A new 'fact of life': mass surveillance of telecommunications and its implications for psychoanalytic confidentiality.[1]

John Churcher
British Psychoanalytical Society

Abstract

Telecommunications are subject to surveillance and the contents of private conversations are stored for potential use in protecting national security, fighting terrorism, etc. If at some point in the future an authoritarian and undemocratic regime were to achieve power, it could inherit this stored information and use it for repressive measures against individuals. A new factor in the present situation is the recently-acquired capacity of the state to intercept and store the communications of all or most citizens. This would have serious implications for psychoanalytic practice under adverse conditions that could arise in the future, especially for 'remote analysis', but it also has implications for current practice.

*Confidentiality is an essential condition of psychoanalysis. It is undermined by external circumstances which interfere with the possibility of free association in the patient and evenly-suspended attention in the analyst. Whether under conditions of extreme state violence, such as in Argentina during 1975-83, or in a liberal democracy, external social reality has effects on inner mental life. Mass surveillance is widely subject to disavowal (*Verleugnung*), and 'splitting of the ego': we continue using the internet while turning a blind eye to future danger. Confidentiality is undermined by surveillance in the same way as it is by legal obligations to report on patients, but surveillance cannot be fought by reasserting the primacy of professional ethics. The splitting is between neurotic and psychotic parts of the personality, and the latter is deposited unconsciously in the psychoanalytic setting. When the setting includes telecommunications, we need to be curious about what is deposited in the communications system itself, but we know little about how this complex system works.*

IPA advice acknowledges the problem of confidentiality in telecommunications and urges psychoanalysts to ensure that the technology they are using is secure. Unfortunately, this is an intractable problem. Both encryption and endpoint security are required. These are not guaranteed by Skype, and they could only be guaranteed by any system, if at all, under strict regulation that would be incompatible with our professional culture, and which could not be imposed on patients. This leaves an ethical problem for 'remote analysis': what to convey to patients about the lifetime risk to confidentiality. It would be unethical to repeat misleading statements about Skype that we know to be false. We cannot adequately assure our patients about confidentiality on the basis of our ignorance about technology.

Introduction

The use of telecommunications in psychoanalytic treatment raises two central problems: how to preserve confidentiality, and whether virtual presence can adequately substitute for

[1] Paper to be presented at the 50th Congress of the International Psychoanalytical Association, Buenos Aires, 25-29 July 2017. Not to be reproduced without the author's permission.

physical presence. These problems are related because both confidentiality and presence are necessary conditions of the psychoanalytic setting, and doubts about either have both technical and ethical implications. In this paper I shall address only the problem of confidentiality.

A new historical situation

It is possible that at some point in the future one or more of the countries in which psychoanalysis is currently practised will fall under the control of an authoritarian and undemocratic regime. Such a regime would probably be prepared to intercept the private communications of citizens in order to decide whom to subject to arbitrary arrest and detention, or worse. For some countries, if this has not yet happened, it may be only a matter of time, and for some countries it would not be the first time.

Following the revelations by Edward Snowden in 2013, there are good grounds for believing that telecommunications traffic, including voice and video conversations as well as email and texts, are now being monitored on an industrial scale by various national governments, notably the USA and Britain (Greenwald, et al., 2013; The Guardian, 2013; Spiegel Staff, 2014; National Security Agency, 2012). It can be assumed that recordings of at least some of these conversations, transcriptions of their contents, or metadata derived from them are being stored for as long as possible, subject only to technical and/or budgetary constraints. Developments in techniques such as automatic speech recognition and database management, as well as growth in processing power and storage capacity, suggest that the content of conversations may now be being preserved indefinitely.

This is a new situation historically. The fact that documents and records created under one regime can be inherited by its successors and used in new ways is, of course, not new. What is new is the capacity of the state to intercept indiscriminately the communications of all or most of its citizens, to process these automatically in ways which render them both more useful as intelligence and less expensive to store, and to store the resulting data indefinitely for potential use at a later date.

Given that there is a legitimate need, in democratic states, to gather intelligence that can be used to protect national security, and to prevent or limit terrorism and other serious crimes, the motive for indiscriminate and inclusive monitoring of communications is clear. If it is not possible to know in advance which communications might be useful, the best option is to collect all of them. Unfortunately, this brings with it new dangers to civil liberties. An authoritarian regime coming into power anywhere in the world today would probably find itself in a position retrospectively to access and utilise the contents of private communications over the telephone, internet, Skype, etc., which had been accumulated in the period before it achieved power. Snowden has described this situation as the secret building of a massive surveillance machine which threatens to destroy privacy and basic freedoms (Greenwald, et al., 2013; Poitras, 2014).

