Sexual Addiction & Compulsivity: The Journal of Treatment & Prevention
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/usac20

Filtering and Monitoring Internet Content: A Primer for Helping Professionals

Richard Joseph Behun [a], Valerie Sweeney [b], David L. Delmonico [a] & Elizabeth J. Griffin [c]

[a] Duquesne University, Pittsburgh, Pennsylvania

[b] Pittsburgh, Pennsylvania

[c] Internet Behavior Consulting, Minneapolis, Minnesota

Version of record first published: 09 Apr 2012.

To cite this article: Richard Joseph Behun, Valerie Sweeney, David L. Delmonico & Elizabeth J. Griffin (2012): Filtering and Monitoring Internet Content: A Primer for Helping Professionals, Sexual Addiction & Compulsivity: The Journal of Treatment & Prevention, 19:1-2, 140-155

To link to this article: http://dx.doi.org/10.1080/10720162.2012.666425

Sexual Addiction & Compulsivity, 19:140–155, 2012

ISSN: 1072-0162 print / 1532-5318 online
DOI: 10.1080/10720162.2012.666425

Routledge
Taylor & Francis Group

Filtering and Monitoring Internet Content: A Primer for Helping Professionals

RICHARD JOSEPH BEHUN
Duquesne University, Pittsburgh, Pennsylvania

VALERIE SWEENEY
Pittsburgh, Pennsylvania

DAVID L. DELMONICO
Duquesne University, Pittsburgh, Pennsylvania

ELIZABETH J. GRIFFIN
Internet Behavior Consulting, Minneapolis, Minnesota

Helping professionals are often in the position to offer guidance on how best to protect individuals, couples, and families from dangerous and/or inappropriate content on the Internet and other technological devices. However, they often do not have current data on blocking, filtering, and monitoring methods available to offer such protection. The purpose of this article is twofold. First, it is designed to educate helping professionals on how many of the latest blocking, filtering, and monitoring technologies operate. As new products become available, the helping professional should easily be able to understand how the product works, and then make judgment about its appropriateness for their respective client. Second, specific sample products are named to give the helping professional an immediate list of possible options for clients, keeping in mind that the list of products is constantly evolving. At the completion of reading this article, the helping professional should be equipped to help clients understand their options when considering blocking, filtering, and/or monitoring software.

Address correspondence to David L. Delmonico, Ph.D., Duquesne University; School of Education; 600 Forbes Avenue, Pittsburgh, PA 15282-0001. E-mail: delmonico@duq.edu

INTRODUCTION

The worldwide Internet population grew 380% from 2008 to 2009. It is estimated that nearly 75% of the entire North American continent has access to the Internet. Commercial producers of cybersex activities see the potential to profit from this segment with practically no overhead costs. In 2006, Internet pornography accounted for nearly $3 billion (23%) of the total market share of pornography in the United States (Family Safe Media, 2010). As a result, more and more individuals are experiencing significant problems with cybersex related addictions. These include both the use of computers and other technologies that access the Internet.

No one is exempt from developing online problems. One of every three visitors to adult pornography web sites is likely to be female, and nearly 60% of those who use the search term *adult sex* on Internet search engines are female (Family Safe Media, 2010). The average annual income for consumers of Internet pornography is a reported $75,000 plus. Not to mention the measured increase in adolescent use of online sexual materials and behaviors. Use of the Internet among teens in the United States continues to rise, with an observed 24% increase of teen use between 2001 and 2005 (Lenhart, Hiltlin, & Madden, 2005). In 2007, an estimated 93% of children ages 12 to 17 accessed the Internet on a regular basis in the United States (Macgill, 2007). Wolak, Mitchell, and Finkelhor (2007) found 34% of teens indicated they were exposed to unwanted online sexual material, a figure that rose 9% over the past 5 years. This continued growth and exposure of teens to inappropriate online sexual material increases the likelihood that such issues will need to be addressed in clinical settings. Delmonico and Griffin (2010) outline ideas for clinicians in order to better prepare them to discuss a broad range of issues related to this topic including information on blocking, filtering, monitoring, etc.

Clinicians working with individuals, teens, and families often recommend the use of blocking, filtering, and/or monitoring software. The recommendation may be made to a client who is struggling with pornography use, compulsive gambling, compulsive gaming, or who is simply struggling with excessive time spent online.

