What the practicing psychoanalyst needs to know about the technology and confidentiality of remote working[1]

John Churcher
British Psychoanalytical Society

Introduction

First I want to thank Peter Rudnytsky and Kevin Kelly for inviting me to participate in this APsaA discussion group meeting. Secondly, I should say a word about the limitations of what I can contribute to this discussion. Before retiring from clinical work some years ago, I saw patients for mainly five-times-weekly psychoanalysis in my private practice. My only experience of remote clinical working was a small number of telephone sessions arranged to cover emergencies. I also want to reiterate that although I currently chair the Confidentiality Committee of the IPA, I am speaking today in a personal capacity, and not everything I say should be regarded as the agreed view of the Committee, or of the IPA.

A year ago, although many psychoanalysts already had some experience of working remotely, the majority were still seeing patients mostly in person, in the consulting room (or 'office', as I believe it is usually called in North America). The shift to remote working brought about by exigencies of the pandemic was sudden and massive. For many analysts, though *not* all, it appears to have become permanent. The topic of this discussion is therefore timely.

From the announcement of this session in the conference schedule, I see that Roy Huggins and I are to present information about how to protect confidential material when working remotely. For reasons that I shall try to explain, I think this is very difficult to do adequately. At the same time, I believe we have an ethical responsibility to inform ourselves as fully as possible about the nature of the problem.

[1] Presented at the 2021 National Meeting of the American Psychoanalytic Association, Discussion Group 25: 'Protecting Confidentiality In Video Analysis', 21 February 2021.

Confidentiality and the privacy of the psychoanalytic setting

When we start a psychoanalysis we invite the patient to try to follow the fundamental rule of saying whatever comes to mind, without reservation. We know that this instruction is easier to give than to follow, but even attempting to follow it presupposes certain conditions, among which are that the conversation is private and kept confidential.

As well as being an ethical requirement, the professional undertaking of confidentiality that we make to a patient, whether we make it explicitly or implicitly, is part of the psychoanalytic setting. It is one among many conditions which differentiate a psychoanalysis from the rest of the patient's (or the analyst's) life, and it depends for its credibility on other mundane aspects of the setting, in particular the provision of a secluded physical space.

Tacit knowledge in the classical setting

When a patient came to my consulting room, I was in a position to provide an assurance that our conversation would be private. In fact the question was rarely asked, so that the assurance usually remained implicit, but that implicit assurance of privacy was essential.

In theory it was always possible that, without my knowing it, either I or my patient was under surveillance for some reason, and that the room was bugged. If I had been worried about this possibility, in theory I could have taken elaborate precautions against it, such as having the room electronically swept for bugs. But I knew enough about the physical setting that I was working in - its history, who had access, where the neighbours were, the acoustic insulation of its walls, etc. - to be confident that only a sophisticated eavesdropper with considerable resources and making a targeted attack would have been able to eavesdrop while remaining undetected.

Some of this knowledge was explicit, in the sense that I would have been able to explain it if asked, but much of it was tacit. Michael Polanyi[2] defined tacit knowledge as knowledge that cannot put into words. Roy Huggins, my fellow presenter in this discussion, refers to an intuitive or

[2] Polanyi, M. (1967). *The Tacit Dimension*. London: Routledge & Kegan Paul

'spidey' sense, which enables us to know whether or not our conversation is private. I don't know to what extent we should think of this faculty as conscious or unconscious, but it is rooted in everyday experience of the physical world, even if it also draws on elementary knowledge of physics acquired at school, as well as being the content of unconscious phantasy. Everyday experience teaches us the acoustic and optical properties of buildings, walls, doors, windows, curtains, etc, so that we generally know reliably when we are audible or inaudible, visible or invisible, to others.

Ignorance in the remote setting & dangers to privacy

As soon as we use a telephone, or make a video call, we are in a totally different world. An immensely complex technology of telecommunications and digital signal processing creates an illusion of the presence of the other person, who in reality may be hundreds or thousands of miles away.

Most psychoanalysts have very little understanding of the technology which makes this possible. They may have a vague notion that speech sounds are somehow transmuted into electrical signals by a microphone, that these signals are somehow transmitted from one place to another, and converted back into sound by an earpiece or loudspeaker. Most are unaware that during their journey these signals are digitised, multiply encoded, divided into short sequences (called 'packets'), each of which finds its own path across the internet by a series of jumps via many different computers (called 'servers') located in different parts of the globe, to be reassembled at their destination in the correct sequence, and decoded, all in a few thousandths of a second. And most would say: "But I don't *need* to know that stuff! I just know that it works, most of the time, and that I can use it to communicate with my patient, as I do with with colleagues, friends, and family members."

In a perfect world this might be true. In the world we currently live in, unfortunately, there are numerous dangers to privacy that the practising analyst needs to be aware of when considering how to maintain confidentiality for his or her patients.

