To some practically-minded readers the obvious question is “why is this chapter so near the end?” It’s a fair question. Many parents simply want the tools to prevent their children’s access to harmful online material, which is perfectly understandable. Parents want to protect their children from all kinds of harms, and it’s a world full of dangers. It’s been the thesis of this book all along that the best protection for your children is to engender in them a world view, one in which sexuality is seen, not from the values and sliding mores of our culture, but one that is enlivened from God’s view of sex and our bodies. A worldview that gives good reason for avoiding temptations, and waiting for a married life of satisfying sex.

Still, you need the tools to protect your kids as they grow, and many parents are not equipped with the technological savvy they need, and don’t always make the best choices in software options. The advances in technology, especially mobile technology, can be confusing for all of us. Your family may have a home computer, laptops, Smartphones, tablets, eBook readers, iPods, game systems – all places where pornography can be accessed. Any approach that is not comprehensive enough can lead to simply moving the problem to another device.
I’ll do my best to navigate these waters, but I want to begin with a word of warning: though you can prevent most inadvertent access to pornography, you cannot stop a determined seeker. As I said earlier, before your children graduate high school they will have seen pornography; it’s practically unavoidable. Some children will become obsessed with finding it, and you can’t prevent it. That’s hard news for us parents, especially those who have taken great measures.

Many children don’t find pornography at home, but they will at a friend’s house, which is often where the first exposure to porn starts. You can’t do much about the places your children might see porn outside of your home, but you can do a lot about their behaviors at your home, and on the devices they typically own and use.

**Types of Protection**

*Accountability Software* – Accountability software records and evaluates online locations, ranking those that are more likely to contain objectionable content, and making a report of those findings available to you.

*Site Blockers* – A site blocker has either a black list of sites that will be blocked if you try to access them, or a white list of sites that are the only ones allowed. These are also called filters.

*Domain Blockers* – These are similar to site blockers in that they restrict access to certain web sites, but they do so by the domain name. A domain name, like www.google.com, is really just an alias for an IP address, like 74.125.225.177 (which is one of Google’s many IP addresses). A domain blocker uses lists of domains that are
known to be pornographic, or contain some objectionable material, and allow you the option of blocking them. Let’s discuss each of these approaches in general first.

**Accountability Software**

I think this is the most important solution. Accountability software doesn’t prevent your child from doing anything, so why is it so important? Accountability software gives you a window into your child’s online activity. It enables you to see the overall trend of what they do online, and gives you the opportunity of discussing how they travel the web. If you find that questionable sites begin to show up more frequently, or in greater density, it might indicate that your child is moving toward more adult material.

Having accountability software is about having a conversation, not about being a parole officer. It gives you the opportunity to talk with your son or daughter about what interests them, what they’re curious about, since the Internet has become the place where much of their curiosity expresses itself. Boys are curious about women’s bodies – that’s natural – and you can discuss that curiosity with them in a calm manner when you see things on the accountability report that indicate that they’re exploring. Girls are curious too, and parents can talk with them about what they’re thinking about, what they’re reading and looking at.

Having a blocker by itself doesn’t give you this opportunity. If your son spent two hours “trying” to find porn with no success, you would never know about that with just a blocker. It won’t show you that your son spent time
the other day looking at swimsuit and lingerie ads on Amazon, or that he’s taken a real interest in the women’s Olympic diving team. Although I consider some kind of blocker important, it’s not as important as accountability software.

There are a number of accountability software products available: Covenant Eyes, X3Watch, Accountable2You, Safe Eyes, WiseChoice, and each one has different benefits and features. I won’t go in to reviewing the pros and cons of each, because I have not tried them all, and I wouldn’t be qualified to give an exhaustive review. Some of them are fairly easy to circumvent. Some are free, and others have a subscription that must be paid every month. In this area, I think you get what you pay for, and I consider the minor cost well worth it.

I consider Covenant Eyes the best solution overall. Their software is high-quality, has the best and most flexible reporting options, and is the hardest to defeat. The company continues to make improvements to their software and is passionate about helping families protect their children. You can learn more about them at www.covenanteyes.com.

Site Blockers

Just in case you skipped to this section without reading the last, I’ll reiterate: a site blocker is not a good total solution. I have talked to many young men whose parents put a filter on the family computer and found it easy to look at pornography. All of the young men I’ve talked to say that their parents putting a blocker was ineffective at preventing them from looking at porn. Part of this is
because blockers are not 100% successful at blocking content, part of this is because boys can be quite savvy technically, and part of this is because porn is so ubiquitous – it’s everywhere.

Having said that a blocker is not a good total solution, it should still be in your toolbox. Many young people report that their first exposure to pornography was inadvertent. In addition, many sites are so egregious, so perverted that, not only are they not suitable for children, they are not suitable for anybody. As Paul said, “it is shameful even to speak of the things that they do in secret.” (Ephesians 5:12)

A site blocker works by comparing any web site request against a list of known pages, or simply by evaluating the content of the page itself, and deciding to either permit or deny access to that page. Most blockers use a black list - that is, a list of pages that are known to have pornography on them. Others will restrict access only to certain pages – a white list.

