THE DEMISE OF AND ANSWER TO SKYPE

Skype began as a very cool service. I used it and recommended it - a lot.

Skype (originally *Sky peer-to-peer*) was a peer to peer voice system, which means that there was no central computer controlling everything. It was also encrypted, though the internal details were never revealed.

But, as will a lot of good tech ideas, the developers were persuaded to sell it. In this case, to eBay in 2005. (For $2.5 billion, which is a lot of persuasion!) Then, after doing very little with the tech for several years, eBay sold it to Microsoft for $8.5 billion in 2011.

That's when the serious trouble began. Here are the highlights:

· Microsoft filed a patent on technology for spying on Skype in 2009. (Before they bought it!)

· In November 2010, it was learned that a flaw in Skype allowed hackers to secretly record user IP addresses. As of a few months ago, it still wasn't fixed.

· It has been known since 2012 that Skype has made online chats and other user information available to police. (Not just to the Feds, but to local cops.) They also allow your local cops to see your addresses and credit card numbers.

· In November 2012, Skype was reported to have handed over user data of a pro-Wikileaks activist to a private security company called iSIGHT Partners, without a warrant or court order. Once this was revealed, Skype said that they would conduct "an internal investigation."

· In May 2013, it was documented that a URL sent via a Skype instant messaging session was usurped by the Skype service and subsequently used for information retrieval originating from an IP address registered to Microsoft headquarters.

· Skype participates in PRISM, the U.S. Government spy program by allowing the NSA unfettered access to its data center.

Now you know.

So, with Skype spilling its (your!) guts to DC agencies, their contractors, and even to your local enforcer, what should you do?

Obviously, you stop using Skype for anything that matters.

I'm sure, however, that you'd still like to talk to distant friends. And there are ways to do it. (I'll pass

up chat in this article; you can get that info in *Cryptohippie's Guide to Online Privacy,* here.)

Voice conversations over the Internet are called *VoIP* (voice over IP). One good VoIP system is Jitsi. Jitsi uses the same protocols as many chat systems, but sends voice instead of text.

The first time you connect with someone using Jitsi, you'll have to go through an authentication process, to verify that no one is trying to spoof identities. But once you're done authenticating, you shouldn't have to do it again. Call quality won't match that of a wired telephone, but it is more than good enough.

If you want to call regular telephones from your computer using VoIP, you can use a service such as DiamondCard. If you pay them anonymously (using Pecunix or Bitcoin), you will retain your privacy... except for whatever you say in your conversations, of course. Remember: All standard telephone conversations are likely to be recorded these days. Big Brother is here, now.

The best option is Cryptohippie's new voice system, inside of their anonymity network. That means that you can speak to your friends and associates through an encrypted, anonymous connection. Not only can't the call be understood by anyone else, but no one will know who you talked to, for how long, or when.

This system works via computer, but it also works with smartphones! That means that *you can be truly secure while talking on your cell phone.*

The system actually functions more like a chat system than a regular phone, but it is very easy to use on either computers or mobiles.

Obviously, only calls between Cryptohippie users will be anonymous. During conversations outside of the network your location would be masked, but your conversation would be accessible to snoops on the other end.

Instructions can be found on the Cryptohippie support Wiki, here.

Paul Rosenberg-"prosberg" in the TTP Forum - is a computer security specialist and founder of Cryptohippie. *TTP endorses Cryptohippie for your personal online security.*