It is important for helping professionals to understand the methods of protecting clients and their families from inappropriate or dangerous online content/conversations. For professionals who assist individuals with problematic sexual behavior, this responsibility is even more salient. However, even armed with all the information, no technology is 100% failsafe. The technologies discussed in this article proportionally relate to a client's motivation. The more motivated a client is to take personal responsibility for protecting themselves or their family, the more effective the protection technologies. As in every clinical situation, the clinician can only be accountable for providing the best information to help a client make an informed

decision and follow through with that decision on his/her own. The purpose of this article is to provide clinicians with the knowledge and tools necessary to assist clients and their families in understanding their options for blocking, filtering, and monitoring Internet content.

There are hundreds of software products available for blocking, filtering, and monitoring Internet content, and new products are added to this list each day. The purpose of this article is not to review specific software packages, but rather to help clinicians understand the basic anatomy of how a particular type of software functions. The article will assist clinicians in recommending a course of action to clients whose technology-based behaviors are concerning. While the main goal is not to provide reviews of specific products, Table 1 contains names of specific software titles that provide blocking, filtering, and monitoring capabilities. It is hoped that by both explaining the general anatomy of how blocking, filtering, and monitoring software works, combined with examples of products, the clinician will be well-equipped to assist clients for whom problematic online behavior is a concern.

It is recommended this article be read from start to finish in order to gain a comprehensive understanding of what options are available for blocking, filtering, and monitoring on all types of devices. Reading only the section that appears applicable to a specific situation may limit options covered in the latter part of the article.

OPERATING SYSTEMS AND PLATFORMS

In order to understand blocking, filtering, and monitoring, it is important to understand the various "operating systems" or "platforms. These terms refer to the underlying software used to make a specific device work properly. The most common platforms are Windows and Macintosh (Mac). Software written for one platform does not work on the other—platforms are not interchangeable—this is often referred to as "compatibility." Other platforms referred to throughout this article include "iOS" and "Android" (Droid). These operating systems were designed specifically for mobile devices. Any device running iOS is an Apple built device (e.g., iPad, iPod, iPhone, etc.). The Android platform is supported by Google and was designed to be a direct competitor to Apple devices. Many different mobile devices use the Android platform (e.g., cell phones, tablet computers, etc.). It is important to know which platform your client uses (Windows, Macintosh, Droid, iOS, etc.), since not all products are available for all platforms. There are also other platforms not specifically addressed in this article, which may be discovered while learning more about blocking, filtering, and monitoring software. These include Windows Mobile, Windows Phone (WP), Blackberry, Linux, Opera, and others. Windows, Mac, iOS, and Droid are the most common operating

TABLE 1 Sampling of Blocking, Filtering, and Monitoring Products

Product	Mac	Windows	iOS	Android	Blackberry	Windows Mobile	Blocking/ Filtering	Accountability	Monitoring	Website
AT & T Wireless			x		x	x	x			http://www.att.net/smartcontrols
BrowseControl	x	x	x				x		x	http://browsecontrol.com
ClearOS	x	x	x		x		x			http://www.clearfoundation.com/
Covenant Eyes	x	x	x			x		x		http://www.covenanteyes.com
Cyclope-Series		x					x		x	http://www.cyclope-series.com/
DansGuardian	x						x		x	http://dansguardian.org/
Finjan SecureBrowser		x					x			http://www.m86security.com/securebrowsing/
iBot	x	x							x	www.brickhousesecurity.com/
iSheriff	x	x	x	x	x		x		x	http://www.isheriff.com/
K9 Web Protection	x	x	x				x		x	http://www.k9webprotection.com/
Lightspeed Rocket/My Big Campus	x	x	x	x	x		x		x	http://www.lightspeedsystems.com/
Mobicip			x				x		x	http://www.mobicip.com
MobileSpy			x	x	x	x	x			http://www.retinax.com/
Mobizim				x	x	x			x	http://www.mobizim.com/
My Mobile WatchDog			x	x	x	x	x		x	http://www.mymobilewatchdog.com/
MyFone				x					x	http://us.myfone.mobi/
Naomi Internet Filter		x					x		x	http://naomi-internet-filter.softpedia.com/
NetNanny	x	x	x	x		x	x		x	http://www.netnanny.com/
NetSentron		x					x			http://www.netsentron.com/
Nintendo DSi & DSi XL							X		x	http://www.nintendo.com/consumer/systems/dsi/en_na/settingsParentalControls.jsp
OnlineFamily.Norton	x	x					x		x	https://onlinefamily.norton.com
OpenChoice							x			http://www.ischool.utexas.edu/~choice/
OpenDNS	x	x	x	x	x		x		x	http://www.opendns.com/
Phone Sheriff			x	x	x	x	x	x	x	http://www.retinax.com/phonesheriff
Playstation (PS3)							x		x	http://manuals.playstation.net/document/en/ps3/current/basicoperations/parentallock.html

