Is Skype Safe for Judges?

By Martin Felsky, PhD, JD, for the Judges Technology Advisory Committee, Canadian Judicial Council,[1] Version 2.0 July 6, 2010

In this article I will try to help judges understand whether Skype and services like Skype are safe. The bottom line is that Skype and other internet-based telephony services may be used safely, both for personal calls and for carrying on judicial business, but only if users are aware of security issues and certain precautions are taken.

Many judges may not be familiar with Skype, and so I have devoted the first part of this article to a discussion of what Skype is and how it works. By understanding how Skype works, I believe that users can better protect their privacy and the privacy of others.

If you are already familiar with how Skype works, you can skip the first few sections. I have tried to keep the discussion here at a non-technical level. For readers who require more technical information about Skype security, I highly recommend "Skype: A Practical Security Analysis," by Bert Hayes, published online in 2008 by the respected SANS Institute[2]. Courthouse network administrators concerned about the use of Skype (whether authorized or not) are encouraged to read the article and implement the applicable security settings outlined by the author. Interestingly, Hayes advises against Skype use in highly secure network environments because the use of Skype allows people to have private conversations that cannot be tracked or monitored!

Introduction: The Plain Old Telephone System

The telephone system we grew up with (the Plain Old Telephone System or "POTS") runs on a public switched telephone network ("PSTN"). Over the years, the PSTN has evolved from analog signals (in which voice sound waves are converted to electrical signals and then back to sound) to digital (in which voice is converted to a digital signal of 1s and 0s). The PSTN is associated with telephone poles, copper wire, landlines, switchboards, operators, and exchanges (where calls are connected). The PSTN is mostly used for voice calls but can also be used for dial-up Internet access and fax transmission. The earliest commercial telephone exchanges started operating in the late 1880s.

[1] The opinions expressed in this article are those of the author and do not represent any official position or views of the Canadian Judicial Council.

[2] Bert Hayes, 2008 SANS Institute: http://www.sans.org/reading_room/whitepapers/voip/skype-practical-security-analysis_32918

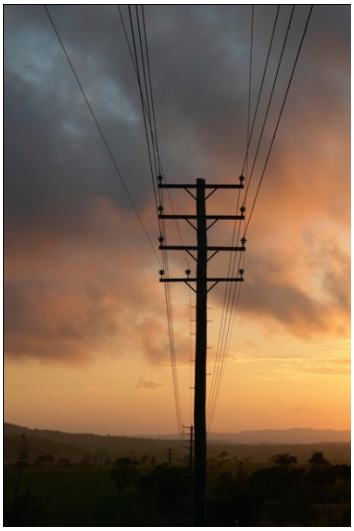

Figure 1: Telephone pole on the PSTN

Figure 2: Bell switchboard (US National Archives)

The PSTN, then, is a large, complex and commercially-managed network allowing voice and other types of communication to occur through transmission of electric signals. At each end of a connection is a telephone, fax machine or similar device. To use the PSTN you must subscribe, whereupon you are provided with a unique telephone number.

Pricing

In North America, on the plain old telephone system, we pay a flat monthly fee for all *local* calls, and a per-minute charge for *long distance* calls, or calls made to subscribers outside of our local exchange.

Enter the Internet

The Internet was opened to commercial traffic in 1988. The Internet is a large, complex public/private network supporting the communication of text and multimedia information (any kind of digital information – including voice) through a standard called IP, or Internet Protocol. When the PSTN in Canada and other countries was upgraded to digital from analog, this opened up the possibility of offering "broadband" internet access instead of dial-up, through a protocol called ADSL.[3] Broadband Internet access is "always on," making it suitable for voice communication. Broadband Internet access may be hosted by the PSTN itself (through a telephone system provider), by cable TV networks (through a cable TV provider), and by satellite communications systems. To use the Internet you must subscribe through an Internet service provider ("ISP") whereupon you are provided with a unique (or often shared) number, called an "IP address".

Pricing

Unlike on the POTS, broadband Internet pricing is a fixed monthly fee for a certain amount of data traffic. There is no differentiation between "local" or "long distance" transactions on the Internet, even though as we e-mail and surf the web we may be accessing servers and web pages located and stored anywhere around the world.

Telephone Service over the Internet

For judges at home using Internet access through their telephone or cable provider, we can now understand how the various connections work.

Say a judge working at home plugs her laptop into her telephone company-supplied ADSL router, which is in turn plugged into a standard telephone wall outlet. She can check e-mail, surf the world-wide web, download music, or participate in a webinar.

