CHATHAM HOUSE

Chatham House, 10 St James's Square, London SW1Y 4LE
T: +44 (0)20 7957 5700 E: contact@chathamhouse.org
F: +44 (0)20 7957 5710 www.chathamhouse.org
Charity Registration Number: 208223

Transcript Q&A

Surveillance in an Information Society: Who Watches the Watchers?

Professor Sir David Omand GCB

Visiting Professor, King's College London; Security and Intelligence Coordinator, Cabinet Office, UK (2002-05)

Duncan Campbell

Investigative Journalist

Geoffrey Robertson QC

Founder and Head, Doughty Street Chambers

Chair: Dr Patricia Lewis

Research Director, International Security, Chatham House

17 July 2013

Question 1:

A question largely for David: I wonder if you'd like to say something about the quality of the oversight that is actually available here in the UK at the moment. We've got a couple of judges, two commissioners, Duncan said that the performance of one of them before the joint committee on the Communications Data Bill was pretty awful and I think I agree. But they've both got tiny little staff, and if we look at the ISC you've got nine members of parliament, only two of them seem to me have had, looking at their background, any sort of previous experience of dealing in detail with the intelligence agencies and they don't seem to have any expert support, and in particular expert support in relation to the use of computers. A particular problem is that as more and more data is created, more and more data is collected, there is a greater capacity to sort it out. The pattern gets, everything gets changed, and my question is: do we think that the oversight members, the people who are directly involved in, actually have the capacity to ask the right questions?

Question 2:

My question regards the minimum force on legality and the use of it as conventional warfare and unconventional warfare… [unclear]

Patricia Lewis:

Okay, can I just say that this a meeting about the surveillance society, so could you talk about that issue please. Sorry but we don't have enough time to go into too many other issues tonight.

Question 2:

Yes, thank you very much. So what I'm saying is he actually used this information to further his aims; do you think that conventional routes like that… [unclear] …to stop or deter further movement of such individuals?

Question 3:

At no point has there been a denial of the essential capabilities that GCHQ and the NSA now possess to take all of the data that is − as you pointed out,

it may not be seen by a human, but it can be collected. I doubt that I've done anything that would merit my being caught up in these keyword searches, but my question is: politicians, I know from experience, are a pretty malleable bunch; they change. Why should we have − the argument seems to be essentially that we should trust politicians, trust the law, trust the deep security state. I guess my question is: why?

Question 4:

Some of what I've been hearing sounds slightly alarmist and a little bit like a sci-fi movie. I wondered if anyone on the panel could comment on where you believe that we might be say even in 20 years. I mean think back to the 1990s, clearly things were so much less developed and things are moving very quickly, but where do you think we will be in either 20 or even 50 years' time?

Question 5:

Geoffrey, I wonder if you see any likelihood at all in the medium term of international law addressing the current completely lawless state of foreign intelligence gathering, and particularly the fact that the US that has all these internet companies headquartered there seemingly has no interest in the privacy of non-Americans.

Question 6:

I take great comfort in Mrs Merkel and Commissioner Reding's disquiet about the goings on, and I'm really happy to see that Geoffrey Robertson has picked up on the history of the Gestapo. The point that worries me is where we'd be in three or four years' time when we have President Palin in the US and perhaps some of the red-blooded Eurosceptic Christian Zionists that we have hoping to be in government. What's to prevent them getting carried away and sending people I disagree with round to fill me in?

Question 7:

I would like to ask Geoffrey Robertson at what stage does he think it would be acceptable in a democratic society, or what he calls a civil society, for judges who are not elected to make rules which he thinks are more importantly made

by judges than by elected people, whether they be politicians or others? Is he suggesting perhaps judges should now be elected to make it a proper decision?

Question 8:

My question is: before these Snowdon revelations, the prime target of the criticism of cyber spying is China, mainly from United States politicians and the mainstream media in the English world. So I really want to hear some comment from the panellists, what do you think the difference between the Chinese being the culprit and this Snowdon revelation? Is there any difference − so is that the political implications you mentioned of Snowdon's revelation?

