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

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

Patricia Lewis:

Welcome everybody. My name is Patricia Lewis, I'm the research director here for International Security and it's my great privilege to introduce our panel to you, who are going to be speaking on 'Surveillance in an Information Society: Who Watches the Watchers?' Our speakers here today will be addressing the debates that have been sparked by the revelations that came from Mr Snowdon over what national intelligence agencies should be allowed to do with personal digital data, and where the divide between security and civil liberties should be drawn. It's a very important debate for our societies to be having.

The amount of global information being generated through web-based communication and mobile usage is vast and hypothetically extremely useful in making intelligence-based linkages between terrorists and criminals. However, recent reports around the Prism database and large scale internet filtering seem to suggest that some national intelligence services have obtained access to numerous data centres and illegal authorities that are either secret or interpreted more widely perhaps than previously publicly understood. So the panel will discuss these revelations and explore the potential implications for national intelligence agencies and individuals, and consider the potential long-term political, social and economic impacts, and whether this will persuade people to review their internet activity and pay more attention to privacy. And at that I will tell you that our hashtag for tonight is #surveillancesociety, and if you use it of course you will be surveyed, so at your peril.

It's a conversation that we're having here, it's not a debate. We have not set this panel up to have a big fight on our hands, to create controversy. What we want to do is make everybody think, and so we've looked for a range of views, and three people who we know are highly articulate, highly expert, and will be able to explore with us some of the very important issues that are raised by these revelations. We have with us Professor Sir David Omand, who is the visiting professor at King's College London. We also have Duncan Campbell, who's an investigative journalist, and Geoffrey Robertson QC, who is an expert human rights lawyer.

What I'm going to do is turn to each of the speakers in that order, they will each speak for between six and eight minutes, hopefully we'll stick to time, and then open up the floor for questions and answers.

So first of all I'm going to turn to you, David. You were the first UK security and intelligence coordinator responsible to the prime minister for the

professional health of the intelligence community, national counterterrorism strategy and homeland security. You served for seven years on the Joint Intelligence Committee. You were a permanent secretary of the Home Office from 1997 to 2000, and before that you were director of GCHQ and deputy undersecretary of state for policy at the Ministry of Defence. Most impressive to me, however, is that you've just completed a degree in mathematics and theoretical physics with the Open University, and I wish to congratulate you in public on that, I think it's a marvellous achievement. David.

David Omand:

Thank you very much Patricia, and good evening everybody. Let me start with Mr Snowdon. His leaks strike me as falling into three groups. First of all we have confirmation of what we either already knew, at least those of us working in the academic intelligence studies field, or had suspected. It was Chapman Pincher in the *Daily Express* in 1967, for example, who revealed, if you remember, to Harold Wilson's fury, that cable traffic leaving the United Kingdom was being monitored. And serious books have been written about the National Security Agency and GCHQ's ability with legal authority to access, via the internet companies, much of the internet traffic of those they suspect of being terrorists, narcotics traffickers, arms proliferators, and no doubt other international criminals. So in my view, we should be glad that it is indeed possible to track such people, even in an internet age.

A past director of the US Central Intelligence Agency, Stansfield Turner, wrote, 'There is one overall test of the ethics of human intelligence activities, that is whether those approving them feel they could defend their decisions before the public if their actions became public.' William Hague, I note, was commendably quick to defend our access to such information. I see this afternoon that the Parliamentary Intelligence and Security Committee have confirmed that GCHQ's access to Prism was lawful. And as Duncan Campbell told parliament recently, it is fit, proper and necessary that interception of communications and processing of communications data be available as part of the armoury.

But what we should be asking ourselves is: what are the rules? Who's entitled to enter that armoury and why, and at whom may they aim their enquiries? And who is it who checks on our behalf that an acceptable balance is being struck within the basket of human rights that secure our liberty between, on the one hand, our right to security and, on the other, our right to privacy?

