Privacy, Telecommunications and the Psychoanalytic Setting[1]

John Churcher, British Psychoanalytical Society

Abstract

What are the implications for privacy when telecommunications (telephone, Skype, etc.) are introduced into the psychoanalytic setting? In the classical setting, shared tacit knowledge about buildings enables privacy to be maintained, but this is insufficient when telecommunications are involved. We find it hard to know where to turn for expert advice, but there are conspicuous examples of bad advice, e.g. concerning Skype. From revelations by Edward Snowden in 2013, we now know that interception of telecommunications, including telephone and video conversations, is occurring on a massive scale and indiscriminately. Our reaction may be to turn a blind eye, disavowing the danger to privacy that this interception entails. As Freud showed, this is a defence against a psychical trauma, the fear of something intolerable happening in the future, and involves a splitting of the ego. José Bleger's view of the setting as a depository for the psychotic part of the personality implies that this splitting will undermine our work in a particular way. It will also tend to happen differently in countries and communities with differing social and political norms. It is unclear whether 'good enough' security of telecommunications is in principle available, or what it would cost, but even the best systems are compromised by our poor 'endpoint security'. Our only option, if we wish to continue using telecommunications as part of the psychoanalytic setting, is to try to analyse these difficulties within the setting itself. This will mean being honest with patients and ourselves about the new situation, undoing the disavowal, and proceeding on the basis of an 'acceptance' of the uncertainty.

Introduction

From the beginnings of psychoanalysis there have been experiments with modifications of the classical setting, some more successful than others, most of them controversial. Modern telecommunications, beginning with the telephone and now including videoconferencing such as Skype via the Internet, are increasingly being used to substitute for the physical co-presence of analyst and patient at the same location. This raises many questions for psychoanalytic practice, which are leading to a rapidly growing area of research and debate (see e.g. Lin, 2012; Lemma & Caparrotta, 2013; Scharff, 2013; Björklind, 2014; Werbin et al., 2014, Churcher, 2015a,b; Lemma, 2015)

One such question concerns the consequences of telecommunication for confidentiality and the maintenance of privacy, and how this affects the setting. In this paper I will not rehearse the technical and ethical arguments for maintaining confidentiality between analyst and patient, and therefore the privacy of their conversation in the consulting room, as these have been amply developed elsewhere by others (Hayman, 1965; Bollas & Sundelson, 1996; Gabbard, 2000; Cordess, 2001; Forrester, 2003; Garvey & Layton, 2004; Stimmel, 2013). Instead, I shall assume that as psychoanalysts we are agreed that confidentiality is a necessary condition of our work, and that any modification of the setting must therefore preserve its privacy if it is to be capable of supporting a psychoanalytic process. [1]

[1] This paper was read at the 28th Annual Conference of the EPF (European Psychoanalytical Federation), Stockholm, 26th-29th March 2015. It has appeared in the EPF Bulletin (Volume 69, 2015, pp. 221-223), in the Bulletin of the British Psychoanalytical Society (Volume 51,No. 5, pp. 13-22), and will be published in Scharff, J.S. (*Ed*.) (2017) *Psychoanalysis Online 3*. London: Karnac.

I want to consider the implications for privacy when telecommunications, of any kind, are introduced into the psychoanalytic setting. An adequate assessment of these implications needs to be informed both by an understanding of the technology itself and by a psychoanalytic way of thinking about how the technology and its evolving social organisation come to inhabit the setting, including the internal setting in the minds of both analyst and patient. [2]

In his discussion of the psychoanalytic setting, José Bleger argued that it functions as a depository for the psychotic part of the personality that is present in all of us as the residuum of early symbiosis with the mother and with the world. According to Bleger, the setting is also a social institution, which forms part of the personality of each individual who participates in it (Bleger, 2013 [1967]). Rosemary Davies, in her paper for a Clinical Panel at this conference, discusses the value of Bleger's ideas for her clinical work within a classical setting (Davies, 2015). Here, I am using the same ideas to help me to think about a specific problem that arises in settings which involve telecommunication.

An implication of Bleger's argument, in my view, is that we tend to establish a symbiotic relation with *any* invariants that we discover and adapt to, whether in our own bodies or in the rest of the world, and that we do so not only in the psychoanalytic setting but also in everyday life (Churcher, 2015a, b). Wherever we find something stable, secure, constant, we sooner or later 'take it for granted', and treat it as something that is not to be questioned. A primitive part of the mind spontaneously establishes a silent and hidden symbiotic relation with the invariant, using it as a depository for undifferentiated parts of ourselves that are always seeking a home. This is both a social and a physical process, as we participate in various institutions.