Among the many social consequences of such a regime, there would obviously be serious implications for the possibility of conducting any kind of psychoanalytic consultation by

telephone or internet. At best, we may imagine, there would be a rapid retrenchment in the use of telecommunications, with reversion to purely in-the-room consultation. At worst there could be an effective abandonment of psychoanalytic practice altogether. How psychoanalysts and their patients would adapt to such a change of circumstances would doubtless be informed in part by their cultural history and experience. People who have previously lived under a dictatorship might react differently, both in their external actions and in their internal worlds, from those who have not. But it is hard to imagine any community in which the practice of 'remote analysis', if it had taken root, could simply continue as before.

Moreover, and this is the main point of this paper, mass surveillance of telecommunications has implications for our *current* psychoanalytic practice, anywhere in the world. This is because of the ways in which we share knowledge and ignorance concerning this new situation, both consciously and unconsciously, with our patients and with each other, and because of the specific way in which it connects with the requirement of confidentiality in psychoanalytic work.

The necessity of psychoanalytic confidentiality

The technical and ethical arguments for maintaining confidentiality between analyst and patient, and therefore the privacy of their conversation, have been amply explored elsewhere by others (Hayman, 1965; Bollas & Sundelson, 1995; Gabbard, 2000; Cordess, 2001; Forrester, 2003; Garvey & Layton, 2004; Stimmel, 2013).

More than twenty years ago, Bollas and Sundelson (1995) considered the effects on psychoanalytic confidentiality of changes in the law which required practitioners in the USA and elsewhere to breach confidentiality under certain circumstances. They compared the situation thus created to that in Eastern Europe before the fall of the Soviet-backed regimes. They pointed out that whereas members of other professions might be able to function adequately under such conditions, the psychoanalyst "relies upon the psychic inner freedom of his own mind in order to receive his analysand fully and properly" (pp. 98-99). Psychoanalysts and patients, they argued, need to "form that inner psychic space that is essential to the creation of psychoanalysis." (p. 99).

In other words, psychoanalysis is incompatible with external circumstances which interfere with the kind of intimacy between patient and the analyst which makes it possible for the patient to try to free-associate and for the analyst to try to listen with evenly-suspended attention. We know, of course, that these mental conditions of psychoanalysis can only ever be imperfectly realised, but a requirement of the psychoanalytic setting is that it be sufficiently free from external interference for it to be possible for both parties to make a sustained attempt at realising them.

Different external realities, similar questions

Some years before the publication of Bollas & Sundelson's book, the effects on psychoanalytic practice of extreme state violence in Argentina during the dictatorship of 1975-83 had been documented by various writers. Puget and Wender (1982) described how

analysts and patients were living in 'overlapping worlds' of uncertainties and threats created by the regime, feeling obliged to share information about their external circumstances, and thereby undermining the necessary seclusion of analytic work. Janine Puget (1989, 2002) described a 'state of threat' pervading civil society, which produced observable disturbances in the psychoanalytic situation. Silvia Amati Sas (1985, 1989, 2004) has described an 'adaptation to anything whatsoever', initially observable clinically in survivors of torture, but also as a more widespread form of passively adaptive defence against awareness of traumatic social violence. René Kaës (1987, 1989, 1994) describes a form of trans-subjective unconscious alliance that he called a 'negative pact', which creates zones of silence and a tacit, unconscious agreement not to take notice of certain facts.

In a liberal democracy in which civil liberties are protected, life is a world away from the state of threat documented by Puget, even when you know that information is daily being gathered and stored which one day could be used against you. Nevertheless, similar questions arise concerning the effects of this external social reality on inner mental life. I have argued elsewhere (Churcher, 2017) that we can understand the way in which we are currently managing anxieties arising from what we know about surveillance, in terms of Freud's concepts of denial or disavowal (*Verleugnung*) and 'splitting of the ego', and of José Bleger's thinking about the psychoanalytic setting.

