

**AMERICAN CIVIL LIBERTIES UNION  
OF UTAH FOUNDATION, INC.**  
Darcy Goddard (Utah Bar No. 13426)  
355 North 300 West  
Salt Lake City, UT 84103  
Telephone: (801) 521-9682, x108  
Facsimile: (801) 532-2850  
Email: dgoddard@aclu.org

**SNR DENTON US LLP**  
Michael A. Bamberger (Pro Hac Vice)  
Richard Zuckerman (Pro Hac Vice)  
1221 Avenue of the Americas  
New York, NY 10020  
Telephone: (212) 768-6756  
Facsimile: (212) 767-6800  
Email: michael.bamberger@sndenton.com  
richard.zuckerman@sndenton.com

**CENTER FOR DEMOCRACY  
& TECHNOLOGY**  
John B. Morris, Jr. (Pro Hac Vice)  
1634 Eye Street, NW # 1100  
Washington, DC 20006  
Telephone: (202) 637-9800 ext. 116  
Facsimile: (202) 637-0968  
Email: jmorris@cdt.org

Attorneys for Plaintiffs

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF UTAH, CENTRAL DIVISION**

---

NATHAN FLORENCE, et al., )  
Plaintiffs, ) Civil No. 2:05CV00485 DB  
vs. )  
MARK SHURTLEFF, et al., )  
Defendants. )  
Judge Dee Benson  
Magistrate Judge Samuel Alba

---

**EXPERT DECLARATION OF SCOTT BRADNER**

I, Scott Bradner, depose and state as follows:

1. I have been retained by plaintiffs as an expert in this case and am submitting this declaration in support of plaintiffs' motion for injunctive relief.
2. I am not being paid for my time for work on this case but will bill plaintiffs for any expenses.

3. With respect to this particular case, I have read the Complaint and the Utah statutes at issue, Utah Code §§ 76-10-1206 and 76-10-1233, as amended by H.B. 260 and H.B. 5 (the "Challenged Statutes").
4. I am currently employed as the University Technology Security Officer in the Harvard University's Office of the CIO.
5. Starting in 1972, and continuing for many years afterward, I was involved in Harvard's connection to the ARPANET, the precursor to the Internet.
6. Starting in 1986, and continuing for many years afterward, I was involved in the design and operation of Harvard's Internet connection. I was also involved in the design and operation of Harvard's initial e-mail, USENET and web servers and services.
7. I was responsible for establishing the first USENET newsgroup server at Harvard University almost 30 years ago. Similarly, I have established and operated a variety of "mail exploder" programs and services (sometimes known as "listservs") at the University over the past 30 years. I developed most of Harvard's original e-mail connections and the University's e-mail aliasing system. I have also supervised the operation of some of the World Wide Web servers at the University.
8. I have also been involved in the Internet Engineering Task Force (IETF), the group that is primarily responsible for the technical standards used to operate the Internet. Over the years I served in a number of management roles in the IETF. The IETF is composed of multiple Areas, each of which deals with standards and activities of a facet of the Internet. I was co-director of the Operational Requirements Area, the part of the IETF that deals with standards and procedures for operating the Internet, from 1993 to 1997. I was co-director of a special IP Next Generation Area, which was charged with developing the standard for the future Internet communications protocol, from 1993 to 1996. I was co-director of the Transport Area, which is responsible for the development of standards relating to end-to-end communications over the Internet, from 1997 to 2003. I was also co-director of a special Sub-IP Area, which was responsible for technical standards used in organization-to-organization communications over the Internet, from 2001 to 2003. In addition I was or am the chair or the co-chair of seven different IETF working groups, where the actual standards development takes place, between 1991 and the present. I was also the liaison between the IETF and the International Telecommunication Union Telecommunication Standardization Sector (ITU-T), which is responsible for international telecommunication standards, from 1995 to 2009.
9. The Internet Society (ISOC) is a nonprofit organization founded in 1992 to provide leadership in Internet related standards, education, and policy. With offices in Washington D.C., USA, and Geneva, Switzerland, it is dedicated to ensuring the open development, evolution and use of the Internet for the benefit of people throughout the world. The IETF is an organized activity of the ISOC. I served as an elected trustee of the ISOC and a member of the ISOC Board of Trustees from 1993 to 1999, as the ISOC Vice President for Standards from 1995 to 2003 and am currently Secretary to the ISOC Board.

