**Statement by Professor Ian Leigh and Mr Aidan Wills,**
**LIBE Committee 'Inquiry on Electronic Mass Surveillance of EU Citizens', Hearing on 7 November 2013**

## Introductory

Thank you for your invitation to give evidence to the LIBE Committee.

Ian Leigh is Professor of Law at Durham Law School and has a longstanding research interest in national security law, and especially the accountability of intelligence agencies.

Aidan Wills is an independent consultant on security sector governance; he previously worked on intelligence governance for six years at DCAF Geneva. He was heavily involved in the development of the *UN compilation of good practices on intelligence services and their oversight*, a member of the core drafting team of the *Global Principles on National Security and Access to Information*, and co-authored the major European Parliament study of the oversight of security and intelligence agencies in the European Union.

Together with Dr Hans Born of the Geneva Centre for Democratic Control of Armed Forces and in conjunction with the Norwegian EOS Committee we are engaged in a multi-year project on international intelligence cooperation and accountability.[1]

1. After some introductory remarks about surveillance and international intelligence cooperation and intelligence oversight, our comments will address the following questions:

   -the challenges of international intelligence cooperation for oversight bodies
   -positive steps that oversight bodies are taking with regard to cooperation
   -and recommendations for oversight of international cooperation at the national level, together with what could be done at the EU level

2. The exchange of information, joint surveillance programmes, and joint development and sharing of technologies or means to better access information are all forms of international intelligence cooperation. Allegations relating to a combination of these issues are central to the Committee's current inquiry. Our presentation will not focus on these allegations per se; we will address the current state of intelligence oversight and the difficulties that oversight bodies have scrutinising intelligence activities that include cooperation with foreign entities. In referring to oversight we are talking about oversight by institutions that are external to intelligence services and associated ministers or executive bodies. Our focus will be on standing intelligence oversight bodies, we will not address the role played by the courts or ad hoc

[1] See H. Born, I. Leigh and A. Wills (eds.), *International Intelligence Cooperation and Accountability*, (Routledge, 2011). A policy guide is to be published in 2014.

commissions of inquiry. Intelligence services'[2] internal oversight mechanisms and oversight by the executive are also important but we will not cover this subject today.

3. It is important to start by recalling that the challenge of countering trans-national threats from networks engaged terrorism, the proliferation of weapons of mass destruction and in organised crime requires intelligence services to cooperate with foreign partners. There can be no doubt that various forms of cooperation play a fundamentally important role in helping states to protect the human rights of persons under their jurisdictions.

4. Since 9/11, however, there has been an exponential increase in both the scope and scale of intelligence cooperation. The fight against international terrorism has driven a significant increase in the volume of information shared between agencies of different countries and the number of joint operations. When coupled with technological change, one result is the extent of access to communications and exchange of personal data of European citizens that the Committee is now investigating.

5. International cooperation in the field of surveillance is long established. States cooperate in the collection and analysis of intelligence as well as in the development of systems and infrastructure for these purposes. Collaboration in the collection and exploitation of signals intelligence dates back the Second World War - the best known alliance, UKUSA was developed through a series of agreements in the 1940s and 1950s. Although methods of communication and surveillance have changed dramatically, the fundamental rationales for cooperation in area of communications surveillance still apply. Intelligence services whose states have shared geopolitical interests cooperate to take advantage of their respective knowhow, geographical, technological, cultural and linguistic attributes.

6. Collaborative surveillance creates difficulties of attribution and risks of circumventing nationally based legal mandates and oversight schemes for the agencies. Specifically, intelligence and security services may receive from partners' information that they could not lawfully gather themselves. Given that surveillance infrastructure may be shared and information exchanged largely automatically, information may be received from a foreign partner without it having been explicitly requested.

7. Although many states have created systems to oversee their security and intelligence agencies there are significant differences in the forms that these take.[3] Broadly, we

[2] By 'intelligence services' we mean state bodies responsible for the collection, analysis and/or dissemination of information in the fields of national security and defence.

