Is Skype Safe for Judges?

By Martin Felsky, PhD, JD, for the Canadian Judicial Council,[1] Version 3.0 January 17, 2014

Microsoft Skype is a software application that permits its tens of millions of subscribers to make and receive voice or video calls over the Internet. In this article I will try to help judges understand whether Skype is safe for communicating judicial information. The bottom line is that Internet-based telephone services should not be used for carrying on sensitive judicial business unless the application has been approved and installed for judicial use by court services, in accordance with the principles set out in the *Blueprint for the Security of Judicial Information*.[2] For non-sensitive conversations when calling from home or on the road, Internet-based telephony offers free, convenience service. Even then, all users should be aware that internet-based telephony in general is inherently less secure than the "plain old telephone system" (POTS).

Many judges may not be familiar with Skype, 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.

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[3]. Reference should also be made to David Persky, "VoIP Security Vulnerabilities" (2007)[4]. Courthouse network administrators concerned about the use of Skype on court networks are encouraged to read these articles and implement the applicable security settings outlined by the authors.

Introduction: The Plain Old Telephone System

The traditional telephone system 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 transmissions. 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] Canadian Judicial Council, 4th edition, 2013, at http://www.cjc-ccm.gc.ca/cmslib/general/Revised%20Blueprint%202013-08-12%20for%20CJC%20approval.pdf.
[3] Bert Hayes, 2008 SANS Institute: http://www.sans.org/reading_room/whitepapers/voip/skype-practical-security-analysis_32918
[4] http://www.sans.org/reading-room/whitepapers/voip/voip-security-vulnerabilities-2036.

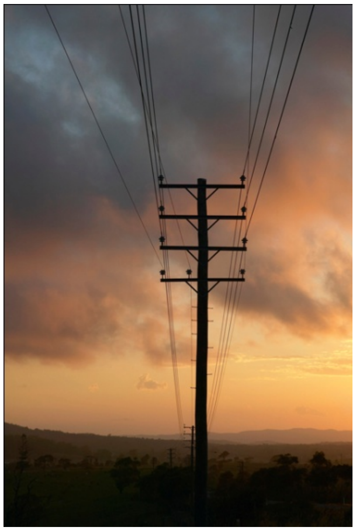


Figure 1: Telephone pole on the PSTN

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.

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.[5] Broadband Internet access is “always on,” making it suitable for interactive, live voice communication. Broadband Internet access is provisioned 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 assigned either a fixed or variable identifier, called an “IP address.”

Telephone Service over the Internet

A judge in Ottawa wishes to consult with a colleague in Vancouver via videoconference. They are both Skype users. The Ottawa judge opens Skype on his laptop, which is plugged into his home broadband modem. The Vancouver judge is one of his Skype contacts, and a symbol next to her name indicates she is online (i.e. available to connect). He clicks on her name to initiate the video call.

The Vancouver judge is at the airport in Hong Kong reading a magazine on her iPad. It beeps to indicate she has an incoming video call from her Ottawa colleague. She touches her screen to accept the call. They interact for ½ hour, exchanging text messages and sharing their screens during the call.

Skype works 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. You simply have a listing in the Skype Directory, which can be searched by full name, Skype name (username) or email address.

How Skype Works

In order to use Skype you must download software from the Skype website and create an account. All calls are made and received on your computer or mobile device. If not built in, you also need a microphone to speak into and speakers to hear, or a USB headset or USB telephone handset.

For video calling you also need a webcam hooked up to your computer. Most laptops and most tablets today come with front-facing cameras. Another option is to use a dedicated VoIP telephone, which looks like a regular phone but can plug right into a network connection.

The Skype VoIP is a largely a decentralized system, operating on what’s called “peer-to-peer” architecture, as opposed to a “client-server” or hub-and-spoke architecture. Skype has evolved its system over the years to a more centralized structure, although it is still primarily a peer-to-peer network, relying on the computing power and bandwidth of all its users to handle traffic without a costly centralized hub or independent communications network.

