out any information they wish to receive.<sup>176</sup> If the government or parents are concerned because of the material

that may fall into their children's hands, there are existing technologies to block or filter such materials.<sup>177</sup> Parents must take the responsibility and utilize such software to ensure what materials are being transmitted into their homes.<sup>178</sup>

For example, most online service providers have developed certain "blocking" software options<sup>179</sup> which allows users to limit exposure to potentially inappropriate, indecent, or "dangerous" material. In fact, some screening software allows the user to block access to all Internet sites except for those the parent specifically chooses to make accessible.<sup>180</sup> Thus, a parent can institute such precautions and take the responsibility for what material their child is seeking out and is being transmitted into their home.

Furthermore, if the concern is that anonymity may allow deceptive communications in the luring of children from their homes, the same accountability concept should adequately answer such concerns. The parents must take an active role in guiding their child through the computer revolution.<sup>181</sup> An adult's freedom in accessing sensitive or distasteful information while being protected with anonymity cannot give way to the paternalistic fears we may have over our children.<sup>182</sup>

Parents should and must take the appropriate precautions instead of allowing the government to regulate the Internet. The industry has provided the tools for parents, they must now implement them.<sup>183</sup> "Anything less will reduce the Internet to a playground fit only for children, transforming the vast library of the Internet into a children's reading room, whereby only subjects suitable for children could be discussed."<sup>184</sup>

Moreover, the online community has developed its own "laws" or standards of behavior. These standards are known as "cyber-etiquette" or "Netiquette."<sup>185</sup> Such norms generally reflect the common real-life community concerns that most are worried about preserving on the Net. Nevertheless, these norms provide the basic rules on the information highway and allow members online to effectively punish those who breach the established norms.<sup>186</sup>

A recent example illustrates the power that the online cyber-citizens possess. The case was that of "Mr. Bungle."<sup>187</sup> Mr. Bungle was a member of a MUD or multi-user dimension.<sup>188</sup> A MUD is basically a virtual community in cyberspace allowing members to interact with one another by the sharing of e-mail messages.<sup>189</sup>

Mr. Bungle committed several disgusting acts of rape and violence against several other members of this virtual community.<sup>190</sup> His actions were so vile, so contradictory to the common norms of Netiquette, that the vast majority of members in the MUD decided to "toad" Mr. Bungle.<sup>191</sup> This "toading" basically erases the person's account from the Internet service and he or she is no longer part of this particular cyber-community.<sup>192</sup> Mr. Bungle was banished from this portion of cyberspace by breaching standards established by other users in the same domain. His story illustrates that the online community is not wholly unregulated and that it does police itself from those who users feel may pose a danger to society, even the cyber-society.

This type of self policing and regulation may prove to be the only workable standards in this new and revolutionary medium. In fact, recent legislative attempts at regulating some aspects of the Internet have so far proven to be ineffective and undesirable,<sup>193</sup> the most prominent example of which has been the Communication Decency Act.<sup>194</sup>

## VIII. CONCLUSION

The First Amendment is the cornerstone of our Independence. Society has come to value the freedom of speech and expression more than any other of our Constitutional rights. Thus, the First Amendment and its protections have had to continuously adapt to new and unique circumstances and technologies in order to secure these ideals.<sup>195</sup>

The Internet, as a new and developing technology, tends to scare those who have a limited understanding of its capabilities and place in society. This feeling of uneasiness with new forms of communications and expression have in the past been used in attempts to limit our core First Amendment protections.<sup>196</sup> Besides our basic fears and ignorance of the Internet, there does appear to be some "compelling" justifications for attempted prohibitions against online anonymity, including pornography, pedophilia, and hate crimes.<sup>197</sup>

Online anonymity has been argued as a major cost to society in eliminating accountability, allowing cyber-criminals to evade law enforcement and responsibilities for their Internet-crimes.<sup>198</sup> Such potential costs and disadvantages do not, however, provide the compelling justification one must show to survive a strict scrutiny test under our well-established Constitutional doctrine. The sharing of ideas, sensitive information, and general public discourse on virtually every social and political issue are all fostered by the ability of the Internet-user to feel secure, for whatever reason, in not revealing his or her identity. This is especially true for those who the Internet may be their only way to gain and share sensitive information regarding such topics as AIDS or child abuse support groups, or those seeking to criticize their government or employer.

The basic principles of free speech mandate the widest and most far reaching means of communication possible.<sup>199</sup> The Internet's ability to almost instantaneously transmit information and ideas to millions of people and this Nation's strong reaffirmance in unrestricted political speech, mandates that our basic First Amendment rights survive online. "[T]he life of the First Amendment has not been logic, it has been experience."<sup>200</sup> Our history and experience tells us that we afford "greater weight to the value of free speech than to the dangers of its misuse."<sup>201</sup> The potential and fear of misuse of the Internet, cannot justify over-reaching regulations encroaching on basic civil liberties.

**JAY KRASOVEC**

1The author has used the generic term "cyberspace" to encompass the use of electronic communications over computer networks mainly via the Internet. The Internet is only a small portion of "cyberspace." Anne M. Fulton, Comment, *Cyberspace and the Internet: Who Will Be the Privacy Police?*, 3 *COMMLAW Conspectus* 63, 63 (1995).

Realistically, cyberspace "encompasses all electronic messaging and information systems including: Bulletin Board Systems . . . ; commercial data services; research data networks; electronic publishing; public and 'private' networks and network nodes; e-mail systems; data banks with personal medical, credit, membership, purchasing habit, and census information; electronic data interchange systems; and electronic fund transfer systems." *Id.* The term "cyberspace" is originally attributable to the science fiction author William Gibson in his novel *Neuromancer*. EDWARD A. CAVAZOS & GAVINO MORIN, *CYBERSPACE AND THE LAW: YOUR RIGHTS AND DUTIES IN THE ONLINE WORLD* 1 (1994); see also Michael Johns, Comment, *The First Amendment and Cyberspace: Trying to Teach Old Doctrines New Tricks*, 64 *U. CIN. L. REV.* 1383, 1383 (1996) (defining cyberspace as the "conceptual space where words, human relationships, data, wealth, and power are manifested by people using computer technology.") (see also HOWARD RHEINGOLD, *THE VIRTUAL COMMUNITY* 5 (1993)).

2*Turner Broadcasting Sys. v. F.C.C.*, 114 S. Ct. 2445, 2458 (1994); see also *Associated Press v. United States* 326 U.S. 1, 20 (1945) (noting that the First Amendment "rests on the assumption that the widest possible dissemination of information from diverse and antagonistic sources is essential to the welfare of the public."); *Roth v. United States*, 354 U.S. 476, 484 (1957) ("The protection given speech and press was fashioned to assure unfettered interchange of ideas for the bringing about of political and social changes desired by the people"); *Stanley v. Georgia*, 394 U.S. 557, 598 (1969) ("If the First Amendment means anything, it means that a State has no business telling a man, sitting alone in his house, what books he may read or what films he may watch.").

3"The 'Internet' is a worldwide system of interconnected computers and computer networks." Henry H. Perritt, Jr., *What is the Internet?*, in *WHAT LAWYERS NEED TO KNOW ABOUT THE INTERNET*, at 11, 13 (PLI Pat., Copyrights, Trademarks, and Literary Prop. Course Handbook Series No. 443, 1996); see Amy Knoll, Comment, *Any Which Way But Loose: Nations Regulate the Internet*, 4 *TUL. J. INT'L & COMP. L.* 275, 277 (1996) (defining the Internet as "a vast web of telecommunication links--a worldwide web--connecting computers all over the world."); John Zanghi, "Community Standards" in Cyberspace, 21 *U. DAYTON L. REV.* 95, 106 (1995) (stating the Internet comprises the biggest portion of cyberspace and "[u]ntil something better comes along to replace it, the Internet is cyberspace.") (quoting Philip Elmer-DeWitt, Special Issue: Welcome to Cyberspace, *TIME*, Spring 1995, at 9).

4See Anne W. Branscomb, *Anonymity, Autonomy, and Accountability: Challenges to the First Amendment in Cyberspaces*, 104 *YALE L.J.* 1639, 1639 n.2 (1995) ("[A]ssuring that the public has access to a multiplicity of information sources is a governmental purpose of the highest order, for it promotes values central to the First Amendment.") (quoting *Turner Broadcasting Sys. v. F.C.C.*, 114 S. Ct. 2445, 2470 (1994)).

5See infra notes 108-10 and accompanying text.

6See infra notes 60-64 and accompanying text.

7See infra notes 10-35 and accompanying text.

8 See infra notes 36-52 and accompanying text.

9 See infra notes 53-80 and accompanying text.

10Paul H. Arne, *New Wine in Old Bottles: The Developing Law of the Internet*, in *INTELLECTUAL PROPERTY LAW INSTITUTE: 1995*, at 9, 13 (PLI Pat., Copyrights, Trademarks, and Literary Prop. Course Handbook Series No. 416, 1995).

11Giorgio Bovenzi, *Liabilities of System Operators on the Internet*, 11 *BERKELEY TECH. L.J.* 93, 97 (1996) ("Thousands of local networks connect in a sort of spider's web in which communication software . . . manages communications between computers. The user perceives the system to be a unique network: the Internet.").

12The software is called Transmission Control Protocol/Internet Protocol (TCP/IP). *Id.*; see also *THE INTERNET UNLEASHED 1996* 4 (Alice M. Smith et al. eds., 1995). The authors note the Internet is the network of networks connected using protocols standardized by TCP/IPs. "The number of networks linked to the Internet is now in excess of 45,000 with approximately 5 million host computers connected to these networks." *Id.* Network growth is continuing and many countries have numerous networks linked to the Internet including: Australia (825), Austria (377), Belgium (123), Brazil (162), Canada (3,295), Chile (86), Czech republic (369), Ecuador (85), Finland (605), France (1,843), Germany (1,620), Greece (95), Hong Kong (80), Hungary (163), Indonesia (50), Ireland (167), Israel (195), Italy (478), Japan (1,669), South Korea (449), Mexico (114), Netherlands (350), New Zealand (354), Norway (211), Peru (116), Poland (131), Portugal (92), Russian Federate (369), Singapore (101), Slovakia (69), South Africa (363), Spain (252), Sweden (356), Taiwan (632), Thailand (77), Turkey (90), Ukraine (52), Untied Kingdom (1,394), United States (26,681). *Id.* at 26-27, Table 3.1.

13*THE INTERNET UNLEASHED 1996*, supra note 12, at 10; see also *Shea ex rel. American Reporter v. Reno*, 930 F. Supp. 916, 925-27 (S.D.N.Y. 1996) (discussing the development of the Internet and its beginnings as an experimental project of the Department of Defense's Advanced Research Projects Administration).

