**Professor Iain Cameron,[1] Venice Commission, Speaking Notes European Parliament Hearing on Mass Surveillance, 7th November 2013**

I am delighted that European Parliament has asked the Venice Commission to give evidence. The main Venice Commission document of relevance to the present inquiry is the Report on the democratic oversight of the security services, adopted by the Venice Commission at its 71st Plenary Session (Venice, 1-2 June 2007). In addition to this, however, there are other reports of interest, inter alia the 2006 on rendition, and the 2008 report on control of the Armed Services.[2] I am the rapporteur for the update of the 2007 report which the Parliamentary Assembly has requested, and which will be discussed and hopefully adopted at the Venice Commission plenary session in March 2014. I will speak briefly about the 2007 Report as well as saying something about the particular problems of oversight of strategic surveillance.

As you probably know, the membership of the Venice Commission – serving and former judges in constitutional courts, former ministers of justice, professors in the field of public law and public international law - gives it a unique blend of competence. The Venice Commission has now had many years of experience of identifying what functions well in constitutional contexts, and so knowing how to go about strengthening legal institutions and political and judicial accountability mechanisms.

Our 60-page report from 2007 discusses forms and models of accountability for security services, in order to identify the strengths and weaknesses of each of them. This report has influenced the work which has been done subsequently in the field, inter alia the important principles on intelligence oversight recommended in 2010 by the UN Special Rapporteur on Terrorism and Human Rights, and

[1] Faculty of Law, Uppsala University, Sweden.

[2] All of these are available at the Venice Commission website http://www.venice.coe.int.

the European Parliament Report on intelligence oversight of 2012. The 2007 Report did not look at strategic surveillance as such. However, the update will do so, insofar as strategic surveillance impacts on internal security.

I will begin by emphasizing the problem generally for security intelligence: the vulnerability of democratic societies combined with the diffuse nature of the threats against them means that intelligence is nowadays wanted on everything which is, or can become, a danger. Unless external limits are imposed, and continually re-imposed, then the natural tendency on all security and intelligence agencies is to over-collect information. This is at the heart of the present European Parliament inquiry. Internal limits will not suffice because, while the staff of a security agency should set limits on the collection of data, it is not primarily their job to think about the damage which over-collection of intelligence can do to the vital values of democratic societies.

Here I should note that the present allegations of mass surveillance primarily concern the activities of the US and UK. So it is democratically elected politicians, as the taskmasters of the surveillance agencies, who ultimately bear responsibility for over-collection of intelligence.

Physical and administrative capacities may previously have set limits on the extent to which a security agency could interfere with peoples' human rights. However, major technological advances, particularly in data collection, retention, processing and analysis and in surveillance, have dramatically increased the capacity of a security agency in this respect. Again, this is well demonstrated by the present inquiry. Moreover, it is, obviously, not simply a question of collecting intelligence. Intelligence is collected in order to be used in a number of ways, e.g. in criminal inquiries and prosecutions, for security screening and in relation to decisions to grant citizenship or to deport aliens, and most controversially as regards the US, for rendition or drone attacks.

In simplified form, the Venice Commission report identified four different forms of State accountability beyond that of the internal,

governmental or bureaucratic level of accountability, namely, parliamentary accountability, judicial accountability, accountability to an independent expert body and complaints mechanisms. The latter two forms are supplements or replacements for the first two forms of accountability, which do not work well for security intelligence. The terms "oversight" and "oversight body" are often used to refer to accountability in different forms and to the body or bodies established to exercise the accountability functions.

The main reason why accountability is difficult in this field has to do with the special nature of security intelligence. The heart of a security agency is its intelligence files. Security data consists to a large extent of risk assessments. Unless and until the accountability mechanisms are in a position to provide a meaningful "second opinion" on the risk assessments made, they are not real safeguards, In the worst case analysis, they serve as ideological constructions, a smokescreen, justifying special powers.

But although external accountability forms are absolutely necessary, they serve mainly to back up, or strengthen, internal controls, i.e. the control exercised by the agency over itself and by permanent civil servants in government departments to which the agency is subordinated (or to prosecutors, where the agency is a security police). The staff working in intelligence and security agencies must be committed to the democratic values of the state and to respecting human rights. For this reason, the mandate of an oversight body should be broad, to cover the important issues of recruitment, training, ethical awareness etc.