To improve performance for all users, Skype would automatically designate many computers on the network as “supernodes,” unbenknownst to the users. The additional traffic and computing burden placed upon these supernodes caused many headaches for network administrators, and made Skype very unpopular in courthouses as in many other organizations.

[5] Asymmetric Digital Subscriber Line

A few versions ago, Skype gave users the ability to prevent their computer from becoming a supernode. Since 2010-2011, Skype now hosts thousands of its own supernodes in secure data centres. This represents a significant change in its network architecture and alleviated some of the concerns expressed earlier.

Security

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

1. Is it safe for me to use Skype at home or on the road?
2. Is the content of Skype communications private?
3. When I use Skype on the court's network, is it safe for other users?

Is it safe for me to use Skype at home or on the road?

There are many reasons why VoiP in general, and Skype in particular, present security risks for users. It is much more difficult technically to intercept a phone call on the POTS than it is to intercept an internet communication (though Skype calls are encrypted). It is even easier when one party is using a wireless connection, as the Vancouver judge would be in the example given above.[6] Skype is a popular service and is thus an attractive target for hackers and malware, and for phishing exploits which can lead to identity theft. Even though the content of calls is encrypted, much of the related data and metadata is not. The history of calls is stored on the user's local device.

Is the Content of my Skype communications private?

As the world found out in 2013 thanks to NSA whistle-blower Edward Snowden , very little on the Internet seems to be private. In fact, it is reported that Skype has "back doors" built in to allow certain governments to monitor conversations, and there is good evidence that Skype itself has the capability to decrypt traffic.[7] We know that Skype monitors text-based traffic, checking for security risks such as spam, but it is not known whether the same is done for voice calls (probably not). Besides built-in monitoring, the risk of a live conversation being intercepted and decrypted by others is quite low, but it would be relatively easy for someone to determine that you are having a conversation, and what the IP addresses are for each user. (Your IP address by default is broadcast to anyone you call unless that setting is changed – see recommended step #5 below.) 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.

[6] See "Wireless Network Security When on the Road," Canadian Judicial Council, 2d edition, 2014.

[7] The Wikipedia entry on "Skype Security" should be checked from time to time as new revelations of security breaches and vulnerabilities come to light. See http://en.wikipedia.org/wiki/Skype_security.

When I use Skype on the court's network, is it safe for other users?

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

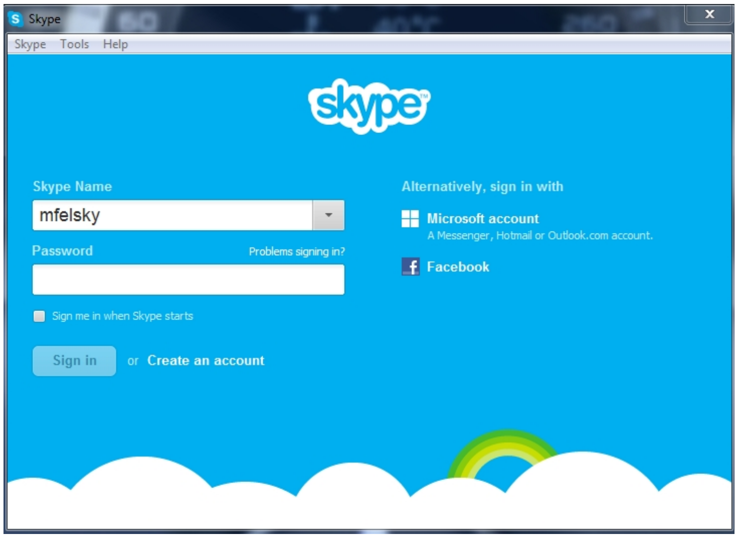
There is another reason that network administrators dislike Skype: it can use a disproportionate amount of bandwidth. Bandwidth is the pipeline that a court has for the transfer of information through the Internet. Bandwidth is purchased based on the average and peak volume needed. If users are holding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

Since the redesign of Skype, it appears that the concerns about bandwidth and security associated with any user becoming a supernode appear to have been alleviated. However, concerns about privacy have increased, because in a more centralized server system, surveillance is easier.