14*THE INTERNET UNLEASHED 1996*, supra note 12, at 10. "By the late 1960s every major federally funded research center, including for-profit business and universities, had a computer facility equipped with the latest technology that America's burgeoning computer industry could offer." *Id.*

15Jo-Ann M. Adams, *Controlling Cyberspace: Applying the Computer Fraud and Abuse Act to the Internet*, 12 SANTA CLARA COMPUTER & HIGH TECH. L.J. 403, 405 (1996).

16Id. at 405-06. A major development by the government was the National Science Foundation (NSF) net. Id. at 405. This network linked a few supercomputer research centers with researchers at remote academic and government institutions. Id. The NSF network began to expand dramatically and is primarily responsible for shaping the modern Internet. Id. at 406-07. See also Arne, *supra* note 10, at 14 (discussing the early formation of the Internet as a tool for the research and academic community).

17Adams, *supra* note 15, at 406-07. Adams notes the government developers had not totally envisioned the monster they were creating and its ramifications, Adams notes one of the main developers initial reaction to the DOD request was: "Sure we could build such a thing, but I don't see why anybody would want it." Id. (quoting Gary Anthes, *The History of the Future: As the ARPNET Turns 25, its Founders Reunite to Talk About the Network That Became the Internet*, COMPUTERWORLD, Oct. 3, 1994, at 101).

18George P. Long, III Comment, *Who are You?: Identity and Anonymity in Cyberspace*, 55 U. PITT L.REV. 1177, 1178 (1994) (noting that the Internet is conservatively estimated to connect well over twenty million people) (quoting Barbara Kantrowitz et al, *Live Wires*, NEWSWEEK, Sept. 6, 1993 at 42,43); see also Adams, *supra* note 15, at 406-07 (stating the Internet is growing at the rate of five to eight percent per month and reaches ninety-two countries) (quoting Joe Clark, *The Online Universe: Find Out Why Some 30 Million People Count Themselves as Citizens of this Mysterious World*, TORONTO STAR, Oct. 20, 1994, at J1; *Internet Crime Soars*, INFORMATIONWEEK Oct 10, 1994, at 20).

19THE INTERNET UNLEASHED 1996, *supra* note 12, at 4. The authors note the Internet "is the largest international association of people . . . and is growing everyday." Id. "The number of networks linked to the Internet now is in excess of 45,000 with approximately 5 million host computers." Id.

20Long, *supra* note 18, at 1178 (quoting Philip Elmer-Dewitt, *First Nation in Cyberspace*, TIME, Dec. 6, 1993, at 62). Long notes that the Internet is really the forerunner of the so called "information superhighway" and it will be vital in helping to form a new national information infrastructure. Id.

21See generally Richard Wiley and Robert Butler, *National Information Infrastructure: Preserving Personal Space in Cyberspace*, 12-Fall COMM. LAW. 1 (1994) (discussing the power of electronic media and online communications have in informing the public and shaping the way we conduct both our professional business and personal relationships and the problems such potential brings in the form of intruding on our perceived privacy); Richard Carelli, *Supreme Court Agrees to Decide on Restricting Access to the Internet*, CLEVELAND PLAIN DEALER, Dec. 7, 1996 at A12 (noting that it is difficult to estimate the size of the Internet because of its rapid growth).

22Adams, *supra* note 15, at 408 (defining the Wild West as the western United States in its frontier period (citing WEBSTER THIRD NEW INTERNATIONAL DICTIONARY OF THE ENGLISH LANGUAGE Unabridged 2616 (3d ed. 1986))); see also Long, *supra* note 18, at 1181 (comparing the Internet today "to the American West of the 1800s: an uncharted 'electronic frontier' that has yet to be fully explored.") (citing ELECTRONIC FRONTIER FOUNDATION, BIG DUMMY'S GUIDE TO THE INTERNET (1993)).

23 See *infra* Part IV.

24THE INTERNET UNLEASHED 1996, *supra* note 12, at 4 (noting the Internet is a cooperative venture with no central authority that began as an education and scientific network). See also *ACLU v. Reno*, 929 F. Supp. 824 (E.D. Pa. 1996). "The Internet is an international system." *Id.* at 831. It is "a decentralized, global medium of communications--or 'cyberspace'--that links people, institutions, corporations, and governments around the world. . . . This communications medium allows any of the literally tens of millions of people with access to the Internet to exchange information." *Id.* "No single entity--academic, corporate, governmental, or non-profit--administers the Internet. It exists and functions as a result of the fact that hundreds of thousands of separate operators of computers and computer networks independently decided to use common data transfer protocol to exchange communications and information with other computers (which in turn exchange communications and information with still other computers)." *Id.* at 832.

25Adams, *supra* note 15, at 408. See also Fulton, *supra* note 1, at 69 (stating the FCC has "determined that it will not regulate computer communication in any manner different from voice communication" and "[w]ithout direction from Congress, the FCC will continue to regard computer communications as being outside the realm of regulation.").

26See *ACLU v. Reno*, 929 F. Supp. 824, 832 (E.D. Pa. 1996) ("There is no centralized storage location, control point, or communications channel for the Internet, and it would not be technically feasible for a single entity to control all of the information conveyed on the Internet.").

27Long, *supra* note 18, at 1181 (arguing the same decentralization of the Internet that makes it difficult to use in exploring and searching for subjects, will also make it difficult if not impossible to regulate in any effective manner).

28THE INTERNET UNLEASHED 1996, *supra* note 12, at 31. The Society is a voluntary body whose stated goal is:

The Society will provide assistance and support to groups and organizations involved in the use, operation, and evolution of the Internet. It will provide support for forums in which technical and operational questions can be discussed and provide mechanisms through which the interested parties can be informed and educated about the Internet, its function, use, operation, and the interest of its constituents.

Id.

29Id. at 31-32.

30 Id. at 4.

31Id.

32See Adams, *supra* note 15, at 408. (stating the Internet's "roots lie in liberal U.S. academic institutions, and freedom of speech and an 'anything goes' credo are vital components of 'Internet ethos'") (quoting Malcom Wheatley, Auntie Ventures into Taboo Zone, *THE INDEPENDENT ON SUNDAY*, July 31, 1994, at 12).

33Long, *supra* note 18, at 1182 (noting that with this benefit comes the potential for abuse).

34Adams, *supra* note 15, at 404. Adams goes on to note that because of its rapid expansion, "The Internet has developed its own dark alleys and red light districts." *Id.*

35 See *infra* Part IV.

36See Note, The Constitutional Right to Anonymity: Free Speech, Disclosure and the Devil, 70 *YALE L.J.* 1084 (1961) (tracing the history and importance of anonymous writing in our society and early case law developments leading up to what the authors call the constitutional right to anonymity). See also Saul Levmore, The Anonymity Tool, 144 *U. PA. L. REV.* 2191 (1996) (discussing the legal and social rules and norms surrounding anonymity, stating, "If parties with valuable information can choose between making anonymous and non-anonymous communication, it is likely they will convey more (or simply more accurate) information than they would in a world where anonymous communications are effectively barred by social conventions or enforceable legal rules. Anonymity allows communication without retribution.") *Id.* at 2192-93.

37The best example is *Roe v. Wade*, 410 U.S. 113 (1973) (confronting the controversial issue of a woman's constitutional right to abortion). See also *Doe v. Bolton* 410 U.S. 179 (1973) (the companion case to *Roe v. Wade*). See generally Adam A. Milani, *Doe v. Roe: An Argument for Defendant Anonymity when a Pseudonymous Plaintiff Alleges a Stigmatizing Intentional Tort*, 41 *WAYNE L.REV.* 1659 (1995); Joan Steinman, *Public Trial, Pseudonymous Parties: When Should Litigants be Permitted to Keep Their Identities Confidential?*, 37 *HASTINGS L.J.* 1 (1985); Wendy M. Rosenberger, Note, *Anonymity in Civil Litigation: The "Doe" Plaintiff*, 57 *NOTRE DAME L. REV.* 580 (1982).

38But see I. Trotter Hardy, *The Proper Legal Regime for "Cyberspace"*, 55 *U. PITT. L. REV.* 993, 1011-12 (1994). Hardy notes that such traditional forms of anonymous communications such as letters and phone calls have a semi built-in deterrence due to some added costs such as mailing and the time constraints in making phone calls in

addition to being more likely to leave a paper trail. Id. These forms of communications lack the ability to reach thousands, perhaps millions, of people almost instantaneously like electronic forms of communications such as e-mail. Id. at 1012 & 1027 n.80. Thus, while anonymity may be available to us presently in these traditional forms, the new medium of cyberspace drastically reduces their current deterrent elements so as to make the "problem of anonymity . . . a 'new' one." Id. at 1011-12.

39See Michael Froomkin, Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases, 15 J.L. & COM. 395, 402 (1996) ("There is no consensus, nor is there likely to be, as to whether, on balance anonymity is good. Anonymity has both valuable and harmful consequences, and different persons weigh these differently."); see also Levmore, supra note 36 (outlining the use of anonymity in society and how it may encourage some communications).

40See E. Brian Davis, A Look at One of the Most Popular Services in Cyberspace: Usenet, 42 FED. LAW. 15 (July 1995). Davis defines a Usenet newsgroup as "a discussion area designed to allow the exchange of 'articles' or 'posts' sent to the newsgroup. Id. Each article can be accessed by everyone subscribed to the newsgroup. Id. Follow-ups can then be sent to the newsgroup to engage the discussion, or a reply can be sent only to the person who posted the original article." Id. See also Long, supra note 18, at 1181-82 (describing the difference between the Internet and the Usenet as the Usenet existing as a part on the Internet but is more confined in its application). See THE INTERNET UNLEASHED 1996, supra note 12, at 281. Although the Usenet is often described as a network, it is not one in a formal sense. Id. "Instead, it is a number of machines that exchange electronic mail tagged with predetermined subject headers." Id.

41THE INTERNET UNLEASHED, supra note 12, at 280.

42Long, supra note 18, at 1181-82 (Long likens a Usenet newsgroup to a physical bulletin board in being able to post messages, but notes that online messages are much different in their wide reach and instantaneous delivery).

43Long, supra note 18, at 1183. The information your message carries is called the header. Id. This portion of your message contains the computer equivalent of the geographic origin of the message and the senders name and often the e-mail address, much like the return address on an envelope. Id.

44Id.

45See CAVAZOS & MORIN, supra note 1, at 14-17 (discussing the concept of anonymity on the Net noting that a large portion of the activities occur under assumed names or "handles." They also discuss the use of the anonymous remailers and file transfer protocols which allow the transfer of files at high speeds anonymously).

46David G. Post, Pooling Intellectual Capital: Thoughts on Anonymity, Pseudonymity, and Limited Liability in Cyberspace, 1996 U. CHI. LEGAL F. 139, 150 (discussing the traceability of e-mail with a pseudonymous address).