She now wants to make a long distance phone call. Her traditional telephone handset is plugged into a standard telephone wall outlet as well, and she makes the call using the PSTN.

So far so good – but where does Skype come in? Skype is a kind of software that allows a live feed of voice (or video and voice) to be transmitted through an Internet connection (like ADSL) instead of the PSTN. It does this by using a special protocol call VoIP – pronounced "*voyp*" and standing for "Voice over Internet Protocol." When you use Skype you do not need to receive a phone number (unless you pay for one, which allows non-Skype users to call you on Skype). You simply have a listing in the Skype Directory:

[3] Asymmetric Digital Subscriber Line

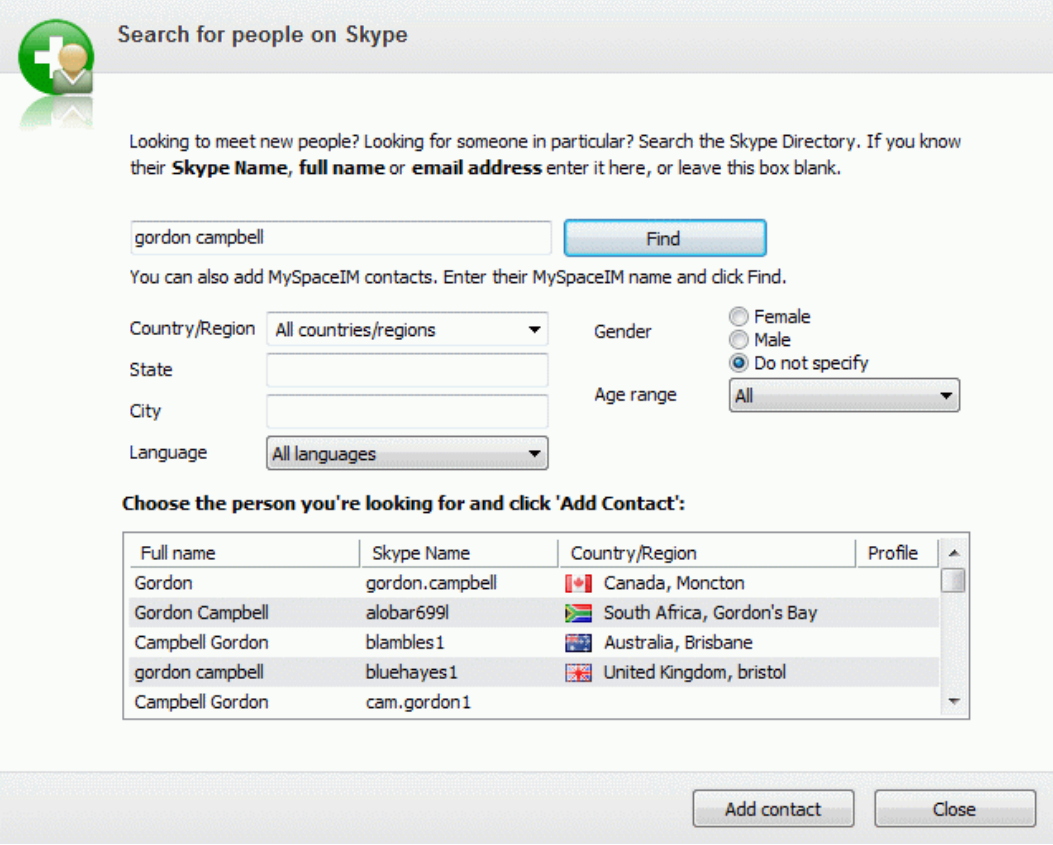

Figure 3 Skype directory showing Gordon Campbell, Moncton

Mass-market consumer VoIP got started as recently as 2004. Skype is well known but is only one of several VOIP services available. Other players include Vonage, Comwave and MagicJack.

Pricing

There is no charge to use Skype as long as you are calling computer to computer – i.e. if you wish to call from your computer to a landline or cellphone number, there is a charge. MagicJack has a one-time purchase price of $49.95 which includes one year of unlimited calls worldwide, to any phone number including cellphones and landlines. The USB adapter itself contains the VoIP software so there is nothing to download, and the adapter can therefore be used on any broadband-connected computer.

How Skype Works

In order to use Skype you must download software from the provider's website and create an account. All calls are made and received on your computer. You also need some way to physically make a call – i.e. you need a microphone to speak into and speakers to hear. For video calling you also need a web cam hooked up to your computer. Most laptops today come with all of the above built in. You can also plug in a headset with microphone for more privacy. Other options include a VoIP telephone, which looks like a regular phone but can plug right into an Internet broadband router without the use of a

computer, or an adapter that allows you to plug any ordinary phone into your computer through a USB port (this is how MagicJack works.)