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.*"[8]

Recommended Settings and Best Practices

1. Use a strong password, do not share your password, and do not use the same password as for other services.



Skype Name: mfelsky

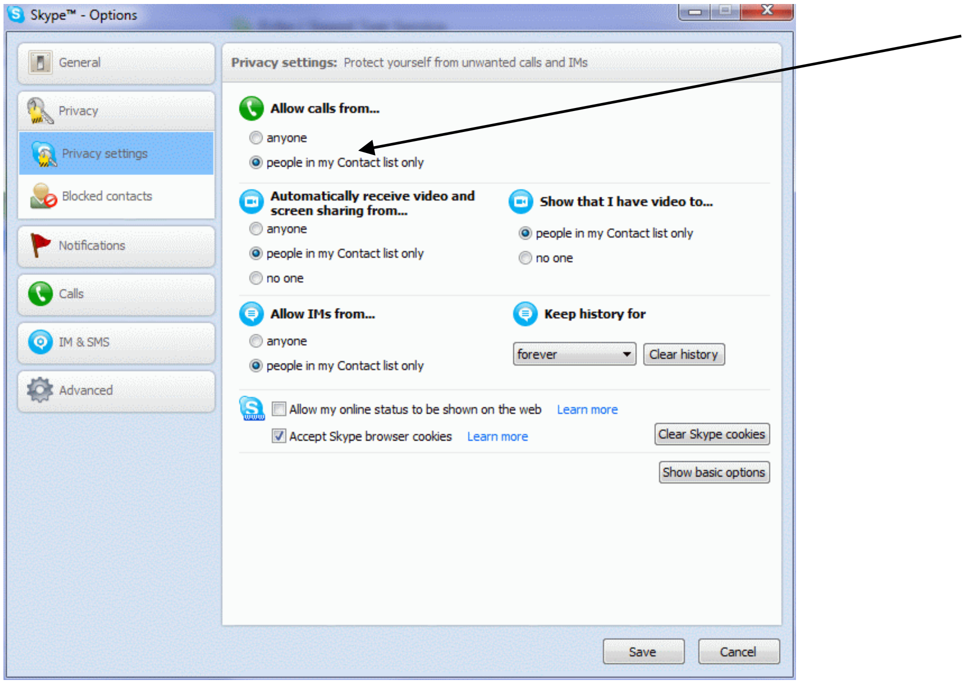
Password:

□ Sign me in when Skype starts

Figure 3 The login screen

[8] 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 as Skype contacts).



Privacy settings: Protect yourself from unwanted calls and IMs

Allow calls from...

○ anyone

● people in my Contact list only

Automatically receive video and screen sharing from...

○ anyone

● people in my Contact list only

○ no one

Show that I have video to...

● people in my Contact list only

○ no one

Allow IMs from...