I know that many colleagues find it difficult to imagine *why* anyone would want to exploit a breach in the privacy of their communications with a patient. So I will briefly indicate some possible motives, and I will group these under three main headings:

1. Personal

There is a rapidly growing market for software that can be covertly installed on the phone of a spouse or intimate partner to spy on them. Known as 'stalkerware', or sometimes as 'spouseware', such applications can monitor a target's conversations, read their documents, track their movements, etc. Large increases in the use of stalkerware for domestic abuse since the start of the pandemic have been reported by more than one agency, and by the Coalition Against Stalkerware[3], an alliance of non-profit organisations and cybersecurity experts formed in 2019.

2. Financial.

Theft of private data affords many opportunities for criminal financial gain, whether by selling it to interested parties or by blackmail and extortion. A common example of 'ransomware' is when someone receives a message informing them that their files have been encrypted, or their computer or phone is unusable, and demanding a ransom be paid to have them unencrypted and normal usage restored. Increasingly, ransomware is aimed at corporations, which generally are capable of paying larger sums than most individuals.

In September last year in Finland, a nationwide psychotherapy service with about 40,000 patients had its central server taken over by ransomware.[4] The hackers initially demanded a ransom equivalent to half a million US dollars from the owners, payable in BitCoin. When this was refused, they started contacting patients individually and asking for ransom payments of about $240 each, rising to $600 if not paid within 24 hours, in return for not publishing their personal records. Several hundred patients were contacted in this way, including a member of the Finnish parliament. The Finnish government held an emergency session

[3] https://stopstalkerware.org/

[4] https://apnews.com/article/psychotherapy-cabinets-finland-6b27c895df0abd532a4fb000c9d5d517

to address the situation. As far as I know, the perpetrators have not yet been caught by law enforcement. Although in this case the attack was against psychotherapy records made by practitioners, rather than against actual sessions, a similar financial motive would exist for attacking sessions if their content were accessible.

3. Political

There is obviously a legitimate need for government agencies to gather intelligence that can be used to protect national security and prevent or limit terrorism and other serious crimes. Where individuals are identified as suspects or as persons of interest by one of these agencies, they can be monitored selectively. However, since it is not always possible to know in advance whom to monitor, the safest option is to monitor everyone. Thus the motive for mass surveillance of communications is clear, and since the revelations by Edward Snowden in 2013 it has been evident that telecommunications traffic, including voice and video conversations as well as email and texts, are indiscriminately monitored on a massive scale by various national governments, notably the USA and Britain.[5] 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 (ASR) and database management, as well as growth in processing power and storage capacity, suggest that the content of conversations that has been gathered indiscriminately may now be being preserved indefinitely.

For analysts or patients who currently live under an authoritarian regime, this is already a problem. For those living in a society where there is legal protection of privacy and where citizens are not subject to arbitrary actions by the state, there may appear to be no problem. One sometimes hears it said: "Since I am not doing anything wrong, I have nothing to fear." Unfortunately, doing nothing wrong is no protection against tomorrow if there is a change of political regime. Less than two months ago it seemed possible that democratic institutions in the USA would be overthrown by an insurrection. If the endeavor had succeeded,

[5] https://www.aclu.org/nsa-documents-search https://www.cjfe.org/snowden

it is not unreasonable to assume that data already gathered and stored by the NSA would have been inherited by a new regime. Any data already derived from online communications between psychoanalysts and their patients could then have been used to discriminate actively against some of them.

Can anything be done to protect online privacy?

In considering what can be done to protect against the dangers that arise from these various motives, it is helpful to distinguish between *endpoint security* and *security of communications between endpoints*. The endpoints of a conversation can be roughly defined as the personal devices (personal computers, tablets, or mobile phones) plus their immediate physical environments, as distinct from the telecommunications networks which carry signals between them.

Unlike in a modern corporate environment, where the devices that staff may use are regulated by a centralised corporate IT service, psychoanalysts and their patients are diverse and unregulated in their choices of hardware and software. Even if we could impose common standards on ourselves, it is hard to imagine doing the same for our patients, who bring to the analytic encounter whatever devices they have, with whatever software is installed on them, and which they will use in whatever domestic settings are available to them. In many cases these devices will be poorly protected. Someone who is the target of systematic abuse within a family, for example, may be unaware that stalkerware has been installed on their phone, or they may be aware but unable to prevent it.

In the case of mass surveillance, the primary vulnerability is in communication between endpoints, rather than the endpoints themselves. The disclosures made by Snowden showed that bulk monitoring of telecommunications happens at convenient points in the physical insfrastructure of the internet through which most global traffic has to pass. The volume of this traffic is so large that it can only be stored in a raw form for a limited period of time, even by the NSA (in 2013 it was just a few days). However, preliminary pre-processing, e.g. using ASR, can reduce this volume by several orders of magnitude,

allowing the resulting text to be stored indefinitely, and rendering it also readily searchable for particular words or names.