In a psychoanalysis that is being conducted remotely by means of telecommunications, such as the telephone or Skype, we therefore need to be curious about what may be being deposited silently in the telecommunication system itself.

Shared tacit knowledge & common sense in the classical setting

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* conditions, which are seldom made explicit because they can usually be safely assumed. These include the fact that consultations typically take place in a room within a building, which is reasonably quiet, and 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. We usually have enough tacit knowledge (Polanyi, 1966) about our immediate physical and social environment to make reliable judgments about whether a conversation is private

Tacit knowledge of this kind is to a large degree socially shared, and normally the analyst's confidence in the acoustic isolation of the consulting room will be met by a similar confidence in the patient. Indeed, it is only against such a background of shared tacit knowledge (or 'common sense'), that occasions when it is called into question, for example by a patient who repeatedly expresses anxiety about being

overheard by a third party, can be taken as indications of pathological functioning. This normative aspect of clinical thinking is unavoidable.

From a psychoanalytic perspective, of course, the idea of tacit knowledge has to be understood in the context of unconscious phantasies that are part of both normal and pathological functioning. Clinical observation repeatedly confirms that buildings, and rooms within buildings, as well as serving in dreams and waking dream-thoughts as symbols for the body, are generally experienced in unconscious phantasy as protective containers, although they may also be experienced as dangerous ones provoking claustrophobia (Meltzer, 1992). Privacy of conversation in the consulting room, although it may be experienced as dangerous, is thus generally experienced in phantasy as an aspect of protective containment, which explains why the emotional reactions of a patient to any deliberate or accidental breach of privacy can be so powerful.

Privacy can be breached in many different ways, but for the purpose of the present discussion the most relevant instance is eavesdropping. The English word ‘eavesdropping’, now frequently applied to interception of telecommunications, derives originally from an architectural term. The ‘eaves’ are a projection of a roof beyond the walls of a building, to allow rain to fall away from them, the space beneath being the ‘eavesdrop’, where someone might stand for the purpose of overhearing a conversation within. Eavesdropping has been subject to social disapproval and legal regulation for at least 400 years, although the conflicting interests of governments in wishing simultaneously to allow eavesdropping by the state while disallowing or at least regulating its use by others has led to a complex history of legislation (Stevens & Doyle, 2002; Spencer, 2009).

In the classical psychoanalytic setting, eavesdropping is in principle possible if the walls are thin, or if the arrangements for maintaining acoustic isolation are in some other way compromised, but reports of its occurrence in clinical practice are rare. If there have been times and places in the past where psychoanalysis was practiced under social and political conditions in which eavesdropping was commonplace, we wouldn’t necessarily expect it to be openly documented in our professional literature.

Vulnerability of telecommunications and the insufficiency of common sense

As soon as we introduce modern telecommunications into the setting, this background of shared knowledge about the acoustics of buildings is no longer sufficient. We are obliged to consider in addition the knowledge and beliefs of the participants concerning the technology itself.

Interception of telephone conversations by governments and individuals, both legally and illegally, has been occurring since the early 1890s, and like the telephone itself is thus even older than psychoanalysis. There is little reason to doubt that interception has been practiced on a significant scale continuously ever since then. In the 1960s, when the global telephone network was still mainly analogue rather than digital, and reliant on electromechanical switching of electrical circuits for the routing of calls, interception typically required the involvement of staff in local telephone exchanges. I can remember my father, who was a telephone engineer, advising me fifty years ago never to say on the telephone anything that I would not be prepared to write on a postcard.

Since the revelations by Edward Snowden in 2013, it has become clear that government agencies in the USA, UK and various other countries, are routinely intercepting telecommunications traffic of all kinds, including voice and video conversations as well as email and text messages, on an industrial scale and more or less indiscriminately. Publication of these revelations has led to public discussion and controversy concerning the proper balance of privacy and surveillance in democratic societies faced with dangers from terrorism and organized crime. (Greenwald, et al., 2013; The Guardian, 2013))

The diversity and sophistication of techniques now available for interception, as detailed in the documents published by Snowden, greatly exceed those employed a generation ago. For the purpose of this discussion, however, the most significant aspect is perhaps the massively increased *scale* of interception, which has been made possible by the development of global digital communications and by advances in techniques such as automatic speech recognition, and the management of large databases. Whereas interception was once necessarily selective, because of the amount human labour involved, the aim of programmes such as Prism and Tempora is now to be inclusive: to intercept and record *all* telecommunications.