○ anyone

● people in my Contact list only

Keep history for

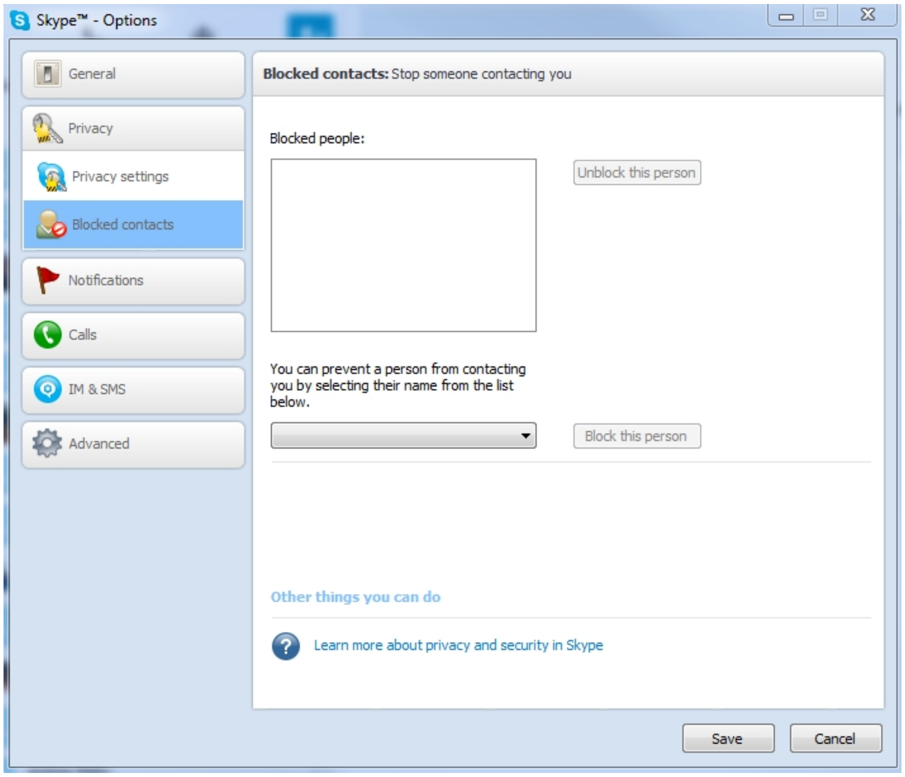
forever

□ Allow my online status to be shown on the web Learn more

☑ Accept Skype browser cookies Learn more

Figure 4 Skype privacy settings (advanced)