10. The American Registry for Internet Numbers (ARIN) is the organization responsible for assigning Internet addresses in the US, Canada and part of the Caribbean. I have been a Trustee and a member of ARIN's Board of Trustees since ARIN's founding in 1997.
11. I was a co-founder of the New England Academic and Research Network (NEARnet), the first high-speed Internet service provider in the Boston area. I served on the NEARnet Steering Committee and as the chair of the NEARnet Technical Committee from 1989 to 1995.
12. I also operate my own web, domain name and email servers to support my personal website, [www.sobco.com](http://www.sobco.com), a website for my photography, [www.scottbradner.com](http://www.scottbradner.com) and a website for my sister's art, [www.kaybradner.com](http://www.kaybradner.com).
13. In the course of my work with the Internet Engineering Task Force, the Internet Society, NEARnet, Harvard University and in support of my own Internet presence, I have developed extensive knowledge of all aspects of Internet communications and operations.
14. On the basis of my knowledge, skill, training, and experience, I consider myself qualified to testify as an expert in the area of the operations and capabilities of the Internet, in particular in the areas of the methods of communication over the Internet and the technological and practical feasibility of modifications to those communications standards.
15. A copy of a fuller resume is attached hereto as Attachment A.
16. This document is based on, and updated from, the declaration I provided in the Communications Decency Act challenge in 1996 ([ACLU v. Reno](#), 521 U.S. 844 (1997)).

### **Summary Of Areas And Opinions Covered In This Declaration**

17. This declaration includes the following subject areas and opinions:
18. For the vast majority of Internet communications and information, including those potentially subject to prosecution under the Amended Statute, it is not technically, economically and/or practically feasible for organizational or individual speakers to ascertain the age of persons accessing materials over the Internet, or to restrict or prevent access by minors to them.
19. For the vast majority of Internet communications and information, including those potentially subject to prosecution under the Amended Statute, it is not economically and/or practically feasible for organizational or individual speakers to ascertain the geographic location of persons accessing materials over the Internet, or is it technically, economically and/or practically feasible to restrict or prevent these communications and materials from traveling through or being received in Utah.
20. Most communications and information on the Internet are available for free, even when displayed or disseminated by a commercial organization. Requiring users to register and provide personal data in order to receive such information will deter them from exploring or

receiving such information to the detriment of commercial interests, users, and the development of new business models made possible by the Internet.

21. The majority of communications and materials on the Internet that could be subject to the prohibitions of the Amended Statute are published outside the United States, and such material will continue to be as available to minors searching for it as information displayed or posted in Utah itself.
22. Widely available, user-based methods and tools, which can block out unwanted material or services regardless of geography or commercial purpose, provide a far more effective and less restrictive alternative for parents and families to control access by minors to information that is deemed unsuitable based on individual family values and circumstances.

## **1. Control and Oversight over the Internet**

23. The use of the Internet is very wide-spread in the US and in the rest of the world. According to a 2010 ITU-T report, world-wide Internet usage reached 1.7 billion people (26% of the world's population) in 2009 and 62% of US households had internet access in 2008. The percentage is undoubtedly quite a bit higher by now. A 2011 report by the US Central Intelligence Agency listed 216 countries as having Internet access in 2009. The same report counted 245 million US Internet users – that means that the US accounts for only about 15% of the global Internet users. The Internet, which started in the US, is now far larger outside the US than inside. The Internet research site Netcraft reported that there were 206 million websites on the Internet in June 2010.
24. No organization or entity operates or controls the Internet. The Internet consists of tens of millions of local networks linking hundreds of millions of computers, owned by governments, public institutions, non-profit organizations, private companies and individuals around the world. These local networks are linked together by thousands of commercial and non-commercial Internet service providers (ISPs) that interconnect at dozens of exchange points throughout the world. None of these entities, however, controls the Internet; each entity that operates a part of the global Internet only controls its own computers and computer networks.
25. Although no organization controls the Internet, a limited number of organizations are responsible for the development of communications and operational standards and protocols used on the Internet. These standards and protocols are what allow the millions of different (and sometimes incompatible) computers worldwide to communicate with each other. These standards and protocols are not imposed on any computer or computer network, but any computer or computer network must follow at least some of the standards and protocols to be able to communicate with other computers over the Internet.
26. The Internet Engineering Task Force (IETF), mentioned above, is a self-organized group of people operating under the auspices of the Internet Society (ISOC) who make technical and other contributions to the engineering and evolution of the Internet and its technologies. It is the principal body engaged in the development of new Internet standard specifications.