Now, a significant obstacle to such surveillance is created if communication can be conducted with *end-to-end encryption*. 'End-to-end' means that only at the endpoints is the data unencrypted; everywhere in between the data is encrypted, so that if intercepted by someone who does not have the key, it appears as unintelligible noise. And while there is some doubt about whether any encryption method is *absolutely* unbreakable, there is widespread confidence among security professionals that the current *de facto* standard method, called AES (Advanced Encryption Standard), when properly used is secure against all currently known methods of attack. AES now underpins much of the world's confidential communications, as well as being accepted by the US government for use with classified information.

The main reason why encryption is an obstacle to mass surveillance is economic: it transforms the problem for an attacker from one that is solvable at an affordable cost into one that consumes huge resources with no guarantee of success. Permanent bulk storage of raw encrypted data is expensive, and even if stored there is no guarantee that in the foreseeable future it could be decrypted.

A psychoanalyst and a patient who converse over an end-to-end encrypted channel are therefore more likely to lose their privacy if one or both of their endpoints is compromised. Indiscriminate surveillance of endpoints does occur, but its scope is more limited than the mass surveillance of communications between them. For example, so called IMSI-catchers[6] can be used by law enforcement to monitor all mobile phones in a particular locality[7]. Otherwise, a targeted attack of some kind would be necessary, and except for stalkerware that is deployed by someone who knows the target personally, such attacks are resource-intensive and can only be made selectively, although when successful they can be highly effective. Software developed by the Israeli company NSO Group, for example, which they claim is sold only to governments,

[6] 'International Mobile Subscriber Identity catcher'

[7] https://privacyinternational.org/sites/default/files/2020-06/IMSI%20catchers%20legal%20analysis.pdf

has been used against journalists and activists, including members of Amnesty International.[8]

Risk and uncertainty

In advice that was published by the IPA Confidentiality Committee in April last year we mentioned the desirability of end-to-end encryption. We also referred to simple steps that can be taken to reduce the risk of a breach of confidentiality, such as the use of strong passwords, and we compared these to simple hygiene measures during the pandemic such as hand-washing, which reduce the risk of infection but cannot reduce it to zero.

Note that this way of thinking relies on the idea that risk is a quantity that can be measured, or at least estimated. This seems to make sense for many situations. If you use a strong password you are statistically less likely to be hacked than if you use '1234' or 'password', just as if you use a heavy-duty lock on your front door you are less likely to be burgled, or if you wash your hands and wear a mask regularly you are less likely catch or transmit the virus.

But how do we measure or estimate, even in principle, the probablity of the next pandemic; or of a successful *coup d'etat* in the United States; or of a particular patient becoming, for reasons quite unknown to us, a target for someone who has the capability and motivation to breach the privacy of their phone or computer? This is the territory of *uncertainty*, as distinct from risk, or what Mervyn King and John Kay have recently termed *'radical uncertainty'*[9]. Risk is quantifable; radical uncertainty is not. When we imagine that it is, we are telling ourselves comfortable stories.

We live every day with a combination of risks and uncertainties, both in the office and in the rest of our lives. A natural disaster, such as an earthquake, can occur equally during a psychoanalytic session or during breakfast. But as far as breaches of privacy are concerned, when the patient comes to the office we already know, tacitly, what we need to

[8] https://citizenlab.ca/2020/12/the-great-ipwn-journalists-hacked-with-suspected-nso-group-imessage-zero-click-exploit/

[9] Kay, M. and King, M. (2020) *Radical Uncertainty: Decision-making for an unknowable future*. New York: W. W. Norton & Co.

know in order to judge whether privacy is sufficiently assured for us to make the promise of confidentiality that psychoanalysis requires. Our capacity to make this judgement is not undermined or invalidated by any of the normal, background uncertainty that exists in our daily lives, because we know enough about our immediate surroundings.

By contrast, in the world of modern telecommunications we simply do not have comparable tacit knowledge about the total environment, which is almost entirely beyond our reach and effectively unlimited in space and time. Words uttered in the office are ephemeral; they physically die in the air withiin a fraction of a second, even though they may reverberate privately in the minds of analyst and patient for many years. Words uttered in a telephone or video session, on the other hand, can be recorded and preserved in digital form in multiple locations, for an indefinite period.

I have already argued that this difference between the two settings is not abolished by the theoretical possibility of sophisticated and targeted local surveillance in the office. However, we do have to consider as a transitional case the situation where a patient brings a phone to the session. The personal habits of patients vary in this regard, but psychoanalysts need to be aware that any such device imported into the setting potentially converts it to a remote analysis as far as cybersecurity is concerned. So it might be necessary to ask a patient not to bring their phone to the session, or else to ensure that it is powered off.