3. You can block specific people from contacting you (below), and using the Video settings, you can prevent anyone who is not in your contact list from making a video call to you:



Skype™ - Options

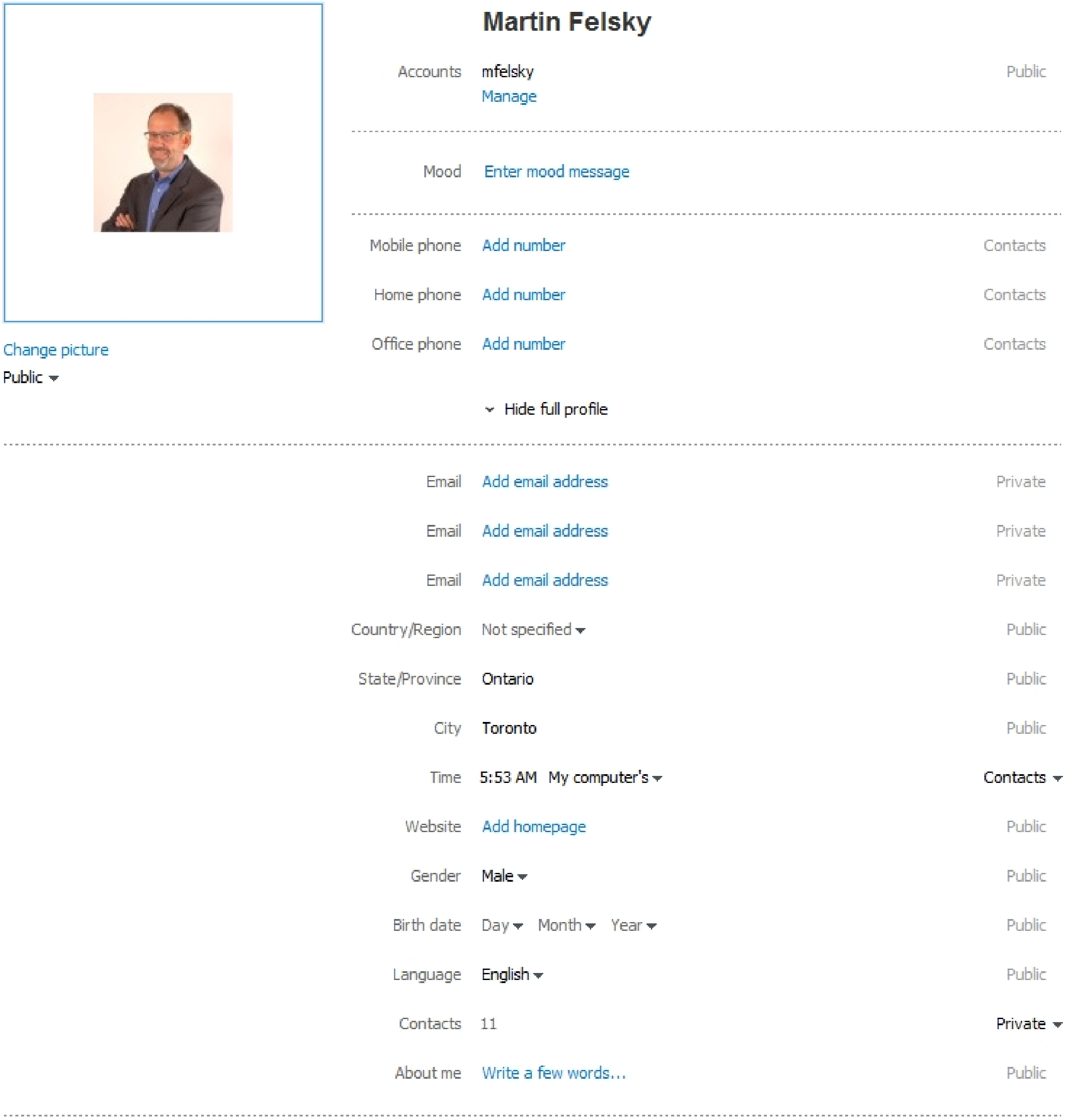
Blocked contacts: Stop someone contacting you