Because we have come to depend so heavily on the internet, anything which casts doubt on the viability of this dependence provides an occasion for psychic defence. A widespread reaction to the Snowden revelations is disavowal, which Freud originally described as the starting point of fetishism, and which can result in perversely 'turning of a blind eye' towards reality (Steiner, 1985). Freud's description of a split in the ego, between a part which recognises a danger and a part which rejects knowledge of it (Freud, 1938, p. 275-6), aptly describes our predicament today in the face of the new 'fact of life' which is the mass surveillance of our communications. Freud was describing a child threatened with castration as a punishment for masturbation, but his description fits our attitude to the internet: unwilling to forego its compulsive pleasures and the convenience of its use in the relative peace and calm of the present, we turn a blind eye to the anticipated danger of a dystopian future.

The specificity of surveillance as a problem for psychoanalysis

Surveillance of telecommunications is not the only source of anxiety capable of generating disavowal on a social scale. Nuclear and other weapons of mass destruction, climate change, nuclear power, risk of pandemics, terrorism, instability of the global financial system, etc., all occasion deep anxieties about the future, which are felt by psychoanalysts and patients alike, and which find expression in the consulting room. (Segal, 1987; Tuckett, 2011; Weintrobe, 2013; Hoggett, 2013). What distinguishes mass surveillance from these other sources of anxiety is its potential for undermining psychoanalytic confidentiality in precisely the same way as Bollas and Sundelson argued in respect of legal limitation of professional privilege. Unlike legal restrictions, however, it cannot be fought simply by reasserting the primacy of professional ethics over legal obligations. Instead, its effects can only be avoided by

abandoning the use of telecommunications in the setting and reverting to classical, 'in-the-room' analysis, where privacy can normally be guaranteed.

In Bleger's view, Freud's 'splitting of the ego' was "a splitting between a more developed, adult part of the personality that recognizes reality and another infantile part that still adheres to a primitive organization", which is to say "a splitting between the neurotic and the psychotic part of the personality" (Bleger, 2013 [1967], 258-259). In a psychoanalysis, the psychotic part is quickly and quietly deposited in the setting, where it remains as part of the 'non-ego', hidden and unanalysed, until a disruption of some kind causes it to become manifest. The setting, Bleger argued, as the part of the psychoanalytic situation that is deliberately kept as constant as possible, functions as a depository for this primitive part of the mind that is present in all of us as a residuum of early symbiosis with the mother and with the world. Throughout life it continues, wherever and whenever possible, to establish symbiotic relations with anything that is stable, secure, unchanging, and then to treat this as something not to be questioned.

When telecommunications are made part of the setting we therefore need to be curious about the part of the mind that is deposited in the communication system itself. It is then a serious problem if, as psychoanalysts, we know little about how this very complex system actually works.

Why it is not feasible for psychoanalysts to construct secure systems for telecommunication

The IPA has circulated a '*Practice Note on the use of Skype, Telephone or Other VoIP Technologies in Analysis'.* It acknowledges that there are "issues regarding security, privacy protection and confidentiality over all forms of telecommunications", and it states that "Analysts must satisfy themselves that the technology they are using is secure and protects the patient's confidentiality" (International Psychoanalytical Association, 2016).

How can analysts do this? If we consider what would be involved in a serious attempt to establish a secure setting for remote psychoanalysis, we can get a measure of just how intractable this problem is.

Psychoanalysts who offer remote consultation currently use a variety of communication systems for doing so, but schematically we may consider any of them as having three components: a device used by the analyst, a device used by the patient, and the network which links them, with many different kinds of software running simultaneously in each component. The devices may be desktop or laptop computers, tablets, fixed or mobile telephones; the network may be the internet, the public switched telephone network (PSTN), or some other network. For simplicity I will consider the paradigm of two desktop computers linked via the internet, and both running Skype or some other form of VoIP software.

In the first place, it is necessary to ensure that communications which pass through the internet are securely encrypted during their passage, and that they can only be decrypted by the parties concerned, the analyst and the patient, and not by a third party. Whether this is

possible using resources that are readily available to most internet users is doubtful. Much of the recent debate about 'back doors' in commercially available hardware and software has involved conflict between government agencies which want to retain the possibility of access to any communication, and those who, for commercial, political, or ethical reasons, seek to preserve privacy (Abelson et al., 2015).

