Professor Iain Cameron
Venice Commission
Speaking Notes, 28th May 2015

Council of Europe, Venice Commission Update of the 2007 Report on the Democratic Oversight of the Security Services and Report on the Democratic Oversight of Signals Intelligence Agencies, CDL-AD(2015)006

May I begin by expressing my thanks to the organisers for inviting me. I am speaking today as a member of the Council of Europe (CE) Venice Commission. The Venice Commission is the CE advisory body in constitutional and international law. The Venice Commission is the product of an open agreement, so there are non-European members. Amongst the 57 members (since 2014) is the USA. 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.

The Venice Commission produced a detailed 60 page report in 2007 setting out best practices in regulating and making accountable domestic security agencies. Together with the UN Special rapporteur's best practices from 2010 they form the best elaboration of international standards in the field. The present report from April 2015 – I was the rapporteur - is partly an update of the 2007 report, but focuses particularly on signals intelligence.

In more detail, the 2015 report:

- Explains what signals intelligence is
- Explains why, up till now, signals intelligence has been not been subject to sufficient external controls and oversight
- Explains the ways which signals intelligence impacts on privacy and other human rights, with particular reference to the case law of the European Court of Human Rights
- Discusses best national practices in regulating signals intelligence.

Both the 2007 and the 2015 reports are available on the Venice Commission website, www.venice.coe.int.

Signals intelligence impacts upon human rights (especially privacy, but also freedom of association, information and expression).
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 on collection of intelligence, and continually re-imposed, then the natural tendency on all agencies is to over-collect information. Internal limits will not suffice because, while the staff of security and intelligence agencies 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. 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, processing and analysis and in surveillance, have

dramatically increased the capacity of security and intelligence agencies in this respect.
Since the September 11 2001 terrorist attacks the budgets and manpower of many signals intelligence agencies have been increased significantly. Such rapid expansion creates various risks. The natural tendency on intelligence agencies to gather too much intelligence can be insufficiently held in check, especially if the integrity and professionalism of the staff (the main restraint on too much intelligence gathering) is weakened by political pressure.

Without the reassurance strong and well-functioning controls and oversight give, the public will have the – justified – fear that the special powers signals intelligence agencies have to deal with terrorism, proliferation of weapons of mass destruction and other threats are being abused. The secrecy which must surround intelligence and security agencies also means that the scrutiny that the media in a democracy normally provide of the effectiveness of the administration will not work in this field. Thus oversight is also a replacement for this media scrutiny.

In simplified form, the Venice Commission 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. In practice, there are hybrid forms.

Why have weaker controls applied to signals intelligence?

Not all states have a signals intelligence capacity, though all now need a defensive, cyber-security capability. In those states which have them, agencies engaged in signals intelligence tend to have the bulk of the intelligence budget, and produce most intelligence, but they have tended to have weaker systems of oversight. There are a variety of explanations for this. The first is that access to mere metadata is assumed not to seriously affect privacy. This is no longer correct.

A second, historical, explanation is the fact that international telecommunications used to be by means of radio. Expectations of privacy were generally less with radio.[1] However, the vast bulk of both national and international telecommunications is now by fibre-optic cable. Moreover, the amount of such traffic has increased enormously.

A third explanation is that strategic surveillance has grown out of military signals intelligence and is (or is intended to be) aimed at external (foreign) communications. Thus, one could argue that the impact of privacy was less, and/or that only foreigners' privacy was affected. It is true that much signals intelligence is about military threats, but the dividing line between civil and military threats is no longer clear. And as regards external communications, monitoring how one's citizens' communicate with foreigners also means monitoring one's citizens. Moreover, as regards the internet, any communication with a foreign server, or by using a foreign internet service provider, is an "external" communication. Even if attempts are made automatically to filter out communications

[1] The "reasonable expectations of privacy" test can be criticized, inter alia for making privacy contingent on technology. At least for states bound by the ECHR, no distinctions between radio and cable traffic can be drawn today.

which both originate and terminate in the national territory, the technical difficulties in separating external from internal communications mean that it is inevitable that a large number of internal communications will also be collected.

A fourth explanation for the fact that weaker controls have applied has been the technical complexity and rapid technological growth of the area. It has been difficult for politicians and lawyers to understand how strategic surveillance works, how it affects privacy and other human rights and how to go about devising appropriate checks and balances.

Fifthly, the primacy the executive has in many states in the areas of foreign policy and defence, either by virtue of the Constitution, or de facto, by virtue of its control over information in these areas, can also have contributed to the lack of legislation in certain states.

Sixthly, signals intelligence is to a significant extent an international cooperative network, and there are particular problems involved in overseeing an international network

Security priorities/the content of the mandate.

