LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens

Hearing, European Parliament, 14 October 2013

Statement by Professor Martin Scheinin (EUI), formerly UN Special Rapporteur on human rights and counter-terrorism, currently leader of the FP7 consortium SURVEILLE (Surveillance: Ethical Issues, Legal Limitations, and Efficiency)

Speaking notes (see, also***, Supporting documents)***

1. International law and the issue of electronic mass surveillance

Most of the technical details about the programmes for the collection of communications data, including internet data, by the United States of America (including the NSA) and the United Kingdom (including the GCHQ) are yet incomplete, even if the so-called Snowden revelations and their further substantiation by investigative journalists provide sufficient factual information[1] for a legal assessment as to the compliance with international law by the two countries just mentioned.

The short answer to the question of lawfulness is that both the United States and the United Kingdom have been involved, and continue to be involved, in activities that are in violation of their legally binding obligations under the International Covenant on Civil and Political Rights of 1966. The Covenant (or the ICCPR) is one of the main United Nations human rights treaties, binding upon 167 states in the world. It includes a specific provision that prohibits *unlawful or arbitrary interference* with anyone's privacy. While the Covenant in many respects mirrors the European Convention on Human Rights (1950), which in fact was based on an early draft of the Covenant, there are also important differences between the two treaties, including the explicit use of the term 'privacy' in the ICCPR, and certain structural differences compared to article 8 of the ECHR.

Neither the United States nor the United Kingdom have accepted the right of *individual complaint* under the Covenant, which would allow the pertinent quasi-judicial body of independent experts, the Human Rights Committee, to assess whether the country violated the Covenant in respect of a specific individual. There are, nevertheless, two other mechanisms through which the same Committee can address treaty compliance by these two countries. Both have accepted the procedure for *inter-state complaints* under article 41 of the Covenant. Even if this procedure has never been resorted to, the current context

[1] Refrence is made to Caspar Bowden, The US National Security Agency (NSA) surveillance programmes (PRISM) and Foreign Intelligence Surveillance Act (FISA) activities and their impact on EU citizens' fundamental rights. Briefing note produced for the European Parliament 2013.

of two Western democracies involved in what appears to be a massive interference with the privacy rights of EU citizens (and others), coupled with the unavailability of individual redress, would provide an instance where EU countries should seriously consider triggering the inter-state complaint procedure. Independently of that option, both countries are subject to the single mandatory monitoring mechanism under the Covenant, the duty to submit *periodic reports* for the consideration by the Human Rights Committee which will in its Concluding Observations assess compliance or non-compliance. By coincidence, the United States is up for such review later *this week*,[2] and the United Kingdom *next year*.

2. Why are the United States practices in breach of ICCPR Article 17?

The central privacy provision in the ICCPR is brief, as it for instance lacks a fully articulated test for permissible limitations. But this does not mean that there would not be a clear and binding legal norm, capable of being applied through institutionalised practices of interpretation and the resulting interpretations gradually accumulating as *subsequent practice,* explicitly or tacitly accepted by the states parties.

ICCPR Article 17 prohibits *arbitrary or unlawful interference* with anyone's privacy or correspondence, and it establishes for all states parties a positive obligation to create a legal framework for the effective protection of privacy rights against interference or attacks, irrespective of whether such interference or attacks come from the state itself, foreign states, or private actors.

In 1988, indeed already a quarter of a century ago, the Human Rights Committee adopted a General Comment (No. 16) on Article 17. Usually General Comments codify the Committee's interpretations of a specific treaty provision, based on earlier practice including the consideration of state reports and of individual complaints. By 1988 such material under article 17 was quite limited and therefore the General Comment could not possibly address all current concerns related to privacy rights.