In the case of a commercial product such as Skype, in which the method of encryption and the source code are not open to public scrutiny, there is little ground for confidence that communications cannot be decrypted by third parties, or that a 'back door' has not been designed into the system, even if this is denied by the providers. Even in the case of open source alternatives, where the method of encryption is known and estimates of its security can be publicly evaluated, uncertainties concerning the implementations give rise to doubts among cybersecurity professionals.

Secondly, there is the problem of 'endpoint security': the need to ensure that communications are not subject to interception before they are encrypted, or after they have been decrypted. When you speak into the microphone of your computer, your voice is necessarily represented as an unencrypted data stream before being encrypted for transmission. The same is true of the data stream arriving from the person you are speaking to, after it has been decrypted in order to be converted back into audible speech. If one or both computers has been compromised, unencrypted audio data may be being copied to a third party. It follows that even if the 'end-to-end' encryption across the network is good enough, the security of the system as a whole can be vitiated by inadequate endpoint security. A chain is only as strong as its weakest link.

It is unclear whether it is possible for anyone nowadays to make a communications system that would be reliably invulnerable to interception. Perhaps in a corporate, military or governmental organisation, with strict regulation of who uses what hardware and software, it might be possible to guarantee endpoint security. Certainly most psychoanalysts do not possess the necessary technical knowledge, nor is our professional culture compatible with that kind of regulation.

Even if we could build such a system, we would be obliged to subject our patients as well as ourselves to the necessary discipline and control in using it, and it is hard to imagine how this would either be practicable or compatible with any kind of psychoanalytic setting.

An ethical problem

An ethical problem therefore confronts psychoanalysts who wish to offer consultations remotely. What should they convey to their patients, whether explicitly or implicitly, about the lifetime risks to confidentiality involved, bearing in mind that whatever they say will be heard in a context in which knowledge of the Snowden revelations is already widely diffused, and already widely disavowed. I don't have an answer to this question.

A manifestly unethical approach would be to repeat advice that we know to be false. I have previously drawn attention to misleading statements published in recent years which have

suggested that Skype is secure against eavesdropping (Churcher, 2012, 2017; see also: Lombard, 2011-2016; Spiegel Staff, 2014; National Security Agency, 2012). Unfortunately, such advice continues to be given out publicly by some analysts. For example, at the time of writing (July 2016) a page advertising low fee treatment on one of the websites of the China American Psychoanalytic Alliance (CAPA) still carries the following statement: "Treatments are conducted via Skype, which, unlike telephones and email, is totally secure." (CAPA, 2016).

There is a contradiction in our present attitude to confidentiality: we often go to great lengths to protect it in the classical setting, but as soon as technology is involved "our minds become sieves" (Russell, 2016). In a separate paper I have discussed the asymmetry between our shared tacit knowledge about the buildings we inhabit and our ignorance about the workings of the electronic devices and systems that we bring in to them (Churcher, 2017). We cannot adequately assure our patients about confidentiality on the basis of this ignorance.

References

Amati Sas, S. (1985) Mégamorts, unité de mesure ou métaphore ? *Bulletin de la Société Suisse de Psychanalyse.*18: 11-19.

Amati Sas, S. (1989) Recupérer la honte. In: Puget, J. and Kaës, R. (eds .) *Violence d'état et psychanalyse*. Paris: Dunod. Pp. 105-21.

Amati Sas, S. (2004). Traumatic Social Violence: Challenging our Unconscious Adaptation. *Int. Forum Psychoanal.*, 13: 51-59

Bleger, J. (2013 [1967]). *Symbiosis and ambiguity: a psychoanalytic study*. [(1967) Simbiosis y ambigüedad: estudio psicoanalítico]. Rogers S, Bleger L & Churcher J, translators; Churcher J, & Bleger L, editors. New Library of Psychoanalysis. London (Routledge).

Bollas, C. and Sundelson, D. (1996). *The New Informants: Betrayal of Confidentiality in Psychoanalysis and Psychotherapy*. London: Karnac Books.

CAPA (2016) http://www.capachina.org/#!programs/vstc3=treatment-program [Accessed 25 July 2016]

Churcher, J. (2012). On: Skype and privacy. *International Journal of Psychoanalysis, 93*: 1035-1037.

Churcher, J. (2017) Privacy, Telecommunications and the Psychoanalytic Setting. In: Scharff, J.S. (Ed.) *Psychoanalysis Online 3*. London: Karnac. (Paper read at the 28th Annual Conference of the EPF, Stockholm, 26th-29th March 2015; also available in EPF Bulletin, Vol. 69: 221-223).

