THE ETHICS OF SPYING

Mr Dean, my lords, ladies and gentlemen,

Thank you very much, Mr Dean, for that very generous introduction. It is a great honour to be added to the list of very distinguished people who have previously given the St George's House Annual Lecture. In this historic and beautiful place, the home of the Order of the Garter, the epicentre of English chivalry, I was worried that the second oldest profession was rather a grubby theme for the annual lecture. It was the United States Secretary of State, Henry Stimson, who said in 1929 when refusing to provide funding for the predecessor of the United States National Security Agency 'Gentlemen, don't read other gentlemen's mail'. But then I remembered that on the opening night of the 2012 Olympic Games, the Queen herself was seen to parachute into the Olympic Stadium with James Bond and so I began to think that it might have the Royal seal of approval.

It's certainly a topical theme. There can never have previously been a time of such concern, partly stimulated by the revelations of Ed Snowden, that the state trespasses too far into all our privacy in the interests of protecting us from terrorism and serious crime. Libertarian groups bring legal action against the intelligence agencies alleging misuse of their powers. Last week, David Anderson, the independent reviewer of counterterrorism legislation, produced a 373-page report on the balance between privacy and security. Previously, the Intelligence and Security Committee of Parliament, of which I was a member, produced a very detailed report on the same subject, and, in the new parliament, we're now awaiting government legislation on this subject.

We didn't always agonise so much. In past times, we were prepared to trust our intelligence agencies without asking questions. MI5 and MI6 were founded just over 100 years ago in 1909 and GCHQ after World War I but there was no acknowledgement in the next 50 years that they even existed. We all knew that they did but nobody talked. It's estimated that 10,000 people knew the secret that at Bletchley Park we could intercept and decipher German messages but nobody talked for 30 years. Churchill said, 'The people at Bletchley Park were my geese that laid the golden eggs and never cackled'. Of course, the intelligence services appeared in novels - *The Riddle of the Sands*, James Bond, John le Carré - but no one knew what the facts were, nor expected to know. The headquarters of the agencies in London were

a closely guarded secret. There was no law governing the intelligence agencies' activities. As somebody said, they could bug and burgle their way round London just as they saw fit. We believed that they were on our side and we let them get on with it.

Now, it has become much more complicated. Why? I don't believe it's just the end of the age of deference. Of course, it was something of a shock after the Second World War when it emerged that some of the members of the intelligence agencies weren't on our side after all: Kim Philby, Burgess, Maclean, Blake. But, again, I don't think that is the reason why now such transparency is demanded of the intelligence agencies.

One of the factors is that technology has changed so hugely. Spying is no longer just a matter of decrypting enemy wireless messages or even hacking telephones and intercepting letters. Now, we're all subject to a huge amount of surveillance every day. Satellites up there in the sky could read the time on your watch as you walked across the ward to the chapel. There could be a hole the size of a pinhead in these walls - actually they'd have some difficulty in putting them into *these* walls - but those of you who have seen the American programme, *Homeland*, will remember that a pinhead camera could record and transmit everything that was going on in a room to a distant location. There are remote listening devices that could be a locational hearing aid 200 metres away which could hear everything that I'm saying in this room. Actually, they wouldn't bother to do that now. What they'ld do is to activate one of your mobile phones and that would act as a transmitter, so that they could hear what was going on. A beacon could be put in your car, so that your movements in your car could be traced. You've been photographed many times today on closed circuit television cameras. It is said that when a child goes to school in London, they're probably filmed on CCTV some 300 times. The communications data on your mobile phone will tell those who want to know where you are.

I remember, two or three years ago, being amazed when I asked my grandson at half-term what his friends were doing. He said, 'Wait a minute, Grandpa, I'll tell you'. He got out his mobile phone and looked at an app and he said, 'Well, Tom is in Norwich with his parents, Harry is visiting his grandmother in Harrogate and Dick is up to no good in London'.

And now, of course, we have drones which can be used to watch over us at the will of people who control them remotely. So, the technology of George Orwell's *1984* and big brother is a reality. It is here and it's with us.

Much, of course, is beneficial. Communications data help the police in 95 per cent of the prosecutions they bring for serious crime. CCTV cameras, similarly, help to solve crime. Remember the sad case of the girl, Alice, who earlier this year was abducted and murdered on the Thames towpath. Even this morning, I was reading *The Times* and my eye was taken by an item headed, 'Burglar outfoxed'. It said that a burglar has been jailed for four and a half years after being caught red-handed by a camera set up in a South London garden by a BBC *Springwatch* crew hoping to record the nocturnal activities of urban foxes. Nigel Batten, 43, of Lewisham, was filmed trying to break into a studio office in Herne Hill where I used to live.