The Venice Commission does not take a stand on whether there should be parliamentary accountability or expert accountability. There are different advantages and disadvantages with these, and each state must make its own decision on which is best. One can have a hybrid system, where part of the membership consists of serving or retired politicians. This works in some states where institutional factors mean that the risk of abuse is less, and so the principle of the separation of powers does not need to apply so strongly. One can also have both a level of expert accountability and

parliamentary accountability – although here it is important that the two cooperate rather than compete. There is much to be said for hybrid or expert plus parliamentary accountability solutions. The European Parliament report generally recommends both an expert and a parliamentary level of accountability. In my view, as far as strategic surveillance is concerned, the technicalities involved, and the extensive degree of international cooperation, mean that purely parliamentary oversight/accountability is not adequate.

Here I should also note that the case law of the European Court of Human Rights (ECtHR) requires, for surveillance, including strategic surveillance, some form of independent controls at both the authorisation and follow-up stages. The US experience with the Foreign Intelligence Surveillance (FISA) Court is that independent authorisation is not enough: you need a follow-up stage to check that the agency is actually complying with the terms of the authorisation. This means a permanent expert oversight body with powers to investigate proprio motu.

The report which was presented earlier today, on national mass surveillance programs carried out by EU member states, dismisses as inadequate the UK, German and Swedish oversight/accountability systems. The value of independent authorisation and the value of independent follow-up obviously depend on how tightly the law regulates the targets and methods of strategic surveillance. I would agree that the UK law is lax and the UK oversight system is poor. But the German and Swedish laws are more detailed as to what are the permissible goals of strategic surveillance. Their operations are much smaller and their systems of oversight, while certainly not perfect, are much stronger than the British system.

I have mentioned two problems with oversight of strategic surveillance, its very technical nature, requiring expert knowledge, and the accountability problems which arise from trying to control, nationally, what is in fact a network of international cooperation.

I will take up three other problems. This is not meant to be an exhaustive list, and my solutions to these problems at this stage are only tentative suggestions.

The first problem is the very negative effects which mass surveillance has on society. It might previously have been thought that intercepting and analysing traffic or "meta" data was not so great an interference with personal integrity. But our use of the internet and social media means that people leave a digital footprint which reveals a great deal about them.

If we accept that strategic surveillance is here to stay, there are a number of ways of minimizing the intervention in personal integrity.

One should limit the purposes for which strategic surveillance is used as much as possible. As mentioned, the German and Swedish laws are better in this respect than the British. But as these purposes must, of necessity, be framed in general terms, this in itself will not suffice to curb overuse.

In particular, in order to limit the risk of economic espionage, one can forbid collection on very loosely formulated grounds such as "for the economic well-being of the nation". This should be combined with a prohibition on letting the Department of Trade/Commerce task the strategic surveillance agency. Having said this, there are at least three areas of business activity where strategic surveillance is useful (in addition to whatever use in might have in guarding against offensive economic espionage directed against one's own corporations). These three areas are proliferation of weapons of mass destruction, circumvention of UN/EU sanctions and major money laundering. One can say in particular as regards proliferation, that if you have an export-oriented economy, such as the German economy, then it makes sense to keep track of where all the dual use components are going.

One can limit the amount of communication capacity which is taken at any one time. As I understand it, the German practice is not to take more than 20% of the capacity.

The second problem of strategic surveillance is the risk of errors, with deleterious effects for individuals, as a result of mixing of private data, assembled for other purposes, and without the same type of quality control, with public data. The EU legislator has grappled with this problem before, e.g. as regards Passenger Name

Records (PNR). One way to begin minimizing the risks of this is to require labelling of all data obtained as a result of strategic surveillance. The ECtHR has stressed the need for this safeguard. One should in addition require strong quality-assurance controls before such data is used to open, or add to, a file on an individual. One should also make checking of the collection, processing and retention of personal data by the strategic surveillance agency a priority for an independent oversight body. The third problem is the potential which strategic surveillance has to circumvent more rigorous controls which might exist at national law on targeted individual surveillance (telephone tapping, bugging etc.). A legal limit might exist, e.g. allowing only "international" communications to be monitored. But as a great deal of domestic communication in fact crosses an international boundary, such a legal limit can have little relevance in practice. Strategic surveillance often begins by monitoring patterns of communication, but once patterns have been established and a suspect individual or group identified (or naturally, where a target's telephone number or IP address is already known through some other form of intelligence gathering) then strategic surveillance can obviously be used to snap up the content of the identified person's, or group's, communications and internet activity.