27. The World Wide Web Consortium (W3C) has developed technical specifications for information exchange and display used in the World Wide Web, which runs over the Internet, and on websites such as [www.cnn.com](http://www.cnn.com), [www.harvard.edu](http://www.harvard.edu) and [www.kaybradner.com](http://www.kaybradner.com).
28. A number of other standards development organizations (SDOs) develop Internet-related technical standards. For example, the International Telecommunication Union (ITU), the Institute of Electrical and Electronics Engineers (IEEE) and the American National Standards Institute (ANSI) all develop standard for the communications links over which the Internet runs.
29. None of these organizations controls, governs, runs, or pays for the Internet. None of these organizations controls the substantive content available on the Internet, nor do they control the publishers of this content. None of these organizations has the power or authority to require content providers to alter, screen, or restrict access to content on the Internet other than content that they themselves create.

## **2. Internet Architecture and Operations**

30. All information on the Internet, including e-mail messages, web pages, Internet video, Internet telephone, Internet chat and all other types of communications is broken up into packets. Packets are small chunks of information that are forwarded from the sending computer, through one or more locally managed networks to a destination computer. The packets that make up a single communication (for example, an Internet phone call) can take different paths through the Internet on their way from the sending computer to the receiving computer.
31. There are a number of different types of networks making up the Internet. Most non-mobile Internet-connected computers are connected to Ethernets. Ethernet is an IEEE developed standard for communication over physical wires. Ethernets are used in most corporations and in many homes. Mobile Internet-connected computers generally use one of two types of wireless (radio) networking standards. WiFi (officially 802.11) is an IEEE developed standard for wireless networks. WiFi is used in corporations, hotels, coffee shops, bookstores, airports, homes and in some public spaces. The other type of wireless, used to connect mobile computers to the Internet, is the same type of cellular radio as is used in cell phones. There are hundreds of millions of Internet-enabled cell phones; many of them should be considered portable computers with the same power as many desktops - these cell phones are commonly referred to as "smartphones."
32. Local networks are connected to the rest of the Internet by way of Internet service providers (ISPs). For example, I buy Internet connectivity from an ISP operated by a cable TV company to connect the network in my home to the rest of the Internet. Harvard buys Internet connectivity from two large commercial ISPs and is also connected to other US research universities through "Internet 2," which is essentially an ISP run by a university collective. Smaller ISPs interconnect with each other at exchange points located at many places around the world and they buy connectivity to the parts of the Internet they can not reach directly from larger ISPs, which in turn interconnect with other large ISPs at the same

exchange points or through private connections. A packet that is a part of a communication between two Internet-connected computers may traverse many ISPs between the computer that sent the packet and the computer that receives the packet. The specific paths that packets take through the Internet are generally invisible to Internet users.