(Continued on next page)

TABLE 1 Sampling of Blocking, Filtering, and Monitoring Products *(Continued)*

Product	Mac	Windows	iOS	Android	Blackberry	Windows Mobile	Blocking/ Filtering	Accountability	Monitoring	Website
ProblemPoker		x					x	x	x	http://www.problempoker.com/
PSP (PlayStation portable)							x		x	http://us.playstation.com/psp/features/ps_psp_other_features.html
RangerPro				x			x			http://www.mobsafety.com/
SafeSquid		x					x		x	http://www.safesquid.com/html/portal.php?page=107
Secure Web SmartFilter EDU (Bess)		x					x			http://www.mcafee.com/us/products/smartfilter.aspx
Sentry Parental Controls		x					x		x	http://www.sentryparentalcontrols.com/
SmartWeb			x				x		x	http://www.tigerme.com
Surf Balance			x				x		x	http://www.surfbalance.com
Surf Control		x		x	x		x			http://www.websense.com
Surfwatch	x	x					x		x	
T-Mobile Web Guard				x	x	x	x			http://www.t-mobile.com
True Vine Online							x	x	x	http://www.christianbroadband.com/
Verizon Wireless			x	x	x		x		x	http://www.verizonwireless.com
Wii parental controls							x		x	http://www.nintendo.com/consumer/systems/wii/en_na/ht_settings.jsp?menu=pc
Windows Live Family Safety		x					x		x	http://explore.live.com/windows-live-essentials-other-programs?T1=t5
X3Watch	x	x	x	x				x		http://www.x3watch.com/
Xbox 360 console parental controls							x		x	http://support.xbox.com/en-US/billing-and-subscriptions/parental-controls/xbox-live-parental-control
Xbox 360 Kinect family settings							x		x	http://www.xbox.com/en-US/Kinect/PrivacyandOnlineSafety#FamilySafety1
Xbox Live							x		x	http://support.xbox.com/en-US/xbox-live/online-privacy-and-safety/online-safety

systems for which blocking, filtering, and monitoring software is developed and therefore this article is primarily limited to discussing these platforms.

ANATOMY OF BLOCKING/FILTERING

The following sections address several types of product that can be used to assist in the blocking and filtering of various technologies including computers and mobile/portable devices.

Blocking and Filtering on Personal Computers

The purpose of blocking/filtering software is to restrict inappropriate or dangerous content from being delivered to a home or office computer. The filtering process is based on "rules" that the filtering software establishes. These rules differ for each software package, and are the "proprietary secret" for each company since it determines the effectiveness of the software.

Essentially, all software uses two basic methods for filtering content. The first is based on a "blacklist" of known inappropriate sites that are either blocked completely or "graded" (E = Everyone, 9+ = ages nine and older, M = Mature, etc.). In addition, some software packages use the Entertainment Software Rating Board (ESRB) and Motion Picture Association of America (MPAA) ratings to assist in filtering content. Computer users who have the software's security password can add their own websites to the "blacklist" or override the blacklist and allow access to certain sites. This level of customization is common on most software packages and can assist in adapting the software to individualized needs.

The second method of filtering can be referred to as "on-the-fly" content analysis. If a site is not on the black or white list, the software does a quick review of the text on the site and matches it to a list of known words that would render the site inappropriate and inaccessible. For example, if the site had the word "porn" listed anywhere on the page, the software would detect this and block the site based on the keyword match. In addition, most software packages also can be configured electronically to notify (e.g., e-mail, text message, etc.) the administrator of the computer that a website has been blocked and provide the URL of that page.