What are the options?

The question we are addressing in this discussion appears to be a practical one, like asking what we need to know about a motor car in order to drive safely. I think this appearance is deceptive. I want to argue instead that the more we find out about the technology, the more we become aware of the extent of our ignorance, and the clearer it becomes that we cannot offer confidentiality with the same assurance as we do in the office. Paradoxically, this is also the reason why I think psychoanalysts should find out as much as they can about the technology. We need to be more aware of how much we don't know, and of how much we cannot know, and the only way to do this is to dive as

deeply as we can into the nerdish waters of the technology, instead of leaving it to others.

Educational resources for doing this are readily available on the web, at a range of levels from elementary to advanced. One good example is the Surveillance Self Defence page of the *Electronic Frontier Foundation*, a leading non-profit organisation[10], which the IPA Committee cited in its advice to members last year[11]. A resource that is oriented specifically towards mental health professionals is Roy Huggins's *Person Centred Tech* website[12]. This offers a clear grounding in technical concepts and is particularly valuable for its thorough explanations of HIPAA[13], whose regulatory framework practitioners in the USA are obliged to work within. I am anticipating that Roy's presentation, which will follow shortly, will be a tad less pessimistic than mine, so we shall not lack issues to discuss.

I want to close by considering briefly what ethical options are open to a psychoanalyst who works remotely.

One approach would be to adopt the precautionary principle of assuming that every patient is potentially as vulnerable as one whose privacy is the target of a determined attack by a capable opponent. This would entail taking elaborate precautions, requiring elaborate cooperation by each patient, and it would probably not be feasible with all patients. Even for those patients with whom it did seem feasible, you probably would not feel confident of success in preventing a breach.

An alternative approach would be to assess each patient's circumstances individually, to try to weigh up the specific risks they are each subject to, and to balance these against the benefits of offering treatment, or of continuing one that is already begun. If you happen to have a patient who you believe is particularly at risk you might have to take elaborate precautions in their case. Note that this approach involves ignoring the distinction made earlier between risk and

10 https://ssd.eff.org/en https://www.eff.org/

11 https://www.ipa.world/IPA/en/News/remote_confidentiality.aspx

12 https://personcenteredtech.com/

13 Health Insurance Portability and Accountability Act https://www.hhs.gov/hipaa/index.html

uncertainty. It treats everything as risk, and therefore as quantitative; this is implied by the idea of 'balancing' risks and benefits.

Now, I am well aware that most psychoanalysts currently working remotely do not enjoy the luxury of being able to consider options in this way before deciding on what approach to take. Analyses were already under way when the pandemic arrived, and both patients and analysts had to learn suddenly how to work remotely with whatever resources were to hand, and then to carry on doing so, day after day.

Under the mental and emotional pressures created by this situation, and given our almost total dependence now on telecommunications in every aspect of our lives, it would not be surprising if analysts and patients alike were to have recourse to the psychic defence of denial as a way of coping. I mentioned earlier that Roy Huggins refers to a 'spidey sense' that we have concerning the in-person setting in the office. This is an allusion to the sixth sense that warned Spiderman of imminent danger, thereby enabling him to take adaptive action in good time. In considering the remote setting, I am reminded of a different invention of science-fiction: the 'peril-sensitive sunglasses' that Douglas Adams describes in *The Restaurant The End Of The Universe*. These were "specially designed to help people develop a relaxed attitude to danger. At the first hint of trouble they turn totally black and thus prevent you from seeing anything that might alarm you."[14] This is a beautiful concretisation of a reaction that I encounter repeatedly when trying to interest colleagues in this topic!

Perhaps preferable in the long run to wearing special sunglasses would be the approach which was suggested as an option by the IPA Committee in its published advice last year: namely, to discuss the situation frankly with the patient, acknowledging openly both the impossibility of guaranteeing confidentiality and the limits to our understanding of the technology. Such a conversation might well put into question the feasibility of the patient's continuing to try to follow the fundamental rule, and thereby raise the question: what kind of work are we now doing? This does not mean, however, that necessarily it would undermine the therapeutic value of the work in helping to restore or

[14] Adams, D. (1980) *The Restaurant At The End Of The Universe* London: Pan Books. p. 28.

maintain a patient's mental health. Nor does it necessarily mean that the work cannot be psychoanalytic in character.

Obviously this touches on the contentious and much wider debate about remote analysis, in which confidentiality is only one among many aspects of a radically altered setting that need to be better understood. That debate still has a long way to go, even though it is clear from numerous individual reports during the past year that some analysts who never expected it have been surprised to find that with some patients an alive psychoanalytic process can arise during remote work. I think we need to understand how the question of confidentiality is, or is not, being addressed in that work.