So that's one category of revelations from Snowdon. Secondly, we have some revelations that are frankly embarrassing to the governments concerned. As with all spying operations when uncovered, there is nothing to be done except refuse to comment and hold your nerve. And we're not alone. *Le Monde* wrote last week of the DGSE's − French external services − operation to access and store a large part of the electronic communications within and across France, and Snowdon himself has talked about the links between the German intelligence agencies and the National Security Agency. As the German interior minister said, it annoys him when some in Germany immediately criticize the US without having exact knowledge of the situation. As he said, without the information from the US and the good collaboration with the intelligence agencies, we most likely would not have been able to prevent terrorist attacks in Germany.

And then there's a third category of revelations from Mr Snowdon, and that is that he has quite unnecessarily compromised detailed intelligence sources and methods and has already caused real damage to US and to our own intelligence effort, and thus to our national security. And that was simply not necessary for the purpose, which he says he had, of raising the issue of internet interception. So I'm afraid he does appear to be guilty of espionage as well as of whistle-blowing. I don't propose to discuss that aspect any further because I don't want to compound the damage he's already caused.

So in the remaining time that I've got in these opening remarks, let me just focus in on the principles that should govern the use and oversight of these powerful capabilities. Alan Rusbridger, the editor of the *Guardian*, wrote on his blog that he'd read about these principles that I'm about to talk about in my book, and had adopted a version of them to guide investigative journalism in the *Guardian.* So I cite that as evidence in favour of these principles.

The first principle: we should be very clear about the intelligence equivalent of *jus ad bellum* − for what purposes do we allow this intelligence machine to exist? British legislation restricts the purposes to national security, detection and prevention of serious crime, and economic wellbeing. National security I feel quite comfortable about; it's no longer just for the executive to define, the judges have started to take an interest in this, as we saw in the Belmarsh case, and I'm sure that will continue. Detection and prevention of serious crime I have a question mark about. It's very broad. It's any offence − I think Geoffrey will correct me − that carries a sentence on first conviction of more than three years. So that covers − should we be thinking about trying to narrow that? I raise the question for later discussion. And economic wellbeing, contrary to what you read in the newspapers, does not mean

commercial espionage. It's, to give you an example, investigating the current wave of cyber attacks on the financial institutions and the banks, something that is very necessary to keep an eye on. We should, I think, constrain any tendency for the secret world to encroach into areas that are unjustified by the scale of potential harm to national interests. So paedophilia, yes, tax evasion, question mark in my mind. It's that sort of discussion we should have.

The second principle: there must be integrity of motive. No hidden agendas. The integrity of the whole system, from collection all the way to final use must be assured. And British public servants, I would maintain − and I declare an interest, I was one − have a deservedly high reputation for integrity around the world. But that has to be checked, and I think that's a legitimate task for the oversight of the intelligence community by the parliamentarians on the Intelligence and Security Committee.

The third principle is proportionality: the moral hazard such as the degree of intrusion into privacy must be proportionate to the harm that it sought to prevent. That's a legal requirement in the legislation and the very senior judge, the interception commissioner, should be keeping a very active eye on that. Does that commissioner have sufficient staff to do that? I think it's a legitimate question.

The fourth principle: there must be right and lawful authority all the way up the chain of command that actually makes oversight possible. What we didn't see in the case of the Metropolitan Police's undercover operations. I cannot agree with the director of Liberty who said, 'Matters so grave for public trust, human rights and democracy cannot adequately be investigated by a secretive committee taking spin from spooks in the dark.' Nicely put, but in my view completely inappropriate. We have to give our parliamentarians a chance.

The fifth principle: there must be discrimination and a reasonable prospect of success. No fishing expeditions. All intelligence operations need careful risk management, and the likelihood of unintended consequences, including to others, has to be taken into account when the decisions are taken. The director of policy for Liberty last week said, 'We suspect GCHQ of intercepting billions of private emails and messages without parliamentary knowledge or approval.' As we heard this afternoon, that was simply false, and such exaggerations help no one. The computers have to sort through millions of items to find the needle in the haystack. That doesn't mean that any human being is looking at millions of items.

A final ethical principle, and then I'll conclude, which is necessity. Recourse to secret intelligence should be a last resort, and that too is built into the act.

There should be no reasonable alternative way of acquiring the information by non-secret methods.

So to conclude, let us respect the work of the British intelligence agencies in keeping us safe. Be glad they're subject to the rule of law in a democracy, and ensure they have the tools to keep up to date with the internet age.