Another feature includes the ability to customize the software for a level of filtering "strictness" depending on the computer users' ages and/or specific needs. This allows for multiple users of the computer to have different levels of content filtering. For example, a family who has a 6-year-old, a 15-year-old, and an adult user could all be set up for different levels of filtering. Content "strictness" can range from child pornography, adult/fetish pornography, graphic language, gang or cult sites, travel sites (to prevent

kids from arranging their own travel), chatting sites, references to alcohol or tobacco, etc. It is critical to have multiple user accounts established for each household user in order to take advantage of this feature.

Most, if not all, blocking and filtering software utilizes both a pre-established database (blacklist) and on-the-fly filtering and blocking. The combination of these two methods provides an efficient and effective method of blocking and filtering inappropriate websites.

Finally, many software packages also offer "time management" features that allow the computer administrator to limit the number of hours per day the user may be on the Internet and/or the time of day that the user has access to the Internet. For example, the administrator could configure the software to allow access 3 hours per day, but restrict any use between 10:00 p.m. and 7:00 a.m.

Some key features to look for in blocking and filtering software include the ability to:

- Override filters with password entry
- Manage the amount of time a person spends online each day
- Manage the hours of the day the Internet can be accessed
- Send electronic notifications when a site is blocked
- Send electronic notification when the software is tampered with
- Set up for multiple users with differing levels of filtering
- Be installed and licensed on multiple computers/devices
- Be remotely managed via the Internet

Blocking and filtering software for personal computers (both Windows and Macintosh based) has been under constant development for many years. It provides an effective tool in assisting clients and families from accidentally discovering inappropriate web-based content. The software can also be effective for adults who are struggling with their own online behavior with both the filtering and time management options. The main disadvantage includes the ease of which blocking/filtering software can be tampered with or disabled.

Blocking and Filtering for Apple and Droid Devices

The previous section discussed blocking and filtering software developed specifically for Windows or Macintosh personal computers. The long history of these platforms has yielded many user-friendly and efficient software packages for the blocking and filtering of Internet based content. However, newer platforms, such as iOS (Apple's mobile platform for iPhones, iPads, etc.) and Android OS (Droid) are still in their infancy of determining the best ways to filter/block Internet content.

One consideration on mobile devices is blocking/filtering of the World Wide Web. Devices that utilize the iOS and Droid operating systems employ built in web browsers to access the Internet. Most commonly these browsers are Google Mobile for Droid devices and Safari for Apple devices. In order to filter web-based content on these devices, the user must install a specially developed filtering browser that will *replace* Google Mobile or Safari. This differs from the personal computer software, since it was designed to work WITH the existing browser. The most common filtering browsers for these platforms include *MobiCIP, Mobile Watchdog,* and *Ranger Pro*. These browsers can be purchased through the device's application store. Once the application is successfully installed, the device must be configured to disable or delete the default browser. The goal is to only allow web browsing to occur through the newly installed filtering application.

The second related consideration is configuring the "restrictions" on the mobile device to prevent users from downloading inappropriate applications or using web browsers that will bypass the filtered browser. The first step is to secure the restriction settings by establishing an administrator password or PIN to prevent settings from being changed. The next step is to configure the device so the native web-browser (Google Mobile, Safari) will be hidden or disabled. Other possible device restrictions include blocking access to certain applications (e.g., YouTube, e-mail, Facebook, etc.), setting up e-mail notifications of suspicious downloading (e.g., attempting to download a non-filtered web browser), and filtering movie/music/app content based on content ratings (e.g., PG, PG-13, M, etc.). Although this process of configuring restrictions sounds complicated, it is not. However, it does involve a number of steps. While it is beyond the scope of this article to guide on how to perform these configuration settings, the mobile filtering products have step by step instructions (with photographs) on configuring your device. For example, *MobiCIP* has 27 tutorials with step-by-step instructions on configuring their specific device. (http://content.mobicip.com/faq). Other mobile filtering products have similar assistance available.