33. Each computer that is connected to the Internet is assigned an Internet Protocol (IP) address. These IP addresses are used in packets to indicate the sender and intended receiver of each packet. The IP address of a computer connected to a particular network must be unique to the scope of that network. For many computers the scope of the network is the entire Internet so the IP address must be unique across the entire Internet.
34. Many enterprise networks and most WiFi networks are connected to the rest of the Internet using a device that translates the IP addresses in packets as the packets flow from one network to another. These translating devices are known as Network Address Translators (NATs). The IP addresses of computers on networks connected to the Internet through a NAT must only be unique within that network. Most of the networks connected to the Internet through a NAT use ranges of IP addresses that were set aside by the IETF for this purpose. They are known as "private addresses" or RFC 1918 addresses" (after the IETF publication that assigned these ranges of addresses). IP addresses not in the ranges assigned by RFC 1918 are known as "public addresses" and are used when IP addresses must be unique throughout the Internet. To the rest of the Internet it looks like the computers on a network "behind" a NAT all have the same IP address -- that address is the public address of the NAT.
35. Public IP addresses are assigned by regional address registries (RIRs). There are five RIRs, each with its own geographic area. As mentioned above, the RIR that is responsible for the geographic area that includes the US, Canada and much of the Caribbean is the American Registry for Internet Numbers (ARIN). RIRs generally assign ranges of IP addresses to ISPs that, in turn, assign parts of the ranges to the ISP's customers. Some enterprises have also received assignments of IP addresses directly from RIRs.
36. In some cases computers are assigned fixed IP addresses. This is usually the case with Internet-based computers that are offering services to Internet users, such as web sites. But many users' computers on all types of networks are not assigned fixed addresses. They are assigned an IP address out of a pool of addresses when the computer first is turned on or when it is connected to a network. The same IP address will be used by different computers at different times, and the same computer can be assigned different IP addresses at different times.
37. IP addresses are used to indicate just where, in terms of network topology, a particular computer is attached to a network that makes up the Internet. There is no geographic component in an IP address that can be used to determine where the computer is in the real world, only where it is in the network topology. A user connecting to an Internet computer, a web site for example, has no way of knowing where in the world the computer is actually located unless the site itself were to say, on a web page for example, where it was.

38. Some companies collect information on the geographic location of networks, and in some cases, individual computers. Some of these companies offer commercial services that attempt to pinpoint the geographic locations of IP addresses. Such services are used, for example, to select advertising may be relevant to someone in a particular location -- such as the names of local restaurants. Such services are not totally reliable, for example, they can be fooled by wide-area networks that use NATs. Similarly, portable computers using virtual private networking (VPN) for security do not change their IP address even if they are moved from one location to another. A laptop or smart phone using VPN can appear to be in Paris when it is actually in Boston. All the users of such a network appears to be in a single location - the location of the NAT - even when the network, and its users, maybe be national or international in scope. In any event, these are commercial services that charge a fee for their services and thus are not suited for web sites, such as my own, who do not charge for access or even for smaller commercial sites that often cannot afford additional expenses.
39. IP addresses cannot be reliably used to identify particular Internet users. Although IP addresses on the Internet are unique and, in many cases, uniquely identify a particular computer, the computer can be assigned different IP addresses over time, the computer might be on a network connected to the rest of the Internet with a NAT, in which case multiple computers on the local network appear to have the same IP address, or multiple people can use a single computer, as often happens in homes.
40. It is rare for Internet users to actually make direct use of IP addresses. Almost always an Internet user will use a "domain name" to specify which Internet computer they want to communicate with. Examples of domain names include www.cnn.com, www.harvard.edu and www.scottbradner.com. Domain names are human friendly names given to computers and services on the Internet. But since actual Internet communications require the use of IP addresses, domain names are translated into IP addresses when needed using the distributed Internet "domain name system."
41. The right-most part of a domain name is known as the "top-level domain." There are two general types of top-level domains. The first type is known as "generic top-level domains (gTLDs)." These include ".com", ".net", ".org" and ".biz." The other type of top-level domain is the "country code top-level domain (ccTLDs)" type. ccTLDs use international standard two character codes for world economic zones to indicate countries. Examples of ccTLDs include ".us", for United States, ".fr" for France and ".tv" for the South Pacific island nation of Tuvalu . In most cases the use of a ccTLD indicates that the computer is located in, or provides services to, a particular country. A computer may move while maintaining the same domain name. Some ccTLDs have been developed for general, rather than country-specific, use. One example is .tv, which has been marked around the world for TV stations and TV-related services. An email address or a website with a domain name ending in a gTLD, such as .com or .edu, could be located anywhere in the world and there is no reliable way for an Internet user to determine that location.
42. Users connect their computers to the Internet in a number of different ways. Those users whose computers are connected to an Ethernet in an enterprise or a home sometimes have to identify themselves to a server on the network and sometimes to not, depending on how the network was set up. The ISP that connected the enterprise or home to the rest of the Internet

has no way of knowing if the user had to identify themselves nor does it have any way to know what identity was used. Many wireless networks do not require users to identify themselves when they connect to the network. Wireless networks in many hotels, coffee shops, bookstores, airports, homes and public spaces do not request any identification before permitting the user to connect to the Internet. Some wireless networks, and some wired networks in hotels, do require some identification, and, often a credit card number to bill the connection to but they do not collect information on the age of the user.

