Privacy International
46 Bedford Row
London
WC1R 4LR
United Kingdom

+44 (0) 20 7242 2836
@privacyint

UK Charity No. 1147471

Friday, 27 July 2012

Dear Mr Bates,

I am writing to request further information about the privacy implications of recent developments at Skype, as reported in the Washington Post.[1] We were delighted to read that you believe these reports are "inaccurate" and"could mislead the Skype community", and that you want to "clear this up". [2]

The growth of Skype since its launch in 2003 to become the world's leading VoIP provider has been driven by service that is affordable, high quality and, above all, secure. From an early stage in its development, Skype has assured its customers of the security of their communications. Press releases and product descriptions from 2005 boast of "end-to-end encryption for superior privacy" that "nobody can intercept".[3] In 2008, a spokesperson reassured users that "[w]e have not received any subpoenas or court orders asking us to perform a live interception or wiretap of Skype-to-Skype communications" and "[i]n any event, because of Skype's peer-to-peer architecture and encryption techniques, Skype would not be able to comply with such a request".[4]

In short, a promise was made to Skype customers that the privacy of their conversations and file transfers would be protected.

As I'm sure you know, among Skype's 663 million registered users across the world are human rights defenders and pro-democracy activists living under autocratic regimes. In an environment where most channels of communication are pervasively monitored and the contents of an email or

---

[1] Skype makes chats and user data more available to police, By Craig Timberg and Ellen Nakashima, July 26 2012 http://www.washingtonpost.com/business/economy/skype-makes-chats-and-user-data-more-available-to-police/2012/07/25/gJQAobI39W_story.html

[2] http://blogs.skype.com/en/2012/07/what_does_skypes_architecture_do.html

[3] Skype for Mac OSX and Linux - Press release - http://about.skype.com/press/2005/02/skype_for_mac_os_x_and_linux.html#more; http:://skype.com/products archived from 28 August 2005 -http://web.archive.org/web/20050828033447/http://skype.com/products/
"'Nobody's listening in. When it comes to talking, instant messaging or transferring files, we've gone to great lengths to make it secure. Skype automatically encrypts everything before sending it through the internet. Likewise, on arrival everything is decrypted on-the-spot and presented as crystal clear speak, text or a file transfer nobody can intercept."

[4] http://news.cnet.com/8301-13578_3-9963028-38.html

text message may result in detention without trial, torture or worse, these groups have historically relied on Skype as one of the very few means to communicate securely. We believe that Skype should be proud of the role its technology has played in facilitating secure communication and supporting individuals' right to privacy in some of the world's most repressive regimes.

Given that your past assurances have led users to put their complete trust in Skype as a secure channel of communication, we believe that any changes to Skype's services that might affect security must be made as explicit as possible. For vulnerable communities in certain parts of the world, the cost of ambiguity could be very great.

In light of these recent developments, we would be grateful if you could uphold your commitment to "acting as a responsible global citizen"[5] and provide answers to the following questions:

1. With the developments of Skype, will previous privacy protections such as end-to-end encryption be preserved?
2. For calls, IMs and other Skype functions, is it possible for you, or law enforcement, to access and record
   a) communications content,
   b) traffic data, or
   c) countries of call origin and destination, and other country information of users when this information is not voluntarily provided.
3. We note that recent attacks on the communications of individuals by repressive regimes have used targeted and trojaned Skype as an interception mechanism. What steps are being taken to mitigate this threat?
4. Will you begin using SSL for downloads, and also verifying updates offered to Skype, to prevent fake updates?
5. Will Skype publish statistics, by country, on the number of lawful access requests received, and the percentage complied with?

Yours sincerely,

Eric King
Head of Research
Privacy International

[5] http://blogs.skype.com/en/2012/07/what_does_skypes_architecture_do.html