As UN Special Rapporteur on human rights and counter-terrorism (2005-2011), this speaker issued an annual report to the main intergovernmental human rights body of the United Nations, the Human Rights Council, of direct relevance for the current inquiry. The thematic report on the right to privacy in the fight against terrorism was considered by the Human Rights Council in March 2010.[3] The report includes a proposal that the Human Rights Committee would replace

[2] The Committee's questions to the United States include a relevant one (No. 22), and the written answer given by the US government (para. 115, in particular) is manifestly inadequate. See the Supporting documents of this statement.
[3] The right to privacy. Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin (A/HRC/13/37, December 2009).

its existing General Comment on Article 17 with a new one, building upon the work of the Committee since 1988.[4]

Based upon the text of article 17 of the ICCPR, the old General Comment, as well as other practice by the Human Rights Committee (including on individual complaints under article 17, as well as a parallel General Comment No. 27 on article 12 related to freedom of movement), the report presents an analytically rigorous test for permissible limitations upon privacy rights (including data protection). This test includes the following cumulative conditions for the determination whether an interference with privacy rights is justified, or whether it amounts to a violation of the ICCPR:

(a) Any restrictions must be provided by the law;
(b) The essence of a human right is not subject to restrictions;
(c) Restrictions must be necessary in a democratic society;
(d) Any discretion exercised when implementing the restrictions must not be unfettered;
(e) For a restriction to be permissible, it is not enough that it serves one of the enumerated legitimate aims; it must be necessary for reaching the legitimate aim;
(f) Restrictive measures must conform to the principle of proportionality; they must be appropriate to achieve their protective function; they must be the least intrusive instrument amongst those which might achieve the desired result; and they must be proportionate to the interest to be protected; and
(g) Any restrictions must be consistent with the other rights guaranteed in the Covenant.[5]

It is submitted here that the application of this test results in the conclusion that the electronic mass surveillance by the NSA, as divulged through the so-called Snowden revelations and to a certain extent confirmed by US authorities, did result in breaches of the legal obligations of the United States under ICCPR Article 17 and cannot be justified as permissible limitations. In other words, the surveillance constituted an unlawful or arbitrary interference with privacy or correspondence. This assessment follows independently from multiple grounds, as most of the NSA's mass surveillance programmes fail to comply with several separate elements of the permissible limitations test. While each and every one of those failures may not be applicable to all elements of the separate programmes within the NSA's electronic surveillance architecture, it is to be emphasized that under a proper permissible limitations test one failure is enough to result in a negative conclusion.

Ad a): On the basis of publicly available information, it is possible to conclude that the whole mass electronic surveillance architecture of the NSA generally fails already on the grounds that in order to be permissible, any interference into privacy rights would require a proper *legal basis*. This is not the case. The surveillance has been based on vague and broad provisions of the Foreign

[4] Idem, paras. 19 and 74.
[5] Idem, para 17.

Intelligence Surveillance Act (FISA). While the requirement of a legal basis for restrictions does not always require parliamentary legislation as the only acceptable form of such legal basis, and therefore judicial case law can in principle supplement vague or ambiguous legislation and allow an assessment that -- all things considered -- a proper legal basis existed, this cannot be extended to a situation where neither the publicly available law (FISA) nor the secret case law by a secret court provides to individuals accurate and precise information about the situations where their privacy and correspondence might be subject to surveillance. Accessibility and foreseeability of the legal basis are fundamental elements of the requirement of proper legal basis, so that individuals are able to adjust their conduct to the requirements of the law.

Ad b): In the field of privacy it is possible to discuss a distinction between intrusions into the *core area of privacy*, where no restrictions should be allowed, and more peripheral areas where permissible limitations are legitimate. For instance, certain categories of sensitive personal information (health, sexuality etc) or certain highly sensitive relationships (lawyer-client, priest-parishioner, husband-wife) can be referred to as realms where the core of privacy is at issue. In the context of communications surveillance, a distinction can be made between metadata and content, so that surveillance about the existence, the location, and the timing of communication between two persons could be more legitimately (and with lesser safeguards) made subject to surveillance than accessing the actual substantive content of the communication in question. While this traditional argument as such still has some merit, it does not mean that *any* collection and analysis of metadata would *always* be permissible as it merely relates to the periphery of privacy. The more systematic, wide and sophisticated the collection, retention and analysis of metadata becomes, the closer it moves towards the core of privacy, so that in the end comprehensive collection and analysis of 'mere' metadata can be used to interfere in the core of privacy, for instance divulging the sexual orientation of the person by analysing his personal contacts, the locations he visits and his internet browsing profile. Hence, the sophistication of the NSA's mass surveillance programmes allows the conclusion that already the degree of intrusion through the mass collection of metadata affected the inviolable core of privacy. Equally important, the surveillance was not limited to metadata but metadata analysis was often just a filtering mechanism to identify persons whose content data would also be accessed. Besides, when a person was not identified as being protected by US constitutional law principles of privacy, his or her content data was a legitimate target even without any prior filtering.