[3] See further: H. Born, L. Johnson and I. Leigh (eds.), *Who is Watching the Spies* (Dulles, Virginia: Potomac Books, 2005) and H. Born and M. Caparini, *Democratic Control of Intelligence Services:*

can distinguish between, on the one hand, parliamentary oversight bodies and on the other, expert oversight bodies.[4]

8. Parliamentary oversight is primarily conducted by committees with a specific mandate to scrutinise intelligence services.

9. Expert oversight bodies are neither parliamentary nor executive entities that are created exclusively for the purposes of scrutinising the work of intelligence services. An advantage of expert bodies is their ability to conduct more in-depth scrutiny than committees comprised of parliamentarians who are effectively part-time overseers. They often enjoy greater access to detailed classified information because their members are vetted and security cleared, an option that is not widely accepted as being appropriate for members of parliament.

10. Very few statutes regulating external oversight of intelligence explicitly mandate scrutiny of international intelligence cooperation, however.[5]

**The challenges of international intelligence cooperation for oversight bodies**

11. International cooperation is a challenging subject for national oversight and review mechanisms, which were designed primarily to protect against domestic abuses by security and intelligence agencies. It has become increasingly evident that many national oversight bodies are ill-equipped to hold intelligence services and related executive bodies to account for their cooperation activities. We will highlight just some of the reasons for this.

12. Overseers cannot conduct scrutiny, draw conclusions and hold people or organisations to account if they do not have access to all relevant information. Importantly, oversight based on incomplete access to information can result in misleading conclusions and may give rise to a false sense of accountability. Yet, the most formidable challenge facing overseers seeking to scrutinise intelligence activities involving cooperation with foreign entities is a lack of information.

---

Co*ntaining Rogue Elephants* (Aldershot: Ashgate, 2007. For policy studies; H. Born and A. Wills, *Overseeing Intelligence Services : A Toolkit,* (DCAF : Geneva, 2012); H. Born and I. Leigh, *Making Intelligence Accountable* (Norwegian Parliament: Oslo, 2005); UN Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Combating Terrorism 2010, *Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies,* UN General Assembly, A/HRC/14/46, 17 May 2010.

[4] European Commission for Democracy Through Law (Venice Commission), *Report on Democratic Oversight of the Security Services in Council of Europe States, Study 388/2006 (CDL_DEM 2007-001)* (June 2007); *Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies*.

[5] A rare exception is Canada's CSIS Act, which requires CSIS to provide the Security Intelligence Review Committe with copies of cooperation agreements : Canadaian Security Intelligence Service Act 1984, s. 17(2). SIRC has referred in its annual reports to several reviews of liaison at CSIS overseas stations.

13. A significant factor that can serve to limit overseers' access to information is the *third party rule* or the *control principle*, which underpins information sharing between intelligence services. This principle is very simple: information provided by a foreign entity cannot be transmitted to any third party or used for any other purpose that was not agreed upon the transfer of the information without the prior consent of the originator. This is intended to enable intelligence services to retain a measure of control over information they send to foreign partners.

14. In some countries this practice has been protected by in a nearly impenetrable wall of statutory exemptions that prevent disclosure of even procedural aspects of cooperation not just to the public but also to democratic oversight bodies.[6] In this way the third party rule can serve to undermine oversight bodies' access to information if intelligence services and/or their partners view oversight bodies as third parties so that a service would need to seek the permission of a foreign partner before its own oversight body could view information provided by that partner. A process of seeking and granting such permission from foreign partners has the potential to seriously undermine oversight.

15. Applying the third party rule to oversight bodies grants foreign services an effective veto on the scope of intelligence oversight in another state. A foreign partner may simply refuse to grant permission in order to prevent possible scrutiny of, for examples, information sharing.

16. It is doubtful, however, that oversight bodies should be regarded as third parties in this way since the primary purpose of the third party rule is to prevent the passing of shared information to the services of other countries. Some countries' oversight bodies operate on the presumption that information shared by partners with their services is shared subject to oversight.

17. Intelligence services could undoubtedly (mis)use the third party rule to shield given activities or files from external scrutiny. It is not inconceivable that – faced with a request from its overseer to view foreign information – an intelligence service could ask the question and provide the answer (no) when 'seeking' the requisite permission from that foreign partner.