47See Long, *supra* note 18, at 1183-87 (discussing the growth and debate over anonymous servers and how they are becoming increasingly criticized by some Usenet groups); see also Froomkin, *supra* note 39, at 414-27 (outlining how the Internet enables anonymous communication through the use of these remailers which will allow both traceable and untraceable anonymity).

48See Froomkin, *supra* note 39, at 415-16 (discussing the features of anonymous remailing services noting all serious remailers share this feature of deleting identifying information).

49 *Id.*

50Froomkin, *supra* note 39, at 417-18. See also Long, *supra* note 18, at 1184-85. Long discusses the use of the anon.penet.fi remailer server, in which the service administrator still has the ultimate access to the information of who sent the original message and may upon being pressured by law enforcement or others reveal the source. *Id.* "[O]nly an anonymous server with a trustworthy administrator will offer virtually complete anonymity." *Id.* Froomkin noted the dangers and risks of such services by providing the recent example of the Church of Scientology who sued and used subpoenas against one such remailer service to obtain the identity of the person they alleged was spreading copyrighted Church teaching online. Froomkin, *supra* note 39, at 425-26. See also Noah Levine, Note Establishing Legal Accountability for Anonymous Communication in Cyberspace, 96 COLUM. L. REV. 1526 (1996). Minimal liability is imposed on remailers so long as they remain ignorant of the content of the messages they are remailing. *Id.* at 1557. This encourages remailers to adopt a no questions asked attitude. *Id.* Levine argues that reform is needed so that anonymous remailers would be encouraged to operate their services more responsibly. The best way to do this the author argues is to subject the administrators to liability for illegal acts of their users in those situations in which a "responsible" operator would have prevented such an act from occurring. *Id.* at 1558.

51See Froomkin, *supra* note 39, at 418-21. Froomkin describes the "chained remailing" process as probably the most anonymous form of directed communication available. This process along with encryption will ensure the user that:

(1) none of the remailer operators will be able to read the text of the message because it has been multiply encrypted in a fashion that requires the participation of each operator in turn before the message can be read; (2) neither the recipient nor any remailer operators in the chain (other than the first in line) can identify the sender of the text without the cooperation of every prior remailer's operator; (3) therefore it is impossible for the recipient of the message to connect the sender to the text unless every single remailer in

the chain both keeps a log of its message traffic and is willing to share this information with the recipient (or is compelled to do so by a court or other authority).

Id.

52See Levine, *supra* note 50, at 1530-31 (1996) (describing the remailer as the "anonymity tool" having significant benefit in encouraging open and frank discussions on a variety of difficult topics such as child abuse, AIDS, unpopular beliefs and whistle blowing, with the most significant benefit of facilitating free speech and that "[t]his benefit should not be underestimated.").

53See Patrick F. McGowan, *The Internet and Intellectual Property Issues*, in *GLOBAL TRADEMARK AND COPYRIGHT 1996: MANAGEMENT AND PROTECTION* at 303, 307 (PLI Pat., Copyrights, Trademarks, and Literary Prop. Course Handbook Series No. 455, 1996). McGowan maintains the Internet will eventually reach and effect virtually every aspect of society. *Id.* He notes a search on the legal database of NEXIS for the term "Internet" in 1984 revealed only 75 hits. *Id.* By 1994, the same search resulted in 37,220 hits. *Id.* He conservatively projects the amount for the year end of 1996 to be well over 300,000. *Id.* He goes on to illustrate the commercial opportunities on the Net, noting that in 1995, advertisers spent up to \$140 million on Internet ads. *Id.* at 316. He notes that by the year 2000 this amount spent on Internet advertising is projected to go as high as \$4 billion. *Id.* The opportunities are virtually limitless in light of the Telecommunication Act of 1996 which will allow the television, phone, and cable industries to compete in each others markets. *Id.* at 324. Single companies can now own a much larger and more comprehensive piece of the telecommunications pie as a result of the Telecommunications Act of 1996 and the recently relaxed ownership restrictions in both the broadcasting and telephone industries. *Id.* See also *THE INTERNET UNLEASHED 1996*, *supra* note 12, at 35. Commercialization is growing on the Internet as "Tens of thousands of businesses are already actively using the Internet for a multitude of business functions, including marketing and sales." As transactions become more secure, expect virtual storefronts and cybermalls to grow dramatically. *Id.* at 35.

54McGowan, *supra* note 53, at 307 (describing intellectual property issues as the "most important substantive legal issues involving information being transmitted over the Internet."); see generally Byron Marchant, *Online on the Internet: First Amendment and Intellectual Property Uncertainties in the On Line World*, 39 *HOW. L.J.* 477 (1996) (discussing the Internet and intellectual property issues in depth and attempting to determine the most cost effective means of law enforcement and regulation of such issues in the online world and discussing the various forms of civil liability involving issues of defamation, privacy violations, and slander or libel); See also Victoria A. Cundiff, *Stop Cyber Theft: Respecting Intellectual Property Rights on the Internet*, in *16TH ANNUAL INSTITUTE ON COMPUTER LAW* at 93, 96 (PLI Pat., Trademarks, and Literary Prop. Course Handbook Series No. 444, 1996) (analyzing the potential problems and legal issues that are involved that can be encountered in posting, downloading, or retransmitting messages on the Internet).

55See David Bender, *Emerging Personal Jurisdictional Issues on the Internet*, in *PLI'S SECOND ANNUAL INSTITUTE FOR INTELLECTUAL PROPERTY LAW* at 7, 10 (PLI Pat., Trademarks, and Literary Prop. Course Handbook Series No. 453, 1996) (discussing the issue of the extent a web site operator in one state or forum submits themselves to the jurisdiction of another state or forum by the establishment of the site and allowing or partaking in related activities). See also Richard S. Zembek, *Comment, Jurisdiction and the Internet: Fundamental Fairness in the Networked World of Cyberspace*, 6 *ALB. L.J. SCI. & TECH.* 339, 367 (1996) (tracing the traditional concepts of jurisdiction into the new computer medium and arguing that the existing rules and norms can be adapted to deal with the issues that arise when a non-resident defendant's contacts with a forum state are simply electronic travels or communications in the medium of cyberspace).

56See Randy Gainer, *Allocating the Risk of Loss for Bank Card Fraud on the Internet*, 15 *J. MARSHALL J. COMPUTER & INFO. L.* 39 (1996) (analyzing the risks involved in electronic transfer of funds over the Internet and examining the statutory and contractual framework that determines who should bear the loss if Internet consumer's data are misused). See also A. Michael Froomkin, *The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 *U. PA. L. REV.* 709 (1995) (discussing cryptography which is the art of creating and disguising messages so only certain people can see the true message, and the value of encryption to the banks, ATM-users, electronic transactor, businesses with commercial and trade secrets, and the general public who use cellular telephones, faxes, e-mail, or who send other sensitive personal data electronically).

57See Brian G. Gilpin, *Attorney Advertising and Solicitation on the Internet: Complying with Ethics Regulations and Netiquette*, 13 *J. MARSHALL J. COMPUTER & INFO. L.* 697 (1995) (examining how attorneys can utilize the Internet to advertise their professional services without violating ethics regulations or breaching Netiquette).

58See e.g., Richard A. Horning, *Has Hal Signed A Contract: The Statute of Frauds in Cyberspace*, 12 *SANTA CLARA COMPUTER & HIGH TECH. L.J.* 253 (1996) (discussing the opportunities on the Net for contract formation by interchange of electronic messages and whether such contracts are compatible with the statute of frauds); Paul E. Geller, *Conflicts of Laws in Cyberspace: Rethinking International Copyright in a Digitally Networked World*, 20 *COLUM.-VLA J.L. & ARTS* 571 (1996) (analyzing how to reconcile traditional conflict and choice of law concepts in the emerging medium of cyberspace and if these two concepts can be reconciled in dealing copyright issues on the Internet); James D. Cigler et al., *Cyberspace: The Final Frontier for International Tax Concepts?*, 7 *J. INT'L TAX'N* 340 (1996) (examining traditional tax laws and their consequences as commerce is expanding to global proportions over the Internet); Albert Gidari, *Privilege and Confidentiality in Cyberspace*, 13 *COMPUTER L.* 1 (No. 2, 1996) (discussing the debate over security, privilege, and confidentiality in cyberspace); Michael Adler, *Note, Cyberspace, General Searches, and Digital Contraband: The Fourth Amendment and the Net-Wide Search*, 105 *YALE L.J.* 1093, 1093 (1996) (examining "what restraints might exist under the Fourth Amendment doctrine on the government's

ability to discover and prosecute possession of [ ] 'digital contraband"); Natacha D. Steimer, Note, *Cyberlaw: Legal Malpractice in the Age of Online Lawyers*, 63 GEO. WASH. L. REV. 332 (1995) (illustrating how legal professionals have increasingly utilized the Internet to solicit new clients with the use of electronic bulletin boards where subscribers can ask legal questions and the attorney respond hoping to bring in a client and noting that when subscribers rely on this information and suffer an injury, they may be able to obtain recourse against the attorney providing the information through a legal malpractice action); David K. McGraw, Note, *Sexual Harassment in Cyberspace: The Problem of Unwelcome E-Mail*, 21 RUTGERS COMPUTER & TECH. L.J. 491 (1995) (discussing the use of sexually offensive e-mail messages on the Net and what legal remedies are available or should be available for people who receive such unwanted messages).

59 See Adams, *supra* note 15.

60 See Levine, *supra* note 50, at 1533. The risks are reduced for such crimes as electronic stalking, hate mail, libel, trademark or copyright infringement if such activities are conducted anonymous. *Id.* at 1534. Unlike regular mail, in which inherent clues in a message may reveal the sender's identity, in cyberspace there are no real fingerprints so when the remailer strips the "digital fingerprint" little risk remains that the sender's identity will be discovered. Even though it is possible to deliver the message electronically in a manner that makes it essentially untraceable the risk still remains that writing patterns, or other intrinsic identifiers, will reveal the identity of the author. Froomkin, *supra* note 39, at 402. *Id.* See also Anonymous, Note, *supra* note 36 ("Anonymity, it is asserted, will serve as a cloak for the progenitor of irresponsible ideas; it may encourage the making of unfounded charges which the author would fear to raise if he knew he would be subject to public censure were they probably false.").

61 *McIntyre v. Ohio Elections Comm'n*, 115 S. Ct. 1511, 1537 (1995) (Scalia, J., dissenting). Scalia was discussing anonymity in the context of campaign literature and an Ohio election disclosure law. *Id.* at 1537. The majority struck down Ohio's statutory prohibition against distribution of any anonymous campaign literature as they found it to violate the First Amendment. *Id.* at 1524. Scalia goes on in disagreeing with the majority stating, "to strike down the Ohio law in its general application--and similar laws of 48 other states and the Federal Government--on the ground that all anonymous communication in our society traditionally sacrosanct, seems to me a distortion of the past that will lead to a coarsening of the future." *Id.*

62 See Branscomb, *supra* note 4, at 1645 (discussing accountability of anonymous defamatory or illegal messages and noting that "without accountability, there is no basis upon which an injured party can initiate a tort action to redress grievances.").

