

VoIP ethics

Prof. Simon Rogerson

**Originally published as ETHicol in the IMIS Journal Volume 18
No 2 (April 2008)**

Voice over Internet Protocol (VoIP) is a protocol that allows basic communications functions, such as voice calls, voice messaging and facsimile over the internet instead of the traditional telephone network. It is hard to find data on VoIP usage but it is suggested from several sources that around 2 billion people have used this internet facility. This article focuses on one of the many VoIP service providers, Skype. It is based on experiences as a first time Skype user with a keen interest in service integrity!

Loading the free software for Skype is very easy and within no time you can be a registered Skype user communicating with people around the world. However, unbeknown to the new user are the default values on installation. On booting up your computer Skype opens automatically. Why might this be a problem? It is because of the default privacy settings on installation which are "allow calls from anyone", "automatically receive video from anyone", "allow chats from anyone", "allow my status to be shown on the web", "accept Skype browser cookies" and "keep chat history forever". This maximum visibility makes Skype users vulnerable. Is it acceptable for a VoIP service provider to operate an "opt-out" strategy rather than an "opt-in" strategy and give no apparent warning of this? Once a connection is made and a web camera is activated the recipient can see you and can capture still images and video streams without your knowledge or consent. Once captured these can be easily manipulated and distributed. This potentially covert capture of visual information increases Skype users' vulnerability as such information can be used in a number of unsavoury and questionable ways.

It is likely that a Skype user will want to portray himself or herself as someone whom people would like to talk to. Skype allows you add facts about yourself such as full name, date-of- birth, gender, home location and narrative about yourself, for example, where you could describe your social and sporting interests and your favourite music. All these details will always be seen by all Skype users. How many Skype users will consider that adding too much personal data increases your vulnerability? Skype also allows you to share personal data with the social networking site MySpace. Such interconnectivity further increases vulnerability.

Skype is supported by a website which enables Skype users to manage and pay for services. Skype's privacy policy, which was last revised on September 8, 2007, is published on this website. (<http://www.skype.com/intl/en-gb/legal/privacy/general/> accessed 17 March 2007) The policy raises a number of ethical issues. Consider these extracts, each of which is followed by an issue that they raise.

"Skype collects and processes, or has third party service providers acting on Skype's behalf collecting and processing, personal data relating to you ..." - It is unclear who are the third parties and how such organisations are vetted regarding privacy of Skype users.

"Your information may be stored and processed in any country in which Skype and the Skype group maintain facilities, including outside of the EU." - It is not mentioned that there are some countries which the EU will not allow personal data to be transferred to due to that country's unacceptable track record on personal data. What would Skype do if it operated in such a country?

"...personal information of Skype users will generally be one of the transferred business assets. We reserve the right to include your personal information, collected as an asset, in any such transfer to a third party." - Skype clearly views personal data as a business asset which can be sold as part of company sale. What safeguards do Skype users have regarding the use or abuse of their personal data in such situations?

"Cookies enable Skype to gain information about the use of its websites. This information may be analyzed by third parties on our behalf." - Once again it is unclear who the third parties are and how they have been vetted.

"Skype websites may contain links that will let you leave Skype's website and access another website. Linked websites are not under the control of Skype and it is possible that these websites have a different privacy policy." - As a marketing strategy Skype has established these links to enhance the attractiveness of Skype to potential users but seems to have abdicated any responsibility about the integrity of the websites it has exposed Skype users to.

"Skype and, where relevant, the Skype group entities will retain your information for as long as is necessary ..." - Given Skype views such personal information as a business asset would imply that data is kept forever.

The Skype entry on Wikipedia (http://en.wikipedia.org/wiki/Skype#Security_concerns accessed 16 March 2008) includes a number of associated concerns about privacy policy and security of Skype communications. It states, "Skype was also found to access BIOS data to identify individual computers and provide DRM protection for plug-ins. It can not be assured that Skype calls are not interceptable. Skype provides end to end encryption for connections between users however in an interview at cnet.com Skype chief security officer Kurt Sauer would not eliminate this possibility. Skype is owned by eBay, whose privacy policy is perhaps the most liberal of any large corporation - eBay claims it goes above and beyond what it is required to do by law, seeking out and giving police all the information it stores about users excluding some financial data, for which they require a subpoena"

VoIP services are a relatively new example of ways in which we can use the internet to link up with people round the world. Users of such services have an obligation to ensure

they are careful in how they use such services and do not put themselves at risk. Equally the service providers have an obligation to minimise user vulnerability through clear advice and through integrity of their services and associated policies. It would seem there is a long way to go before such obligations are understood and acted upon.

Please send your views on ethical and social responsibility issues and cases of ethical dilemmas to:

Professor Simon Rogerson
Director
Centre for Computing and Social Responsibility
Faculty of Computing Sciences and Engineering
De Montfort University
The Gateway
Leicester
LE1 9BH
Tel: (+44) 116 257 7475
Fax: (+44) 116 207 8159
Email: <srog@dmu.ac.uk>
Website: (<http://www.ccsr.cse.dmu.ac.uk/>)