Parliamentary Assembly
Assemblée parlementaire
http://assembly.coe.int

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Declassified*
AS/Jur (2014) 02
23 January 2014
ajdoc02 2014

Committee on Legal Affairs and Human Rights

"Massive Eavesdropping" and "Additional Protocol to the ECHR on Protection of whistleblowers"

Draft Introductory memorandum

Rapporteur: Mr Pieter Omtzigt, Netherlands, Group of the European People's Party

1. Introduction

1. On 6 November 2013, the Committee on Legal Affairs and Human Rights appointed me as Rapporteur for two inter-related subjects: "Massive Eavesdropping"[1] and "Additional Protocol to the ECHR on Protection of whistleblowers"[2]. In order to start work on these important topics as soon as possible, I asked the Committee, at the same meeting, for its authorisation to invite the eavesdropping whistleblower Edward Snowden to Strasbourg for a hearing before the Committee during the January 2014 part-session of the Assembly. The Committee, following a stimulating round of discussion, invited me to first present the usual "introductory memorandum" presenting the scope of the future report(s), the current state of affairs and the fact-finding methods I intend to use in order to complete my report. The present memorandum is intended as my response to this request and as a basis for the continuation of our discussion. It shall cover the first phase of both my rapporteur mandates: to present my understanding of the scope of the mandates, to take a first look at existing and ongoing work done elsewhere, and to propose appropriate fact-finding activities. Given the number and importance of the issues that fall under the two mandates, I wish to propose to the Committee that I present two separate final reports and draft resolutions and/or recommendations for the two subjects. In other words, a separate report for each subject.

2. Massive eavesdropping and whistleblowing – two subjects linked by one person: Edward Snowden

2. Mr Snowden's action obviously plays an important role for both subjects: he has disclosed detailed information on mass surveillance carried out by the NSA and others, thus triggering a massive public debate on privacy in the internet age. At the same time, the manner in which he has made his disclosures has also re-ignited the discussion on the protection of whistleblowers. This said, I agree with the majority of the speakers during our first round of discussion on 6 November 2013 that neither the one nor the other subject is intended to become a report about the person of Mr Snowden. But we cannot close our eyes to the fact that it was Mr Snowden whose disclosures have triggered the public debate on the protection of privacy in which we intend to participate in the first report, and that his case provides a particularly interesting example for the kind of balancing of interests underlying the rules on the protection of whistleblowers, which we intend to look into in the second report.

* Document declassified by the Committee on 28 January 2014.
1 Motion for a resolution doc. 13288 of 6 August 2013.
2 Motion for a resolution doc. 13278 of 5 July 2013.

3. The scope of the future reports

3.1. Massive eavesdropping (Mass surveillance)

3.1.1. Overview

3. As to the title of our first subject, I would prefer the term of "mass surveillance" over that of "massive eavesdropping". The former is a neutral description of the activity we intend to look at whereas the latter has a polemic, pejorative undertone.

4. On this subject, I should like to present the information available on the extent and nature of the surveillance that we are all subjected to, potentially or actually, as users of modern communications such as cell phones, email and social networks. Much of this information is already in the public domain, following the disclosures of Mr Snowden[3]. Additional details, for example regarding the extent to which the NSA has been cooperating with its counterparts in Europe, are still becoming known[4].

5. I should then like to look into the consequences of mass surveillance, from two perspectives:

(1) The human rights perspective: the impact of mass surveillance on the rights and freedoms protected under the European Convention on Human Rights (ECHR), and
(2) The perspective of international cooperation (in particular, the transatlantic partnership between the United States and her European allies).

6. Last but not least, I should like to reflect on possible solutions to minimize the negative consequences of mass surveillance and the contribution the Council of Europe might be able to make to this effect.

7. This is an ambitious project, and in view of the limited resources available to this Assembly, I intend to make the best possible use of existing expertise and of work already done, in particular at the level of the European Union (European Parliament and European Commission).