Ad c and e): The mere breadth and width of the NSA e-surveillance architecture, coupled with the publicly available results achieved, towards the actual prevention of terrorism or other crime, justifies the conclusion that the programmes, as operated, were not *necessary in a democratic society*. Undoubtedly the prevention of terrorism or other serious crime is a legitimate social aim that could justify some degree of privacy intrusion. But that degree of intrusion must be assessed through the actual benefit towards such prevention, so that it can be shown necessary for achieving the goal. Furthermore, parts of the NSA e-surveillance architecture fail the permissible limitations test already

because of the absence of a legitimate aim: FISA authorises surveillance not only for the prevention of terrorism but also for the purpose of serving the 'conduct of the foreign affairs' of the United States. This is a legitimate national interest to be pursued by lawful means that do *not* interfere with human rights but *not* a pressing social need that would justify interference with the privacy of ordinary people.

Ad d): Broad and vague laws, such as FISA, leave room for *unfetterd discretion* unless coupled with effective oversight. On the basis of information in the public domain,[6] it must be assessed that both judicial and parliamentary mechanisms of oversight failed in keeping the surveillance authorised by FISA under any effective oversight that could prevent abuses.

Ad f) : The depth and breadth of NSA surveillance, coupled with the very limited benefit towards actual prevention of terrorism (or any other legitimate aim), shows that the resulting privacy intrusion was *disproportionate* when compared to the true benefits obtained. The failures to provide any privacy protection to non-citizens in the first place, as well as the use of up to three "hops" in establishing connections between individuals as grounds for targeting them for surveillance, and the outcome of large numbers of totally innocent people being targeted, support the conclusion that the programmes fail under the proportionality requirement.

Ad g): Finally, as the NSA mass surveillance architecture was based on broad and vague laws, was not subject to proper oversight and did not include a proper guarantee of proportionality, it was open for abuse, including discriminatory application resulting in violations of *other human rights* besides the right to privacy. For instance, the right to non-discrimination, freedom of expression, freedom of association and freedom of movement would in many cases be affected without proper justification.

There is one further issue in the assessment of the NSA programmes under the legally binding standards of the ICCPR, related to the US position that its own constitutional protection of privacy extends to foreigners only to a limited extent and not at all when they happen to be outside the territory of the United States of America. The United States may entertain a similar position as to the territorial scope of its ICCPR obligations, with reference to ICCPR Article 2, paragraph 1, which establishes the general obligation of a state party "to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant". Seemingly, the provision would establish the double requirement that the person is *both* within the geographical territory of the country *and* subject to its effective jurisdiction as a precondition for ICCPR protections. This would, however, be a misperception. Right from the very beginning the Human Rights Committee has in its practice acknowledged

[6] See, *Court: Ability to police U.S. spying program limited*, Washington Post 16 August 2013; *Lawmakers say obstacles limited oversight of NSA's telephone surveillance program*, Washington Post 11 August 2013.

the extraterritorial effect of the ICCPR,[7] and the fairly recent codification of the Committee's practice in the form of General Comment No. 31 on Article 2 confirms this position.[8]

Above, the permissible limitations test under ICCPR Article 17 was applied to the architecture of NSA mass surveillance programmes on a rather general level. Due to the multiple dimensions on which the separate programmes within the overall architecture fail to meet the various requirements under the test, it was easy to conclude that the United States is in breach of its legally binding ICCPR obligations. A detailed assessment of the various programmes within the NSA mass surveillance architecture, and of the whole range of technological solutions applied to conduct the surveillance in question, would require more factual information than was utilised for this statement. The *Matrix of Surveillance Technologies*, developed in the current FP7 project SURVEILLE, demonstrates a methodogy that could be applied for such detailed assessment.[9] The most important parameters for that methodology are a semi-quantitative assessment of the importance of a fundamental right in a given context (with scores 1, 2 or 4) and an analogous semi-quantitative assessment of the depth of intrusion into the fundamental right (again, with scores 1, 2 and 4). These two factors are multiplied with each other and then with scores related to the reliability of the assessment and the existence or non-existence of judicial authorisation for the intrusion. This methodology allows for a comparison between various forms of interference with human rights through scores ranging from 0 (no interference) to 16 (maximal interference, by definition amounting to a violation of the fundamental right in question).