Question 9:

My question pertains really to all three of the panellists who may wish to comment. Straying away for a moment from the applicability towards crime or towards terrorism, I mean there's also a less publicized but no less important implication of these sorts of programmes, which is the fact that they are used in the proper enforcement in pursuit of national security interests and against national security problems. That is to say not only in the UK and the US, but every country of any strategic relevance has prioritized this, that is to say cyber security, intelligence, surveillance, counterintelligence, at the very top of their strategic issues, and towards which they're pursuing it with more funding, manpower, innovation and aggression than just about any security issue we've seen since the rise of, well, international terrorism. To what extent do these programmes have bearing on cyber security, surveillance, intelligence, counterintelligence, as an international security and a national security problem? What does that have to do with the human rights debate?

Question 10:

Does the panel agree that with the tools now available to the security services, man's fallible temptation to delve will nullify in practice any rules which are created to regulate them, and that the inquisitor will always be ahead of the legislator?

Question 11:

My question really has two parts. The first, if you like, the first term is metadata and the second is corporate power, and they're mainly aimed to David and to Duncan. One thing that I've learned since the Snowdon revelations is the importance of metadata. That's to say, as I understand it, not the collection of content but the collection of a complete pattern of people's movements from their phone records mashed and integrated to all of their internet communications, and the holding of that by the security services, by NSA and by GCHQ. Now is that taking place? Can that be held beyond the holding of content, which is illegal? So GCHQ we're told is dispersing of the content that it's collected, but is it keeping and integrating the metadata? And I suppose the question to Geoffrey is: how does metadata affect the question of human rights?

And on the question of corporate power, I take the point that was put very forcefully by Sir David that we have to be very careful who has access to this information, how it is used, but isn't it the case that there's a growing integration of corporate gathering of information? Snowdon did not work for the American state; he worked for a private company. And how can these vast databases be secured from penetration by the large corporations?

Patricia Lewis:

Thank you. That's actually our last question, because the other speaker said no. So we have five minutes, so let's say 10, so it means pick and choose your questions. I'm really sorry that not everyone had the chance to ask questions, but please, I'm going to go in reverse order. Geoffrey, your starter for 10.

Geoffrey Robertson:

Right, I'll answer the questions about judges versus politicians this way. Once upon a time, the director of a company in Coventry accused of a charge that would have sent him to prison for seven years came to me and said it was breaching lying on your export−import form, sending machine tools to make weapons to Saddam Hussein. And the evidence was this high and it was overwhelming. And I said to him: how can you plead not guilty? This shows you're obviously guilty. He said well, a cabinet minister told me what to put down, the lies on the form, and I reported back to MI6. I said if this is true there will be documents in various departments of state, and you'll be

acquitted. Do you think those departments of state or the politicians who ran those departments of state were prepared to reveal that truth? No. They wanted this man to go to prison for seven years to avoid the fact that the Thatcher government had sold arms to Saddam Hussein. Mr Rifkind was one of those who signed a Public Interest Immunity Certificate to supress that. Mr Rifkind is now the chair of the body that has cleared GCHQ today.

That is what I think of politicians. They, Mr Rifkind and his ilk, are those who have general warrants put in front of them, they fear that if something goes wrong down the track they'll be blamed, of course they sign those certificates in a matter of minutes, maybe an hour or two.

A judge at least is independent of politics. A judge will spend hours, perhaps a day, perhaps a week, looking at the evidence. Judges are trained to look for evidence. That seems to me to be a reassurance that other countries − Canada, Australia − have that we don't. And so that is my response I think to the question particularly here.

Should we elect judges? Of course we shouldn't. Judges are trained, they're independent. They've shown − particularly in this country, unlike Russia where 99 per cent of them, 99.6 in Georgia, 99.8 in Ukraine, find against the defendant and in favour of the state − that they are independent and they. And I suspect only judges and at the end of the day newspapers, in cases of public interest leaks, can be really trusted and provide a reassurance that privacy is not being violated.