18. A related issue is the significance of reputation in international intelligence cooperation. There is no doubt that some intelligence services fear that being subject to robust oversight may be viewed as vulnerability by some their foreign partners.

19. National oversight bodies are only responsible for evaluating the activities of their own country's intelligence services, including their own services' involvement in surveillance programmes. It is not their prerogative to scrutinise the actions

[6] Increasingly courts too are being faced with claims based upon the threaten of loss or withdrawal of intelligence cooperation unless they accede to demands for total secrecy.

foreign intelligence services and their governments, for which they have neither the legal mandate to nor the powers to access information. This can make it difficult for oversight bodies to get a complete picture of intelligence activities that involve foreign partners. They can only examine a given activity on the basis of information held by their own services; they cannot access foreign intelligence officials or documents.

20. Modern surveillance activity includes the use of extremely complex technology. This is particularly true of the methods used for collecting and sorting electronic information, especially when such mechanisms are part of broader collaborative surveillance systems. For many overseers it is extremely difficult to understand the functioning and capacities of such systems and, crucially, to understand their implications for human rights.

21. The treatment of international intelligence cooperation in domestic legislation varies between countries, from legislative silence[7] to broad authorisation of cooperation in the mandates of intelligence agencies, and specific requirements that must be undertaken for certain forms of cooperation. In many countries cooperation with foreign entities is viewed as a subcategory of operations and guidelines on cooperation are included in ministerial directives and internal operational policies. It is likely that the omission of the topic of international intelligence cooperation from legislation in some countries is due simply to legislators' lack of awareness in earlier of its future significance. Omission makes it harder, however, for oversight bodies to examine aspects of the topic involving the agencies under their jurisdiction.

**Positive steps to oversee international intelligence cooperation**

22. Revelations about the human rights implications of international intelligence cooperation in the context of counterterrorism have compelled some oversight bodies to examine some aspects cooperation including rendition and secret detention. Nevertheless, with some notable exceptions, intelligence cooperation remains an under-scrutinised area of intelligence services' work.[8] Oversight bodies have yet to examine in a systematic or regular manner their services' cooperation with foreign partners. We will highlight some aspects of intelligence services' international cooperation that overseers may wish to focus on.

---

[7] It is not for example, mentioned in the following: in Germany ( Act of 22 December 1990) for the Bundesnachrichtendienst (BND); in France, (Decree of 2 April 1982) for the Direction générale de la sécurité extérieure (DGSE); in Austria ( Act of 23 July 2001), for the HeeresNachrichtenAmt (HnaA); or in the Czech Republic (Act of 30 July 2004), for the Security Information Service. See P. Hayez 'National Oversight of International Intelligence Cooperation' in H. Born, I.Leigh and A.Wills (eds.), *International Intelligence Cooperation and Accountability*, (Routledge, 2011).

[8] See, for example, the comprehensive study undertaken by the Dutch Review Committee on the Intelligence and Security Services. Netherlands, Review Committee for the Intelligence and Security Services (CTIVD), *Review report on the cooperation of GISS with foreign intelligence and/or security services,* no. 22A, (The Hague, 2009).

23. In view of the serious implications that sharing personal data can have for human rights it is essential that there is external oversight of both the data exchanged and procedures relating to such exchanges. Overseers should examine factors such as whether: data exchanges comply with applicable laws (including on legitimate purposes for personal data sharing and proportionality requirements); data exchanges are properly recorded; appropriate caveats were attached to the information; and/or any assurances were sought from a foreign service. The German G10 Commission's powers, for example, cover the collection, processing and use of the personal data by the federal intelligence services. Another good example of what oversight bodies should be doing is the Norwegian EOS Committee's regular examinations of personal data exchanges. The Committee assesses who data was sent to, whether disclosures were made for lawful purposes and whether they are proportionate from a human rights perspective.[9]

24. Scrutiny of incoming information is also important. Overseers may wish to focus on the requests for information their intelligence services transmit to foreign partners. An important question in this context is whether requests made to foreign intelligence services solicit information that the service could not have lawfully gathered itself or that it could not have gathered without a warrant. Overseers may also wish to check how incoming is evaluated and marked before being stored. This treatment of incoming information is important for ensuring that any concerns about reliability or a dubious human rights footprint are recorded.