Blocked people:

You can prevent a person from contacting you by selecting their name from the list below.

Figure 5 Blocked contact list is customizable

4. Minimize personal information in your profile and limit who can see that information (only you, only contacts, or public):



Martin Felsky

Accounts	mfelsky Manage	Public
Mood	Enter mood message	
Mobile phone	Add number	Contacts
Home phone	Add number	Contacts
Office phone	Add number	Contacts

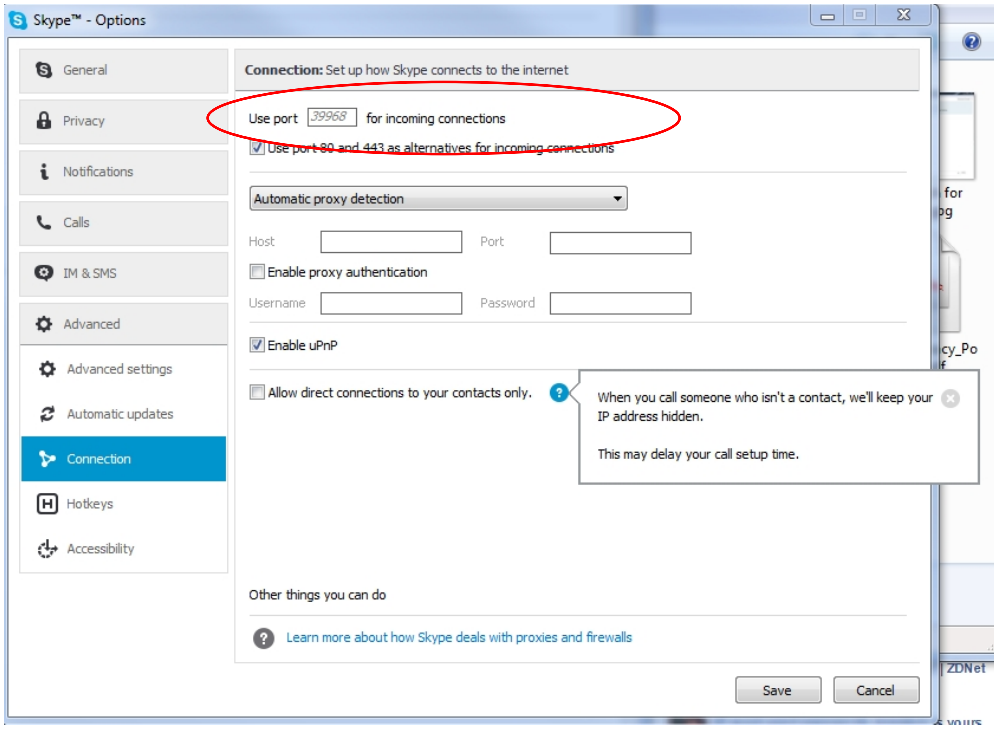
Change picture
Public ▾

⌄ Hide full profile

Email	Add email address	Private
Email	Add email address	Private
Email	Add email address	Private
Country/Region	Not specified ▾	Public
State/Province	Ontario	Public
City	Toronto	Public
Time	5:53 AM My computer's ▾	Contacts ▾
Website	Add homepage	Public
Gender	Male ▾	Public
Birth date	Day ▾ Month ▾ Year ▾	Public
Language	English ▾	Public
Contacts	11	Private ▾
About me	Write a few words…	Public

Figure 6 User profile can be minimized

5. Use Tools – Options – Advanced to disable (uncheck) Ports 80 and 443 – they are checked by default, and check the box that says “Allow direct connections to your contacts only” to make sure non-contacts cannot have access to your IP address:



Skype™ - Options

Connection: Set up how Skype connects to the internet

Use port 39968 for incoming connections

☑ Use port 80 and 443 as alternatives for incoming connections

Automatic proxy detection

Host: Port:

□ Enable proxy authentication

Username: Password:

☑ Enable uPnP

□ Allow direct connections to your contacts only.

When you call someone who isn't a contact, we'll keep your IP address hidden.

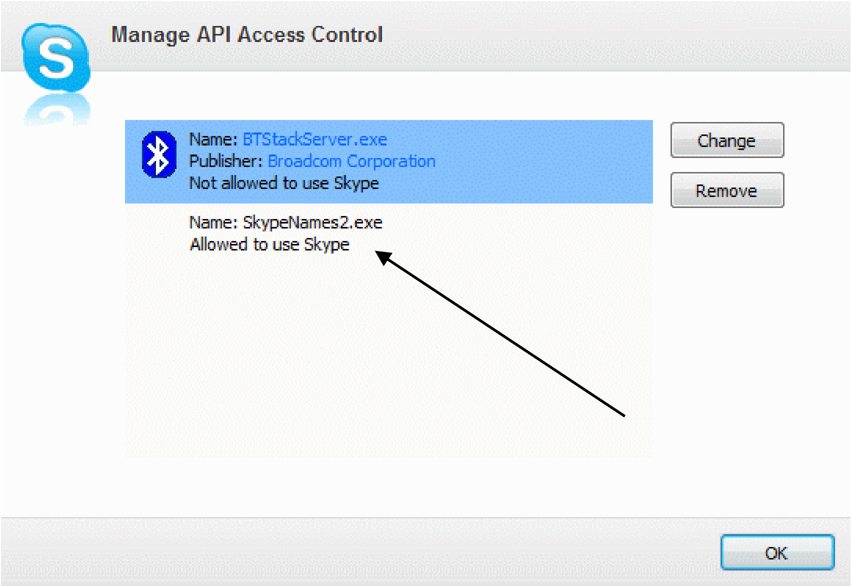
This may delay your call setup time.

Other things you can do

Learn more about how Skype deals with proxies and firewalls

Figure 7 Disable Ports – Advanced

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



Manage API Access Control

Name: BTStackServer.exe
Publisher: Broadcom Corporation
Not allowed to use Skype

Name: SkypeNames2.exe
Allowed to use Skype

Figure 8 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 and local 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 computer 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 can designate yourself as unavailable, or quit Skype entirely.