The advantage of these applications is that they extend filtering capabilities beyond the computer and address many of the concerns associated with portable devices. The disadvantage is this software can be somewhat complicated to install and does not adequately filter applications installed on the mobile device.

Blocking and Filtering for Other Internet Capable Devices

Other devices can also access the Internet. These include Xbox 360, PlayStation Portable, Wii, and Kindle Fire, just to name a few. These devices have proprietary operating systems that only allow the manufacturer of the device develop software capable of blocking, filtering, or otherwise managing

Internet content. Some of these devices have built in "parental controls" allowing the device to be configured to limit the Internet connection. However, these restrictions are extremely limited and do little to control the overall content of the device (e.g., games, books, etc.). Therefore, these built in parental controls are extremely limited in their functioning and effectiveness. If blocking or filtering is desired on such devices, it is best to visit the website associated with the specific device to learn about the potential for parental controls; however, it will be disappointing to learn that little is available for these devices even though the dangerousness and problematic use is just as great as on other devices. For this reason, additional supervision regarding the use of these devices is highly recommended.

Internet Service Provider Filtering

An Internet Service Provider (ISP) is a company that provides access to the Internet. This is commonly a cable or phone company, but there are also a number of independent ISPs across the country. Since the Internet connection is made through their high-capacity network computers (also called servers), the ISP has the ability to block or filter content *prior* to its arrival on your computer. Most ISPs allow full and open access to all aspects of the Internet, leaving it to the consumer on how best to manage the content once it is delivered. However, there are a number of ISPs that specialize in blocking/filtering content before its delivery. The main advantage of this method is it requires less knowledge and maintenance by the computer user. In addition, there is a decreased likelihood of tampering with the filter since the filtering takes place at an inaccessible ISP point rather than on the computer itself. The disadvantage of this method of filtering is the user relies on the ISP to determine the content that is filtered or permitted. Many individual users find this method of blocking/filtering far too limiting, since the ISP tends to err on the side of filtering too much rather than not enough. There is also no way to allow for instant overrides with a password. Finally, most filtering ISPs provide Internet access via dial-up service which is extremely slow for today's multimedia content—although some filtering ISPs have faster DSL services in certain geographic locations. Even with its disadvantages, some people enjoy the convenience of such filtering, and are willing to forfeit aspects of their Internet content for the safety and security of ISP filtering.

In order to locate a filtered ISP, use a search engine such as Google and search for the words "filtered internet service provider." Many of these ISPs charge a monthly fee that includes both access to the Internet and the filtering service. The majority of these ISPs are Christian based, but some are not. Depending on your particular needs, it is important to research the services offered by each, and weigh the advantages and disadvantages

to determine if ISP filtering is a viable option. Common providers include: *integrity.com; truevine.net; pkfamily.com; familyfellowship.com*.

Domain Name System Filtering

A completely different type filtering is called Domain Name System (DNS) filtering. This may also be referred to as "cloud-based filtering." Essentially this is software that makes a small change to the Internet-hub (router) in a home. The router is a device that delivers Internet access to a home or business, including both computers and wireless networks (if installed). DNS filtering works in tandem with the Internet Service Provider. The change made to the router sends all requests for webpage content through a company other than your Internet Service Provider. That third-party then filters the content before it is delivered. For example, when a web address such as www.google.com is typed into the browser, the router would typically communicate with the ISP to retrieve and display the page, but the DNS filter adds another company to the transmission and the Google page is first sent to that company for review, then content is delivered if deemed appropriate. This additional step takes only milliseconds to occur. The advantage of this method is twofold. First, it is difficult to tamper with the filtering since a third company is responsible for the filtering. Second, since the filtering takes place before the router, the DNS filtering method filters content to all devices that connect to the home network—including iPods, cell phones (using wireless), laptops, etc. The disadvantage is that it is only useful for blocking webpage content and does not work for other Internet technologies. In addition, devices that use cellular data (i.e., cell phones, Kindles, other portable devices) would not be filtered since they typically do not use the home's Internet connection (unless configured to do so). This emerging technology may be useful, especially if a safer web-browsing network for all devices is the goal. Currently, the only reliable provider of this service to date is http://www.opendns.com.