Patricia Lewis:

Thank you David. I'm now going to go straight to Duncan, who is an investigative journalist and computer forensic expert, and has reported on surveillance and secrecy issues for, dare we say, 40 years or so. He first revealed the function and nature of GCHQ in 1976 at a time when its existence, budget and function were officially secret, unknown to parliament and the public. He was subsequently and unsuccessfully prosecuted under the Official Secrets Act. In 1987 he revealed in a BBC programme how GCHQ had evaded parliamentary scrutiny in commissioning a spy satellite system, which some of you will remember as Zircon. In 1988 he revealed the precursor project to Prism, known as Echelon. The European Parliament has commissioned and published his report on the effect of secret communications surveillance. He was the expert witness in the 2008 case before the European Court of Human Rights of *Liberty v UK*, in which GCHQ's methods of collecting all communications to and from the UK were held not to comply with law. And he continues to work resolutely in exposing all sorts of goings on, and making us think. So Duncan, welcome and thank you very much indeed.

Duncan Campbell:

It's an epochal moment to be sitting beside David, with whom I have an extraordinary amount of background in common as well as that which seems utterly opposed, and I thank him for elegantly framing the human rights issues in this matter. The title of our talk, *quis custodiet ipsos custodes* − who watches the watchers − is the fundamental question. Can the public trust that we are not, again in David's words, heading for a panoptic state or the tyranny of absolute knowledge guaranteed by the conduct of public servants? David would say yes and I would say absolutely not, on the evidence, and on the evidence going back 50 years.

The first couple of items are simply that GCHQ itself was a secret in those days of 1976, and precursors to David as director saw to it with some venom

that we were prosecuted and hopefully, but unsuccessfully, put away for a number of years. Now what GCHQ learned from that is that it didn't hurt. The Mongolian hordes did not come across Essex; we do not live under the caliphate. GCHQ these days puts far more information on its website than I ever knew or could publish in 1977 or 1987, or indeed 1997. They can live with transparency, and if there is to be an answer to the very serious questions put before us all by Edward Snowdon, it is that that transparency must be progressed and rapidly progressed. The walls of secrecy have to come down. We are an adult society, we have grown up to understand that terrorists are among us and that secret surveillance is among us.

What I would suggest in this gathering is that the duty of public officials to be accountable has been misplaced and replaced with misleading statements, with concealment, and in effect the systematic subversion of proper governance. And in the short time available for these starting remarks, I'll try and give a few examples. But it is important that we don't have any of the dumb arguments. Terrorists are out there and they mean us harm and they use the internet. We can move on from that. And the same for criminals − they're bad, they mean us harm. But to leap from that to the proposition that GCHQ's Project Tempora − which is far, far more critical and disturbing than the Prism system − was ever justified or ever explained to parliament is simply extraordinary. It is non sequitur. It breaches the core principles of human rights, which Geoff will be able to elucidate on more. And were it not for Snowdon, GCHQ would have escaped discovery and reproach because of that wall of secrecy.

The most compelling example of deception in recent times has been something called the Communications Data Bill. David correctly, and accurately I'm sure, quoted from something I said to the committee, and I'll stand by that, but that was a farrago of deception. Parliament was told − I sat there watching Charles Farr from the Home Office giving evidence − there is a communications capability gap; we're losing things. Well he must have known and, to be quite honest − and I know I have a distinguished lawyer sitting beside me − that calls for the L word, the lie word. He wasn't just accidentally misleading parliament, he was complicit in deceit. The home secretary I do not know because of how much she is actually informed we have not been told.

But there wasn't a capability gap. If there was any gap, given the disclosures we have about the soaking up of all of the internet and the level of systematic and effective access that Prism provided to GCHQ and British agencies through the FBI and through NSA, it is that the gap was that GCHQ weren't

prepared to share with the police, who are the ones charged with keeping our streets safe.

When the home secretary reached, shamefully in my mind, for support for that discredited bill in the wake of the horrible murder of trooper Rigby in Woolwich, it was simply inexcusable. It was only days after that statement that the Snowdon revelations began and we discovered that if there were any communications that could have alerted authorities to prevent that attack, they were harvested, or almost certain to have been harvested anyway, and certainly there was no basis for calling for new legislation for the communication, for the capability gap.