3. Recent and current developments at United Nations level

In addition to the articulation of a permissible limitations test under ICCPR Article 17 and the initiative of a new General Comment, the 2009 privacy report by this speaker as United Nations Special Rapporteur on human rights as counter-terrorism included a proposal that the intergovernmental United Nations human rights body, the Human Rights Council would initiate a global declaration on data protection and data privacy, as a 'soft law' complement to the 'hard law' in the area.[10]

---

[7] See, *Lopez Burgos v. Uruguay* (Communication 52/1979).
[8] General Comment No. 31, adopted by the Human Rights Committee in 2004, paraphrases the relevant part of Article 2, paragraph 1, as follows: "10. States Parties are required by article 2, paragraph 1, to respect and to ensure the Covenant rights to all persons who may be within their territory and to all persons subject to their jurisdiction."
[9] SURVEILLE (Surveillance: Ethical Issues, Legal Limitations, and Efficiency), Deliverable 2.6, Matrix of Surveillance Technologies. See, www.surveille.eu
[10] The right to privacy. Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin (A/HRC/13/37, December 2009), para 73.

Another area where my earlier work as Special Rapporteur is of relevance is the question of compliance with human rights by intelligence agencies and of improving intelligence oversight. An annual thematic report,[11] and a subsequent complementary report identifying 'good practice' in the area were produced.[12] This line of work,[13] conducted in close collaboration with the think-tank DCAF (Geneva Centre for the Democratic Control of Armed Forces) has inspired the subsequent elaboration of the Global Principles on National Security and the Right to Information ("The Tshwane Principles" of 2013)[14], recently endorsed by the Parliamentary Assembly of the Council of Europe.[15]

As to the use of electronic mass surveillance to counter terrorism, it may be noted that the current UN Special Rapporteur on human rights and counter-terrorism, Mr Ben Emmerson, QC, did not, at least in his initial response to the revelations by Edward Snowden, see internet and telecommunications surveillance as a priority issue under his mandate.[16] That said, it is quite remarkable that the UN High Commissioner for Human Rights, Mrs Navi Pillay, came out one month later loud and clear in stressing the importance of the issue.[17]

---

[11] The role of intelligence agencies and their oversight in the fight against terrorism. Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin (A/HRC/10/3, February 2009).

[12] Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight. Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin (A/HRC/14/46, May 2010). For instance, Practice 18 in this compilation includes a formulation of so-called whistleblower protection: "… Members of intelligence services who, acting in good faith, report wrongdoing are legally protected from any form of reprisal. These protections extend to disclosures made to the media or the public at large if they are made as a last resort and pertain to matters of significant public concern."

[13] See, Aidan Wills, Mathias Vermeulen et al., Parliamentary Oversight of Security and Intelligence Agencies in The European Union. Study for the LIBE Committee. European Parliament, Brussels 2011.

[14] See, http://issat.dcaf.ch/Community-of-Practice/Resource-Library/Policy-and-Research-Papers/GLOBAL-PRINCIPLES-ON-NATIONAL-SECURITY-AND-THE-RIGHT-TO-INFORMATION-THE-TSHWANE-PRINCIPLES

[15] PACE Recommendation 2024 (2013), National security and access to information (2 October 2013).