We willingly allow Amazon and Google to track our purchasing habits. We may not realise that we willingly do it but we sign something which enables them to, so that they can bring to our attention goods and services we may want to buy. Sometimes, the results may surprise us. I wondered why I was receiving so many emails urging me to buy highly unsuitable articles of clothing until I remembered that I'd bought on the internet a tie with a bathing beauty pin-up on it for my part in last Christmas' village panto.

My eye was also taken by a story in *The Times* a few weeks ago and I think this is worth sharing with you. The heading was, 'Rugby women play a blinder to solve crime', and the story was that a women's rugby team helped police to recover stolen valuables by using internet technology to track down the alleged thief. About 20 mobile phones, cash, wedding rings and other belongings were taken from the Henley Hawks' changing room while they were playing a match against Hove Rugby Club. Later, one of the stolen phones was used to take a picture of another one of the phones lying on a red bedspread. Police believe that the thief took a photo of one of the phones with a view to selling it online and this photograph popped up on a One Drive web account (which allows users to access photos remotely) owned by Alistair Mortimore, the coach of Henley Hawks. Meanwhile, Amy Atkinson, a player, managed to follow the movement of her stolen phone using a tracking application. Another player used the Trip Advisor website to search for hotels and bed and breakfasts on the Brighton sea front close to the last known location of Miss Atkinson's phone. She then spotted a photo from a hotel that matched the bedspread in the photograph on the One Drive account. The club tipped off Sussex Police who went to the Atlantic Seafront Hotel and arrested a man. Police said, 'that a substantial proportion of the women's belongings were recovered and a 62-year-old man of no fixed address had been charged with theft'. I think we could all describe that as

ethical spying.

So, it's the change of technology. The fact that, however innocent we are, we're all under observation all the time. But it's not just that, I think there's another factor as well, and that is the change of the targets. A hundred years ago or less, for example in the Second World War, we only spied on foreigners. We didn't do it to our own people. But then, 40 years ago, with the rise of terrorism in Ireland and subsequently with the rise of Islamic terrorism, we are forced not only to use these means of interception and surveillance on foreigners but on our own citizens. That changes the game, so that it becomes necessary to have controls. When there are such powers in the hands of the intelligence agencies and the police and they can use them against the citizens of our own country, there is a need for controls over them.

There's also need for controls over the media for whom hacking telephones was famously for many years a source of their best stories. But it's the state I think we've got to worry about most. The laws that govern how these surveillance tools are used started during the mid-1980s and have grown like Topsy. Now they are a bewildering complex of legislation. Just to give you an example of the amount of laws that have been passed on this subject - the *Telecommunications Act 1984* first governed the interception of telecommunications; the *Interception of Communications Act 1985*; the *Security Service Act 1989* and another one in 1996; the *Intelligence Services Act 1994*; the *Human Rights Act 1998*; the *Regulation of Investigatory Powers Act 2000*; and then in the last few years, the *Justice and Security Act 2013*, the *Data Retention and Security Act 2013*, the *Counterterrorism and Security Act 2015*. This legislation like Pelion piled on Ossa, has become so complicated that no layman can understand it and some conspiracy theorists suspect that this was deliberate in order that the authorities could find gaps that they could go through to spy on you and me. So, there had to be a structure of protection and this country has set up a very strong structure of protection.

What the basic laws say is that these means of surveillance, whether on our own citizens or indeed overseas, can only be used for very narrowly defined purposes and the two purposes are national security and the prevention or detection of serious crime. If the police or the intelligence agencies use their powers for any other purpose, they're breaking the law. Also the actions they take have to be capable of being shown as necessary and proportionate, that they couldn't do without them and that the purpose for which they're using them is proportionate to the intrusion. I think people don't recognise quite how restrictive the law

rightly is.

If the police or the intelligence agencies want to look at the content of messages we pass to each other, if they want to listen to our telephones, if they want to open our letters, they have to get the authority of an independent person. In Britain, it's a minister, the Foreign Secretary or the Home Secretary. In other countries, it's the courts and the independent reviewer of counterterrorism legislation would like to see the courts and judges used to give that authority in Britain. That is a controversial matter. But the judges do come into it in Britain because there are commissioners, former judges, who audit what the Foreign Secretary and the Home Secretary approve, to ensure that it does comply with the requirements of necessity and proportionality and that it is only being done for the purposes of protecting national security and dealing with serious crime. But there's also then a tribunal - I bet not many of you know this. If you think that your telephone is being hacked, and some of us do because we hear strange clicks on the line, you can go to the tribunal and ask them to look into it. The tribunal will look into it and they will tell you if this is being done improperly. They won't tell you actually whether it's being done but the answer you will get 99.99 per cent of the time is that, when the tribunals has looked at all the papers, the law hasn't been broken. Now, that could mean you are a legitimate suspect and your phone is being hacked but it's more likely to mean that no such thing has happened.