Prism also would appear to have made no difference at all in the case of the Boston bombings because the two suspects now facing trial were established FBI targets, and one of the small items that you may or may not have noticed from the slides that have come through is that it's actually the FBI that handles Prism and accesses the information from the American companies. Nor would the capability, either the real but secret one of Tempora or the remedying of the imagined capability gap, have done anything about 9/11. Retrospective reports show that they simply did not use modern electronic communications, and I think it is right to say − although I'd be corrected if there was an error in this − that the same is true of the July bombings in London. They went under the radar for precisely that reason, that they long ago learned not to trust Western-administered communication systems.

So there is a long, long history to this, and I admire David for having got out the D-notice story of 1968 [*sic*] which is indeed, I agree, the precursor. I can only counter that this story starts in 1920, as you know, when the Official Secrets Act in its first generation in fact grabbed the power to intercept all cables at a time, what, 60 years before GCHQ even existed.

Yes, the desire to go out there and get everything has been built in and operated in secret right from the beginning. There is an agreement about that, without question. What *is* to be questioned is the appropriateness or proportionality of simply grabbing everything and sticking it into a computer storage system to sort out retrospectively.

On the one occasion that this was tested in a human rights forum, it was the result of an article where I'd unearthed yet another of GCHQ's projects, this time a listening tower they built in the north of England to stick into the radio beams that carried all of the Irish government and Republic of Ireland's international communications. Now again, under the law that we all know − and we were facing Irish terrorism at the time − any suspect could have been

targeted specifically as to any means of identifying their communication. But that is not what GCHQ did. Indeed, they were plainly, it seems in the evidence, acting outwith the law, because had they used the law and the licensing terms that they have used to get access to all our fibre optic cables for Project Tempora, they could have simply gone to BT and said 'hey, when this microwave beam comes into Manchester, you can intercept what we need and send it down to us in Cheltenham'. Instead, in secret, on Ministry of Defence land, in the middle of the beam, and therefore unknown to British Telecom in principle, they stuck systems to collect everything, sift it down and send it in over fibre optic.

That was found in the only judgement of its kind not to comply with human rights. The only reason that things didn't change is that the laboriously cumbersome processes of the European court − I think we can probably all agree on that − meant that by the time the judgment was passed, new legislation in Britain, RIPA, the Regulation of Investigatory Powers, had been passed and allowed GCHQ to slip away.

But that is the core issue. So if I suggest that there is one issue that needs focus above all, it is not Prism. As has been said, Sir Malcolm Rifkind's committee today has reported and says that it's happy about Prism. It didn't even mention Project Tempora. It didn't mention the internet tapping of six different major communications companies involving fibre optic probes physically inserted to scoop up everything that's going in and out of Britain. It didn't look into how that was shared in a project with the Americans, where no regulation was applied to how they might use the information or for what purpose.

There *is* a culture of attempted compliance in GCHQ, but it doesn't work, it isn't tested. The interception commissioner was an embarrassment when he appeared before the Communications Data Bill committee. He isn't staffed for it. The MPs were never briefed and they've been embarrassed to rush, to have to change their reports now that these projects have been forced out into the open. The key question is this mass surveillance, the panoptic, the scooping up of all the communications and then going in and sifting afterwards. It's done under a legal regime called certificated warrants, which is authorized − and it is the easy answer to say yes, it's legal. It's legal in a law that no one understood, parliamentarians couldn't grasp. Interception is a judge-free zone because under those laws no court may enquire as to whether interception has taken place, at least unless it's taken place outside the United Kingdom.

I personally have taken part in a case involving cocaine trafficking, as alleged, where communications interception was brought in because it took place in Colombia. And then they tried to bring in some data that clearly didn't come from Colombia. Perhaps it came from Cheltenham. But either way the result of this was that it was so suspicious that at the end of the day the House of Lords chose to overturn convictions. Now if protecting the secrecy of Cheltenham's methods means − and of course I've got to say it's a matter for the jury at the end of the day, what verdict they were to file − but if protecting Cheltenham's turf comes above all other objectives it shows how far out of kilter those who manage it and oversee it from within have gone off the proper track of civil society, in my opinion. Thank you.