Knowledge of these changes has been widely disseminated in recent months, but the way in which this knowledge informs our awareness is radically different from the way in which we know about the buildings we inhabit. Such is the division of labour in technologically advanced societies that we often rely on the skills of builders, plumbers, and electricians to fix problems in our homes and offices, just as we rely on the skills of computer scientists, electronics technicians, and software engineers to build and maintain our telephones, computers and the Internet. The difference is that while we retain our common-sense ability to judge if the roof is leaking, or if the walls are permeable to sound, we generally cannot tell whether our phone has been converted into an eavesdropping device, or our emails or Skype conversations are being intercepted. There is too much to know about the digital world, and not enough common sense to guide us through it.

Lacking sufficient knowledge ourselves, we turn to experts: a technician, a colleague who ‘knows about computers’, a younger person. But can we trust whoever fixes the computer or telephone to tell us reliably about the privacy of our communications when we use it? Who really knows, and how do we know that they know? The question is analogous to one that Hanna Segal, quoting the Roman poet Juvenal, once asked about nuclear weapons: *quis custodiet ipsos custodies*? On the wild frontiers of the Internet, who certifies the certifiers?

There are some conspicuous examples of bad advice being offered recently to the psychoanalytic profession. A recent paper on introducing psychoanalytic psychotherapy into China asserts:

“*The special feature that makes Skype uniquely suitable for psychotherapeutic treatment is the security of computer-to-computer video calls. Skype uses a proprietary encryption protocol, which makes it impossible to eavesdrop on any computer-to-computer call (Berson, 2010). With Skype computer to computer connections, there is no central server. Encrypted packets of data are exchanged between many computers so that at any given moment, there is a virtual network that is fluid and continually chaining during the same call….. This technology is so*

solidly secure that it is nearly impossible to detect even whether Skype is in use at any given time." (Fishkin and Fishkin, 2014)

These statements are misleading. The fact that Skype uses a proprietary encryption protocol that is not open to scrutiny is one of the principal reasons that many people have argued that it should *not* be regarded as secure. Packet-switching, which the authors describe as if it were a special feature of Skype, is the common basis of *all* communications across the Internet, and offers no special security from interception. Methods for detecting Skype traffic have been described in the literature for at least six years (see Bonfiglio et al., 2008), and five years ago the source code of a Trojan was published which taps Skype voice conversations (Symantec, 2009). In December last year, *Der Spiegel* published a document leaked by Snowden which shows that 'sustained' interception of Skype traffic by the NSA began in February 2011 (Spiegel Staff, 2014).

Similarly misleading statements about Skype were published three years ago in the IJP (Scharff, 2012a), resulting in editorial correspondence (Churcher, 2012; Scharff, 2012b). Meanwhile, Skype continues to be used on a considerable scale, including for online psychoanalysis and psychotherapy. Alternatives to Skype have been suggested, such as VSee, or WebEx, on grounds of their supposed greater security. As we shall see shortly, such claims are problematic.

Turning a blind eye to the risks

Having come to depend on the Internet in so many aspects of our lives, from maintaining contact with friends to the very operation of the social infrastructure (in transport, health, electrical power distribution, finance, etc.), any knowledge which puts the viability of this dependence into doubt provides an occasion for psychic defence. A widespread reaction to the Snowden revelations is similar to that which Hanna Segal described as a response to the threat of nuclear war (Segal, 1987), and which has more recently been discussed in the context of climate change (Weintrobe, 2013; Hoggett, 2013), and instability of financial markets (Tuckett, 2011). This is the defence of disavowal (*Verleugnung*), which Freud described as the starting point of fetishism, and which Steiner has discussed as the basis of a perverse attitude of 'turning of a blind eye' in the direction of reality (Steiner, 1985).

For Freud, disavowal is a defence against a psychical trauma: "*a child's ego is under the sway of a powerful instinctual demand which it is accustomed to satisfy and … it is suddenly frightened by an experience which teaches it that the continuance of this satisfaction will result in an almost intolerable real danger*". The ego responds by disavowing the reality of the situation, "*[making] itself believe there is no reason for fear, so that it may be able to retain the satisfaction*", while simultaneously recognizing the danger and converting the fear into a symptom The outcome is a "*rift in the ego which never heals but which increases as time goes on*." (Freud, 1938, p. 275-6).