The intelligence agencies have ethics advisers and staff counsellors which they need and that's to prevent the sort of thing that Ed Snowden thought it was necessary to do, to go to the press and, in his case, to go to China and Russia when he felt that things were being done which offended his conscience and he thought the world ought to know about. Finally, there is parliamentary oversight, the Intelligence and Security Committee, which I mentioned before, and of which I have served as a member.

So, there is, in this country, very restrictive legislation which controls the actions of the intelligence agencies and the police but, nonetheless, people are very disturbed about it and they were particularly disturbed by the revelations of Ed Snowden. What disturbed them most I think about the revelations of Ed Snowden was his disclosure that the GCHQ can collect in bulk messages which are transmitted including phone messages, internet messages and so on, which they screen in order to pick out the ones that might be dangerous. This was felt in some quarters to be mass surveillance. It was certainly in accordance with the law and actually the

remarkable thing about Ed Snowden, which should comfort us, is that he walked off with a million reports of the American National Security Agency and 60,000 of GCHQs which we had shared with the Americans and I am not aware that any of them showed that either of these agencies had acted in breach of the law.

When you think a million NSA reports, 60,000 GCHQ reports, what's surprising is how little embarrassment that has caused. It's caused shocking loss to the effectiveness of our security but it hasn't showed either breaches of the law or, for the most part - I'll come back to the tapping of Chancellor Merkel's mobile phone - not things that were embarrassing. But, nonetheless, people have been shocked by his revealing bulk collection. As I say, the impression got around that everybody's communications were vulnerable to interception. But the fact is that the agencies only have access to a very small proportion of the cables that carry the world's traffic. They then have to decide which of those - that very small proportion of carriers - are most likely to carry traffic which might reveal terrorist plots. They then have computerised sifting devices which pick out communications that might be suspicious and this is long before any human being has looked at what this mechanism produces. When eventually a human being does look at any of these messages, it is an infinitesimally small fraction of the traffic. I think we in this hall can sleep easy in our beds that it's not going to be any of our internet messenger.

Nevertheless, legitimate concerns remain and so in this age in which electronic communication and the storage of data is set to be so dominant in our lives and when the instruments of intrusion are so pervasive and so powerful, we have to decide what is good spying and what is bad. When I told a friend that the title of this lecture was going to be the ethics of spying, he said, 'But that's a contradiction in terms. Spying can't be good', and since spying involves stealing other people's property, which they often don't want you to have, you can see his point. Yet I've seen enough people who work in our intelligence agencies to know that they are people of the highest integrity. They're highly ethical people and, indeed, it is a criterion for their recruitment that they should be so. This is one of the qualities that the recruiters are most looking for. So, how do we resolve this paradox? How do we tell the difference between good spying and bad spying?

First of all, why do we do it at all? Well, let's just remind ourselves of some of the benefits. In war these days, intelligence is absolutely essential, more essential than it has ever

been. When we have precisely targeted weapons which can land virtually on a sixpence, we need to know which sixpence they should land on and that is information that is acquired by intelligence. It is crucial that we understand what are the enemy's aims and, indeed, I'll give you two instances where I think it played a vital part in preventing the outbreak of a third world war. I'm old enough to remember the Cuban crisis and remember when my wife and I were newly married, going home one night - and many of you may have similar memories - and not knowing whether by the next day the United States would have launched nuclear missiles at Cuba. Why did that not happen? Well, it didn't happen because the United States had an agent in the Soviet Union, Penkovsky, who was able to tell the president that these missile sites, which had been seen from the air, were not armed and it would take several months before they were armed. So, the Americans were able to deal with the matter by a blockade and, in the end, the Russians drew back and the crisis was averted but, without the information, which Penkovsky gave, the Third World War could have been triggered.

Similarly, although it's not comfortable to remind ourselves of this, the fact that the Russians penetrated NATO meant that they knew that NATO's aims were defensive rather than aggressive. They were always deeply suspicious but through their penetration of NATO the Russians were able to satisfy themselves as to what the real intentions of NATO were. So, in war, spying is very, very important. But in peace time also, it helps - and we all know this, though we may not know the details - to prevent many terrorist attacks and serious crime and anybody who remembers 9/11 or 7/7, and everybody in this room will, knows that in dealing with terrorism, prevention is so much better than cure. So, intelligence collecting – spying - is crucial in our lives. So what is the borderline between good spying and bad spying? Because there is bad spying as well as good spying. How are we to draw the line?