63 *Id.* Victims seeking some form of compensation will be unable to track down the anonymous source or if they are fortunate enough to do so, the source may prove to be uncollectible without any resources. *Id.* Thus, "potential litigants and their legal counsel have not hesitated to seek the source of the deepest pockets." *Id.*

64 Id.

65See Anthony L. Clapes, *The Wages of Sin: Pornography and Internet Providers*, 13 *COMPUTER L.* 1 (No. 7, 1996) (discussing the passage of the Telecommunication Act of 1996 which brought technology and the First Amendment to clash as the Act aims to control obscene and indecent online communications); Dawn L. Johnson, *It's 1996: Do You Know Where Your Cyberkids Are? Captive Audiences and Content Regulation on the Internet*, 15 *J. MARSHALL J. COMPUTER & INFO. L.* 51, 60-63 (1996) (discussing the First Amendment's guarantees and noting that its protections do not extend to obscenity and the right to distribute or transmit obscene materials); Jeffrey E. Faucette, *The Freedom of Speech at Risk in Cyberspace: Obscenity Doctrine and a Frightened University's Censorship of Sex on the Internet*, 44 *DUKE L.J.* 1155 (1995) (discussing how Carnegie Mellon University removed a group of topics from the Usenet newsgroups subscribed to by the University computer system and available on the Internet to its students because they contained encoded sexually explicit images. The University feared some of the images may be "obscene" by the Supreme Court and the university feared liability under a state obscenity statute).

66See Andrew Spett, Comment, *A Pig in the Parlor: An Examination of Legislation Directed at Obscenity and Indecency on the Internet*, 26 *GOLDEN GATE U.L. REV.* 599, 603-11 (1996). Spett notes that obscenity has been unprotected expression since the holding in *Commonwealth v. Sharpless*, 2 S.R. 91 (1815) because it lacks any social value or importance. *Id.* at 603. The common law conviction in *Sharpless* was "premised upon the exhibition, for profit, of a nude picture." *Id.* at 603 n.30. Spett offers the Supreme Court's reasoning for upholding laws that prohibit obscenity:

(1) An arguable correlation between exposure to obscene material and crime; (2) The power of the states "to make morally neutral judgments" that public exhibition of obscene material, or commerce in the obscene, tends to "injure the community as a whole" by polluting the "public environment"; and (3) The deleterious effect that obscene material has upon the public, because "what is commonly read and seen and heard and done intrudes upon us all, want it or not."

*Id.* at 603-04 (citing LAURENCE H. TRIBE, *AMERICAN CONSTITUTIONAL LAW* §§12-16 at 917 (2nd ed. 1988))(quoting from *Paris Adult Theater I v. Slaton*, 413 U.S. 49, 58-60 (1973)).

67See *infra* Part V (discussing the Communications and Decency Act, 47 U.S.C. ( 223 which is primarily aimed at restricting the access of minors to indecent or offensive material via the Internet or any "telecommunications device").

68Adams, *supra* note 15, at 412-13 (citing a Carnegie Mellon University study found in Dan Coats, "Dark side" of the Internet, *Wash. Post*, June 30, 1995 at A23. But see Clapes, *supra* note 65, at 2 noting that, while the Carnegie Mellon study (with its "methodological flaws and conclusory leaps") collected volumes of material from one

portion of the Internet, "the proportion of all Internet - accessible information that is pornographic is probably vanishingly small").

69See Spett, *supra* note 66, at 606, setting forth the Supreme Court's notion of community standards as:

(a)Whether the average person, applying contemporary community standards, would find that the material, taken as a whole, appeals to the prurient interest; (b)Whether the material depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law; and (c)Whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value.

*Id.* (quoting *Miller v. California*, 413 U.S. 15, 24 (1973)).

70See generally Zanghi, *supra* note 3 (arguing that the Supreme Court needs to reconsider the traditional community standards test in obscenity cases as technological advances and computers have altered the community into a global one). See also *United States v. Thomas*, 74 F.3d 701 (6th Cir. 1996). The Thomas' were a California couple who created and operated an adult bulletin board system from their home. *Id.* at 705. A U.S. Postal Inspector in Tennessee downloaded sexually explicit images from the service. *Id.* The couple was prosecuted and convicted in federal court in Tennessee under Federal obscenity laws. *Id.* at 705-06. A request for change of venue to a Federal court in California was denied, in part, because even under Federal obscenity laws the applicable community standard is that of the receiving community. *Id.* at 710-12.

71 See generally Johnson, *supra* note 65 (discussing the material easily available to children on the Internet).

72See *New York v. Ferber*, 458 U.S. 747 (1982) (rejecting a First Amendment challenge to a New York law which prohibited the distribution of material depicting children involved in sexual conduct, holding "child pornography as a category of material outside the protection of the First Amendment.").

73Arguably such material is found in adult-only bulletin board services requiring subscribers identity. See Pamela A. Huelster, *Cybersex and Community Standards*, 73 B.U. L. Rev. 865, 881 (1995). But see Clapes, *supra* note 65, at 2-3. Clapes maintains that minor obstacles to accessing pornography are easily overcome, primarily because of the Net's focus on usability in creation of site list by topics and hyperlinks. *Id.* A person of any age and hardly any computer experience could find such pornographic material with the ease of selecting a T.V. channel. *Id.*

74See Adams, *supra* note 15, at 413-14 (noting pedophilia stalking is found in both the private and public areas of the Net with the majority taking place in the public chat rooms where participants engage in interactive conversations).

75Id. at 414. See also id. at n.74 recounting various attempts pedophiles have used the Internet to lure children from their homes; see Vincent J. Schodolski, *Online Anonymity Conducive to Vice; Teens are Vulnerable in Cyberspace*, CHI. TRIB. June 11, 1995, at 19 (teenage girl missing since accepting an offer from a man via her computer); Mary Murphy, *Computer Prowlers Stalk Kids*, ORLANDO SENTINEL, July 9, 1995, at 1 (man convicted after using the Net to solicit lewd pictures and then sent the children Polaroid cameras. Another man exchanged explicit e-mail messages and pictures with whom he thought was a teenage boy, the "boy" was actually an undercover officer who arrested the man when he flew to Florida to meet his teenage date); Barbara Kantowitz, et al., *Child Abuse in Cyberspace*, NEWSWEEK, Apr. 18, 1994, at 40 (a professional engineer used the Net to arrange a meeting with a teenage boy. He blindfolded and bound the boy before bringing him to his home. Once there, the boy was spanked, forced to have an enema, have his legs and pubic hair shaved, and was forced to partake in anal and oral sex. The father of the boy found out about the incident when the boy was forced to described the events on line before he could be set free).

76 While this concern for children safety does appear to be a compelling justification for regulation of the Internet, many people seem to ignore the fact that the Internet is uniquely interactive. The user must actively seek out the information transmitted into their homes. Thus, the Internet is unlike the pervasiveness of the T.V. and other mediums where children may be exposed to material without much, if any, active interaction. Parental control must be a guiding concern when children start to explore the Internet. Parents would not let their children talk to any stranger on the street, while just over a million children surf the Internet doing just that. Dee Pridgen, *How will Consumers be Protected on the Information Superhighway?*, 32 LAND & WATER L. REV. 237, 245-46 (1997) (citing Business News Briefing, ROCKY MOUNTAIN NEWS, Jan. 12, 1996, at A56).

77See GERALD GUNTHER, *CONSTITUTIONAL LAW*, 1131-37 (12th ed. 1991) (discussing the extent the First Amendment prevents efforts to limit speech which is thought as harmful and offensive to minorities noting that most of the Supreme Court's decisions in this area deal with speech and demonstrations by Nazi groups and regulations of racist speech on college campuses); Adams, *supra* note 15, at 415 (noting that a broad range of right wing extremists, from the Aryan Nation to militia groups now speak to the world via the Internet and that since Neo Nazi groups have been banned from selling their books in Germany, they now distribute their message worldwide via the Internet); Kenneth A. Wittenberg, *Taking A Bite Out of Hate Crimes*, 57 OR.ST. B. BULL 9, 9-10 (Nov. 1996) (defining a hate crimes as, "assaults and other attacks committed for discriminatory reasons" that are intended to reach beyond the individual victim and intimidate an entire community which may be targeted for its marginalized status).

78Adams, *supra* note 15, at 414. Adams discusses the emerging issues of stalking via computers noting "the ratio of men to women on the Internet is three to one." Id. Adams provides the example of two women in Connecticut who were harassed over the Internet. Id. (citing Jonathan Roubinovitz, *Rules of the Road on the Information Highway: Law*

Makes Harassing by Computer a Crime, N.Y. Times, June 13, 1995, at B4). The first woman, who ran a computer bulletin board from her home was electronically bombarded with files intended to crash her system. Id. The second incident, a woman who was repeatedly threatened by e-mail, prompted a state representative to introduce legislation to address the problem. Id.

79 See supra note 75.

80See Martha Siegel, Anarchy, Chaos, on the Internet Must End, S.F. CHRON. Jan 2, 1995, at A19 (arguing that legislation should be passed to create safety and order in cyberspace and that guidance from the federal communication commission is needed). See also Walter S. Mossberg, Personal Technology, Wall St. J., Jan 26, 1995, at B1 (arguing "accountability is key to democracy" and that "online services [need to] act to strengthen accountability and open civil debate. . . ."; anonymity as the author views it will limit such accountability).

81CONN. GEN. STAT. ANN. § 53a-183 (West 1994 & Supp. 1996). The statute provides:

(a) A person is guilty of harassment in the second degree when: (1) by telephone, he addresses another in or uses indecent or obscene language; or (2) with intent to harass, annoy or alarm another person, he communicates with a person by telegraph or mail, by electronically transmitting a facsimile through connection with a telephone network, by computer network, as defined in section 53a-250, or by any other form of written communication, in a manner likely to cause annoyance or alarm; or (3) with intent to harass, annoy or alarm another person, he makes a telephone call, whether or not a conversation ensues, in a manner likely to cause annoyance or alarm.

(b) For purposes of this section such offense may be deemed to have been committed either at the place where the telephone call was made, or at the place where it was received.

(c)The court may order any person convicted under this section to be examined by one or more psychiatrists.

(d) Harassment in the second degree is a class C misdemeanor.

Id.