25. Overseers should also examine the way in which intelligence services conduct risk assessments before engaging in cooperation and how different risks and benefits are weighed. Oversight bodies may examine the criteria services use for these assessments; what information they draw upon; how they motivate assessments in specific cases; and whether or not assessments of foreign services comport with the conclusions of other bodies such as foreign ministries and major NGOs. The Dutch CTIVD, a non-parliamentary expert oversight body, undertook a detailed assessment of how the intelligence services conduct such assessments in the context of its extensive thematic investigations into the service's cooperation with foreign partners. The Committee looked not only at assessments of risk but also of potential benefits from cooperation.[10]

[9] Norway, EOS Committee, 'The EOS Committees oversight of information exchange with cooperating foreign services,' Memo for DCAF, August 2013; EOS Committee, *Annual Report 2011*.
[10] The Netherlands, Review Committee on the Intelligence and Security Services, *Review report on the cooperation of GISS with foreign intelligence and/or security services.* See also, Norway, EOS Committee, *Annual Report 2005.*

**Recommendations:**
**What can be done at the national level?**

26. We are of the view that national oversight bodies remain the preeminent players in ensuring that international intelligence cooperation, including collaborative surveillance programmes, is conducted in compliance with the rule of law and human rights. They alone have the mandate and (hopefully) access to information to scrutinise intelligence services. Accountability in this area can best be strengthened by ameliorating national oversight on the various sides of intelligence cooperation relationships. It is national legislatures that bear the burden of the responsibility in this regard. They must do more to assess whether oversight systems are working effectively and to ensure that oversight bodies are equipped with the powers and resources that they need. Most EU member states oversee their intelligence services through parliamentary oversight committees. If these committees are ineffective due to factors such as a lack of time, insufficient expertise or politicisation, it may be necessary to follow the lead of Belgium, the Netherlands and Sweden in creating expert oversight bodies outside parliament.

27. Responses to allegations about internet surveillance have tended to focus on the activities of intelligence services themselves and on the legal frameworks governing their work. It is, however, essential that we also use this season of inquiry to reflect on the work of oversight bodies, asking ourselves: what the purposes of oversight are, what we mean by effective oversight and how, on an ongoing, basis we intend to evaluate the efficacy of oversight bodies? The answers to these questions will no doubt vary across member states.

28. Very few states have carried out comprehensive assessments of their oversight systems and sought to inquire as to whether or not their oversight bodies and institutions responsible for the governance of intelligence services are effective. There is a pressing need to examine not only the adequacy of the legal mandates and powers of oversight bodies but to drill down deeper and evaluate the methods they use, the quality of their reporting, the adequacy of their expertise and resources.[11]

29. The danger that international cooperation may undermine human rights protections, in particular by side-stepping the balanced grant of powers by national legislators to intelligence agencies has already been referred to. Recognising the danger, a number of countries already embody safeguards

[11] Examples of formal evaluations of the intelligence governance systems include the Canadian Parliament Special Committee's Review of the CSIS Act and Security Offences Act, *In Flux but Not in Crisis,* 1990; the South African Ministerial Review Commission, *Intelligence in a Constitutional Democracy,* 2008; and the Belgian Parliament's *Evaluation du fonctionnement des comités permanents de contrôle des services de police et de renseignement*, 1995-96. For further discussion, see: Aidan Wills, 'Who's Watching the Overseers ? Ad hoc evaluations of intelligence oversight and control bodies,' in *Regards sur le contrôle: Vingt ans de contrôle démocratique sur les services de renseignement,* eds. W. Van Laethem and J. Vanderborght, (Antwerp: Intersentia, 2013).

designed to protect the fundamental rights of individuals during the course of international intelligence cooperation.