Cordess, C. (Ed.) (2001) *Confidentiality and Mental Health*. London: Jessica Kingsley.

Forrester, J. (2003). Trust, confidentiality, and the possibility of psychoanalysis. In Levin, C., Furlong, A., & O'Neill, M. K. (Eds.). *Confidentiality: Ethical perspectives and clinical dilemmas*, pp. 19-28. Hillsdale, NJ: Analytic Press

Freud, S. (1938). Splitting of the ego in the process of defence. *Standard Edition* 23:271-278.

Gabbard, G. O. (2000). Disguise or consent. *International Journal of Psychoanalysis, 81*:1071-1086.

Garvey, P. and Layton, A., (Eds.) (2004). *Comparative Confidentiality in Psychoanalysis*. London: British Institute of International & Comparative Law (in association with the IPA).

Greenwald, G., MacAskill, E., and Poitras, L. (2013). Edward Snowden: the whistleblower behind the NSA surveillance revelations. *The Guardian*, Monday 10th June.

Guardian (2014). The NSA files. http://www.theguardian.com/us-news/the-nsa-files [Accessed 30 July 2016]

Hayman, A. (1965). Psychoanalyst subpoenaed. *The Lancet*, October 16, 1965, 785-786.

Hoggett, P. (2013). Climate change in a perverse culture. In Weintrobe, S., editor, *Engaging with Climate Change: Psychoanalytic and Interdisciplinary perspectives*, pp. 56-71. London: Routledge.

International Psychoanalytical Association (2016). Practice Note on the use of Skype, Telephone or Other VoIP Technologies in Analysis. http://www.ipa.world/IPA/en/IPA1/Procedural_Code/Practice_Notes/ON_THE_USE_OF_SKYPE__TELEPHONE__OR_OTHER_VoIP_TECHNOLOGIES_IN_ANALYSIS_.aspx [Accessed 30 July 2016]

Kaës, R. (1987) Le pacte dénégatif, éléments pour une métapsychologie des ensembles transsubjectifs. In *Figures et modalités du négatif* (Eds. A. Missenard, G. Rosolato et al). Paris: Dunod.

Kaës, R. (1987) Ruptures catastrophiques et travail de la mémoire. In: Puget, J. and Kaës, R. (eds .) *Violence d'état et psychanalyse*. Paris: Dunod.

Kaes, R. (1994). Psychic Work and Unconscious Alliances in Therapeutic Institutions. *Brit. J. Psychother*, 10:361-371

Lombard, G. (2011-2016) Psychanalyse à distance? http://inconscient.net/psychanalyse_a_distance.htm [Accessed 27 July 2016]

National Security Agency (2012). User's Guide For PRISM Skype Collection. https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASHc2b5.dir/doc.pdf [Accessed 26 July 2016]

Poitras, L. (2014). *Citizenfour*. https://citizenfourfilm.com/ [Accessed 30 July 2016]

Puget, J. (1989) État de menace et psychanalyse. In: Puget, J. and Kaës, R. (eds.) *Violence d'état et psychanalyse*. Paris: Dunod.

Puget, J. (2002). The State of Threat and Psychoanalysis. *Free Associations*, 9: 611-648

Puget, J. and Wender, L. (1982) Analista y paciente en mundos superpuestos. *Psicoanálisis*, 4 (3): 502-532.

Russell, G.I. (2016) Personal communication.

Segal, H. (1987). Silence is the real crime. *International Review of Psychoanalysis,* 14: 3-12.

Spiegel Staff (2014). Prying Eyes: Inside the NSA's War on internet security. *Spiegel Online International,* 28 December 2014. http://www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html [Accessed 26 July 2016]

Steiner, J. (1985). Turning a blind eye: The cover up for Oedipus. *International Review of Psychoanalysis,* 12: 161-172.

Stimmel, B. (2013). The conundrum of confidentiality. *Canadian Journal of Psychoanalysis,* 21: 84-106

Tuckett, D. (2011). *Minding the Markets: An Emotional Finance View of Financial Instability*. Basingstoke, UK: Palgrave Macmillan.

Weintrobe, S. (2013). Introduction. In Weintrobe, S., (Ed.), *Engaging with Climate Change: Psychoanalytic and Interdisciplinary Perspectives*. London: Routledge.