This describes quite accurately our predicament today faced with new knowledge about the extent of interception of our private communications, and our uncertainty about what it might lead to. In his first public interview for the *Guardian*, later reproduced in Laura Poitras' documentary film *Citizenfour*, Snowden said: "… *I can't in good conscience allow the US government to destroy privacy, internet freedom*

and basic liberties for people around the world with this massive surveillance machine they're secretly building", which he described as "*an existential threat to democracy*." (Greenwald, MacAskill, and Poitras, 2013; Poitras, 2014).

The fact that disavowal is a defence activated by a *psychical* trauma, an experience that creates a fear of something intolerable happening in the future, is important in linking the topic of this paper to the wider theme of the conference. The concept of trauma, as Freud noted, implies an overwhelming or flooding of the mental apparatus, which normally maintains a protective barrier to prevent this occurring (Freud, 1950 [1895], 1920). The concept of a psychical trauma implies an incommensurability between the relative peace and calm of the *status quo*, and the terror of an anticipated future.

As Weintrobe (2013) and Hoggett (2013) have argued in connection with climate change, disavowal can form the basis of a perverse culture of denial. However, it is important to add that our psychoanalytic understanding of such defences cannot itself tell us anything about the external reality or unreality of what is being defended against. 'Denial' can be easily misused as a means of discrediting views with which one disagrees, by suggesting that they are pathologically determined, rather than being based on different experiences and/or different interpretations of the evidence. But the validity of beliefs about the world cannot be determined by examining either the fears that they induce or those that they enable us to evade. Because psychoanalysis cannot decide questions of fact arising outside the consulting room, our beliefs and judgments about the wider world need to be informed by other sources of information and knowledge, and psychoanalysis cannot tell us which of these to believe.

When the organisers of this conference wrote that they wished to dedicate it to "those who live, and who make us live, the too much - not enough, and who make us experience the limits of norms" (Frisch, Ylander, and Bleger, 2015), might they have had Edward Snowden in mind, among others? With any scenario of global disaster (climate change, nuclear war, nuclear power, pandemic, financial crash, or any of a dozen others), we are liable to feel paralysed by the sheer scale of the anticipated consequences, the rapidity with which they could develop, the amount of suffering that would be involved, and the insufficiency of our mental resources for facing them, or for keeping up with developments in the world which might help us to face them. Snowden's comments clearly imply a warning against an 'almost intolerable danger' that the surveillance machine might at some point fall into the hands of an undemocratic and oppressive government.

Implications of José Bleger's view of the setting

In Bleger's view, Freud's 'splitting of the ego' is "*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). The psychotic part of the personality as described by Bion, which Bleger also calls the 'agglutinated nucleus', remains ready throughout life to establish new symbiotic relationships characterised by massive projective identifications. In an analysis it is quickly and quietly deposited in the setting, where it remains hidden and unanalysed, until a disruption of some kind causes it to become manifest.

As long as the setting is not disrupted, it remains unnoticed. The agglutinated nucleus, the undifferentiated and unresolved infantile symbiotic relationship, remains hidden. Like a phantom limb that has not yet been experienced as such because the body is still intact, it silently persists in the setting as a 'phantom world', undetected but nonetheless psychically real. The setting thus functions as a tenacious and invisible 'bastion' (Baranger & Baranger 1961-62), a refuge or retreat for the psychotic part of the personality, which demands that nothing shall change. Sooner or later the analyst must therefore try to analyse the setting, and Bleger observes that this meets strong resistance because the symbiosis is something which has never before been recognised by the patient.

In describing the technical requirements for this clinical task, Bleger distinguishes between two different versions of the setting: the one that the analyst provides, and the one that the patient 'brings' to the analysis. The analyst, he writes, needs to 'accept' the setting brought by the patient because within it will be found, in summary form, all of the primitive unresolved symbiosis. At the same time, the analyst must hold firmly to his own setting in order to be able to analyse both the psychoanalytic process and the patient's setting when this has been transformed it into a process. In other words, he 'accepts' the patient's setting in order to interpret it. (Bleger, 2013 [1967], 240-241)

Psychoanalysis is difficult enough when the reality towards which the blind eye is turned is *not* itself part of the psychoanalytic setting, so that there is at least a possibility of doing analytic work on the patient's use of the setting without compromising the setting itself. Bleger notes that precisely because the setting is respected and preserved in psychoanalysis, much of this area of the mind may never be analysed.