Patricia Lewis:

Thank you very much indeed, Duncan. I'm now going to turn to Geoffrey, who is the founder and head of Doughty Street Chambers, the UK's largest human rights practice. He was the first president of the UN war crimes court in Sierra Leone, and served between 2008 and 2012 as distinguished jurist member of the UN's Internal Justice Council. He has written many books, *Crimes Against Humanity*: *The Struggle for Global Justice*, *The Case of the Pope*, *The Tyrannicide Brief*, and *The Justice Game*. And his latest book, *Mullahs Without Mercy: Nuclear Weapons and Human Rights*, takes a very tough look at the human rights situation in Iran, and then a very legal and powerful look at the issue of nuclear weapons. He was involved in the defence of Salman Rushdie, Mike Tyson, Julian Assange, and in the European Court of Human Rights, Yulia Tymoshenko. He was also involved in the prosecution of Hastings Banda and General Pinochet. Geoff.

Geoffrey Robertson:

Gee, it's great to be at Chatham House without Chatham House rules. Perhaps the worst example of the British disease, as Richard Crossman calls it, is our Chatham House rules. The idea that matters of importance can be discussed by important people with important people, or people who think they're important, or have been made to think they're important because they're under Chatham House rules, denied to newspapers and to members of the public is, I think, or someone will write a thesis one day suggesting, that this is one of the worst examples of the British disease. It is something that devious diplomats, although that may be an oxymoron, have used over the

years to hide an awful lot of publicly important things. So here's to the end of Chatham House rules and here are my views as a result on this subject.

Is it really surprising, Snowdon's revelations? Do they come as revelations? We've known about keywords for many years, we could go back to Howard Wilson's fury when Chapman Pincher made that declaration. Do we really wonder that there are 70,000 keywords that if you mention on an email, you will have that email scooped up, that they're words other than Julian Assange or Duncan Campbell? There are 70,000 of them, 40,000 selected by GCHQ, 30,000 by the NSA.

It's all very well for President Obama to say 'we do not collect data on Americans'. That's about as accurate as President Clinton saying 'I did not have sex with that woman' because of course the data on Americans is collected by GCHQ and handed over the NSA. It's all very well to say we have a rule of law, we do everything in Britain under the rule of law. No we don't; we do it under the rule of politicians, politicians who have − not judges, politicians, who are patsies, really, of the Security Service. They sign warrants, general warrants very often, for interception.

Does this matter? And I think the first question is whether it does. Snowdon certainly has revealed an area of, if you like, undercover agreement by Google and Microsoft and so on promising their customers that their data will be safe, even encrypted, and yet supplying it to the NSA at government request. Even this deception is not altogether surprising given the ease with which Microsoft and the ease with which the various credit agencies have complied with the US government not to take or transfer money to WikiLeaks. On Visa or PayPal you can buy Ku Klux Klan uniforms but you can't send any kind of donation to WikiLeaks. That's not a legal requirement, it's an understanding. And so are we surprised?

And I think the three questions that we might address are: first of all does it matter? Does it matter that 1984 is here, does it matter that the state, the government, or at least the governments of Britain and America with a little help from their friends Australia and New Zealand, are in fact scooping up or can scoop up virtually anything? We want Mohamed Atta and the like to be caught; maybe there were emails in Germany prior to 9/11. Terrorism perhaps has prevented us being worried about the consequences; in Britain, apart from the *Guardian* there seems very little concern. Go to Germany of course, there's massive concern, perhaps because of not just memories of the Gestapo, they're fading, but memories of the Stasi. Germans do seem to value privacy in a way that we don't. On the other hand, they haven't had the

courage to offer Snowdon asylum, the opposition talks about it and it may be after the elections in November his very sensible decision to accept Russian hospitality, despite the gag that it comes with, will be replaced by a willingness to go to Germany to testify.