ANATOMY OF MONITORING INTERNET CONTENT

Monitoring on Personal Computers

The primary purpose of "monitoring" software is to record all Internet and/or computer activity that occurs on a device where it is installed. Monitoring software is available for both Windows and Mac based computers. Essentially, the software becomes a "digital recorder" of an individual's computer activity. There are two main aspects to monitoring software.

First, the software can be configured to take a photograph of the contents of the screen at specified intervals (e.g., every 5 minutes, every hour, etc.) These are known as "screen captures." The image captured is stored on

the computer in a secure folder to be reviewed by the "monitor" (individual conducting the monitoring) at a later time or date. The advantage of this type of monitoring is the monitor can see exactly what was on the screen at the time of the digital screen capture. The screen capture may contain snapshots of a chat conversation, web browsing, or a non–Internet related activity (e.g., watching a movie, typing a document, etc.). The disadvantages of this method include needing a relatively large hard drive to store the images, and an excessive amount of time required to review the stored images.

A second feature of monitoring software is its ability to be configured to record every keystroke from the keyboard. Every time a key is pressed it is recorded and strung together in a file stored on the computer's hard drive. This feature allows for the recording of e-mails, chat conversations, password entries, etc. Similar to the screen captures, the file can be opened at a later time/date and reviewed.

More sophisticated monitoring software can detect the initiation of certain programs (e.g, email, chat, instant messenger, etc.) and monitor/record aspects of that program. For example, when an instant messenger program such as AOL Instant Messenger, or MSN Messenger is launched the program records both sides of the private messaging and stores the conversation on the hard drive of the computer.

Finally, most monitoring software can detect if another device was connected to the computer and what files were exchanged with that device. For example, an individual may be attempting to store inappropriate files on a portable hard drive or USB flash drive. The monitoring software detects the use of such a device and records the names of files that were transferred to or from that device. This information can be viewed at a later time or date.

There are more sophisticated monitoring products, such as Internet Probation and Parole Control (IPPC), but this sophisticated software is typically only used by the judicial system to monitor an individual's computer use.

This section provides the basic anatomy of monitoring software. Depending on the product itself, other functions may be available that are not discussed here.

Monitoring on Apple and Droid Devices

Monitoring software / applications (apps) for mobile devices are still in their infancy, but the several products available claim to log/record nearly every feature of the portable device's functions. For example, *MobileSpy* is an application that can be installed on phones of various platforms (e.g., Droid, iOS, Blackberry, etc.). Once installed, it records all call logs, text messages (both incoming and outgoing), GPS locations, additions or deletions to the contact list, task lists, memos created, cell phone tower information, emails, calendar events, websites visited, and photo/video clips stored. In addition, this particular app has a personal computer counterpart that allows the monitoring

individual to access all the information remotely—never having to physically possess the phone other than to conduct the initial installation of the software. The remote access "control panel" also provides a "live view" of the phone's screen, so the monitoring individual can view events on the phone in real time. In addition, the remote software allows for setting adjustments to the phone via the Internet, or the phone may simply be shut down altogether. Once installed, the application runs in the background unbeknownst to the phone user. It should be cautioned that only the legal owner of the cell phone is permitted to install such monitoring software. Installing such software may be in violation of federal, state, and/or local laws.

The widespread use of mobile devices accessing the Internet is certain to lead to more products such as *MobileSpy*. To date, there are no monitoring packages available for other portable devices that connect to the Internet (e.g., Xbox 360, PlayStation Portable, Wii, and Kindle Fire, etc.).

Other Monitoring Devices

In addition to software used to monitor Internet/computer/mobile devices, there is another unique device called *iBot*. The *iBot* is a device that plugs directly into a device's Universal Serial Bus (USB) port. The *iBot* looks like a simple flash storage drive, but in fact, it is a monitoring device that has pre-installed software to record all screen and keyboard activity. The types of information gathered by this device are similar to those discussed previously; however, the advantage to such a device is the ease of use. There is no software to install or settings to be configured. The monitoring individual simply plugs the *iBot* into the device he/she wishes to monitor, and unplugs it to stop the monitoring. The *iBot* is then reviewed at a later date/time for screen captures and keyboard strokes. The main limitation of this device is that it must be plugged into an open USB drive, and many portable devices do not have such ports.