However, when what is being disavowed is itself an aspect of the setting, the difficulty is potentially much more serious. The use of telecommunications in psychoanalysis presents us with precisely such a difficulty. If, in our work as analysts, we turn a blind eye to something that we know about the setting we are offering to our patients, how can we avoid undermining it as the only resource we have for analysing the patient's setting?

Different societies, different norms

Norms of expectation concerning the privacy of telecommunications tend to vary between different countries and communities with differing histories of relations between government and citizens. Reactions to Snowden have been markedly stronger in Germany, for example, where memories of surveillance in the DDR are painful and recent, than in Britain, where, with the notable exception of the *Guardian* newspaper, reactions have been more muted. Psychoanalysts and their patients in countries that were once part of the communist bloc may be making different assumptions about surveillance, and have different sensibilities, from those in the West. In China, it seems that government intervention in the Internet is massive and systematic. And if in the West it has hitherto been possible for psychoanalysts to feel safe in the belief that their private communications really were private, the situation should be no longer so clear (see Wright & Kreissl, 2013). Thus the existence of norms, and the variations between them in different locales, raises in a stark way the ancient problem of distinguishing between paranoia and realism.

Are 'good-enough' telecommunications for psychoanalysis possible?

Can we find a place somewhere between these extremes, and settle for what might be called 'good enough security', by analogy with Winnicott's (1953) notion of the 'good enough mother'? After all, it could be said that this is all that the classical setting can offer anyway.

Arguably, a concept of 'good enough' has already become the norm in many other uses of the Internet, e.g. for personal financial transactions. One form of encryption now widely used for email even has the name PGP, which stands for 'Pretty Good Privacy' (Zimmermann, 1995). PGP has been in use for more than 20 years, and there is no clear evidence that when properly used it has yet been broken. On the other hand, another widely trusted form of encryption used in banking, SSL ('Secure Sockets Layer'), was shown in 2012 to have multiple vulnerabilities, and has since been replaced.

Huge resources are expended on IT security: a global estimate for 2014 is $71.1 billion, and rising at about 8% yearly (PwC, 2014, p.5). Despite this expenditure, and continual technical innovation, it is not clear that anyone has yet found the security they are seeking. There is, in effect, an arms race between commercial enterprises competing in the market, between hostile nation states, and between all of these and organized crime. As in all arms races, the only certain winners are the manufacturers.

It is possible now to buy a communications system which uses the principles of quantum theory to provide 'unconditional secrecy', meaning secrecy whose guarantee is 'independent of any assumptions about the resources available to an eavesdropper' (Gobby, Yuan, & Shields, 2004). This state-of-the-art technology, known as Quantum Key Distribution (QKD) [3], is in use by some banks, military and governmental organisations, but its high price places it beyond the reach of most users, and take-up is further restricted by current limitations on bandwidth and on the distance over which it can operate. Nevertheless, we can use QKD as a kind of object lesson for psychoanalysis, in two ways.

First, the fact that QKD is already being used for videoconferencing makes the point that for some purposes none of the more widely available and cheaper forms of videoconferencing (Skype, WebEx, VSee, etc.) are seen as sufficiently secure. We might then consider whether a system that isn't secure enough for bankers or government departments can be secure enough for psychoanalysts and their patients.

Endpoint security: our weakest link

Secondly, and this is the more important point: a secure communications channel is of limited value unless the endpoints of the communication, the computers or telephones or other devices at each end, where the information is decrypted, are also themselves secure. A chain is only as strong as its weakest link, and if your personal computer, tablet or phone is infected by a Trojan which is quietly copying decrypted information to a third party, then no matter how sophisticated and secure the communications channel, it may be worthless.

In a corporate environment, or in military or governmental organisations, it may be possible to regulate who has access to what equipment, and to establish a strict regime for its use in order to prevent breaches of endpoint security. Large organisations typically define their own 'intranets' and require employees to use them. Psychoanalysts, on the other hand, tend to avoid this kind of corporate discipline. We use a diverse range of devices and operating systems, in highly idiosyncratic ways, and often with minimal attention to security. It is important to note that even systems that are advertised as offering 'end-to-end security' (e.g. VSee and MegaChat, which compete in the same market as Skype) do not address this problem. To address it seriously would require a cultural change that I am not at all sure is feasible or desirable.