8218 PA. CONST. STAT. § 910 (1983 & 1997 Supp.) Section 910 of the statute provides:

(A) Offense defined.--Any person commits an offense if he:

(1) makes, distributes, possesses, uses or assembles an unlawful telecommunication device or modifies, alters, programs or reprograms a telecommunication device designed, adapted or which can be used:

(i) for commission of a theft of telecommunication service or to acquire or facilitate the acquisition of telecommunication service without the consent of the telecommunication service provider; or

(ii) to conceal or to assist another to conceal from any telecommunication service provider or from any lawful authority the existence or place of origin or of destination of any telecommunication; or

(2) sells, possesses, distributes, gives or otherwise transfers to another, or offers, promotes, or advertises for sale, any:

(i) unlawful telecommunication device, or plans or instructions for making or assembling the same, under circumstances evidencing an intent to use or employ such unlawful telecommunication device, or to allow the same to be used or employed for a purpose described in paragraph (1), or knowing or having reason to believe that the same is intended to be so used, or that the aforesaid plans or instructions are intended to be used for the making or assembling such unlawful telecommunication device; or

(ii) material, including hardware, cables, tools, data, computer software or other information or equipment, knowing that the purchaser or a third person intends to use the material in the manufacture of an unlawful telecommunication device.

Id.

83GA. CODE ANN. § 16-9-93.1 (1996). The statute provides:

(A) It shall be unlawful for any person, any organization, or any representative of any organization knowingly to transmit any data through a computer network or over the transmission facilities or through the network facilities of a local telephone network for the purpose of setting up, maintaining, operating, or exchanging data with an electronic mailbox, home page, or any other electronic information storage bank or point of access to electronic information if such data uses any individual name, trade name, registered trademark, logo, legal or official seal, or copyrighted symbol to falsely identify the person, organization, or representative transmitting such data or which would falsely state or imply that such person, organization, or representative has permission or is legally authorized to use such trade name, registered trademark, logo, legal or official seal, or copyrighted symbol for such purpose when such permission or authorization has not been obtained; provided, however, that no telecommunications company or Internet access provider shall violate this Code section solely as a result of carrying or transmitting such data for its customers.

Id.

8447 U.S.C. § 223(a)(1)(C) (1997 Supp.) (making it illegal for whoever, "makes a telephone call or utilizes a telecommunications device, whether or not conversation or communication ensues, without disclosing his identity and with intent to annoy, abuse, threaten, or harass any person at the called number or who receives the communications.").

85See *Shea ex rel. American Reporter v. Reno*, 930 F. Supp 916 (S.D.N.Y. 1996) (challenging 47 U.S.C. § 223(d)) and *ACLU v. Reno*, 929 F. Supp 824 (E.D. Pa. 1996) (challenging 47 U.S.C. §§ 223 (a)(1)(B), (a)(2), d(1), d(2)). See also *Reno v. ACLU* 117 S. Ct. 2329 (1997) (holding the CDA unconstitutionally vague and overbroad).

86See § 223. The section prohibits the use of a telecommunications device to "knowingly make[], create[], or solicit[] and initiate[] the transmission of any "comment request, suggestion, proposal, image or other communication which is obscene or indecent, knowing that the recipient is under 18 years of age." § 223(a)(1)(B). Further, § 223 (d)(1)(B) prohibits the use of a computer to send or display to anyone under 18 "any comment, request, suggestion, proposal, image, or other communication that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs, regardless of whether the user of such service placed the call or initiated the communication." § 223(d)(1)(B).

87 See supra note 84.

88The district court heard the challenge of the CDA under Pub.L. 104-104(a). § 561 provides any civil action challenging the constitutionality of the act or any amendment made by the CDA or any provision thereof, shall be heard by a district court of three judges convened pursuant to the provisions of section 2284 of title 28 U.S.C. Pub. L. 104-104(a) § 561 (1996). Further, any order or judgment holding the unconstitutional is reviewable as a matter of right by direct appeal to the Supreme Court. See Pub.L. 104-104(b) § 561 (1996).

89ACLU, 929 F. Supp. at 856-57. The court goes on to note that enforcement of current obscenity and child pornography laws are adequate to address the problems the CDA sought to rectify and that the Justice Department itself indicated in the hearings on the CDA that it was prosecuting online obscenity, child pornography and child solicitation under existing laws, and would continue to do so. *Id.* Thus, the court determined, "It follows that the CDA is not narrowly tailored, and the government's attempt to defend it on that ground must fail." *Id.*

90 *Reno v. ACLU*, 117 S. Ct. 2329 (1997).

91 *Id.* at 2345.

92 *Id.* Justice Stevens noted that such a burden on adult speech is unacceptable as less restrictive alternatives would be at least as effective in achieving the purposes the CDA was enacted to serve. The Court concluded that as the statute was not narrowly tailored to

meet its objectives, it "threatens to torch a large segment of the Internet community." *Id.* at 2350.

93 *Id.* at 2350.

94 *ACLU*, 929 F. Supp. at 849; see also *id.* at 871-72 (noting that conversations on the AIDS web page includes safer sex discussions in "street language" for easy comprehension and also names specific sexual practices describes the risk for the transmission of the HIV virus associated with each practice, and that operators of similar sites which allow the transmission of traditionally "indecent" material "could legitimately fear prosecution under the Communications Decency Act").

95 See *id.* at 883 discussing the value of the Internet stating:

..the Internet may fairly be regarded as a never-ending worldwide conversation. The Government may not...interrupt that conversation. As the most participatory form of mass speech yet developed, the Internet deserves the highest protection from governmental intrusion....Just as the strength of the Internet is chaos, so the strength of our liberty depends upon the chaos and cacophony of the unfettered speech the First Amendment protects.

See also *Reno v. ACLU*, 117 S. Ct. 2329, 2351 (1997) stating:

As a matter of constitutional tradition, in the absence of evidence to the contrary, we presume that governmental regulation of the content of speech is more likely to interfere with the free exchange of ideas than to encourage it. The interest in encouraging freedom of expression as a democratic society outweighs any theoretical but unproven benefit of censorship.

96 "This is a really important case..that decides freedom to speak and freedom to read for the next century." Danny Weitzner of the Center for Democracy and Technology, quoted by Richard Carelli in, *Supreme Court Agrees to Decide on Restricting Access to Internet*, *CLEVELAND PLAIN DEALER*, Dec. 7, 1996, at 12A.

97 *Reno*, 117 S. Ct. at 2343. The Court reviewed and recognized its precedents on content-based regulations of speech and concluded these cases did not require them to uphold the CDA and were fully consistent with the application of the most stringent review of the statute.

98 It appears the Court is now more confident and unified in approaching cyberspace issues as compared with their previous decision in *Denver Area Educational Telecommunications Consortium v. F.C.C.*, 116 S. Ct. 2374 (1996). There the Court appeared hesitant and fractured about the indecency restrictions in question and how they applied to cable television. In contrast, the Court in *Reno* appeared confident and reached unexpected harmony on some basic principles regarding the Internet and Cyberspace. Justice Steven's opinion was joined by all the Justices except Chief Justice Renquist and

Justice O'Connor who both partially dissented. However, both agreed with the majority on key Internet issues and that the core provisions of the CDA were unconstitutional.

99See U.S. CONST. amend. I.

100See *Milk Wagon Drivers Union v. Meadowmoor Dairies*, 312 U.S. 287, 301-02 (1941) (Black, J., dissenting) ([f]reedom to speak and write about public questions is as important to the life of our government as is the heart to the human body. . . . [T]his privilege is the heart of our government."); *New York Times v. Sullivan*, 376 U.S. 254, 270 (1964) (stating there is a, "profound national commitment to the principle that debate on public issues should be uninhibited, robust, and wide-open. . . ."); *Whitney v. California*, 274 U.S. 357, 377 (Brandeis, J., concurring) ("there [is] time to expose through discussion the falsehood and fallacies, to avert the evil by the process of education, the remedy to be applied is more speech, not enforced silence.").

101See E. Walter Van Valkenburg, *The First Amendment in Cyberspace*, 75 OR. L. REV. 319, 329 (1996) ("The Internet poses the potential for as dramatic a transformation of global communications as the world has ever seen.").

102See *Abrams v. United States*, 250 U.S. 616, 630 (1919) (Holmes, J., dissenting) Holmes observed that when suppression of opposing speech does not yield success "men may come to believe [that] . . . [W]hen the ultimate good desired is better reached by free trade in ideas--that the best test of truth is the power of the thought to get itself accepted in the competition of the market, and that the truth is the only ground upon which their wished safely can be carried out. That at any rate is the theory of our Constitution." *Id.* While our founding fathers surely did not envision the Internet, it stands to serve the basic goals of the First Amendment to allow citizens to express their ideas openly in a public forum without the fear of government restrictions and reprisals for what is said.

103See *ACLU v. Reno*, 929 F. Supp. 824 (E.D. Pa. 1996). "The Internet is . . . a unique and wholly new medium of worldwide human communication." *Id.* at 844. "The types of content now on the Internet defy easy classification . . . It is no exaggeration to conclude that the content on the Internet is as diverse as human thought." *Id.* at 842.

104Ted Anthony, *Cyber Optimist*, CLEVELAND PLAIN DEALER, Dec. 31, 1996, at 5C. The article goes on to discuss Microsoft's new Internet philosophy and how Gates is positioning the company to help guide the Internet through its growing pains.

105See *Roth v. United States*, 354 U.S. 476, 484 (1957) (stating that the purpose of the First Amendment is "to assure unfettered interchange of ideas for the bringing about of political and social changes by the people"). See also *Board of Education v. Pico*, 457 U.S. 853, 866 (1982) ("our precedents have focused not only on the role of the First Amendment in fostering individual self expression but also on its role in affording the public access to discussion, debate, and the dissemination of information and ideas.") (quoting *First National Bank v. Bellotti*, 435 U.S. 765, 783 (1978)).

106See *Edwards v. National Audubon Soc'y*, 556 F.2d 113, 115 (2nd Cir.), cert. denied, 434 U.S. 1002 (1977) (noting that "a democracy cannot long survive unless the people are provided the information needed to form judgments on issues that affect their ability to intelligently govern themselves.").

107 See Long, *supra* note 18.

108Id. at 1178 (citing examples of information that may be sought or shared anonymously or not at all; people who were sexually abused, those suffering from AIDS or other communicable diseases, or the employee seeking to "blow the whistle" on unsafe or discriminatory practices of his or her employer). See also Lee Tien, *Who's Afraid of Anonymous Speech? McIntyre and the Internet*, 75 OR. L. REV. 117, 117 (1996) (asserting anonymity is part of society and giving examples of conventionally recognized practices such as suicide hotlines, Alcoholics Anonymous, and the use of the secret ballot).

109See Fromkin, *supra* note 39, at 408-09 (stating that, in addition to personal benefits, benefits may flow to society such as the overall improvement of public health as the availability of anonymous access to more information on sexually transmitted diseases and AIDS becomes known and is utilized).