The second question is: how do we draw the line, how do we decide how to control or guard the massive scooping up of personal information? And the third question, perhaps we won't have a chance to get onto it, is: how do we protect the whistle-blowers who actually tell us what our masters, political masters, won't tell us, namely the extent of the surveillance? British law goes right back to 1281, where there was actually a law passed against eavesdroppers, those who listen under the eaves of windows to frame malicious rumours. They were prosecuted and punished by the ducking stool. That was the first British common law approach to eavesdropping. Then of course was the cases in the 18th century involving John Wilkes and the treasury solicitor who not only stole the proofs of his newspaper, the *North Briton*, but took under a general warrant his package of condoms. The courts ruled that you simply couldn't in this country under the common law have a general warrant; you had to be specific.

Well spool forward to today, and you have an act, Investigatory Powers Act, RIPA, which only retains specificity in relation to warrants in this country. The foreign secretary may give general warrants for interception of communications abroad. And what we have, as Duncan has said, is not a rule of law but, alone of advanced countries, we have handed interception surveillance warrants entirely over to politicians. And that is crucial I think in the defective aspect. And when Mr Hague talks about 'we have interception purely by the rule of the law', we have it by the rule of politicians, hastily signing warrants put before them by intelligence officials, terrified that is there is a bombing down the line and they don't sign this warrant then they might not get the material.

As far as the international situation, we have a complete lack of coherence. All other countries, advanced countries, use judges − Canada, most European countries. Canada, in particular, requires targets to be notified afterwards so they can make complaints. We have a system which doesn't require targets to be notified and so there are no complaints, or very few. Australia requires judicial warrants. France, on the other hand, probably has the worst system of all: the prime minister's office can authorize an interception without any court oversight. In America there is a court oversight required for snooping on Americans, which gives Americans great cause for concern. They're not concerned at all about snooping on foreigners, as I

discovered. I was in America at the time the Snowdon revelations came about. But they have a court which is a group of judges hand selected by the chief justice, a FISA court, which has only rejected 11 warrants out of 33,000 applications in the last 15 years. So that is hardly effective oversight.

At the end of the day − I'll finish on this, there's a great deal more than can be said − but at the end of the day I think we have to ask ourselves: okay, we want to get terrorists, we all want to get the terrorists, we all want to pick up Mohammed Atta… what is the danger we want to guard against? The danger, I suspect, going right back to the Zinoviev letter of 1926 [*sic*], and many examples in more recent years, is that the state will scoop up personal information on those who are left-wingers or right-wingers or somehow unsatisfactory as far as the state is concerned, and that will be leaked. Careers will be destroyed for political reasons. This data, personal data allows this to be done and it has been done in this country over the years.

So how do we guard against that happening, the misuse and abuse of data? You certainly don't guard against it by our present arrangement, which has some long-retired judge listening to ex post facto complaints and not telling people that data on them has been used so they can make a complaint. That's not a way forward. Certainly criminal laws to prevent misuse of information − but then we come into the third question of how do you protect whistle-blowers by giving them some form of public interest defence? I suspect that is the area in which law reform as a result of Snowdon will have to focus.

Patricia Lewis:

Thank you very much Geoffrey. Before I open the floor, I know David just wants to make a quick point of clarification.

David Omand:

Geoffrey, I heard you say that GCHQ intercepts American citizens and then hands that over to the Americans, this being intercepting the Americans would not be allowed to do for themselves. That's not true.

Geoffrey Robertson:

Well that's what Snowdon suggests, and whether it's true of not, we'll have to…

David Omand:

Well, it's an example that not everything Mr Snowdon has to say is true.

Geoffrey Robertson:

Well it may be, but that is the allegation, or one of the allegations.

Patricia Lewis:

Thank you.

Geoffrey Robertson:

Can Duncan come in on it?

Duncan Campbell:

Just a point of information, as one expert to another, the blanket interception of the optical fibres across the Atlantic and the untrammelled access of that GCHQ product to NSA staff does fit with what Geoff says. There may be safeguards in America, you will say, but you don't know what they are.

David Omand:

Well I think we do know what they are. I just have to say, as a point of information, that it would be unlawful for the US officials to use that particular means of access − and they've got many different means of access − any of those means of access to circumvent the legal restrictions on their interception of American citizens. We know they *can* intercept American citizens, but with certain warrantry and so on. They can't use GCHQ's access as a way round that, period.