In my own practice over the past 25 years I have not been completely consistent. On the one hand, I have avoided all use of Skype or other VOIP, as well as mobile telephones, for all discussion of clinical material; and I created and stored process notes of my patients' sessions in encrypted files, not on the computer I routinely use for the Internet, but on a separate, 'air-gapped' computer that has never been connected to the Internet. On the other hand, I regularly discuss clinical material by land-line telephone, with supervisees and colleagues, and I am party to others doing so when participating by telephone in scientific meetings. I used to justify this to myself by persuading myself that using a land-line was intrinsically less risky than either VoIP or a GSM cellphone, but I didn't really know that, and now Snowden's revelations about GCHQ and Tempora have undermined that belief. My own behaviour is thus consistent with a splitting of the ego as described by Freud.

Conclusion: Implications for psychoanalyses conducted or attempted by means of telecommunications

In conclusion, I feel that I may be bringing some unwelcome news: that as psychoanalysts we cannot simply continue to drift towards ever greater incorporation of telecommunications and computer technology into our clinical work, without facing radical new uncertainties about whether the work can remain private. We may tell ourselves comforting stories: about why we imagine that no-one would be interested in eavesdropping on our work; or why if they did they would learn nothing, because psychoanalysis isn't that sort of talk anyway; or why the patient would not be seriously harmed by it; or that to be concerned about any of this is paranoid thinking; or even that 'privacy is dead', and we need to get over it. In discussions with colleagues and friends I have heard each of these presented as an objection; but each could also be a way of turning a blind eye to something unwelcome and potentially frightening.

In this paper I have deliberately limited myself to just one aspect of the problems created for psychoanalysis by attempting to substitute telecommunications for physical co-presence. We are at a difficult moment in the development of the profession, because a momentum in favour of 'psychoanalysis online' has built up in recent years, but there is as yet no real consensus among us about what is possible or desirable. By focusing on privacy and confidentiality, I am deliberately drawing attention to an issue which has clear ethical implications, but I think these need also to be considered together with other consequences of the use of telecommunications. I have discussed elsewhere the problem of how to define 'presence' as a condition of the possibility of psychoanalysis (Churcher, 2000;

2015a,b). Sabbadini (2013) addresses a similar question, as does Lemma (2015) in her wide-ranging keynote paper for the forthcoming IPA Congress in Boston.

If we suppose, for the purpose of the present discussion, that psychoanalysis is *not* rendered impossible by other aspects of a setting that depends on telecommunications, how should we address the issues of privacy and confidentiality? The only clinically viable option, in my view, would be to follow José Bleger's example and to continue trying to analyse them within the setting. This would mean being honest with our patients and ourselves about the uncertainty, and turning a seeing eye instead of the blind one towards it, undoing the disavowal and proceeding on the basis of an 'acceptance' of uncertainty.

I have put 'acceptance' in quotation marks because I am not sure quite what this would mean. The patient, from the first moment of an analysis, brings his or her most infantile, primitive and unformed parts to the setting. The encounter creates an immediate dependency, and the patient's 'acceptance' of anything, including classical aspects of the setting, the contract, etc., has to be understood in this context. As Faimberg (2014) has emphasised, it is Bleger's distinction between *two* settings, the psychoanalyst's and the patient's, that makes possible a solution to an apparent paradox: that in order to have a chance of overcoming the inherent tendency towards a sterile ritualization of the psychoanalytic setting, we need to keep the setting constant.

Should we then hope that the damage to psychoanalysis which results from living under surveillance can also be overcome or mitigated, provided that the analyst's setting can contain the anxiety without splitting, an analytic process can get under way, and the patient's and our own acceptance of these unwelcome realities can be explored and developed over time? The only alternative, it seems to me, would be to avoid the use of telecommunications in clinical work, despite the economic pressures and temptations, and to proceed on the assumption that for psychoanalysis, as for some other forms of conviviality, actual physical presence is indispensable.

Notes

[1] In his beautiful and compelling book 'The Private Life: Why we remain in the dark' (2013), Josh Cohen writes: "The conception of privacy implicit in public debates around the competing rights of individual and public interest is a rather impoverished one, mired in the confusion of privacy with secrecy." He contrasts this with "another, more essential privacy, namely what I keep private even from myself – and in spite of myself." Unfortunately, we need the first kind of privacy in order to be able to explore the second.