110See Cass Sunstein, *The First Amendment in Cyberspace*, 104 YALE L.J. 1757 (1995) (noting that the future may dramatically change society as online communications eventually allow the best schools, teachers, resources of art, literature, and science, and health care services to be available to everyone without regard to physical locations, distance, or disability). It is true not every person can afford a home computer right now. There is, however, a move to provide Internet access to all students by the year 2000. Clinton, Gore Cite Progress in Wiring Nation's Schools, U.S. Newswire, Feb. 8, 1997, available in Westlaw, ALLNEWSPLUS database (citing a fall 1996 survey done by the U.S. Department of Education's National Center for Education Statistics). An upcoming FCC vote is expected to make \$2.25 billion a year available to provide discounts to assist in the effort to make Internet access available to every school child. Computer Link: Short Circuits, SAN DIEGO UNION-TRIB., Apr. 1, 1997 at 21. Currently, 65% of public schools have at least one Internet connection. Clinton, Gore Cite Progress in Wiring Nation's Schools, *supra*. Seventy-four percent of those that have Internet access make that access available to students, so in approximately 47% of public school districts students have some access to the Internet. Id. That access, however, is primarily in bigger, wealthier, urban districts, as only 31% of schools with high poverty indicators have Internet access. More Schools on the Internet, THE SACRAMENTO BEE, Feb. 17, 1996 at A22 (citing the earlier mentioned study by the U.S. Department of Education). It is also concentrated at the secondary level, with only 46% of elementary schools having any Internet access. Id.

111McIntyre v. Ohio Election Comm'n, 115 S. Ct. 1511, 1516 (1995). The Court in McIntyre goes on to note the significance of anonymity in the literary world by referring to famous authors who used anonymity in publishing their works including; Mark Twain

(Samuel Langhorne Clemens), O. Henry (William Sydney Porter), Benjamin Franklin (various pseudonyms), Voltaire (Francois Marie Arouet), George Eliot (Mary Ann Evans), Charles Dickens ("Boz"). McIntyre at 1516 at n.4.

112Froomkin, *supra* note 39, at 408. Froomkin notes the legitimacy of anonymous communications as a means of self-protection as some people may fear losing their jobs or in the extreme death. *Id.* "Not everyone is so courageous as to which to be known for everything they say, and some timorous speech deserves encouragement." *Id.*

113*Id.* ("Indeed, given the ability to broadcast messages widely using the Internet, anonymous e-mail may become the modern replacement of the anonymous handbill.").

114*Id.* at 427. ("The United States Constitution does not guarantee a right to be anonymous in so many words. The First Amendment's guarantees of free speech and freedom of assembly have, however, been understood for many years to provide protections for at least some, and possibly a great deal of, anonymous speech and secret association.").

115See Anonymous, Note, *supra* note 36, at 1088 (maintaining that there, "is a recognized right to speak and write anonymously and to participate anonymously in group activities. The Supreme Court has developed this right as a derivative of the protection given speech, assembly, the press, religion, and petition by the first and fourteenth amendments.").

116See Brief for Petitioner at 12-15, *McIntyre v. Ohio Elections Comm'n*, 115 S. Ct. 1511 (1995), available on Westlaw, 1994 WL 144557 (discussing how anonymous leaflets have played an important role in the political development of the country by allowing for the expression of views that were unpopular which ultimately broadened the scope of political debate); "Throughout history, anonymity has often been essential for political dissidents who faced persecution if their identities become known. Sometimes their persecution takes the form of official prosecution. Sometimes it takes the form of social ostracism." In either event, the ability to speak anonymously often provides a safe haven for those who wish to express unpopular views. *Id.* at 12.

117See Anonymous, Note, *supra* note 36, at 1085 (noting that the use of anonymity was used extensively by our founding fathers. The name "Publius" was used by Madison, Hamilton, and Jay in publishing the Federalist papers, Hamilton and Madison both used anonymity in using "The Letters of Pacificus" and "Letters of Helvidius" respectively in debating each other, and Chief Justice Marshall writing as "a friend to the Republic." "Between 1789 and 1809 no fewer than six presidents, fifteen cabinet members, twenty senators, and thirty-four congressmen published political writings either unsigned or under pen names.").

118362 U.S. 60 (1960). *Talley* dealt with the prosecution for a violation of a municipal ordinance which prohibited the distribution of anonymous handbills. The Court found the ordinance unconstitutional as it violated the freedom of speech and press. *Id.* at 65.

However, the Court cautioned that it was not making a judgment about the constitutionality of an ordinance that was specifically aimed or narrowly tailored to prevent a particular evil. *Id.* at 64.

119 *Id.* at 64-65. See also *McIntyre v. Ohio Elections Comm'n*, 115 S. Ct. 1511, 1517 at n.6 (1995) (listing famous historical figures who were the probable authors of pseudonymously published political works including; Alexander Hamilton, John Jay, New York Governor George Clinton, Samuel Bryan, Richard Henry Lee, and Robert Yates.)

120 115 S. Ct. 1511 (1995).

121 *McIntyre*, 115 S. Ct. at 1514.

122 *Id.*

123 *Id.* The majority of the leaflets were signed "Concerned Parents and Tax Payers." *Id.* See *id.* n.2 (showing a copy of Mrs. McIntyre's leaflet).

124 *McIntyre*, 115 S. Ct. at 1514.

125 See *id.* n.3 (containing the text of the disclosure statute, OHIO REV. CODE ANN. § 3599.09(A) (1988)). The state supreme court upheld the conviction by a divided vote concluding that the disclosure law "should be upheld if the burden imposed on First Amendment rights were 'reasonable' and 'non-discriminatory.'" *Id.* at 1515. They went on to conclude that the statute was reasonable and non-discriminatory as it did not impact the "content of message nor significantly burden their ability to have it disseminated." *Id.* at 1515.

126 *McIntyre*, 115 S. Ct. at 1518. (holding that political speech is entitled to the highest constitutional protection and that "the identity of the speaker is no different from any other component . . . that the author is free to include or exclude.").

127 *Id.* at 1516.

128 *Id.* at 1518-19 (quoting *Roth v. United States*, 354 U.S. 476, 484 (1957)).

129 The majority concludes its opinion by stating, "Under our Constitution, anonymous pamphleteering is not a pernicious, fraudulent practice, but an honorable tradition of advocacy and of dissent. Anonymity is a shield from the tyranny of the majority. (citation omitted). It thus exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation--and their ideas from suppression--at the hand of an intolerant society." *Id.* at 1524.

130 See Tien, *supra* note 108, at 121 (maintaining that the *McIntyre* decision stands for "protecting the 'lonely pamphleteers' and the 'cheap speech of dissenters'" and that the

Internet is the medium of cheap speech). But see Froomkin, *supra* note 39, at 428-33 (discussing anonymous political speech and its historical protections, but questioning if online political speech will be afforded the same broad First Amendment protection, noting that even traditional forms of political speech are not totally free from all government interference and regulation).

131But see Whitt, *infra* note 137, at 435-38 (criticizing the majority decision in McIntyre, maintaining that the Court did not fully explore why our Nation's founders thought it was necessary to maintain anonymity and whether any legitimate reasons for anonymity still exist today). Serious artistic and literary works continue to fall prey to censorship even within the past few years. See Brief of Amicus Feminists for Free Expression ("FFE") at 2, *Reno v. ACLU*, 117 S. Ct. 2329 (No. 96-511). The FFE gives examples of recent censored works including; the Diary of Anne Frank, Maya Angelou's *I Know Why the Caged Bird Sings*, Margaret Atwood's *The Handmaid's Tale*, Judy Blume's *Are You There, God?, It's Me, Margaret*, Nancy Garder's *Annie on My Mind*, and Alice Walker's *The Color Purple*. *Id.* See also the web site *The Most Frequently Banned Books in the 1990s* at <http://www.cs.cmu.edu/People/spok/most-banned.html>.

132Seth Freimer, *Sunlight, Secrets, and Scarlet Letters: The Tension Between Privacy and Disclosure in Constitutional Law*, 140 U. PA. L. REV. 1, 15 (1991).

133The Republican members of Congress were fearful of communist ideas within the government and advanced using the House Un-American Activities Committee (HUAC) to launch investigations of members of the then Democrat-controlled executive branch. *Id.* at 15-18 and n.44. Soon the anti-Communist fever spread and virtually all segments of society from the entertainment industry to higher education to the private sector became targets for investigation. *Id.* See also Friemer, *supra* note 132 (discussing the background of McCarthyism and its effects on society at 14-26).

134See Freimer, *supra* note 132, at 20. The overall impact was great even on people not directly accused or investigated. A national opinion survey from 1954 found that over 40% of the country felt "some [or all] were not as free to say what they [thought] as they used to." *Id.* (alterations in original) A year later a survey of academic and scientists showed 36% who stated their colleagues were less willing to put forth unpopular views and that over 20% had refrained from expressing any controversial opinions. *Id.*

135Tien, *supra* note 108, at 123.

136Artists, critics, and authors all have valued the ability to work anonymously. A recent example was the book *Primary Colors* which was authored anonymously and was a "fictional" account of a Washington insider during the 1992 Presidential Primaries. ANONYMOUS, *PRIMARY COLORS* (1996). It was later revealed the author was Joe Klein, a CBS news Consultant and Newsweek Columnist who now writes for the *New Yorker*. See *HOUSTON CHRONICLE*, Aug. 12, 1997, 1997 WL 13056036.

137See generally Tien, *supra* note 108. Tien thoroughly analyzes the McIntyre decision and how its reasoning is consistent with society's modern concept of anonymity in general in terms of self-identity and voluntary interaction. *Id.* Tien goes on to note that "the same considerations of viewpoint discrimination that favored protection of anonymous speech in McIntyre favor protection for online anonymous speech generally." *Id.* at 121. See also George Trubow, *Constitution vs. Cyberspace; Has the First Amendment Met its Match?*, 5 *BUS. L. TODAY* 41, 44 (1996) (arguing that while the McIntyre case dealt with anonymous political literature, it will have "implications regarding anonymity in cyberspace"); Levine, *supra* note 50, at 1530-32 (discussing the McIntyre decision and how the Court valued the concept of anonymous speech); Froomkin, *supra* note 39, at 428-43 (analyzing anonymous political speech and its First Amendment protections as discussed in the McIntyre decision and what types of restrictions on online speech are most likely to be upheld). But see *id.* at 433 doubting if such protection will exist online stating, "As ringing a defense of the First Amendment as the Talley and McIntyre decisions may be, they involved political speech. At most, therefore, they merely suggest the outcome for cases involving anonymous speech that is not 'political speech' and also not one of the areas of general public concern such as religion, art, or literature, that commentators usually include within the rubric of so-called 'core' First Amendment speech." For other discussions of the McIntyre decision not necessarily discussing its extended application to the Internet, see *Leading Cases* (pt. F), 109 *HARV. L. REV.* 111, 180-90 (1995); Mark A. Whitt, Note, *McIntyre v. Ohio Elections Comm'n: "A Whole New Boutique of Wonderful First Amendment Litigation Opens its Doors,"* 29 *AKRON L. REV.* 423 (1996).