A number of issues can be raised regarding how a signals intelligence agency's mandate is formulated. How broadly or narrowly this is formulated is a crucial part of limiting the scope for abuse. The mandate of the signals intelligence agency to a large extent determines the tasks of the external control and/or oversight body or bodies. Where the mandate of a signals intelligence agency is framed very broadly to allow the collection of data concerning "relevant" "foreign intelligence" or data of "relevance"

to the investigation of terrorism, then over-collection of intelligence is very likely. Thus the mandate must be relatively tightly defined in primary legislation, and specified further in subordinate legislation. But even if primary legislation is drawn relatively tightly, there will still be considerable room for manoeuver in how this is interpreted by the body or bodies tasking the signals agency to produce intelligence, and by the staff of the signals intelligence agency itself. Laws must be converted into software, and applied by human analysts. Thus, there must be external control mechanisms to check that the legal thresholds for initiating a signals intelligence operation have been met. There must also be follow-up external oversight to check that signals intelligence operations have been carried out correctly, that information not necessary for national security purposes has been deleted, that routines are in place to balance human rights against other interests and that these routines are being properly complied with.

For states bound by the ICCPR or the ECHR, the mandate must also recognise that foreigners have privacy rights. National security cannot be seen as a carte blanche to collect intelligence on individuals and groups simply because they are foreign. There must also be thresholds which must be satisfied before intelligence can be gathered on foreigners, and these should not only be about efficiency in the use of resources.

To deal with this issue in a little more detail. The US has not been alone in operating a distinction between citizens and residents on the one hand, and non-citizens and non-residents on the other. The distinction applies to targeting, but also as regards retention, deletion and communication of data. Because of the frequency with

which communications in the modern globalized world occur between citizens and non-citizens of a particular state, more permissible standards for targeting and retention of communication that involves at least one non-citizen create the potential for abuse, as a loophole to collect information on citizens who would otherwise be protected under domestic law. With the creation of the independent executive agency, the Privacy and Civil Liberties Oversight Board (PCLOB), the US now has a relatively strong system of oversight and control of signals intelligence, which combines authorization of the general types of selectors used by the Foreign Intelligence Surveillance Court (FISC) with follow up controls by PCLOB. But the main focus of US oversight is on protecting the privacy rights of US persons. Moreover, a large portion of US signals intelligence collection is not about monitoring communications between people in the US and elsewhere, and so falls under the supervision of the FISC. Instead, interception of communications between a non-US person and another non-US person usually falls under Executive Order 12333. Independent oversight of this extremely extensive intelligence collection is confined to PCLOB.
At the same time, the global reach and power of the US should also be borne in mind: it is able to use this intelligence in different ways to affect the lives of people outside the US.

In any event, without a recognition that foreigners have some form of privacy rights, and without strong external/independent oversight of the databanks it is not possible to have any confidence that excessive amounts of personal data on foreigners are not being kept (and used in different ways).

Parliamentary supervision of signals intelligence

The 2007 report discusses in detail the advantages and disadvantages of parliamentary, as opposed to expert oversight. A parliamentary oversight body is more legitimate, as it represents the people. The disadvantage is the lack of time, expertise and – in some situations – inclination to exert adequate oversight. There are a number of reasons why parliamentary supervision of signals intelligence is particularly problematic. First, the technical sophistication of signals intelligence makes it difficult for parliamentarians to supervise without the aid of technical experts. Second, the general problem of parliamentarians finding sufficient time for oversight along with all their other duties is particularly acute as regards strategic surveillance. If one wishes to control the dynamic process of refining the selectors (as opposed to a post-hoc scrutiny), then a standing body is necessary. Thirdly, the high degree of network cooperation between certain signals intelligence agencies means an added reluctance to admit in parliamentary oversight, because leaks can damage not simply one's own agencies, but also those of one's allies. But in some states the doctrine of parliamentary privilege means that parliamentary committees cannot be security-screened, adding to an already-existing fear of leaks.

The other, crucial, factor is that signals intelligence involves an interference with individual rights. Supervision of such measures has traditionally been a matter for the judiciary. The constitutional principle of separation of powers can make it problematic for a parliamentary body to play such a quasi-judicial role.

To explain this last point in a bit more detail:, balancing of privacy and other human rights concerns against other interests comes in at

several points in the signals intelligence process, but two crucial points are when a decision is made to use particular selectors, and when human analysts decide whether or not to keep the information in question.

In all states using signals intelligence, the government, or government ministers, will be one of the taskers of the signals intelligence agency. Others can be the armed forces, law enforcement, domestic security agencies or customs. Government decisions that this, or that type of intelligence is desired or required from this or that state or region can be said to be "political" decisions. But the tasking stage can and should be separated from the authorization stage. In some states – eg the UK or the Netherlands – decisions to authorize signals intelligence are taken, formally speaking, by government ministers. However, the very limited time a Minister has to devote to such – highly complicated and technical – issues means that in practice, these authorization decisions are being taken by civil servants; they are thus administrative rather than political decisions. Moreover, the secrecy of the decisions, and the basis for them, means that there is in practice no parliamentary mechanism for holding the minister accountable.