Should we say that good spying is good when the spy is on our side? I don't think that is a satisfactory basis for drawing an ethical distinction. As Edith Cavell said, 'Patriotism is not enough'. Should we admire spies because they're brave? Well, many of them are intensely brave but, again, that's not a sufficient ethical qualification for somebody who's good. A burglar can be brave. So, I think that the best way to solve this paradox is through the analogy of the just war. When we think about war, taking life is an evil but in most of the religions of the world, it can be justified to prevent the triumph of greater evil. So I believe it is with spying. It's justified when it's necessary and it's proportionate to prevent a greater evil and when it is subject to the law - I described the laws there are in this country. So, if we think of the concept

of the just war, we may be getting closer to a resolution of our paradox. Spying outside the law or when authorised by the laws of an evil regime is evil.

But there is still a distinction between spying and war. In war - and here I quote from the book, *Just War* , by my old friends, Field Marshal Lord Guthrie and Sir Michael Quinlan: 'The just war tradition was not framed in the abstract. It represents a careful attempt, gradually and pragmatically developed over many centuries, to put some moral discipline, some humanity, into the business of armed conflict without imposing a straitjacket so rigid as completely to preclude effective action against grave wrong'. We have an international law of war, we have international agreements on the boundary of what is permissible, such as the Geneva Convention, but in the world of intelligence, despite the general principles in the United Nations Declaration of Human Rights and in the European Convention, international agreement on the ethical boundaries has not kept pace with the developments in the spying business. We are having enough trouble in this country adapting our law to the developments just in our country alone and, of course, many nations in the world do not respect the conventions on human rights.

So, many ethical problems remain and let me leave you with just a few to mull over. Firstly, is torture ever permissible as a means of extracting intelligence? I suppose we must make an exception for the theoretical case where we have someone who we know for certain knows the whereabouts of a nuclear bomb which will detonate in a few hours' time and destroy thousands, perhaps millions, of people. But leaving aside purely theoretical constructs of that sort, we have to say that torture is never justified. Torture and other means of coercion such as blackmail or bribery are not only wrong in themselves but are not likely to produce reliable intelligence. As anyone experienced in intelligence collection will tell you, the only reliable agents are those whose motive is belief in your cause.

Should we ever spy on allies? Was it morally wrong for the United States National Security Agency to bug Chancellor Merkel's mobile telephone? It was certainly very unwise because they didn't get anything useful out of it but was it morally wrong? Well, I noticed that President Obama said that he would stop it, that he would not authorise the spying on allies, but he gave himself a little get-out and I think he was right to do so. He would only authorise it when issues of national security are at stake and, in those circumstances, I think we can't rule it out.

Should some potential targets of interception be off limits because of the nature of their profession: priests, lawyers, journalists? Almost always but not if there is a reasonable suspicion that they themselves are involved in serious crime. Nevertheless, they should be entitled, in my view, to special protection. Should our citizens have greater protection than foreigners? In almost all the countries of the world, the citizens of the country have a greater protection because intelligence – gathering was a national activity against other nations and so most nations' laws are built on that premise but is that now out of date? All people have human rights and the requirement that intelligence collection should only be undertaken when it is necessary and proportionate for very limited purposes, should in my view apply to people of foreign nations and not just our own.

Then, also topical at the moment, how do commercial organisations such as Facebook, Yahoo and Google reconcile their duty to support law enforcement with their duty and interest to protect the privacy of honest citizens? The Intelligence and Security Committee, of which I was a member, examined the murder of Fusilier Lee Rigby. The only clue there was, which could have prevented that, was an internet message from one of the killers three months before the attack which said that he wanted to kill a soldier. It was only discovered after the event but could it have been discovered before and used to prevent that outrageous act? In some circumstances, communication providers do accept these obligations. They have mechanisms to close down accounts relating to child pornography and alert authorities to its perpetrators. They say that they will always comply with legal requirements. But, because there is no international consensus, they're subject to conflicting laws in the different countries in which they operate. Some of these laws, for example, in the United States where many of them are based, are designed to protect data relating to the nation's own citizens which prevents the divulging of data to the law enforcement agencies of other nations.

Since terrorism and crime are now international, likeminded countries will need to have a dialogue and to find a way of removing these conflicts in the law. There's already much work going on but it won't be easy and, of course, there are many countries which, in this respect, are not likeminded. So, many ethical and practical problems remain to be solved. Of one thing we can be certain; in our threatening world so full of dangers, in which technology enabling both communication across international boundaries between those who mean us harm and the means for its interception are developing so fast, there are going to be problems to occupy

the minds of ethicists, of lawmakers and of diplomats in relation to the collection of intelligence for many years to come. This is a challenge which will not go away.

ENDS