There are a number of companies that provide content blockers – NetNanny, Safe Eyes, CyberSitter, etc. According to toptenreviews.com, NetNanny has the best content blocking, is highly configurable, and is the easiest to use. If you’re a Covenant Eyes user, you can also add filtering for a low monthly fee. Covenant Eyes filtering works in real time, using the same algorithms that the accountability product uses for reports.

**Domain Blockers**

A domain blocker works just like a site blocker, but operates on domain names only. A domain name is just
a memorable name for an IP address, and usually has sub-domains and many pages. A domain blocker restricts access by domain name. For example youtube.com hosts millions of pages, but if your domain blocker restricts access to it, none of the other URLs will be accessible. This is a good thing, and a bad thing. The good thing is that a domain blocker doesn’t have to keep track of individual pages like a black-list blocker does. The bad thing is that, if there is a pornographic page on an otherwise benign domain, it won’t be blocked, and if something useful is located on a blocked domain, you can’t get to it.

Since most pornography sites are hosted independently, this isn’t much of a problem, but you have to know that there is plenty of porn on so-called “safe sites”. In fact, there is pornography that is pretty easy to find on Youtube, Tumblr, Twitter, Pinterest, Blogger, Amazon, Facebook, and Google. Those are among the most popular sites in the world. This is another reason that blockers (overall, not just domain-based) are a bad total solution. If you’ve blocked your kids from using Google, you might as well sell the computer.

The most-used domain-based solution, and probably the best for the average user, is OpenDNS. By using their DNS servers, which translate domain names into IP addresses, you have access to about 60 levels of content filtering, like Nudity, Pornography, Explicit Language, and so forth. It’s free, and their DNS servers are probably faster than the one your Internet Service Provider supplies.

Before I get into how to install and setup my preferred list, I would encourage you to do some comparison
shopping. Read the reviews of the major products, and make your own decision. Be careful of choosing an option because it’s free; that’s not always the best choice to make. Your criteria should be based on how effective it is in providing opportunities to talk to your children, and in preventing them from accessing pornographic content.

**Installing Covenant Eyes**

You’ll want to install the Covenant Eyes software client on every computer that has Internet access. First, you’ll need to set up an account, which you can do at [www.covenanteyes.com](http://www.covenanteyes.com). Before you do, you should decide whether you want an individual account for every computer user, or one account for the whole family. The downside of having a single account name is that the reports won’t show who was doing what. Having multiple user names on an account allows for better reporting, more flexibility in terms of content control, and prevents those embarrassing phone calls from an accountability partner when your wife is shopping for underwear online.

A single Covenant Eyes account costs $8.99 a month, or $10.49 a month for accountability and filtering. Each additional user name is $2.00 a month, or $3.50 a month with filtering. If you’re a part of our fellowship you should use our promotional code (XENOS) when you check out. That way, you’ll get your first month for free, and 15% of your monthly fees will come back to our church as a donation.

Once you have an account, you can install the client software anywhere; there is no restriction on how many copies of the software you have installed. Most homes
have a number of computers, laptops, and mobile devices, and you won’t be charged extra for them. The billing is based on the number of users on your account, not the number of instances of the software you have installed.

Once the software client is installed, it will start automatically every time you start your computer, and you won’t be able to access the Internet without signing in. You can choose to keep an individual user logged in, so that you don’t have to type your username and password in each time. Use this option if there is only one user of that computer. Any time a computer is shared with others, this option should be left off. Your kids’ passwords should not be shared, so that Andrew can log in as Beatrice to look at porn. This takes getting back at your big sister to a whole new level!

**Configuring Covenant Eyes**

When you sign up for Covenant Eyes, you can select one of more accountability partners for each account. Make yourself an accountability partner for each child. At the same time, you can select the kind of reporting you want, and the level of content you want reported. The reporting levels are as follows:

- **E (Everyone)** - These sites are fitting for young children.
- **Y (Youth)** - Includes ecommerce sites and material that some parents might question for children under 10.
- **T (Teen)** - Includes social networking sites like Facebook, chat rooms, and games with violence.
• MT (Mature Teen) - Includes profanity or mature humor sites, which may be inappropriate for younger teens.

• M (Mature) - Includes dating sites, lingerie, crude humor, intense violence, and material of a sexual nature.

• HM (Highly Mature) - Includes anonymizers, nudity, erotica, and pornography.

Select the level that is most appropriate for your child. You can change this level at any time by logging in to the member site.

**Installing the Covenant Eyes Browser on Apple devices**

There is a bit of work to do to get setup on devices that use iOS, the Apple operating system that runs on the iPhone, iPad, and iPod Touch. First, you should download the Covenant Eyes browser from the Apple App Store. You can do this from the device itself, or from iTunes.
When you first call up the browser, you will have to log in with the account of its user. This can be set so that the login will happen automatically from then on.
Due to the design of the operating system, this app does not work like the desktop version; it cannot run in the background, monitoring your Internet activity through other browsers. It cannot monitor other apps. Only Internet activity logged through this browser is recorded in the Accountability Report. In addition, there is no filtering option available, so you may want to keep that in mind when Johnnie asks for an iPad for Christmas.
You have to set up restrictions on the device next, so that Covenant Eyes is the only way to browse web pages.