Tasking is, or at least is often likely to be, at a relatively high level of abstraction. How to actually obtain the requested intelligence from the mass of data out on the net is a technical matter for the signals intelligence agency. A crucial part of this is the selectors used. A decision to authorize particular selectors resembles, at least in some ways, a decision to authorize targeted surveillance. Many selectors involve no significant privacy concerns. Others do. In the

latter type of case, privacy and other interests have to be balanced against the need for the intelligence which might be produced. It is not practical to separate the authorization process for selectors affecting, respectively not affecting, privacy. So, decisions to use selectors can – and, in my opinion, should - be taken by a judicial or quasi-judicial body. But as decisions on selectors involve considerable policy elements, knowledge of intelligence techniques and foreign policy are also desirable. Finding a group of people who combine all three types of competence is not easy, even for a large state. Thus, it is easier to create a hybrid body of judges and other experts.

The second type of decision which has a particular impact on human rights is the decision to retain particular personal information in the data files. This decision taken by the staff of the signals intelligence agency is of a "data protection" character, balancing different interests. This is something which should be overseen afterwards by an expert, independent administrative body. Such a body must have appropriate powers. This involves checking routines etc., scrutinizing the databases, raising questions on the exact reasons why specific personal data was retained, communicated etc.

So, the conclusion is that some form of expert body, or bodies, is necessary to control and oversee signals intelligence.

But what is left for the parliament to do?
First, it can and should decide the general rules regarding who, and under what circumstances, signals intelligence can be collected or be exchanged with other organisations (law enforcement, domestic security and signals intelligence organisations in friendly states).

Second, it can discuss security priorities: what is of sufficient importance to national security to need intelligence about. This is the type of decision which would benefit from a (closed) discussion in a political body, where different spectrums of opinion are represented. A third role is making a general evaluation of the overall effectiveness and efficacy of signals intelligence measures.
A final role for parliament is to link it in different ways to whatever independent expert body is established. Parliament has democratic legitimacy, and by making the independent expert body answerable to, and appointed by the parliament, this body can obtain an indirect legitimacy. The German model (the G10) is interesting here. The parliament can, where it thinks it necessary, defend the expert body from uninformed public criticism but also, again where it thinks it necessary, encourage it to take a more active role in oversight.

Expert authorization and oversight models

Various models exist for authorisation/oversight. The German model has a quasi-judicial authorization body, the G10 Commission, which is answerable to a Parliamentary body. The G10 Commission also oversees the data collected by signals intelligence operations. The Swedish model has quasi-judicial authorisation (a hybrid body of judges and parliamentarians) and expert oversight (performed by a different quasi-judicial hybrid body).

It is necessary to have both functions: authorization and follow-up oversight. Where separate bodies are established it is necessary to communicate the results of the oversight to the authorizing body. Otherwise, the authorizing body does not know how its authorizations are being used in practice. As regards the follow-up

oversight body, it is important to stress that it must have unrestricted access to the personal information contained in the signals intelligence agency's databanks if they are to be a meaningful safeguard.[2] The "originator" or third party rule cannot apply to the oversight body. While an expert body in this respect mainly functions to check that the signals intelligence agencies own routines on minimization etc. are functioning correctly, to do this task they must be able to do spot checks and thematic studies of the actual data. Thus, they must have their own, residual, investigative capability, preferably (as with the Dutch and Swedish oversight bodies) having direct access to databanks holding personal information.

To focus their attention, one can by law require the signals intelligence agency proactively to provide oversight agencies with certain categories of particularly sensitive categories of data. The issue of who may query the bulk data collected and for what purposes, or how data from it can otherwise be disseminated is also something which must be overseen. The trend is nowadays for "fusion centres" for data of interest to internal security. This can obviously greatly increase the size of the group who have access to personal data obtained through signals intelligence. The same can be said about using private contractors. Lax controls on acquisition, combined with lax minimization rules and lax controls on access to the data is obviously a dangerous combination. But even strong controls on acquisition and minimization will not be sufficient if

[2] See in particular the 2007 Report para 87 "Unless and until they are in a position to make a reasonably informed "second assessment", a monitoring body is not a real safeguard…" and para. 237 "Bearing in mind the crucial importance of data banks to the work of a security agency, and the already mentioned distinction between security intelligence and "hard" data … it is imperative that some such supervisory body exists in every State, and that it has sufficient powers, in law and practice, to perform control functions satisfactorily."

there is wide access to the database, because the database is likely to contain all sorts of interesting intelligence.

Abolishing signals intelligence functions is not going to be regarded as a feasible, or desirable, option by those states which have them. The Venice Commission report shows that signals intelligence can be regulated in a lax fashion, meaning that large number of people are caught up in a net of surveillance, or relatively tightly, and with relatively strong oversight, meaning that the actual infringement of individuals' privacy is more limited.

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