### **3. Characteristics of Internet Communications**

43. There are a wide variety of methods that people use to communicate over the Internet, including electronic mail (e-mail), mail exploders (a.k.a. listservs), Internet Chat, instant messaging, the World Wide Web, blogs, twitter, video streaming, and social networking web sites. Some of these methods can be used in a mode that involves communication from one Internet user to a selected individual other Internet user (a "person-to-person method), these include e-mail, instant messaging, VoIP and audio and video streaming.
44. In a person-to-person method it is possible for a sender to know if the receiver is a minor, if the receiver is personally known to the sender. But, in many cases, the only information a sender has is an identifier (for example an e-mail address) of a receiver. There is no mechanism for a sender to know if a potential receiver is a minor if the receiver is not known to the sender since there is no Internet mechanism to "look up" a email address to find out the age of an Internet user.
45. But all of the above person-to-person methods, as well as the other methods listed above, and many others, can operate in a "one-to-many" mode where a single sender is communicating with more than one receiver. For example, I can post something on my web page that millions of people around the world could read or I can send a message to a mail exploder that could reach thousands of readers.
46. With each of these one-to-many methods of communication, the speaker has little or no way to control or verify who receives the communication or where the user is when they receive the communication. Thus it is not possible for a person sending or posting a communication in this mode to ensure that the communication will not be read or seen by a minor.
47. Except in cases where filters on user's machines or filters installed in the network, such as those in China, block specific communications, anything posted to an Internet site is accessible from anyplace on the Internet. For example information posted to the Louvre Museum's website in Paris, France can be accessed by Internet users in Utah. The cost of accessing a website is the same, regardless of where in the world the computer offering the website is located. Thus, a user can access my websites, located in Massachusetts, the Louvre Museum's website, located in France, and the official website for the 2010 World Cup, located in Cape Town, South Africa for free if the user is having a cup of coffee in a Starbucks, which offers free WiFi Internet access. It should be noted that there is no guarantee that a web site associated with a real-world site, such as the Louvre Museum, is actually located at the museum. In many cases, enterprises out-source their websites to be run by companies that are in the web site business. For example, a museum's web site might

be physically located in a different state, or even in a different country than the museum itself.

48. To enhance performance it is common for larger web sites to contract with companies such as Akamai or Limelight to keep copies of the web site content in many places around the world. This distribution brings the content closer to the users and provides for a better user experience. These systems are known as "content distribution networks (CDNs)." Even if a website were to be in a known physical location, if that website were using a CDN, a user could not know where the content was actually located. Copies of content for a website in New York could just as easily wind up being stored on a CDN server in Utah without the website owner knowing where the copy was stored.
49. Electronic mail (e-mail) is one of the oldest ways to communicate over the Internet. With e-mail one Internet user can send one or more other Internet users a message using a e-mail address (such as scott\_bradner@harvard.edu) to indicate the intended recipient(s) of the message. Hundreds of millions of people all over the world use Internet e-mail. There is no comprehensive list of Internet e-mail addresses, much less a list of e-mail addresses that also includes information about the holders of the addresses that might include, for example, their ages. Thus, given an e-mail address, an Internet user has no way to know if the e-mail address holder is a minor. The act of replying to a received e-mail message could result in sending material to a minor without the sender having any idea that this is the case.
50. Internet users get e-mail accounts from their jobs, schools, their ISPs or from one or more of the many companies, such as Microsoft's Hotmail or Google gmail, that are in the business of providing e-mail accounts. Some of these services are free. The free services do not verify that the person setting up an account is using their real name. None of the services that I know of verify the age of a subscriber. Thus, knowing the email address of another Internet user does not enable a Internet user know anything about that other user, including their age, unless that information is known through some other means, such as a personal relationship with the other Internet user. E-mail accounts are also often shared, which makes it even harder to determine if the user who would read a message is a minor.
51. Many Internet users do not use their real names when setting up Internet e-mail accounts or when accessing web sites because they wish to be anonymous. They may want anonymity because they wish to not disclose their medical condition or their political opinion to people that might know them.
52. With electronic mail, there is a complete electronic and temporal "disconnect" between the sender and recipient in e-mail. E-mail can be routed through numerous computers between the sender and the recipient, and the recipient may not "log in" to retrieve mail until days or even weeks after the sender sent the mail. Thus, at no point in time is there any direct or even indirect electronic linkage between sender and recipient that would allow the sender to interrogate the recipient prior to sending an e-mail message.
53. In addition, there exist "anonymous remailers," which replace the original e-mail address on messages with a randomly chosen new one. The remailer keeps a record of the relationship between the original and the replacement name so that return mail will get forwarded to the

