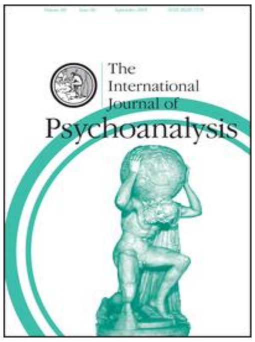

Routledge
Taylor & Francis Group

The International Journal of Psychoanalysis

ISSN: 0020-7578 (Print) 1745-8315 (Online) Journal homepage: https://www.tandfonline.com/loi/ripa20

On: Skype and privacy

John Churcher

To cite this article: John Churcher (2012) On: Skype and privacy, The International Journal of Psychoanalysis, 93:4, 1035-1037, DOI: 10.1111/j.1745-8315.2012.00610.x

To link to this article: https://doi.org/10.1111/j.1745-8315.2012.00610.x

Published online: 31 Dec 2017.

The International Journal of Psychoanalysis

Letter to the Editors

On: Skype and privacy

Dear Editors,

Jill Savege Scharff's recent paper discusses modifications of the psychoanalytic setting (or frame) using the telephone and/or Internet to allow sessions to take place when analyst and patient are in different geographical locations (Scharff, 2012). Her paper has the merit that it addresses both technological and psychoanalytical aspects of the setting, and the relations between them. However, there are inaccuracies in her account of the technology, including VoIP[1] telephony of which Skype is one example, and these could have implications for psychoanalytic practice. Her paper raises many interesting and important issues but my comments here are confined to her assumptions about security and privacy. She writes:

> VOIP has the advantage that it is a secure method of communication … VOIP is thought to be secure because it sends information in fragmented bundles that do not connect until they reach the destination. But because it does not offer encryption, VOIP is not as secure as using a Videotechnology Company (VTC).[2]
>
> (Scharff, 2012, p. 82)

This is not entirely clear or accurate and could be misleading. The phrase "fragmented bundles" apparently refers to packet-switching, which is the basis of all Internet communication, including Internet-based VoIP such as Skype, but also email, web browsing, etc. Packet-switching without encryption offers only limited security against physical interception, and none against eavesdropping techniques that use readily available software. Some VoIP and web-based videoconferencing services do not use encryption, but others do. Skype calls are encrypted, which may partly explain the widely held but unwarranted belief that Skype is secure.

Because Skype uses proprietary software its encryption method is not publicly available and therefore cannot be independently evaluated. Moreover, recent empirical research (Dupasquier *et al.*, 2011) has shown that significant information is recoverable from intercepted Skype voice calls, *without* decryption, using statistical properties of the encrypted data. These authors conclude that:

> This paper has demonstrated the false sense of privacy provided by Skype, a widely used VoIP application, known for its strong security policy … To the knowledge of the authors, this is the first published research that demonstrates that Skype encryption is not entirely secure and that information is leaked allowing content to be inferred.
>
> (Dupasquier *et al.*, 2011, p. 325)

[1] Voice Over Internet Protocol – a protocol for voice and multimedia communication over IP networks such as the Internet.

[2] In this context 'VTC' more usually refers to videoteleconferencing.

Published by Blackwell Publishing, 9600 Garsington Road, Oxford, OX4 2DQ, UK and
350 Main Street, Malden, MA 02148, USA on behalf of the Institute of Psychoanalysis

The nature and extent of the information leakage demonstrated by these authors were limited, but stronger results were subsequently published in an award-winning paper by White *et al.* (2011), who comment that: “The threat is more serious than previously thought” (p. 1). Several research groups now work in this area and progress is rapid; a recent review by Keromytis (2012, in press) summarizes 245 publications on VoIP security, of which 30 relate to ‘eavesdropping, interception and modification’. Current research thus undermines the claim that Skype is secure and, in a world where computer malware (e.g. viruses, Trojans, rootkits), ‘phishing’, voicemail hacking, identity theft, etc. are increasingly employed on an industrial scale, it cannot be assumed that insecure telecommunications will protect the privacy of clinical work.

In the classical psychoanalytic setting, in addition to the elements described by Freud (the fundamental rule, the analytic hour, use of the couch, etc.), there are numerous implicit ones which are seldom stated because they can usually be assumed. These include the fact that consultations typically take place in a room within a building, where patient and analyst can hear each other but cannot be overheard by others. The acoustic properties of a consulting room are usually stable over time, and its privacy is implicit and assumed. The possibility of being overheard may exist in phantasy, but except in situations where covert surveillance of private communications is the norm, or where for some reason it can realistically be anticipated, or if the patient is in a paranoid state, any conscious anxieties about privacy are likely to focus on the analyst’s capacity to maintain boundaries of confidentiality rather than on physical security of communication.

We usually have enough tacit knowledge about our immediate physical and social environment to make reliable judgements about whether a conversation is private, but this is less true of our virtual environment in cyberspace. A telephone conversation, with or without video, can create a compelling illusion of the immediate presence of one other person, and of the absence of others, but this illusion is only a sophisticated *simulacrum*. In a clinical session conducted by telephone the setting partly relies on and incorporates the tacit knowledge and beliefs of the respective participants concerning the technology they are using. An adequate understanding of the implications of modern telecommunications for psychoanalytic practice therefore needs to be informed both by an up-to-date understanding of the technology itself and by a psychoanalytic way of thinking about how both the technology and its evolving social organization come to inhabit the setting, including the internal setting in the minds of both analyst and patient.

I am not arguing for or against the use of communications technology in clinical work, but that we need to inform ourselves better about it, and to try to avoid simplifying or idealizing it. Just as we need our relations with the consulting room, the couch, the fundamental rule, the analytic hour, etc. to be realistic, so we need to avoid basing our use of the telephone, Skype, or the Internet generally, on wishful thinking.

John Churcher
4 Rippingham Road, Withington, Manchester M20 3EX, UK
E-mail: churcher@aulos.co.uk

References

Dupasquier B, Burschka S, McLaughlin K, Sezer S (2011). Analysis of information leakage from encrypted Skype conversations. *Int J Inf Sec* **9**:313–25.

Keromytis AD (forthcoming). A comprehensive survey of voice over IP security research. IEEE Communications Surveys and Tutorials. Also available online at: http://www.cs.columbia.edu/˜angelos/Papers/2011/cst.pdf (accessed 4 April 2012).

Scharff JS (2012). Clinical issues in analyses over the telephone and the internet. *Int J Psychoanal* **93**:81–95.

White AM, Matthews AR, Snow KZ, Monrose F (2011). Phonotactic reconstruction of encrypted VoIP conversations: Hookt on fon-iks. Proceedings of the 32nd IEEE Symposium on Security and Privacy, Berkeley, CA, USA, May 2011.