138See Sunstein, *supra* note 110, at 1783-84 (discussing the economics and democracy of the Internet stating, "[h]igh quality, substantive discussions may well be possible among large numbers of people; town meetings that are genuinely deliberative may become commonplace.").

139See Adams, *supra* note 15 (discussing public chat rooms and the interactive conversations that take place in them).

140See Froomkin, *supra* note 39, at 441-42. Froomkin explains that the operators of remailer services which provide the ability to mask a sender's identity are themselves unable to first tell what kind of "speech" the message contains because the messages are sent to them encrypted. *Id.* at 442. "A ban on anonymous speech cannot therefore meaningfully distinguish by subject matter, nor can it necessarily even distinguish between visual depictions and mere words." *Id.*

141*Pacific Gas & Elec. Co. v. Public Util. Comm'n of Cal.*, 475 U.S. 1, 11 (1986).

142*Hurley v. Irish-American Gay, Lesbian and Bisexual Group of Boston*, 115 S. Ct. 2338, 2347 (1995).

143The evils to be prevented [by the First Amendment] were not censorship of the press merely, but any action of the government by means of which it might prevent such free

and general discussion of public matters as seems absolutely essential to prepare the people for an intelligent exercise of their rights as citizens.

THOMAS MCINTYRE COOLEY, 2 CONSTITUTIONAL LIMITATIONS, at 886 (8th ed. 1927).

144See Tien, *supra* note 108, at 126-29. Tien discusses how the "identity of the speaker or author is an aspect of message content." *Id.* at 126. Tien basis this proposition on the assertion in McIntyre that, "The identity of the speaker is no different from other components of the document's content that the author is free to include or exclude." *Id.* Tien concludes that any attempt of anonymity regulation would basically amount to content regulation and "[a] general prohibition on online anonymity is almost certainly too sweeping to pass constitutional muster because it would regulate protected speech." *Id.* at 128.

145Roberts v. United States Jaycees, 468 U.S. 609, 633 (1984) (O'Connor, J., concurring).

146Turner Broadcasting Sys. v. Federal Communication Comm'n, 114 S. Ct. 2445, 2459 (1994) (alteration in original) (quoting Ward v. Rock Against Racism, 491 U.S. 781, 791 (1989)). See also R.A.V. v. St. Paul, 112 S. Ct. 2538, 2544 (1989) ("The government may not regulate speech based on hostility--or favoritism--towards the underlying message expressed.").

147 See *supra* note 86.

148Turner Broadcasting, 114 S. Ct. at 2470.

[W]hen the government defends a regulation on speech . . . it must do more than simply posit the existence of the disease sought to be cured (citation omitted) . . . It must demonstrate that the recited harms are real, not merely conjectural, and that the regulation will in fact alleviate these harms in a direct and material way.

*Id.*

149The government has the right to restrict or control speech that is classified as obscene or is involved with child pornography. See e.g., Miller v. California, 413 U.S. 15 (1973) (obscenity); New York v. Ferber, 458 U.S. 747 (1982) (actual depiction of sexual acts by a child under sixteen); Roth v. United States, 354 U.S. 476 (1957) (obscenity).

150See Stanley v. Georgia, 394 U.S. 557, 566 (1969) (describing the purpose of the First Amendment, "Its guarantee is not confined to the expression of ideas that are conventional or shared by a majority . . . And in the realm of ideas it protects expression which is eloquent no less than that which is unconvincing.") (quoting Kingsley Int'l Pictures Corp. v. Regents, 360 U.S. 684, 688-89 (1959)); Roth v. United States, 354 U.S. 476, 484 (1957) ("All ideas having even the slightest redeeming social importance--

unorthodox ideas, controversial ideas, even ideas hateful to the prevailing climate of opinion--have the full protection of the guaranties, unless excludable because they encroach upon the limited area of more important interests.").

151 See e.g., *Turner Broadcasting*, 114 S. Ct. at 2458 ("At the heart of the First Amendment lies the principle that each person should decide for him or herself the ideas and beliefs deserving of expression, consideration, and adherence. Our political system and cultural life rest upon this ideal. (citations omitted) Government action that stifles speech on account of its message, or that requires the utterance of a particular message favored by the Government, contravenes this essential right"); *Texas v. Johnson*, 491 U.S. 397 (1989) (holding that the state could not punish a protester who burned the American flag); *Tinker v. Des Moines Indep. Community Sch. Dist.*, 393 U.S. 503 (1969) (holding that students had the right to wear black armbands in school to voice their protest over American involvement in the Vietnam War); *Police Dept. v. Mosley*, 408 U.S. 92 (1972) (holding that an ordinance that prohibited all picketing except labor picketing was unconstitutional because it selectively excluded one type of picketing from a general ban because of the content of the message the picketing was intended to convey).

152 See *Turner Broadcasting*, 114 S. Ct. at 2459 ("Our precedents thus apply the most exacting scrutiny to regulations that suppress, disadvantage, or impose differential burdens upon speech because of its content."). See also *Denver Area Educ. Telecommunications Consortium v. Federal Communications Comm'n*, 116 S. Ct. 2374, 2385 (1996) ("This tradition teaches that the First Amendment embodies an overarching commitment to protect speech from Government regulation through close judicial scrutiny . . .").

153 *ACLU v. Reno*, 929 F. Supp. 824, 866 (E.D. Pa. 1996) (quoting *Sable Communications v. FCC*, 492 U.S. 115, 126 (1989)).

154 See *Shea ex rel. American Reporter v. Reno*, 930 F. Supp. 916 (S.D.N.Y. 1996) (holding that if a "federal statute or regulation purports to limit freedom of expression, its vagueness will 'operate [] to inhibit the exercise' of such freedom and violates the First Amendment").

155 *ACLU*, 929 F. Supp. at 866 (A strict scrutiny analysis will require the government to "demonstrate that the recited harms are real, not merely conjectural, and that the regulation will in fact alleviate these harms in a direct and material way.") (quoting *United States v. National Treasury Employees Union*, 115 S. Ct. 1003, 1017 (1995)).

156 When the author notes "traditional" freedom of speech he means those that "abridge" or directly prohibit certain forms of speech.

157 See *THE INTERNET UNLEASHED* 1996, *supra* note 12.

158NAACP v. Alabama ex rel. Patterson, 357 U.S. 449, 462 (1958) ("Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs"). See also Roberts v. United States Jaycees, 468 U.S. 609, 617 (1984) (maintaining that two important aspects of the First Amendment are the freedom to associate to engage in protected speech and the protection to enter into and maintain certain intimate relationships).

159357 U.S. 449 (1958).

160Id. at 452. The NAACP maintained the position that it was not subject to the statute in question. Id. In the alternative, if it was subject to the statute mandatory disclosure of membership would violate rights of speech and assembly. Id.

161Id. at 452-54. The organization feared reprisals to the individual members if such information was revealed. Id. at 454.

162Id. at 462. The Court shared the same concerns of the NAACP regarding forced identification of membership in that members would face threats forcing them to withdraw and preventing others from joining. Id. at 462-63. The Court noted the, "vital relationship between freedom to associate and privacy in one's associations." Id. at 462.

163See Shelton v. Tucker, 364 U.S. 479 (1960) (invalidating a state statute which required public school teachers to reveal to the state contributions to or memberships in any organization during the previous five years); Gibson v. Florida Legislative Investigation Comm., 372 U.S. 539 (1963) (holding the NAACP could deny the government access to its membership lists on the basis of its right of association.); Bates v. Little Rock, 361 U.S. 516 (1960) (extending protection beyond organizations members to its contributors, when revelation of contributors would essentially be a revelation of members).

164See Roberts v. United States Jaycees, 468 U.S. 609, 622 (1984) (stating the right to associate is the ability "to associate with others in pursuit of a wide variety of political, social, economic, educational, religious, and cultural ends."). See also Tien, *supra* note 108, at 179-84. Tien discusses the Roberts decision and how the Court there distinguished between expressive and intimate association rights noting expressive association rights are protected on "instrumental" grounds while intimate association rights are protected on "intrinsic" grounds as a "fundamental element of personal liberty." Id. at 179 Tien goes on to speculate how association rights may be applied on the Internet noting, "That individuals use online messages to associate provides another basis for First Amendment protection, because prohibition of anonymity will also effectively prevent associations from concealing their members' identities." Id. at 181.

165See Bovenzi, *supra* note 11, at 104.

The identities of people using certain services or advocating certain views through "anonymous" e-mail might well be of interest to the government; but the First Amendment should allow and perhaps require sysops (system operators) to withhold that information. Thus, sysops should be able to prevent the government from accessing all of the information contained in their user records. (footnote omitted) Like the anonymous pamphleteers and the NAACP members, their identities would seem to be protected by the twin rights of privacy and assembly.

Id. (clarification added).

166See Tien, *supra* note 108, at 182.

A significant part of online life takes advantage of the way that online communications allow geographical and other barriers to be transcended, so that persons may exchange information and experiences about medical, sexual, familial, and other matters which go to the heart of personal identity. These associations are both expressive and intimate, and the state should not have the power to interfere with the groups' choice to permit anonymity without substantial justification.

Id.; see also Cavazos & Morin, *supra* note 1, at 15-16 (discussing the Right to Associate online and noting that an organization's mailing lists and bulletin board user lists are the online equivalent of the organization's membership lists which the Court protected in the NAACP case. "Surely, the sense of community that develops in some online situations resembles an association for purposes of constitutional law analysis.").

167Jerry L. McDaniel, III, Comment, *Constitutional Law: Florida's Privacy Protection for Obscenity*, 43 FLA. L. REV. 405, 405-08 & n.10 (1990). The traditional concept of privacy is that of freedom from intrusion into one's home or the "right to let alone" and is often founded on the Ninth Amendment. Id. See also *Olmstead v. United States*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting). Discussing the fundamental right to be free from unwanted governmental intrusions into one's privacy, noting the founders of the Constitution:

undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, and their sensations. They conferred, as against the government, the right to be let alone--the most comprehensive of rights most valued by civilized man.