30. Reference to cooperation with foreign entities in a domestic legal framework has the advantage of conferring on intelligence services the authority to engage in necessary cooperation with foreign states and making it clear that this cooperation has democratic legitimacy. However, the limitations of a domestic legal framework for international intelligence cooperation must also be recognised. Domestic law cannot regulate the conduct of intelligence partners as such. Laws can only address concerns regarding foreign partners' adherence to the rule of law and human rights by imposing procedural requirements upon their own intelligence services. Notably, they could require specific factors to be assessed before commencing or intensifying cooperation and demand specific provisions are included in memoranda of understanding.

31. Legislative safeguards of this kind have also been advocated by the International Commission of Jurists Eminent Jurists Panel.[12] Similarly, the previous UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism recommended that domestic legislation should outline 'clear parameters for intelligence exchange, including the conditions that must be met for information to be shared, the entities with which intelligence may be shared, and the safeguards that apply to exchanges of intelligence'.[13]

32. In its 2007 Report on Democratic Oversight of the Security Services in Council of Europe States the Venice Commission has suggested that where information is received from a foreign or international agency, it should generally be held subject both to the controls applicable in the country of origin and those standards which apply under domestic law.[14] Ideally, this would mean information being subject to oversight in the country that receives foreign-derived intelligence. In some cases, a powerful state on whose supply of intelligence other countries are dependent may be unwilling to accede to such conditions. A possible workable fall-back arrangement, may, however, be to establish a system of certification- where the oversight institution in the state supplying intelligence at least warrants that it has been collected and handled according to local standards of legality.

---

[12] 'States should establish clear policies, regulations and procedures covering the exchange of information with foreign intelligence agencies. Where such procedures exist, by way of binding instruments or understandings, they should be reviewed in light of all relevant human rights standards. In particular, information should never be provided to a foreign country where there is a credible risk that the information will cause or contribute to serious human rights violations.', International Commission of Jurists Eminent Jurists Panel, *Assessing Damage, Urging Action*, (Geneva, 2009), 90.

[13] Compilation of good practice on legal and institutional and measures that ensure respect for human rights by intelligence agencies,. Practice 31.

[14] European Commission for Democracy for Law (Venice Commission), Report on Democratic Oversight of the Security Services in Council of Europe States, Study 388/2006 (CDL_DEM 2007-016) (June 2007), 39-40.

33. As discussed above, it is manifestly good practice for oversight bodies to refuse the proposition that they are third parties and that, in order to access any information provided by a foreign partner, their intelligence services need to obtain the permission of foreign partners.. When drafting statutory provisions on oversight, legislators may need to be more explicit about the fact that overseers right to access information applies regardless of its provenance.

34. Intelligence services cooperate with their counterparts in other countries, would it not be logical for oversight bodies to do the same? Would some form of international cooperation enable overseers to overcome the challenges posed by only having access to part of a relationship? At this stage, we do not think it is realistic to envisage joint investigations or the direct sharing of classified information by overseers. This would raise a host of legal issues and could serve to seriously undermine oversight bodies' scrutiny of their own services. A more promising option may be for oversight bodies to engage in what might be termed 'mutual oversight assistance.' Oversight bodies request foreign counterparts to examine particular issues and then share unclassified conclusions. An overseer could request (or recommend) their counterpart(s) to examine a particular form of cooperation, such as a joint surveillance programme, from 'their' side of their relationship. Overseers could use such collaboration to raise concerns about which their counterparts may not be aware. This may trigger additional scrutiny and, ultimately, rule/policy changes in the other state.

**What can be done at the EU level?**

35. We recommend that the European Parliament can continue to play a role in convoking meetings of national parliamentary committees responsible for overseeing intelligence overseers. These fora provide an opportunity to exchange ideas on approaches to oversight. The European Parliament (and this Committee in particular) may also play a role in promoting minimum standards and good practices on intelligence oversight. In this regard, the UN compilation of good practices and recommendations of the Venice Commission provide excellent benchmarks.

36. We do not see scope for ongoing joint meetings to evolve into to a forum for actually conducting oversight – legitimate concerns about national sovereignty and the protection of information mean that it remains unlikely that any kind of joint oversight will emerge.