Figure 4 MagicJack USB adapter

One of the key differentiating features of Skype as VoIP is that communications are connected point-to-point, and not through an exchange or server. It is a decentralized system, operating on what's called "peer-to-peer" architecture, as opposed to a "client-server" architecture. (The Skype login and user directory features are the only centralized functions.) This is important because it has an impact on security. This is the main Skype screen where a call is made by clicking "Call":

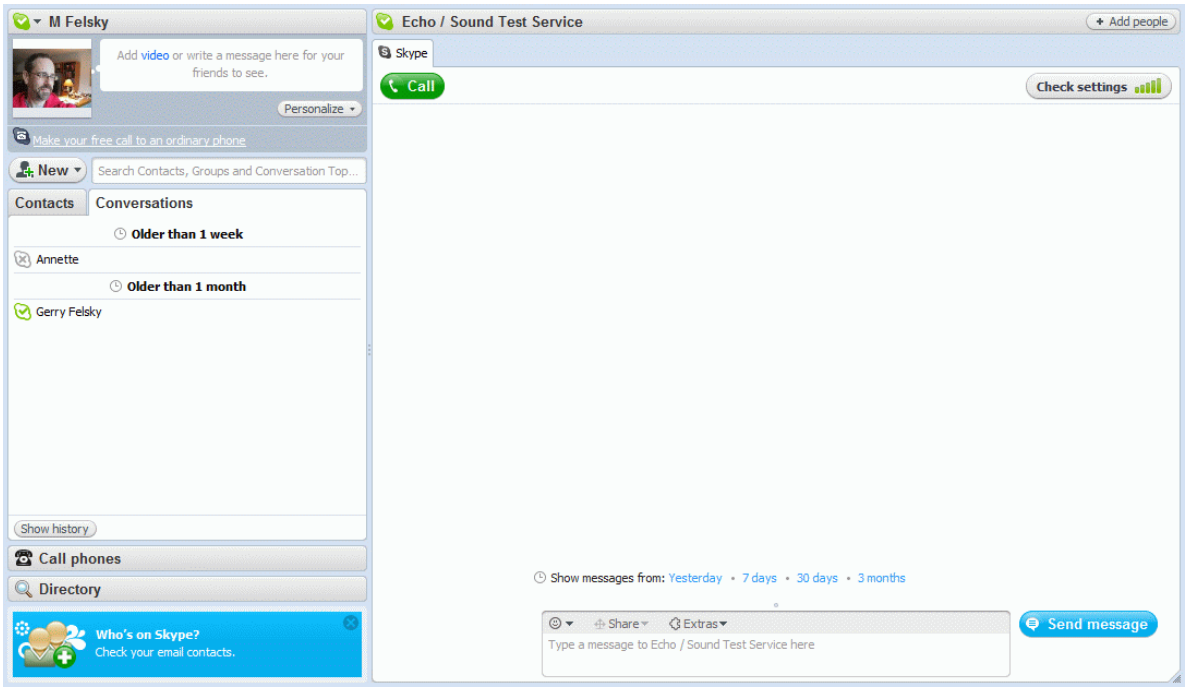

Figure 5 Making a call

Security

In this section I will discuss three key security issues relevant to the use of Skype by judges:

1. Is my identity protected on Skype?

2. Are my Skype communications private?
3. Is it safe to use the Skype on my laptop or PC when connected to the court's network?

Is my identity protected on Skype?

From the Skype website:

> "*Identity theft is big business in the criminal world. Your identity has a value and you must protect this to ensure that you don't become a victim. There are a number of controls in place that protect your information and identity when in use with Skype.*
>
> *When you sign into your account on our site all the information is sent over SSL. SSL encrypts all the information before it leaves your computer and can only be decrypted by our server. This is the technology in place on, for example, your online banking site or when you make a payment on an e-commerce website. When you sign in via Skype itself your information is also encrypted and kept safe from malicious third parties.*
>
> *Skype also uses a technology called digital certificates to provide further assurance that you are in conversation with whom you think you are. Everyone using Skype is issued this digital certificate and it forms part of the protection that is provided to ensure that your Skype account can only be used by you and help to ensure that third parties can't impersonate you. Remember, this identity is protected by your Skype Name and password.*"

Skype Privacy Settings - Video

One of the cooler aspects of Skype is the ability to have real-time video-conferencing.

Note that on the video setup screen, you can determine whether video conferencing is automatic when a call comes in, limited to certain callers, or controlled by you on every call (the recommended default!).