[2] The concept of the 'internal setting' has been developed by various authors: Temperley (1984), Bridge (2013 [1997], 2013), Alizade (2002), Churcher (2005), Parsons (2007), Civitarese (2013 [2011]), Labarthe (2012), and others). Although these authors do not all think of the internal setting in precisely the same way, they all agree that it is precisely when the external setting is disrupted or under threat that the internal setting is most essential for maintaining or restoring the analytic process.

[3] The physical phenomenon of ‘quantum entanglement’ makes it possible for two parties to communicate by optic fibre in such a way that they can reliably detect any eavesdropping by a third party. This method is used to transmit securely a random key, discarding any intercepted signals, and the key is then used to encode data before sending it over an open channel.

References

Alizade, A.M. (2002). *Lo Positivo en Psicoanálisis: Implicancias Teórico-Técnicas*. Buenos Aires – Mexico: Lumen.

Baranger, M. and Baranger, W. (1961-1962). La situación analítica como campo dinámico. *Revista Uruguaya de Psicoanálisis, 4*(1): 3-54; trans. S. Rogers & J. Churcher (2008) ‘The analytic situation as a dynamic field’, *International Journal of Psychoanalysis, 89* (4): 795-826.

Björklind, C. (2014). Psychoanalysis and the new technologies. The future of the talking cure and the bodily ego in the digital era "Psychoanalysis in 2025" Pre-published Papers. http://www.epf-fep.eu/eng/article/psychoanalysis-and-the-new-technologies-the-future-of-the-talking-cure-and-the-bodily-ego-in-the-digital-era

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.

Bonfiglio, D. et al. (2008). Revealing Skype traffic: When randomness plays with You. *ACM SIGCOMM Computer Communication Review "4", Vol.37*, pp.37-48, October 2007

Bridge, M. (2013 [1997]). Why five times a week? A candidate’s perspective. *Bulletin of the British Psychoanalytical Society, 49* (7):3-9.

Bridge, M. (2013). Moving out – disruption and repair to the internal setting. *British Journal of Psychotherapy, 29* (4): 481–493.

Churcher, J. (2000). Clinical meetings, communication technology and presence. *Bulletin of the British Psychoanalytical Society, 36* (1): 26-31.

Churcher, J. (2005). Keeping the psychoanalytic setting in mind. Paper given to the Annual Conference of Lancaster Psychotherapy Clinic in collaboration with the Tavistock Clinic, at St. Martin’s College, Lancaster, 9th September 2005. https://www.academia.edu/4527520
https://www.researchgate.net/publication/277712165

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

Churcher, J. (2015). “The psychoanalytic setting,the body-schema, telecommunications, and telepresence: some implications of José Bleger’s concept of *encuadre*.” Expanded version of a paper presented at the 5th British German Colloquium, 11-13 October 2013, Møller Centre, Cambridge, UK. https://www.academia.edu/12802860 https://www.researchgate.net/publication/277712046

Churcher, J. (2016). Der psychoanalytische Rahmen, das Körperschema, Telekommunikation und Telepräsenz: Implikationen von José Blegers Konzept des *encuadre*. *Psyche: Zeitschrift für Psychoanalyse und ihre Anwendungen, 70*: 60-81.

Civitarese, G. (2013). *The Violence of Emotions: Bion and post-Bionian Psychoanalysis*. [(2011) La violenze delle emozioni: Bion e la psicoanalisi postbioniana]. Harvey, I. translator. New Library of Psychoanalysis. London: Routledge.

Cohen, J. (2013). *The Private Life: Why We Remain in the Dark*. London: VintageCordess, C. (Ed.) (2001) *Confidentiality and Mental Health*. London: Jessica Kingsley.

Davies, R. (2015). Closeness and distance within the analytic setting: whose frame is it anyway? Paper presented to a Clinical Panel at the EPF annual conference. March 2015, Stockholm. http://www.epf-fep.eu/eng/article/closeness-and-distance-within-the-analytic-setting-whose-frame-is-it-anyway

Faimberg, H. (2014). The paternal function in Winnicott: The psychoanalytical frame. *International Journal of Psychoanalysis, 95*: 629–640.

Fishkin, R. E. and Fishkin, L. P. (2014). Introducing psychoanalytic psychotherapy into China: the CAPA experience. In Scharff, D. E. and Varvin, S, editors, *Psychoanalysis in China*, pp. 205-215. London: Karnac.