right person. These remailers are used frequently for discussion or support groups on sensitive or controversial topics such as AIDS. Equivalent anonymizing mechanisms exist for most forms of Internet communication. A minor could make use of such a system to mask their identity when communicating over the Internet.

54. Person to person and person to a small list of other persons are not the only way that e-mail is used in the Internet. An e-mail address can also be the address of a "mail exploder" (a.k.a. listserv) that maintains a list of many, in some cases millions, of e-mail addresses and forwards any messages it receives to each e-mail address in the list. There are millions of e-mail lists of this type on the Internet, each one dedicated to some topic or group. For example, the IETF maintains e-mail lists for each of its working groups as well as a number of additional e-mail lists for people interested in IETF activities. Many e-mail lists, including most of the IETF ones, use a self-subscription mechanism. If you are interested in the work of an IETF working group you can send a subscription request email to the list or go to a web page and request that your e-mail address be added to the mailing list. Some e-mail list servers have a mechanism that enables people to retrieve a list of subscribers but the list is just of e-mail addresses and, sometimes, names. Most do not. The IETF lists do not include such a mechanism because of the risk that people will retrieve e-mail address to be used to send unsolicited advertising messages. It is now common that the list retrieval mechanism is disabled in Internet mailing lists. Because of this there is no way for someone sending to the e-mail list to know who is on the list and will be receiving the message being sent. The sender also has no way to know if any list subscribers are minors.
55. The most common way to access content on the Internet is through the use of the World Wide Web. The World Wide Web consists of hundreds of millions of Internet-connected web sites. The operator of each web site uses it to make content available to Internet users. As mentioned above, most web sites make some or all of their content available for free and most do not require the visiting Internet user to identify themselves. As also mentioned above, I operate a number of personal web sites myself. In addition, I am involved in creating content for the security web site at Harvard ([www.security.harvard.edu](http://www.security.harvard.edu)). Web sites range from quite small, with only a few pages of content, to very large, with tens of thousands of pages. Many different web sites can operate on the same web server and share the same IP address. For example, all of my personal web sites operate on the same server and share that server's IP address even though they all have different domain names. This is the case with the four websites I run on my home computer: [www.sobco.com](http://www.sobco.com), [www.sobco.org](http://www.sobco.org), [www.scottbradner.com](http://www.scottbradner.com) and [www.kaybradner.com](http://www.kaybradner.com). A 2003 study by Ben Edelman, then at the Harvard Law School, determined that 87% of web sites used shared IP addresses and some cases more than 100,000 websites shared the same IP address. ([http://cyber.law.harvard.edu/archived\\_content/people/edelman/ip-sharing/](http://cyber.law.harvard.edu/archived_content/people/edelman/ip-sharing/) - visited 7/16/2010) This sharing of IP addresses means that any attempt to block access to a single website by blocking access to a particular IP address can result in large numbers of unrelated web sites being blocked.
56. Web sites are connected to other websites with hyperlinks. Text that can be clicked on to activate a hyperlink is often displayed as underlined or in a different color on a web page, but that type of differentiation is not required. In addition, a web site can include areas, often known as "buttons", which activate hyperlinks when clicked on. Activating a hyperlink will

cause a user's web browser to jump to another part of the same website or to a different website altogether. There is no reliable way for a user to know where in the real world a hyperlink will take them before they click on it. Web site operators can include hyperlinks that point to any other websites without the knowledge or approval of the operator of the website being pointed to.