See generally Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 15 HARV. L. REV. 193 (1890); *Griswold v. Connecticut*, 381 U.S. 479 (1965). For Supreme Court decisions resting on the concept of "liberty" in the Fourteenth Amendment to encompass a right of privacy See e.g., *Zablocki v. Redhail*, 434 U.S. 374 (1978); *Moore v. City of East Cleveland*, 431 U.S. 494 (1977); *Roe v. Wade*, 410 U.S. 113 (1973); *Eisenstadt v. Baird*, 405 U.S. 438 (1972); *Loving v. Virginia*, 388 U.S. 1 (1967); *Pierce v. Society of*

Sisters, 268 U.S. 510 (1925); Meyer v. Nebraska, 262 U.S. 390 (1923). See generally Paul G. Kauper, Penumbrae, Peripheries, Emanations, Things Fundamental and Things Forgotten: The Griswold Case, 64 MICH. L. REV. 235 (1965); Russell L. Caplan, The History and Meaning of the Ninth Amendment, 69 VA. L. REV. 223 (1983); Thomas B. McAfee, The Original Meaning of the Ninth Amendment, 90 COLUM. L. REV. 1215 (1990).

168See Johns, *supra* note 1, at 1432-36. Johns discusses the privacy concerns of the Internet in describing how the government may be able to avoid the Fourth Amendment requirements by convincing online service providers to monitor private chat rooms or e-mail messages out of the fear of liability being asserted against them. *Id.* The comment notes that the recent investigation of the FBI in cooperation with American Online (AOL) culminated in an FBI search of 125 homes and offices for allegedly using the online service to distribute or receive child pornography. *Id.* at 1435.

169See Brandeis & Warren, *supra* note 167, at 220 ("The common law has always recognized a man's house as his castle, impregnable, often, even to its own officers engaged in the execution of its commands. Shall the courts thus close the front entrance to constituted authority, and open wide the back door to idle or prurient curiosity.").

170In fact, online privacy is valued and is receiving some protection under the Electronic Communications Privacy Act (ECPA), 18 U.S.C. §§ 1367, 2521, 2701-09, 2711, 3117-27 (1997). The Act basically provides that it is illegal for someone to intercept or disclose the contents of any private electronic communication. See also *Steve Jackson Games, Inc. v. United States Secret Serv.*, 816 F. Supp 432 (W.D. Tex.1993) (finding the government violated the ECPA in seizing the plaintiff's computer system containing the company's bulletin board service).

171CAVAZOS AND MORIN, *supra* note 1, at xiii. "The law, especially as it relates to computer-mediated communications is constantly changing. Existing statutes are amended, reinterpreted, and repealed and new statutes are enacted . . . The problems that result from attempts to define a dynamic system using a static medium are obvious-the solutions less so." *Id.* See also *ACLU v. Reno*, 929 F. Supp 824, 858-59 (E.D. Pa. 1996) ("First Amendment jurisprudence has developed into a study of intertwining standards and applications, perhaps as a necessary response to our ever-evolving culture and modes of communication.").

172See Johns, *supra* note 1, at 1437 (stating, "Cyberspace blurs the boundaries between once distinct media and thus demands evolutionary and even revolutionary approaches . . . in formulating new legal doctrine, lawmakers should recognize, empower and learn from the multitude of self-regulating structures that have already been developed by the users and administrators of cyberspace"). See also Fulton, *supra* note 1, at 64 ("The rapid growth of computer technology has left the law in the dust.").

173See Johnson, *supra* note 65, at 66-72 (providing a review of regulations of traditional mass media of broadcast media, cable T.V. and common carriers, noting, "...the

pervasiveness of the medium into the home where children may be present, as well as its concurrent accessibility, have been the pivotal factors courts have used to distinguish broadcast from other mass communications media.") Id. at 66-67.

174See *Cyber Promotions, Inc. v. America Online, Inc.*, 948 F. Supp 436 (E.D. Pa. 1996) ("Communications over the Internet do not 'invade' an individual's home or appear on one's computer screen unbidden. Users seldom encounter content 'by accident.'")(quoting *ACLU v. Reno*, 929 F. Supp 824, 845 (E.D. Pa. 1996)).

175See *ACLU*, 929 F. Supp at 845 ("[T]he receipt of information on the Internet requires a series of affirmative steps more deliberate and directed than merely turning a dial. A child requires some sophistication and some ability to read to retrieve material and thereby to use the Internet unattended.").

176Johnson, *supra* note 65, at 93-94 (discussing the non-intrusive nature of the Internet and that its audience has the ability to choose to avoid objectional speech, "Interactive and online information services do not intrude upon the sanctity of an unwilling viewers home."). See also Jerry Berman & Daniel J. Weitzner, *Abundance and User Control: Renewing the Democratic Hear of the First Amendment in an Age of Interactive Media*, 104 *YALE L.J.* 1619 (1995) (generally discussing how the lack of user control has provided the justification for regulations of the the traditional mass media fields and that the availability of control mechanisms may make similar regulations in cyberspace unconstitutional).

177 See *infra* notes 178 & 180.

178Beyond certain "blocking" software that is available, Microsoft has backed the idea of instituting a worldwide ratings system for online information, enabling parents and teachers to screen out violence and offensive material. See Peter Lewis, *Microsoft Backs Ratings System for the Internet*, *N.Y. TIMES*, Mar. 1, 1996, at D1. Microsoft has labeled such a system as RSAC-I and would offer a blocking option to any site which does not have the appropriate ratings. Id.

179See *Shea v. Reno ex rel. American Reporter*, 930 F. Supp 916, 933-34 (S.D.N.Y. 1996) (discussing the development of filtering software and other "blocking" mechanisms which have been developed by the industry with the most major online service providers allowing these control options free of charge to their customers).

180Id. at 932. The software is called Surfwatch. Id. Another popular screening/blocking software is called Cyber Patrol. Id. They both maintain a list of sites determined by the programmer to carry sexually explicit or indecent material and the user is then blocked for obtaining access to those sites. Id.

181 See *Pierce v. Society of the Sisters of the Holy Names of Jesus and Mary*, 268 U.S. 510, 534-35 (1925) ("[t]he child is not the mere creature of the state; those who nurture him and direct his destiny have the right, coupled with the high duty, to recognize and

prepare him for additional obligations." See also *Parham v. J.R.*, 442 U.S. 584 (1979) stating:

Our Jurisprudence historically has reflected Western civilization concepts of the family as a unit with broad parental authority over minor children . . . the law's concept of the family rests on a presumption that parents possess what a child lacks in maturity, experience, and capacity for judgment required for making life's difficult decisions. More importantly, historically it has been recognized that natural bonds of affection lead parents to act in the best interests of their children.

*Id.* at 602.

182 See *Sable Communications of Calif., FNC. v. F.C.C.*, 492 U.S. 115 (1989); *Bolger v. Yongs Drug Prods. Corp.*, 463 U.S. 60 (1983); *Butler v. Michigan*, 352 U.S. 380 (1957) (each case holding the respective legislation in question with its aim or goal of protecting children could not take precedence over protected First Amendment rights).

183 *Shea*, 930 F. Supp at 932. Describing other attempts the computer industry has taken including the World Wide Web Consortium which "launched the Platform for Internet Content ("PICS") to develop technical standards for attaching electronic ratings to Internet addresses." *Id.* This will include browsers, news group readers, and mail readers. *Id.* Thus, the computer user could readily identify what type of site their computer has accessing and block any one that is found undesirable.

184 See *Johnson*, supra note 65, at 97-98 (quoting a statement by Civil Libertarian Mike Godwin, the staff counsel for the Electronic Frontier Foundation).

185 See *Knoll*, supra note 3, at 278-300 (outlining the development of self-regulation on the Net and how the U.S and other countries are attempting to develop workable regulations).

186 *Knoll*, supra note 3, at n.17 (explaining how inappropriate behavior is governed on the Net. If enough people find the behavior offense or indecent, they may retaliate by sending messages to the offender. If enough people respond and flood the offender's mailbox, this can shut that site down completely) (quoting G. Gurgess Allison, *THE LAWYERS GUIDE TO THE INTERNET* at 338 (1995)).

187 Mr. Bungle was a pseudonym a user utilized in interacting online. See generally, Julian Dibbell, *A Rape in Cybersapce or How an Evil Clown, A Haitian Trickster Spirit, Two Wizards, and a Cast of Dozens Turned a Database into a Society*, 1994, *ANN. SURV. AM. L.* 471 (1994) (thoroughly discussing the Mr. Bungle incident in detail and how it was resolved by the members of the particular virtual community).

188 *Id.* at 471.

189Id. at 473-74. (describing a MUD as a type of virtual reality, a database designed to provide user the sense of being present in a physical space).

190Id. at 471-74 (detailing the actions of Mr. Bungle in the virtual community of 1500 members).

191Dibbell, *supra* note 187, at 477-78 (describing a toading as the equivalent to a "death warrant" in the virtual cyber communitiy).

192Id.

193The Communications and Decency Act (CDA) of 1996, restricted certain indecent communications over computer networks. The CDA was recently struck down by the Supreme Court in *Reno v. ACLU*, 117 S. Ct 2329 (1992). The Court held key provisions of the CDA were overbroad and vague as the statute would effectively keep "indecent" material from adults who have a right to see such material. Id. at 2331-32.

19447 U.S.C. §§ 223 a-233h (1997 electronic update). The CDA is really only part of the larger Telecommunications Act of 1996, which amended the Telecommunications Act of 1934, 47 U.S.C § 201 et. seq. Robert Cannon, *The Legislative History of Senator Exons Communications Decency Act: Regulating Barbarians on the Information Superhighway*, 49 FED. COMM. L.J. 51, 92 (1996).

195See *Denver Area Educational Telecommunications Consortium, Inc. v. Federal Communications Comm'n*, 116 S. Ct. 2374, 2384 (1996) ("The history of this Court's First Amendment jurisprudence . . . is one of continual development . . . the Constitution's general command . . . has been applied to new circumstances requiring different adaptations of prior principles and precedents.").

196See Gara Lamarche, *International Free Expression Principles in Cyberspace*, 17 WHITTIER L. REV. 279 (1995) ("Every new developing technology brings challenges and opportunities which frighten people with power, and empower people without power. That was true of the printing press. It was true of the telegraph. It was true of the telephone, the radio, television, and now it is true of cyberspace.").

197See *supra* part IV.

198See *supra* notes 60-80 and accompanying text.

199See *supra* notes 2 and 4.

200See Van Valkenburg, *supra* note 101, at 329 (paraphrasing Justice Holmes) (quoting OLIVER WENDELL HOLMES, *THE COMMON LAW* 1 ( Boston, Little Brown 1881)). See also *Abrams v. United States*, 250 U.S. 616, 630 (1919) (Holmes, J., dissenting) stating:

[W]hen men have realized that time has upset many fighting faiths, they may come to believe even more than they believe the very foundations of their own conduct that the ultimate good desired is better reached by free trade in ideas--that the best test of truth is the power of the thought to get itself accepted in the competition of the market....

Id.

201McIntyre v. Ohio Elections Comm'n, 115 S. Ct. 1511, 1524 (1995).