Warning: Please note that a web cam on any computer can be remotely activated by nefarious hackers or by well-meaning but ignorant administrators. In February, 2010, a school in Philadelphia was accused of secretly taking thousands of pictures of students who were using school-issued laptops without their knowledge or permission. It may be prudent to put a piece of tape over the lens of your web cam when not in use.[4]

[4] See *Toronto Star*, http://www.thestar.com/news/world/article/797955--school-district-took-secret-webcam-photos-of-students.

Skype Privacy Settings - Contacts

When you sign up for Skype, your name and some limited profile details are entered into a universal directory of users. This is helpful because you need to be able to contact someone to make a Skype call – think of it as the white pages phone book. On the PSTN you can pay extra to have an unlisted number. On Skype, if someone wants to call you they must first make a request, which is then approved by you. Similarly, if you find my name in the Skype directory and wish to call me, you cannot do so unless you identify yourself to me first and I "accept" you as a contact. Each of our names then appears in the other's personal Skype directory.

The other element of privacy that's important on Skype is this. When you are using your computer, if Skype is active, all your contacts can by default see that you are online and ready to receive a phone or video call. You can manually change your status to be offline or away, and Skype also has a voice mail feature that can handle calls while you are busy.

Are my Skype communications private?

The content of Skype communications is encrypted, though Skype and eBay (which owns Skype) have the capability to decrypt traffic. The risk of your conversation being intercepted and decrypted is very low, but it would be relatively easy for someone to determine that you are having a conversation, and what the IP addresses are for the interlocutors. Depending on how your network and Internet access are configured, your IP address may or may not be capable of being traced to you personally, or your home address.

As with any internet-based service, caution is required. Here is a warning about phishing[5] from the Skype website:

"*... [O]nly use your Skype password when signing into the skype.com website or the Skype software itself. We will never ask for your password by phone, email, instant message, etc. Control of your password is your best defence in protecting your Skype account, so don't give that away by either using the same password on other sites or falling for a phishing attack.*"

Is it safe to use Skype on my laptop or PC when connected to the court's network?

As previously mentioned, Skype operates on a peer-to-peer basis, meaning it is not an application that is installed on the court server. Network administrators are very suspicious about the security ramifications of applications like Skype because it bypasses network security safeguards, including firewalls.

There is another reason that network administrators dislike Skype: it can use a disproportionate amount of bandwidth. Bandwidth is the pipeline that a court has for the transfer of information through the Internet. Bandwidth is purchased based on the average and peak volume needed. If users are holding

[5] "Phishing" is a fraudulent attempt to lure users into sharing personal information such as bank accounts and passwords by masquerading as someone who is entitled to the information.

video conferences and making voice calls on Skype when connected to the court network, they are using up much more bandwidth than when they are researching case law, surfing the web or sending e-mail.

As Hayes puts it, "*While these are all valid concerns, they should be considered in the context of local network policies and weighed against the benefits that Skype can provide. In many cases running Skype in a well-managed environment can mitigate these risks.*"[6] For example, if judges use Skype on a regular basis for judicial business, the extra cost of bandwidth (if any) could be more than offset by a larger reduction in long-distance telephone or teleconferencing charges.

Recommended Settings and Best Practices

1. Use a strong password, do not share your password, do not use the same password as for other services, and uncheck both boxes below:

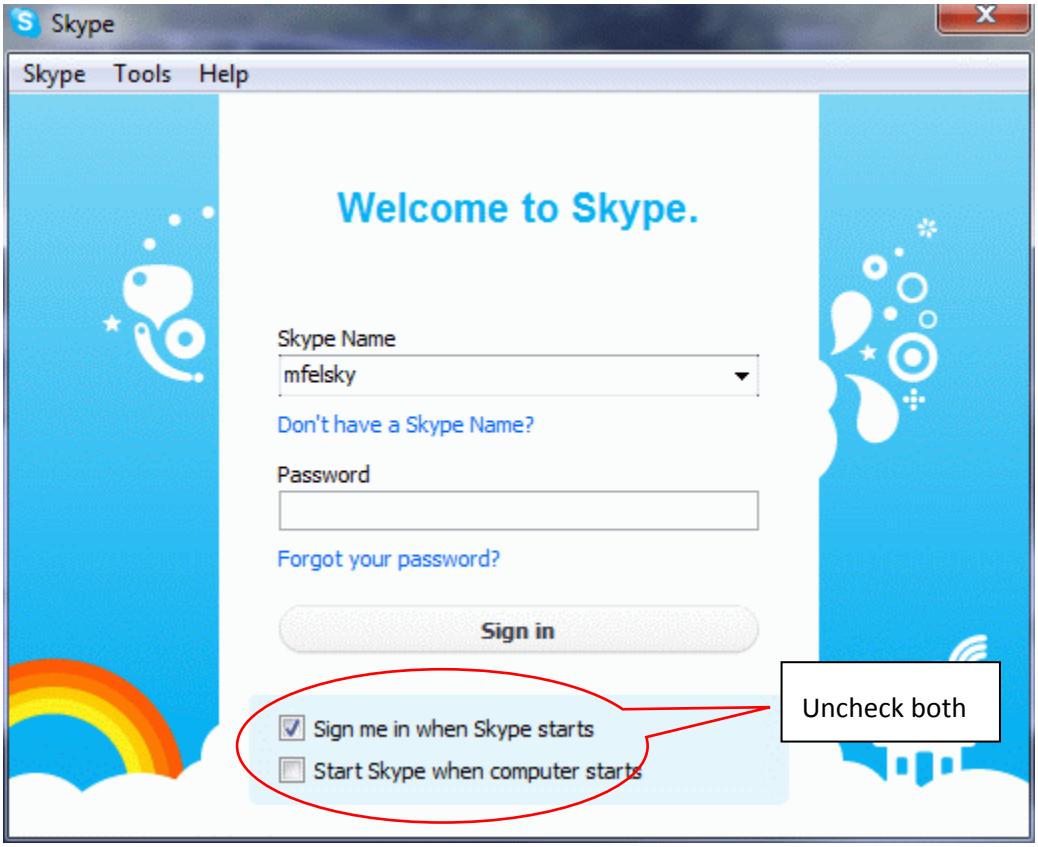

Figure 6 The welcome screen

[6] See Hayes, footnote 2, at page 4.

2. Limit incoming calls and messages to those people in your contact list (i.e. people you know and have accepted).

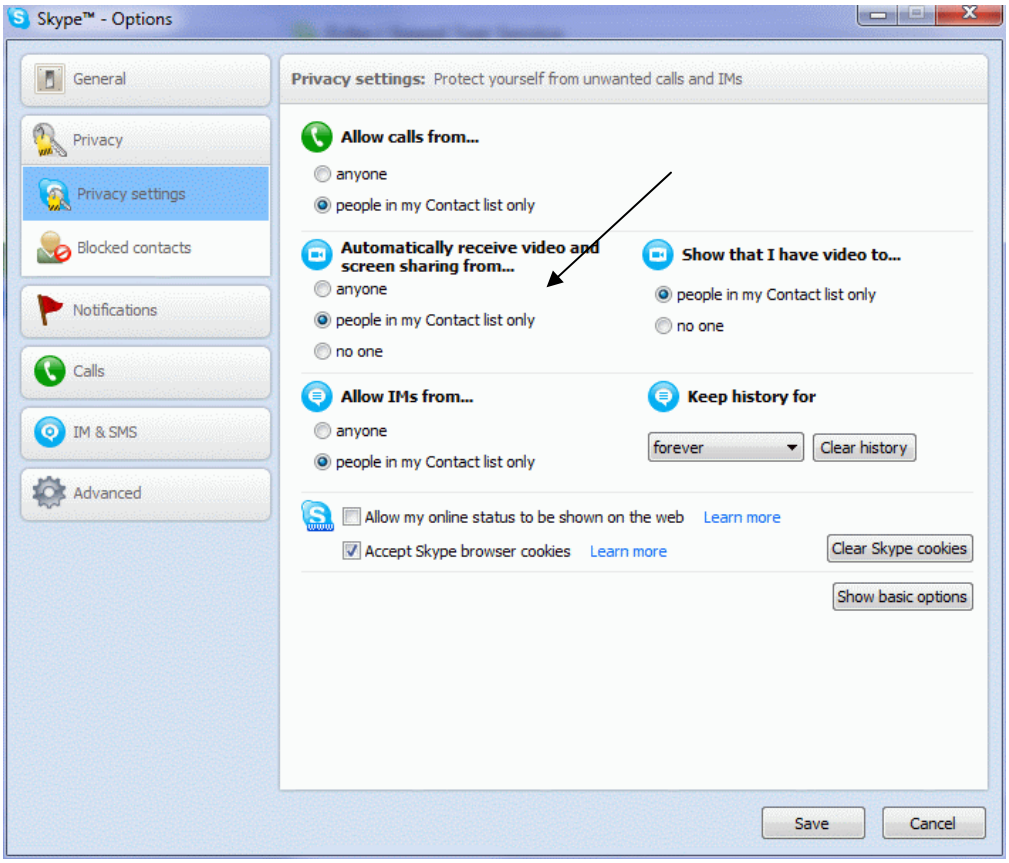

Figure 7 Skype privacy settings (advanced)