[16] "The debate which has been generated by these disclosures is therefore timely. But there have been, and continue to be, far more egregious human rights violations in the counter-terrorism sphere, assuming that wholesale data-mining is indeed a human rights violation in the first place." (Press release of 11 June 2013 by Mr Emmerson)

[17] "Mass surveillance: Pillay urges respect for right to privacy and protection of individuals revealing human rights violations" (Press release of 11 July 2013),

In April this year, another UN Special Rapporteur, Mr Frank La Rue entrusted with the mandate of freedom of expression, elaborated on the theme of digital surveillance and its impact on freedom of expression and strongly endorsed the proposal of a new General Comment on ICCPR article 17.[18]

On 20 September, the German government was one of the conveners of a so-called side event during a UN Human Rights Council session in Geneva, to discuss the challenges of digital surveillance programmes.[19] The German proposal of a new Additional or Ameding Protocol to the ICCPR, as well as the above-mentioned proposal of a new General Comment under existing ICCPR article 17, were discussed. The German proposal was discussed, and supported, also by a major conference of data protection and privacy officials, convened in Warsaw in late September.[20]

As already mentioned, in some days from now (17-18 October), the Human Rights Committee will consider the periodic report of the United States. The Committee has presented a pertinent line of questions on NSA surveillance, and the US has already provided a written response, to be complemented by an oral hearing this week. The Concluding Observations by the Human Rights Committee are expected on 1 November 2013. They may provide an assessment of US compliance with ICCPR article 17, the Committee's recommendations to the US, and possibly also new elements for the discussion on the need for a new Protocol or a new General Comment on e-privacy.

4. Recommendations for action by the European Parliament

The Parliament is recommended to analyse the forthcoming Human Rights Committee Concluding Observations on the United States, expected to be released on 1 November and to contain a compliance assessment under Article 17 of the ICCPR.

---

http://www.un.org/apps/news/story.asp?NewsID=45399&Cr=asylum&Cr1=#.UeEabhZ97ww
http://www.ohchr.org/EN/NewsEvents/Pages/Media.aspx?IsMediaPage=true&LangID=E

[18] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue (A/HRC/23/40, April 2103), para 98. See, also, para. 29 where La Rue takes the position that the permissible limitations test, as presented and applied in this statement is appropriate in the context of the right to privacy.

[19] https://www.eff.org/deeplinks/2013/09/united-nations-meets-thirteen-principles-against-unchecked-surveillance (20 September 2013)

[20]http://www.slate.com/blogs/future_tense/2013/09/26/article_17_surveillance_update_countries_want_digital_privacy_in_the_iccpr.html

The Parliament is recommended to consider the pros and cons of one or more EU Member States resorting to the inter-state complaint procedure against the United States, provided by Article 41 of the ICCPR.

The Parliament is recommended to give its support to the elaboration of a new General Comment by the Human Rights Committee on ICCPR Article 17, not because there would not be a legally binding norm in Article 17 itself but in order to give specific guidance to states in the proper understanding and application of the right to privacy, including its operation in the digital sphere and across national borders.

The Parliament is recommended not to dismiss the German initiative of an Additional or Amending Protocol to the ICCPR, provided that a discussion on such an option creates a platform for broad debates on the status of international law in the matter, without providing to anyone an excuse to suggest that current ICCPR Article 17 would not already provide a legally binding norm in the matter.

The Parliament is recommended to keep itself informed of domestic and European efforts to address the involvement of the United Kingdom and its GCHQ in massive intrusions into the privacy of EU citizens,[21] with a view to determining the need for its own action.

The Parliament is recommended to pursue its earlier line of work in the issue of intelligence oversight in Europe, both at national and EU level.

The Parliament is invited to express its support to the continued funding, including under Horizon 2020, of multidisciplinary research related to the right to privacy, the right to the protection of personal data, and the challenges posed by surveillance and evolving surveillance technologies. Such research should combine assessment of technical effectiveness and efficiency, cost-efficiency, perceptions amongst European citizens, ethical concerns and, last but not least, the limitations upon surveillance stemming from full compliance with the fundamental rights of the individual.

[21] On 3 October, a complaint was filed by certain non-governmental organizations with the European Court of Human Rights against the United Kingdom, basically alleging a violation of ECHR article 8 through UK's involvement in digital mass surveillance, see http://arstechnica.com/tech-policy/2013/10/european-organizations-file-lawsuit-against-uk-over-vast-digital-surveillance/ (3 October 2013).