International law, the second point I'll take: yes, international law is weak. Ironically the country that suggested last year that we have an international convention on data collection was none other than the United States. The White House and its [report] 'Consumer Data Privacy in a Networked World' suggested an international convention. That is something to work for, but the last international convention on the Law of the Sea I think took 19 years.

So you ask about what's happening in 20, 50 years' time? We may have an international convention on this. Whether America will abide by it is a different matter. America tends to think that international law is all very well for countries other than America. Advising Snowdon, for example, on where he could go was very interesting, because you had a commercial flight to Cuba which at the last minute, and probably very wisely, he didn't take, because of concerns that American planes would force him down. That is contrary to international law, but after the *Achille Lauro* incident − you may remember in international airspace Americans forced down the Egyptian civil airliner on which the PLO hijackers had been given leave by the Egyptian government to

go, and there were ways found around international law. So it's not even clear that international law would protect a plane in international airspace.

Finally, I think I was asked about the European Convention, how this factors in to the human rights debate. It factors in in two ways. Firstly as far as the position of leakers or whistle-blowers − it seems some people think there's a distinction − the European Convention provides a protection. I mean someone as worthless as Abu Qatada gets that protection. Someone like Snowdon would get it. First of all, under Article 3, the behaviour, brutal behaviour, towards Bradley Manning would be used to show what happens to people under the Espionage Act. His right under Article 10 to bring matters of public interest out into the open. I think that if he got to Germany he could stay there, giving evidence to German committees and being protected. I would half suspect, I would predict, that the European Court of Human Rights would prevent his spending the rest of his life in an American Supermax for revealing information that *has* been of enormous public importance − as president Obama has conceded, starting a debate.

The other issue of course is Article 8, the right to privacy − where do you draw the line? And there the question must be one of protecting people's personal information, unless there is an overriding national security interest. And it's about time that we started defining national security.

Patricia Lewis:

Geoffrey, I think the issue on Sierra Leone and the information used − if you could be very brief.

Geoffrey Robertson:

Well Charles Taylor of course was indicted by my court back some years ago in Sierra Leone, and he was not in Sierra Leone but he was certainly using information that he had privately as part of, because he was elevated to all sorts of African committees, and he used that information, it was alleged − and he was convicted of using it − to help him supply forces who were committing crimes against humanity. And he knew from that information that crimes against humanity were being perpetrated. And he was convicted, interestingly enough, because he had access to that secret information and therefore knew very well what he was doing, and was complicit in crimes against humanity. So in that situation − and Charles Taylor, of course everyone was against him − but that shows that you can in fact be convicted.

Unless we have that kind of a genuine fear by those operating the secret system that if they misuse information they will be, there is a realistic prospect that they will be prosecuted, there seems to be no satisfactory protection.

Duncan Campbell:

Taking first the point about offensive cyber operations − it's just one of the fascinating Snowdon revelations. What is crystal clear now is that what has been alleged against the Chinese, and with great accuracy I believe, has been also true of the National Security Agency's targeted access operations and GCHQ's counterparts. It's not the primary human rights issue, but what has emerged in the nuances of the documents is how once staid institutions are now the province of hackers as well as snoopers. And that kind of untrammelled mischief-making seems to permeate some of the sideline comments in a most disturbing way.

But the much more disturbing background was unearthed at the time when the Watergate investigating committees first realized that NSA and GCHQ, although its name was kept out of the picture, was already inside all of the cables and inside all of the communications. The chairman, Senator Frank Church, said the power is there to make tyranny total. Now you may think that we ought to be abated by Malcolm Rikind's remarks, but as I said, he didn't even look inside Tempora before assuring us about Prism. And in the wake of what happened with Watergate, at the same time Edgar Hoover ran the FBI, he had a little black book of political information which he used to wield influence.

Now let's fast forward to just before the revelations. The CIA director, Petraeus, was brought down by the FBI based on the detailed unearthing and mapping of yes, the metadata, the communications data records of who called whom from where and when that enabled them to chart the path of the relationship with his mistress, Paula Broadwell, to his humiliation and run him out of office. I don't say that as to the purpose of it, but the capability was there and it came from Prism which is administered by the FBI.