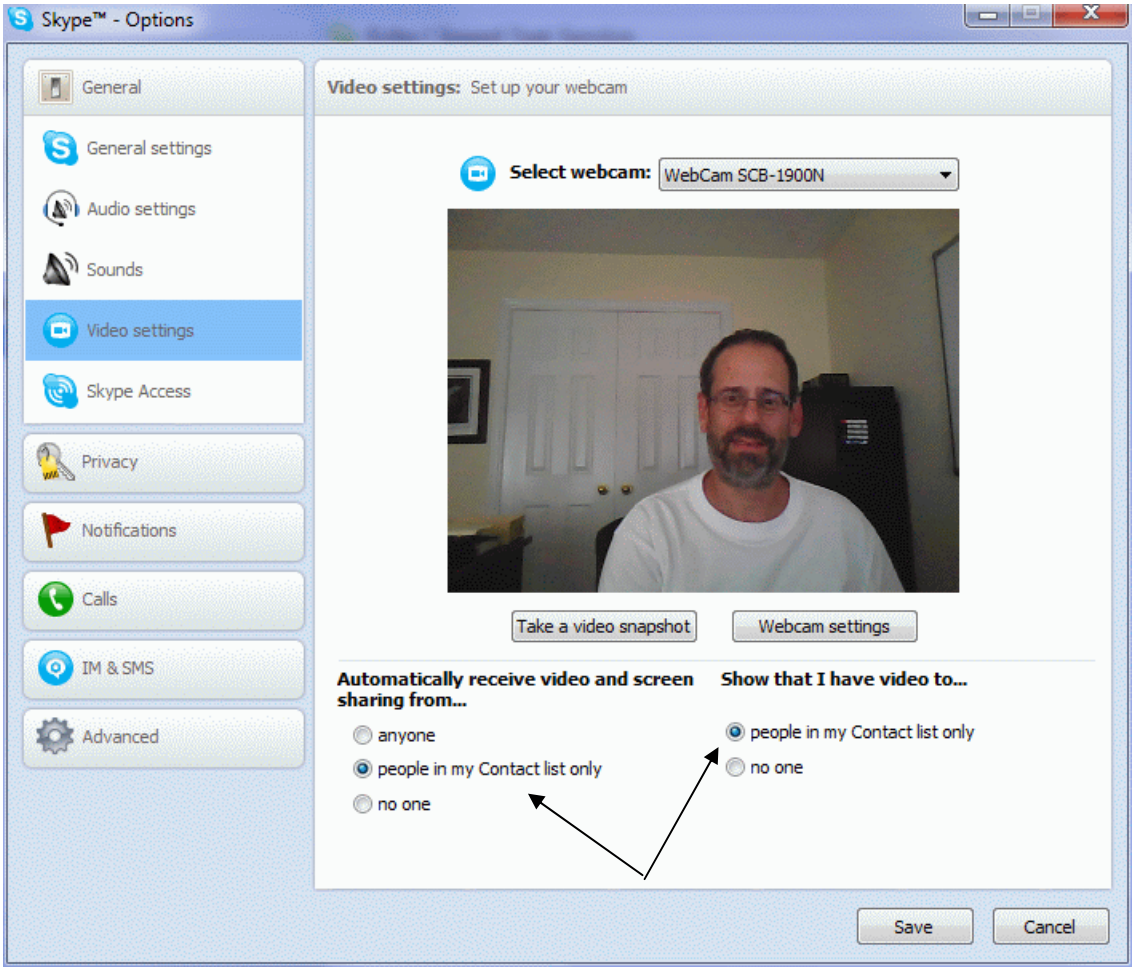

Figure 8 Configure video settings for your web cam

3. You can block specific people from contacting you:

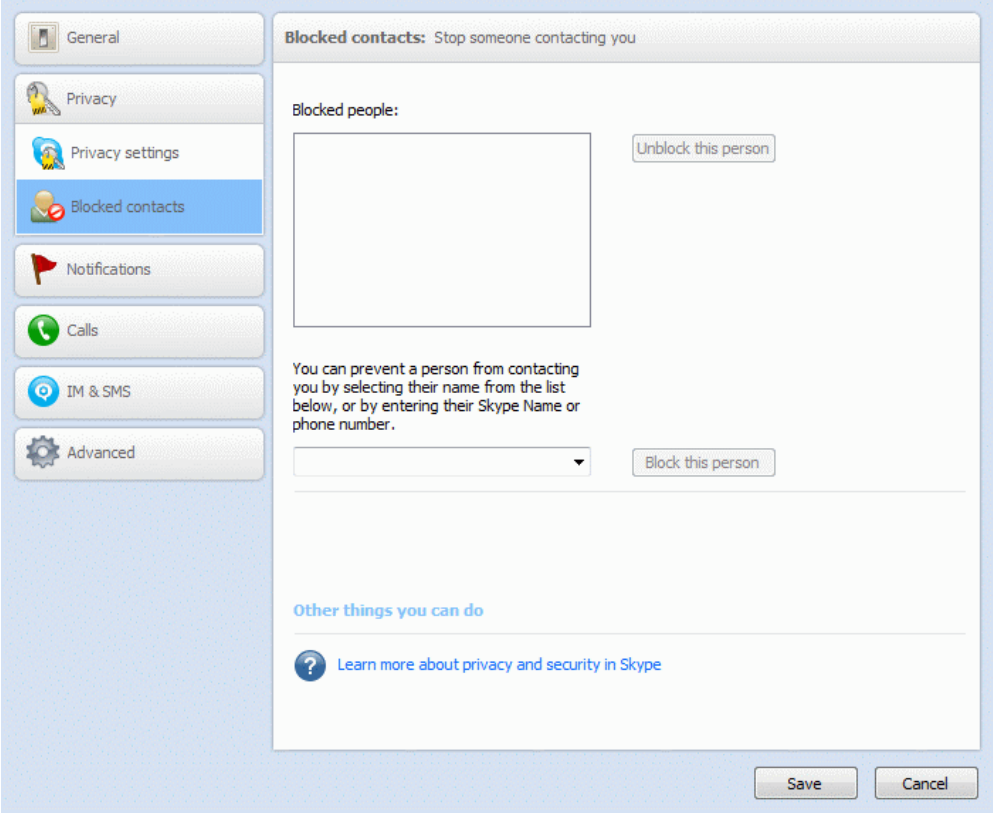

Figure 9 Blocked contact list is customizable

4. Minimize personal information in your profile:

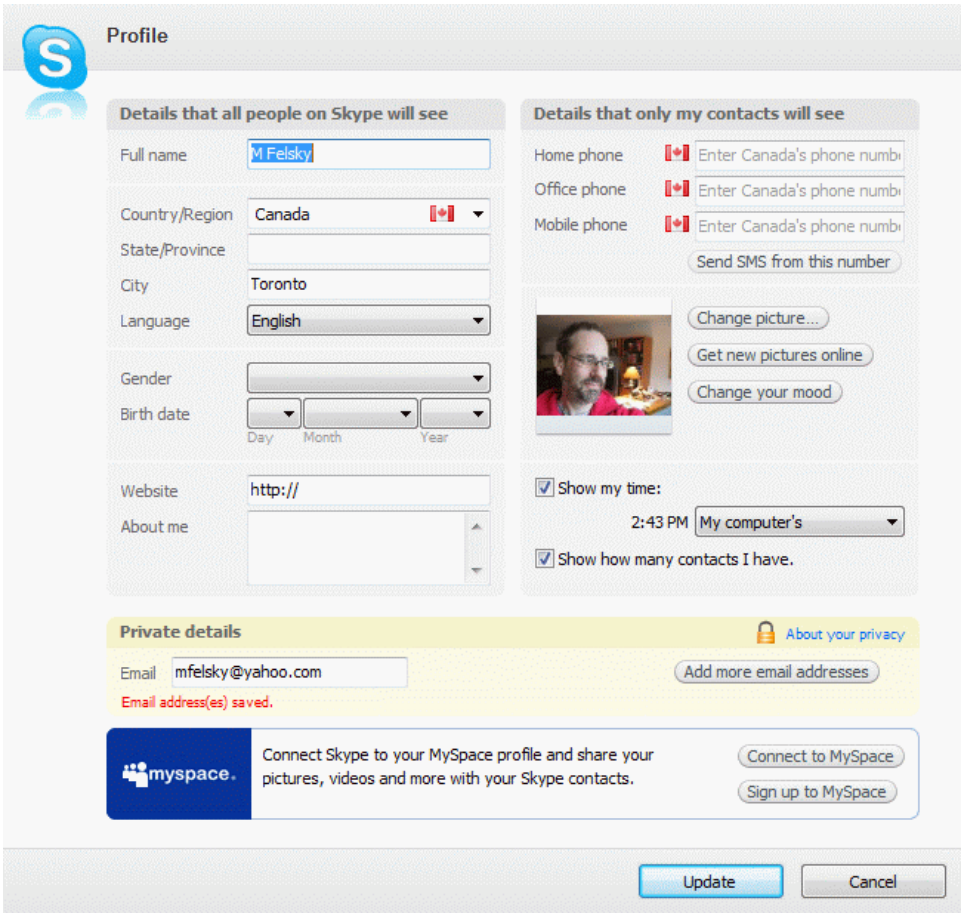

Figure 10 User profile can be minimized

5. Disable Ports 80 and 443:

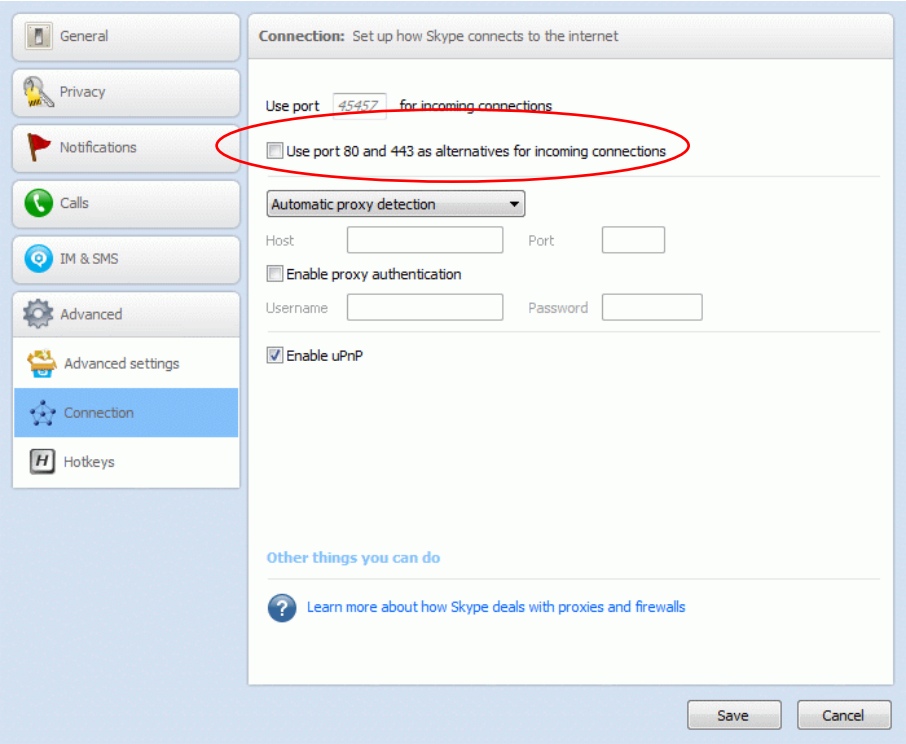