57. Most non-commercial web sites do not require visitors to log in to the web site and few of those that do, verify an identity provided by a visitor. Some commercial web sites charge a fee for access. Those sites generally require that the visitor provide a credit card and thus, attempt to identify their users. But, as widely reported, millions of credit card numbers are stolen each year so the knowledge of a credit card number and matching name does not guarantee that the actual owner is the web site visitor. In addition, many minors either have their own credit cards or given credit card numbers by their parents.
58. Internet blogs are a special type of web site. With most blogs, the blog operator regularly posts messages of commentary about topics of interest to the blog operator. Common blog topics include politics, the blog operator's day-to-day life and experiences, technology, travel and entertainment. Many corporations and politicians run blogs to tell the world what they are doing or their opinion on some topic. Users subscribe to blogs by connecting to the web site. Most blogs do not require any kind of registration for Internet users who just want to read postings. Some blogs also enable readers to post comments on the blog operator's postings. Most of the blogs that support posting do require some type of login and identification but many of them permit the use of pseudonyms thus have no way of knowing the actual identity or age of their readers or posters. Blog posters have no way to know if someone reading the blog is a minor.
59. Twitter has been described a "microbloging site." Twitter is a web site that operates a very popular service that operates in general like a blog site but limits the length of postings to a maximum of 140 characters. As of March 2011 there were around 200 million or more Twitter users sending a billion tweets a week. Twitter requires users set up an account in order to post but does not require an account just to read what others post. Twitter requests a user's full name and email address when an account is set up but does not verify that the name is the user's actual name nor does Twitter ask the user's age. Thus, an Internet user posting on Twitter has no way to know of any minors might be reading their posts.
60. Social media sites are another special type of web site. Social media sites include special programs to support their users forming groups with similar interests and communicating with each other. The most popular social media web site is Facebook, originally founded by Harvard students. Facebook now has over 500 million active users, 70% of whom are outside the US. These users share 25 billion pieces of content each month. Facebook does ask for the user's date of birth when an account is set up but it does not verify that the date provided is accurate or even that the subscriber is a real person. A Facebook subscriber just has to have a working email address. A Facebook user has no way to know if any minors could be reading their postings.
61. An Internet search engine is a service that searches though the web servers in the World Wide Web and indexes the content of the web pages it finds. Internet users can then connect

to the search engine web site in order to search for web pages that include particular words or combinations of words. A search for a popular term can return a very large number of results. For example, a search for "Obama" on Google on 21 May, 2011 reported that there were 501 million web pages that included the word "Obama" on them. Search engines do not require their users to login nor do they check the age of their users when returning results. This means that the operators of web sites containing content that a minor should not see has no way of knowing if a minor will find their web site through the use of a search engine. The major search engines do include optional configurations that will block search results containing explicit text and/or explicit images, but these configurations are set by the user and can be easily changed by a minor if they know how to do so. Minors searching for images of Brittney (misspelling "Britney" when searching for Britney Spears) would find a number of quite racy photos in the default moderate search mode in a search engine and would find a number of images of hard core sex on the first page of the search results if the safe search filter is turned off. A search for videos of Brittney produces similar results.