And yes, you can jump forward to the horrors of a President Palin. We live in a much better time than was administered by the Stasi, but we have lost the memories of fear that are so fresh in Germany and which drove us in Britain to be the architects of the Convention on Human Rights that is now so divided. Heaven forefend that we should have to go through these experiences again, to learn why it matters, but we are looking at a new

generation of snoopers and hackers who have forgotten, and their masters have allowed them, mistresses have allowed them, to forget that it matters.

I noticed, finally, David bridled a little bit on a couple of remarks, and I bridled on one of them when he asserted damage. I'm going to suggest, mischievously perhaps, that there was only proportionate damage to be had from the Snowdon revelations. Certainly he picked out some specific European Union targeting by NSA that cannot have been an immediate end to those operations, but that kind of spying on allies is − although it goes on − is improper and it bloody well ought to be stopped. My own trial in the ABC case resulted in the Foreign Office advisers noting, and it was Geoffrey's point, that all of this was in breach of the Vienna Conventions. It was noted that GCHQ had not been playing by the laws. Well the same goes for NSA. Tough. You weren't playing by the rules, you were breaking the conventions, you may think it was all great fun − to use the language of the briefing for GCHQ's people in NSA − but it wasn't part of the core mission to keep the country safe from terrorists or serious criminals, was it? Spying with Europeans with whom you are negotiating a trade pact? I don't think so.

So in the future, yeah, GCHQ's still going to be there and there's probably going to be a lot more Edward Snowdons and that's going to be interesting and instructive. What it should tell us is that the wrap should come off. We can have more trust, even rebuild some trust, if you get these programmes out in the open. We're not talking about the target lists, but we are talking about these ministerial certificates, themselves top secret, classified strap one – no one must know! And yet they say only the most banal things except for the few details. The compliance regimes have to be huge and distinct and expert and informed. Yes, the interception of communications commissioner's performance was a huge embarrassment. These things can be done, they are achievable. They are part of the price of liberty, which is that we must watch in turn what the watchers do. Eternal vigilance is the call.

Patricia Lewis:

Thank you, Duncan. David, have you got enough time to address anything?

David Omand:

Well just let me address a few points. First, I think we agree on the panel that it is necessary for the protection of society to be able to access the communications of these wrongdoers. Duncan and I certainly believe that,

and I think I almost heard Geoffrey admit that there could be circumstances in which yes, you really ought to be able to do that. So the question we're addressing is not about that, it's the questions Duncan was addressing about what are the limitations on this. My fear would be in 20 years' time, if Geoffrey had his way, actually the internet would be pretty much a free space for terrorists and criminals, because it would seriously inhibit the development of the capabilities necessary to be able to find their communications. It's the needle in the haystack problem. The haystacks get bigger and bigger exponentially, the number of needles we need to find doesn't. It gets harder and harder. Duncan's actually written some very interesting things about how actually there are rather much smarter ways perhaps to address some of these things.

But the second point − and I'm picking up here something that both came from the floor and from Duncan, which is the fact that in the past, all of this was frightfully secret. When I joined GCHQ from Cambridge, I wasn't even allowed to tell my family where I was going to work. Now that world is gone forever. Over the last 50 years we have seen a complete transformation. The degree of openness may not quite reach the standard that Duncan is looking for, and I think nor the standard I would necessarily look for, but compared to where it was. So the Capenhurst tower that Duncan waxed on about came from an era before legislation, before the ECHR Malone case and so on, which actually −

Duncan Campbell:

You're actually wrong about that.

David Omand:

No, no, but the point is that you said that all that was illegal. Well at the time there was no legal basis − it doesn't make it illegal but there was no legal basis for it.

Duncan Campbell:

Capenhurst was 1990. Well past, sorry.