ANATOMY OF ACCOUNTABILITY SOFTWARE

Accountability on Personal Computers

Accountability software assumes a certain amount of personal responsibility by the computer user. The computer user chooses an accountability partner (typically a parent, friend, pastor or counselor, sponsor, etc.) to which the installed accountability software sends Internet usage reports at designated periods of time (daily, weekly, etc.). The reports contain a list of all websites visited by the computer user. If the accountability partner notices any inappropriate websites or usage, they would confront the computer user with the information received.

Some accountability software also has built in blocking/filtering capabilities, while others simply generate a report of all websites visited. The advantage of accountability software lies in its personal responsibility training in helping individuals make better decisions regarding their online behavior. Rather than rely on the computer to block/filter websites, the premise of the accountability software is to encourage internal policing of decisions and behaviors. These choices and behaviors can then be examined in a therapeutic or personal growth setting.

Accountability software can be set to monitor the entire computer, or only specific users on the computer. These tools are especially popular with religious groups and families. The most popular and oldest type of accountability software is *Covenant Eyes*. Several other products exist as well. Some products cover a wide range of monitoring, while other are marketed towards monitoring particular issues, such as gambling or pornography. The features of each these of products are similar, but be certain to research the features of each to make the best determination for specific monitoring needs.

The main disadvantage is that clients must be highly motivated and willing to address their behavior with their accountability partner, especially if such accountability software is not paired with blocking and filtering software.

Accountability on Apple and Droid Devices

Presently, there are limited options for accountability software on iOS and Android OS devices. *Covenant Eyes* does have a mobile edition of their software. However, similar to the blocking and filtering for mobile devices, the native web browser on the device must be replaced and disabled in order to use the monitoring features. See the *Blocking and Filtering for Apple and Droid Devices* section for more explanation about this. Again, as mobile platforms such as iOS and Droid become the norm for accessing the Internet, more solutions will develop to help individuals become more accountable for their online use on such devices.

MULTI-FUNCTION PRODUCTS

The previous sections differentiated a number of technologies (e.g., blocking, monitoring, accountability, etc.) to ensure healthy and safe use of the Internet. Although the sections are divided into distinct categories, most products perform more than one function. For example, it is not unusual to discover monitoring software that also provides blocking/filtering capabilities; or accountability software that also monitors and filters content. Most software has a primary function for which it was originally designed, and secondary

functions which enhance the appeal of the product. The only way to know which product is best is to try the product (many have free trial periods), read online independent reviews, and talk to others who may have used the same or similar products. Independent reviews can be difficult to find since many companies pay other companies to "review" their product, but the review is nothing more than an advertising scheme. The best reviews are from those who use the product. Start with a site like Amazon.com and read reviews of customers who are using the products. Similar to shopping for other products, consumers should use comparison shopping techniques to compare features and prices of various products. The information contained within this article will be a good starting point to determining what type of product would be a good match for particular needs.

Table 1 summarizes several of the most popular products in each category. This table is not a comprehensive listing, nor does inclusion of a product in the table suggest endorsement.

SPECIAL CONSIDERATION

When employing the use of blocking, filtering, or monitoring strategies, it is important to note that it is strongly discouraged to use the client's partner as the technology "police." When one partner is the "holder of the password" or the "accountability partner" a problematic dynamic is created and the situation can be extremely unhealthy for the individuals and the relationship. Such an arrangement should be avoided.

On the other hand, in families the parents have a right and responsibility to block, filter, and/or monitor their child's computer and Internet use. The parent needs to assume their role as the one responsible for keeping family members healthy and safe when using technology. The technologies discussed in this article should be used to empower individuals to engage in healthy and safe online behavior and communication. Balancing this involvement is also the dynamic where the parent becomes so "over-involved" in their children's lives that it develops a level of unhealthy enmeshment and can interfere with the child's development and exploration of the world.