**Setting IOS Restrictions**

- Launch the “Settings” app and then select the icon labeled “General.”
- Select “Restrictions” and tap the button labeled “Enable Restrictions.”

You will be asked for a four-digit passcode. You should use one that you will remember, but not something that it would be easy for your child to figure out. Any time he wants to install a new game, you will have to do use this passcode to disable restrictions, and the re-enable them.

Next, turn off Safari, YouTube, and other apps that might allow objectionable material. Toggle “Installing Apps” to “Off” as well. Note that many apps have built-in browsers used for ads, contact, or comments, which Covenant Eyes does not monitor. This is especially true of free apps, which of course, your child will be eager to download. Test every app that is already installed. If it has ads, click on them. If that launches a browser, or links directly to YouTube, Twitter, Facebook, etc., you will need to disable that app.

At this point, your child will likely complain that you’ve cut them off from everything that brings them joy. Not to worry: the mobile apps for Facebook, Twitter, and so forth can be accessed through the Covenant Eyes Browser, will full accountability. Once the browser is launched, go to facebook.com or twitter.com and the web page will redirect you to the mobile version of the app automatically. Bookmark that page; problem solved.
They can use these apps, and all activity within them will be monitored, including clicking on links to objectionable sites, which are everywhere throughout the most popular destinations.

If you so choose, under “Allowed Content,” toggle off the ability to listen to explicit music and podcasts, and disallow movies and TV shows at inappropriate levels (e.g. NC-17 for movies and TV-MA for TV shows).

**DO NOT** disable apps rated 17+. Because Covenant Eyes offers unfiltered Internet access, Apple rates it 17+. By disabling 17+ apps, you will be disabling Covenant Eyes.

**Setting Android Restrictions**

The Android operation system is a version of Linux, developed and distributed by Google. The Covenant Eyes application for the Android works like the one you install on desktop and laptop computers; there is no separate browser, and all web access and applications will be monitored.

You should be aware that many tablets (Google, Samsung, Asus, Sony, Toshiba, Motorola), e-readers (Nook, newer Kindles), and media players (Samsung Galaxy) also run the Android OS. If your child has a table, e-reader, or media player that cannot install apps, it’s possible that they will have unmonitored access to pornography. For example, the Kindle Fire only allows apps to be installed from Amazon, and has a browser built in. You can modify the operating system so that apps can be installed (often called “rooting” the operating system). This is for the more technical among us, and you can ruin (“brick”)
your Kindle, so you’re on your own here. For those using the paper-style Kindles, Amazon just released parental controls as a recent update. You can set a password for access to the internal web browser.

The Covenant Eyes application can be downloaded from Google Play (formerly called the Android Market). Open Google Play, tap the search button, and search for “Covenant Eyes.” Then, tap and install the Covenant Eyes app.

The first time the app runs, you will be prompted to install Covenant Eyes Helper. To do so, you will need to allow the installation of non-market apps. This step is very important, since the application will not work otherwise. Once you have installed the app, find and open the app on your Android device and sign in using your Covenant Eyes username and password.

If you will be the only person using the Android device, you may want to check the box next to “Stay Signed In?” With the auto sign in feature enabled, the Covenant Eyes app will automatically load and sign you in when you turn on your phone. If you need to turn off the auto sign in feature, open the Covenant Eyes app and uncheck the box.

**What to do when you get a report**

When you first start to get reports from Covenant Eyes you may be concerned that there is anything there at all. A large number of web sites can potentially contain adult content, but that doesn’t mean that your child is looking at porn. Look over the listing carefully and see if there are keywords that could point to trouble. For example, if your
son was looking at guitars on craigslist.org, you should understand that craigslist also has personal ads for adult services. In the URL listing you should see something like: http://somewhere.craigslist.org/search/msa?query=guitar

and not:

http://somewhere.craigslist.org/i/personals...

As an aside, Craigslist has removed their Adult Services category under pressure from human trafficking advocacy groups. They use a content filter on their personal ads to block ads that are just a front for prostitution, but it can’t be perfect.

Let’s say you do see something questionable on the report; what do you do?

Don’t assume that this means that your child is seeking out pornography. Some web sites have ads on the side that load content from adult-oriented advertisers. This is especially true of sports, gaming, and torrent sites. Often the best way to determine this is that there will be a single entry in the report, often from something that looks like an online adult “dating” service. If your child had actually gone to the site there would be a lot more than one entry. The other clue is that the URL will often start with “ad”, like “ad.adultplayers.ad”.

Take a look at search terms from Google or Yahoo. A Google or Yahoo image search for “girls” will present a preview page with hundreds of pictures, mostly of a sexual nature. It’s time to have that curiosity talk.

The important thing here is that these reports create conversation, and you should be wary of using them in a disciplinary manner as a first response. Go in to that
discussion with an informed curiosity, asking questions, not accusing. You may find that you get honesty from your child. It’s far better for him to come to you with the truth than for you to go in there with guns blazing.