Figure 11 Disable Ports – Advanced

6. Make sure there are no nefarious programs using your Skype connection:

Figure 12 Permissions for 3d party program access

7. At the courthouse, advise your administrator or Judicial Information Technology Security Officer about your need for Skype so that network settings and potentially Windows Registry settings can be modified to make your Skype experience safer for you and your colleagues.

8. When a conversation or video call is over, and you close Skype, the program remains running in the background. Depending on how your Windows Taskbar is configured, you may see the Skype icon at the bottom of your screen. When the program is running, you will hear the phone "ring" when someone tries to call you. If you are not ready to receive calls, you should probably not only close the Skype Window, but "Quit Skype" as well.

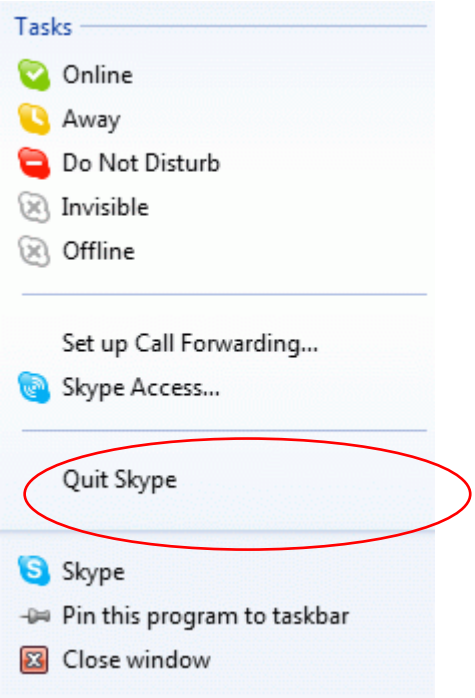

Figure 13 Logging out