62. Internet chat and instant messaging (IM) technologies enable Internet users to send short text messages to each other in real time. Communication can be from one individual to another or between members of a group. Chat and IM groups can be quite large with hundreds or thousands of participants. Chat and IM can also be used between players in some types of interactive Internet games. As with e-mail, chat and IM users cannot be sure of the identity of the Internet users they are communicating with unless they happen to know the other user personally. A sender to a chat or IM group cannot know if there are minors who have subscribed to the group.
63. Web sites such as YouTube offer streaming video on request. YouTube has over 100 million videos to choose from with about 200 thousand new ones uploaded every day. An Internet user needs to have a YouTube account to upload videos but not to view them. YouTube does have a policy that prohibits graphically violent or sexually explicit videos, as well as a number of other types of categories of unacceptable content. But YouTube does not prohibit all types of content that minors should not be viewing. YouTube has a "safety mode" which will block "videos that contain potentially objectionable material" but that mode is not enabled by default. Considering the number of new videos posted every day, YouTube cannot check every video before it is made available for viewing. YouTube depends on its users flagging videos that might violate its policies or videos that should be blocked by the safety mode, YouTube then reviews flagged videos and removes videos that violate the guidelines and tags videos that should be blocked by safety mode. So, at any particular time, YouTube could include thousands of videos that are unsuitable for minors that will not be blocked by safe mode, even if safe mode is enabled. Because Internet users do not have to login to view YouTube videos and because YouTube has no way to know the age of its users, an Internet user posting a video to YouTube has no way of knowing if that video is being viewed by a minor.
64. It is very easy and inexpensive to participate in the Internet. Essentially all personal computers and an increasing number of cell phones come with Internet applications already installed. For example, a person can surf the World Wide Web for free from portable computers, including handheld devices, at over 11,000 McDonalds restaurants in the US. In

addition, all Apple computers come with a web server that can be used to create a personal web site. For example, my web sites run on an out-of-the-box Apple computer.

65. It is easy to produce content for the Internet. For example, most popular personal computer editing programs will save files in a format that can be used on the World Wide Web. This is how I create content for my www.sobco.com website.
66. There are a number of companies that market age verification services to be used by web site or social media site operators to determine the age of their users. These services are fee-based so are not economically feasible for many sites providing free content. Also, many of the services depend on databases which are national in scope so are not useful with Internet users who are outside of the country. In addition, a study of these services by the Harvard Berkman Center for Internet & Society concluded that "[a]ge verification and identity authentication technologies are appealing in concept but challenged in terms of effectiveness. Any system that relies on remote verification of information has potential for inaccuracies. For example, on the user side, it is never certain that the person attempting to verify an identity is using their own actual identity or someone else's. Any system that relies on public records has a better likelihood of accurately verifying an adult than a minor due to extant records. Any system that focuses on third-party in-person verification would require significant political backing and social acceptance. Additionally, any central repository of this type of personal information would raise significant privacy concerns and security issues." (Enhancing Child Safety and Online Technologies, 2010, ISBN 978-1-59460-776-9, page 157)
67. The most reliable method of protecting minors and others from unwanted Internet content is through the use of filtering software installed on the user's own computer. Parents can, and do, install such software on their children's computers and configure it to block access to content that the parent considers unsuitable for the child. Under federal law, such software must be used on public access computers in public libraries that receive federal funds. This type of filtering software is widely available and works without regard to the geographic location of the content and without regard to the commercial or non-commercial nature of the source of the content. The Berkman study concluded that "[f]iltering, monitoring and auditing software can provide parents and other supervisory adults with a useful tool to assist in determining and limiting user access to certain types of inappropriate content. Although not a total solution for minor's online safety, the effective use of these types of tools can be a key part of a holistic solution whereby parental involvement, adult supervision, and software tools work together to provide a safer Internet environment."(Enhancing Child Safety and Online Technologies, 2010, ISBN 978-1-59460-776-9, page 159)
68. Based on my experience and knowledge of the Internet, I believe that the most effective way to monitor, screen, or control the full range of information transmitted over the Internet to block undesired content is at the client end – that is, by using software installed in the individual user's computer. Such software could block certain forms of incoming transmissions by using content descriptive tags in the messages, or could use content ratings developed by third parties to select what can and cannot be retrieved for display on a user's computer.

69. With the exception of electronic mail and e-mail exploders, all of the methods of Internet communications discussed above require an affirmative action by the listener before the communication takes place. A listener must take specific action to receive communications from chat, instant messaging, social networking sites, and the World Wide Web. In general this is also true for e-mail exploders except in the case where a third party subscribes the user to the exploder list. These communications over the Internet do not "invade" a person's home or appear on a person's computer screen unbidden. Instead, a person must almost always take specific affirmative steps to receive information over the Internet.

I declare under penalty of perjury that the foregoing is true and correct.

Executed this 23<sup>rd</sup> day of May, 2011.



SCOTT BRADNER