BEYOND BLOCKING, FILTERING, AND MONITORING

It is important to recognize there are significant limitations to all the options presented in this article. As was mentioned, effectiveness of these options is correlated with client motivation. The biggest concern with the blocking, filtering, and monitoring options is the false sense of security they offer to clinicians, clients, and families. While many of the products are highly effective, they are only one tool among many that should be employed in

helping individuals and families stay healthy and safe with their technology use. Discussing viable software related solutions with your clients should be the start of a number of clinical conversations that examine deeper implications of problematic online behavior. Good clinical skills, combined with increased technology knowledge, are part of an entire package to ensure being helpful in situations where problematic online sexual behavior is involved. In addition, even under the best circumstances, technology solutions are not failsafe. Inappropriate and dangerous content will slip through even the best software packages. Conversations with clients about managing such content are critical. Delmonico, Griffin and Edger (2008) authored an article on establishing Acceptable Use Policies (AUPs) with clients and their families. A review of that article may be useful in helping clients establish clear boundaries and rules about one's computer use. Although it was primarily written for establishing rules within the family, the concepts can be easily adapted for individuals and couples. Ongoing discussions regarding technology use, expectations, online decision making, and problem solving are what will ultimately be the most helpful for clients. Such discussions allow for generalization to a variety of online situations, and do not rely on electronic software as the solution.

CONCLUSIONS

The purpose of this article was to provide the clinician with basic information on understanding how blocking, filtering, and monitoring software works. Through understanding these technologies better, it is hoped clinicians will be able to provide informed guidance to individuals and families on how to keep themselves and their families health and safe when using technology. The included table will help identify more popular products in all of the categories of blocking/filtering, monitoring, and accountability software. The table will also help determine which technology can be used with various platforms.

It is our responsibility as helping professionals not only to stay current on the ways individuals develop online problematic behavior, but also to offer information and guide clients to the best possible solutions. This article was written with that intent in mind.

It is not necessary for clinicians to become computer scientists to assist clients in their healthy and safe use of Internet technologies. However, a minimal amount of knowledge is necessary to fully comprehend the issues involved, and to conduct appropriate assessments of potentially problematic situations. It is strongly recommended that clinicians stay current on various technologies and how such technologies may be unhealthy or unsafe. This article provides basic information on how best to block, filter, and monitor Internet activity with the primary goal of establishing healthier patterns of

technology use; however, this article is a primer and not a replacement for understanding technology in general. One option is to hire a college–age student who can consult and educate about current technologies that may be causing problems for your clients. A parallel metaphor is multi-cultural counseling. Most clinicians understand it is unethical to provide therapy to an individual from a different culture (e.g., immigrant from China) without first understanding the basics of that culture. Technology and the Internet has created a sub-culture that warrants increasing one's knowledge and understanding prior to undertaking clinical interventions.

The blocking, filtering, and monitoring options presented in this article offer clinicians one set of tools that can be used to assist clients and families addressing inappropriate content and unhealthy use of the Internet. However, these are one tool that is most effective when combined with dialogue and conversations about good decision making when using all technologies that allow access to the Internet. The clinician is often seen as a resource for guiding and providing options to clients. This article presented information that will allow helping professionals to serve as that guide when it comes to health and safe technological use.

REFERENCES

Delmonico, D. L., & Griffin, E. J. (2010). Cybersex addiction and compulsivity. In Kimberly S. Young & Cristiano Nabuco de Abreu (Eds.), *Internet addiction: A handbook and guide to evaluation and treatment* (pp. 112–135). New York: Wiley.

Delmonico, D. L., Griffin, E. J., & Edger, K. (2008). Setting limits in a virtual world: Helping families develop acceptable use policies. Illinois Institute for Addiction Recovery: *Paradigm Magazine*, *22*, 12–13.

Family Safe Media. (2010). *Pornography statistics*. Retrieved January 25, 2010 from http://www.familysafemedia.com/pornography_statistics.html

Lenhart, A., Hiltlin, P., & Madden, M. (2005). *Teens and technology: Youth are leading the transition to a fully wired and mobile nation*. Retrieved April 15, 2007 from http://www.pewinternet.org/pdfs/PIP_Teens_Tech_July2005web.pdf

Macgill, A. R. (2007). *Parent and teenager Internet use*. Retrieved November 27, 2007 from http://www.pewinternet.org/pdfs/PIP_Teen_Parents_data_memo_Oct2007.pdf

Wolak, J., Mitchell, K., & Finkelhor, D. (2007). Unwanted and wanted exposure to online pornography in a national sample of youth Internet users. *Pediatrics*, *119*(2), 247–257.