One can, at this point, when strategic surveillance becomes individualized, require the same standards to be satisfied as exist for normal targeted investigations at domestic law. At least such standards can apply as regards surveillance of one's own nationals or residents, wherever they are physically located. One can even require subsequent notification of nationals or residents that they have been subjected to strategic surveillance, once the surveillance operation in question is concluded. This might seem – from a security perspective – bizarre. But this is a requirement of German law. Admittedly exceptions apply, but the German oversight body must in each individual case approve non-notification. Thus the notification requirement, even if it only rarely leads to actual notification, can still serve a useful function in curbing overuse,

because the strategic surveillance agency knows that every time the content of the communications of a citizen or resident has been monitored, it must inform the oversight body of this and convince it that its reasons for not subsequently notifying the person are justified.

A particular issue here, bearing in mind the close cooperation which allegedly exists between certain Western strategic surveillance agencies, is the possibility that the agency in X-land can ask the agency of Y-land to collect intelligence on an X-land citizen or resident, thus avoiding any legal limits which the X-land agency might be subject to as regards domestic intelligence operations. This particular issue can be dealt with by prohibiting, in law, the X-land agency from actively requesting other friendly agencies to collect intelligence on X-land citizens or residents. But the passive receipt of such intelligence should not be prohibited, and therein lies a difficulty, as the boundary-line between active and passive may not be so clear as one might think, when the agencies in question have "shared understandings" developed over many years of cooperation. But here, too, the boundary line can and should be policed by the independent oversight body. One can also say that, in this area, institutional rivalry can buttress such a limit: the agency responsible for internal security in X-land will, or should have, exclusive competence to engage in intelligence-gathering operations in X-land. One ought to be able to rely to some extent on the fact that this agency will jealously guard this exclusive competence.

Circumvention of national standards through international cooperation can take other forms than cooperation in targeted surveillance. Agencies apparently routinely engage in bulk transfer of data to other friendly agencies. This makes sense from the perspective of using available resources (e.g. analytical capacity) most effectively. It might be very difficult to forbid this. At the same time, the data in question obviously has left your "control". If it had been processed by the agency which collected it, it might have given rise to intelligence on individuals (citizens or residents) which the collecting agency might even be forbidden by law to transfer to

other agencies. To put the point most starkly: you do not know if it will be used as part of the targeting decision to make a drone attack. Thus, if bulk transfer is to be permitted, the arrangements for, and practice as regards it, are also things which must be kept under tight oversight.

Special oversight attention should be devoted to all intelligence which has an "individual dimension" going out of, and into, the strategic surveillance agency. The "third party" rule – which routinely applies to intelligence transfer, forbidding the recipient from communicating the intelligence to anyone else without the express permission of the communicator – cannot apply to the oversight body. Otherwise the oversight in question is of very limited use.

Another method for limiting the risk of circumvention is to allow the strategic surveillance agency to communicate intelligence to the internal security agency or police only for a limited number of serious offences. This is a requirement of German law. From a security perspective this might appear to be a waste, or as undermining public safety: intelligence on more minor offences is not being used. But it is a price which I think one should be prepared to pay, bearing in mind the very negative effects on society which mass surveillance, or even a perception of mass surveillance, will undoubtedly cause.

In general I can say that while some states may consider that security is the overriding consideration when dealing with e.g. terrorism, and that there is a conflict between efficiency in security and improved accountability mechanisms, this is not the view of the Venice Commission. Where an agency performing the security or intelligence function does not have the confidence of parliament, and the support of the public in general, it suffers from a lack of legitimacy. The cooperation from the public which is necessary for the efficient policing of a democratic society will not be forthcoming. Improved oversight is thus not in conflict with improved effectiveness in coping with terrorism and other threats to

national security but, in both the medium and long-term, an essential part of that effectiveness.

I will conclude with two specific recommendations for the European Parliament.

Obviously the European Parliament cannot decide over the US, or dictate to the US how it should write its laws. Nor can it re-draft the deficient UK legislation. What it can do is to publicize the inadequacy of the existing legislation and the deficiency of the existing oversight over security surveillance.

The European Parliament can also take a role in encouraging better security and intelligence oversight generally. There is a network of EU security oversight bodies which also includes Switzerland and Norway. The annual meetings held by this network have been a valuable forum for discussing matters of common concern (within the limits of secrecy rules), best practices in oversight etc. However, the network has no financing of its own. The European Parliament, with only a very limited expenditure of money, could host this annual meeting.

Thank you for your attention. I am happy to answer any questions you may have.