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. (1950 [1895]). Project for a scientific psychology. *Standard Edition* 1: 281-391.

Freud, S. (1920). Beyond the pleasure principle. *Standard Edition* 18:1-64.

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

Frisch, S., Ylander, F. and Bleger, L. (2015). Too much – Not enough: Argument of the EPF conference in Stockholm, March 2015. *EPF Bulletin* 69: 2022.

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).

Gobby, C., Yuan, Z. L. & Shields, A. J. (2004). Unconditionally secure quantum key distribution over 50km of standard telecom fibre. *Electronics Letters, 40*: 1603-1604.

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

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.

Labarthe, C. (2012). El encuadre interno del analista: http://www.revistapsicoanalisis.com/el-encuadre-interno-del-analista/

Lemma, A. and Caparrotta, L. (Eds.) (2013). *Psychoanalysis in the Technoculture Era*. London: Routledge.

Lemma, A. (2015). Psychoanalysis in times of technoculture: Some reflections on the fate of the body in virtual space. Keynote paper presented at the IPA Congress, Boston 2015.

Lin, T. (2012). Skype analysis: problems and limitations, *Bulletin of the British Psychoanalytical Society, 48* (4): 1-10.

Meltzer, D. (1992). *The claustrum: An investigation of claustrophobic phenomena.* Perth, Scotland: The Clunie Press.

Parsons, M. (2007). Raiding the inarticulate: the internal analytic setting and listening beyond countertransference. *International Journal of Psychoanalysis, 88*: 1441-1456.

Poitras, L. (2014). Citizenfour. https://citizenfourfilm.com/

Polanyi, M. (1966): *The Tacit Dimension*. Chicago: University of Chicago Press.

PwC (2014). Managing cyber risks in an interconnected world: Key findings from The Global State of Information Security® Survey 2015. http://www.pwc.com/gx/en/consulting-services/information-security-survey/download.jhtml

Sabbadini, A. (2013). New technologies and the psychoanalytic setting. In Lemma, A. and Caparrotta, L. (Eds.) *Psychoanalysis in the Technoculture era*, pp. 23-32. London: Routledge.

Scharff, J. S. (2012a). Clinical issues in analyses over the telephone and the internet. *International Journal of Psychoanalysis, 93*: 81–95

Scharff, J. S. (2012b). On: Reply to 'Skype and Privacy'. *International Journal of Psychoanalysis, 93*:1037-1039

Scharff, J. S. (Ed.) (2013). *Psychoanalysis Online: Mental health, Teletherapy, and Training*. London: Karnac.

Scharff, J. S. (Ed.) (2015). *Psychoanalysis Online 2: Impact of Technology on Development, Training, and Therapy*. London: Karnac.

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

Spencer, J. R. (2009). Telephone tap evidence and administrative detention in the united kingdom. In Wade, M. & Maljevic, A., editors, *War on Terror? The European Stance on a New Threat, Changing Laws and Human Rights Implications*, pp. 373-400.. New York: Springer.

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

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

Stevens, G. M. and Doyle, C. (2002). *Privacy: Wiretapping and Electronic Eavesdropping*. New York: Novinka Books.

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

Symantec (2009). Trojan.Peskyspy—Listening in on your conversations. http://www.symantec.com/connect/blogs/trojanpeskyspy-listening-your-conversations

Temperley, J. (1984). Settings for psychotherapy, *British Journal of Psychotherapy, 1*:101–111.

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.

Werbin, A., Burdet, M., Giménez Noble, F., Sahovaler Litvinoff, D., Hirsch Hardy, J., and Ambort, G. (2014). Remote therapy research: A research on distance psychoanalysis sponsored by the International Psychoanalytic Association. http://www.remotetherapy.net/home.html

Winnicott, D. W. (1953). Transitional objects and transitional phenomena—a study of the first not-me possession. *International Journal of Psychoanalysis, 34*:89-97

Wright, D. and Kreissl, R. (2013) European responses to the Snowden revelations: A discussion paper. *IRISS (Increasing Resilience in Surveillance Societies) Consortium*. http://irissproject.eu/wp- content/uploads/2013/12/IRISS_European-responses-to-the-Snowden-revelations_18-Dec-2013_Final.pdf

Zimmermann, P. R. (1995). *The Official PGP User's Guide*. Cambridge, MA: MIT Press.