David Omand:

1994 was the Intelligence Services Act. But the point is that over the last 50 years we've seen this increased transparency, let's call it that. And I think the serious debate is about where now the boundary is with secrets and methods which, if exposed, would then erode the very capability, the panel agrees, we actually need to have for the protection of society. And that's a genuine debate we should have.

Unlike some home secretaries, indeed or Geoffrey, I don't believe in knocking the judges in quite that way. I remember the senior commissioner coming to inspect me when I was running GCHQ and it was a pretty thorough process, but a very small team and they could only look at a very small amount, and that's why I was in my remarks saying that's something we ought to look at. Nor as a long-term bureaucrat do I believe in knocking elected politicians in quite the way that we seem to be saying, that we've now abandoned trust in the democratic process. We've abandoned trust in our elected politicians, secretaries of state being accountable to parliament. I don't buy that, and the more we go down that line, the more in the long term we will come to regret hollowing out parliament. And giving all this to judges doesn't, in my view, crack that.

Panoptic society, is this the beginning of the Stasi, where will all this end? These are sensible questions to have in one's mind. I've got no complaint about that. But I will just very briefly read out one sentence from Angela Merkel in her interview with *Die Zeit*. 'For me,' said Angela Merkel, 'there is absolutely no comparison between the Stasi in East Germany and the work of intelligence services in democratic states. They are two totally different things, and such comparisons only lead to a trivialization of what the Stasi did to the people of East Germany.' So I think let's just keep some balance, some sense of perspective here.

The point about cyber spying has been well made. The argument − and I'm not going to say whether I agree with this or not, it's a fine distinction − is between spying to safeguard the nation and spying to enrich the nation. I don't think anyone can complain about, given there is no international law, and there will never be international law against espionage, against one country spying on another for national security purposes, but wholesale theft of intellectual property for the enrichment of companies is a different matter. So that I think is the basis of that.

Temptation to delve − a very interesting and obviously very true point about human nature. That's why I could almost, if I was tempted, advance the

argument we're safer with the computers. Computers are not conscious. The millions and millions of emails the computer is going through to find the needles in the haystack, they don't actually read the stuff, they're not conscious. If a human being or 1,000 human beings were sitting in a factory reading all the emails they might well be tempted – 'oh-ho, here's one from Geoffrey Robertson, well we'd better read that one.' That doesn't happen with the computer, so I think I'm not so worried about that.

Metadata − point very well made. It is absolutely essential to fighting crime. It's also very useful for the purposes of counterterrorism, but for crime fighting it is, and all police services would agree with that, one of the most important, if not the most important technical tool in their armoury. And that's why, as *Le Monde* has reminded us recently, our French friends have invested a huge amount in collecting all the metadata in France.

Corporate stuff − I too am very worried about this, it's not a practice that happens in the UK, the body shopping. Yes, technical expertise is brought in to run computers and so on, but the whole-scale body shopping and export contractorization of functions that ought to be exercised by those who have a public service ethos and who are public servants, they should not be exercised by those who have, as it were, bottom line commercial interests. That to me is pretty much an absolute, and I just hope this country won't follow that route.

Damage − well all I can say there is I wasn't referring to friends-on-friends spying, that fell into my embarrassment category, I was referring to other things that Mr Snowdon has taken which would be − well which *are* already damaging. And this is where you can have me, Duncan, because I can't tell you what they are, because you're into detailed sources and methods, and that I think is a debate we need to have about where that dividing line is. Complete transparency, don't even bother with the activity, because you've told the bad guys exactly how to evade it. So with that, thank you.

Patricia Lewis:

Thank you. Well no Chatham House ends successfully without there being a call for more debate. And so I'm very grateful to our three panellists. I will probably be shot when I leave this room because we've gone over time by over 15 minutes, but I thought there was enough interest in the room to hear this and to sustain the conversation. I hope you agree with me. Because of the time, I won't say anything else, I will just thank our three panellists profusely for what I thought was a great conversation. I think we did cover a

lot of track. I thank all of you who participated and those of you who asked questions in particular. I'm sorry there wasn't enough time for all of you, but if you could show your appreciation to the panellists, I'd be very grateful.