3.1.2. Information on the nature and extent of mass surveillance

8. Surveillance as a tool of law enforcement and of intelligence has existed as a means to detect and expose ordinary criminals as well as threats to national security. Such threats are very real, and intercepting communications (SIGINT in NATO shorthand) is a valuable tool in the hands of law enforcement and security services. But over time, the nature of surveillance has changed: originally, surveillance of communications targeted individual suspects. It required court orders based on concrete, individualised grounds for suspicion and was only authorised if it was necessary to expose the suspect and if the infringement of privacy was proportionate to the seriousness of the suspected crime or the intelligence purpose. No third parties other than those who communicated with the suspect were implicated. Nowadays, in actual practice as disclosed by Mr Snowden, enormous quantities of communications from millions of people are intercepted and stored, and then the resulting database is searched for information related to certain suspects, all without weighing the benefits for legitimate purposes against the infringement of the privacy of millions of innocent persons. This shift has taken place, in most countries[5], without a real public debate.

---

[3] See: http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1.

[4] According to Alan Rusbridger, the Guardian's editor in chief, only 1% of the 58 000 files obtained from Mr Snowden have been published to date. Questioned in the UK House of Commons Home Affairs Select Committee if 1% of the files had been published, Mr Rusbridger reportedly replied: "That's approximately correct. We continue to publish stuff, it's about 1% of what we were given." (cf. http://uk.news.yahoo.com/mps-quiz-guardian-editor-snowden-030446879.html).

[5] One exception is Germany, where a law widening the scope of surveillance ("Grosser Lauschangriff"), led to the resignation, in 1995, of then Federal Minister of Justice Sabine Leutheusser-Schnarrenberger, who subsequently attacked this law successfully in the Federal Constitutional Court (link to the judgment, in German: https://www.bundesverfassungsgericht.de/entscheidungen/rs20040303_1bvr237898.html). Ms Leutheusser-Schnarrenberger came back as Federal Minister of Justice in 2009 and in her new position blocked the implementation, by Germany, of the EU Data Retention Directive on storage of communications data without grounds for suspicion. The NSA scandal was also an important topic during the recent election campaign in Germany, and the revelation that the Chancellor's own cell phone was subject to NSA surveillance created a public outrage even among conservative politicians and commentators, who had until then shown less interest in data protection issues (see for example http://www.washingtonpost.com/blogs/worldviews/wp/2013/10/23/obamas-phone-call-with-angela-merkel-

9. To sum up, the following information on the extent of mass surveillance is now in the public domain:

3.1.2.1. "Metadata"

10. "Metadata" is information about the time and location of a phone call or email, as opposed to the contents of those conversations or messages. The first Snowden document published by "The Guardian" was a secret court order showing that the NSA was collecting the telephone records of millions of US customers of Verizon, one of the largest American telecoms providers. Those who defend unfettered metadata collection[6] do not consider this activity as surveillance at all. Others strongly disagree, even with the very use of the term "metadata" (which simply means data describing other data), preferring the term of "summaries" or "abstracts". "Metadata" is a concise, compact representation of the intercepted communication and includes personal information, which can serve to build an even more detailed "profile" of a person than listening into actual content.

3.1.2.2. Upstream data collection: BLARNEY, FAIRVIEW, OAKSTAR and STORMBREW

11. Much of the world's communication traffic passes through the United States or the United Kingdom, its close ally. This "home-field advantage" allows the NSA to intercept traffic flowing into and across the United States. Documents released by Snowden show that the respective surveillance programs (codenames above) function through "partnerships" with major US telecom and internet companies, some of which go back decades. The division inside the NSA dealing with collection programs through private companies is Special Source Operations (SSO), described in documents leaked by Mr Snowden as the "crown jewels" of the NSA.

3.1.2.3. The United Kingdom too: GCHQ's TEMPORA programme

12. The Snowden documents also revealed the existence of TEMPORA, a program established in 2011 by GCHQ (Government Communications Headquarters) that intercepts a large amount of phone and internet traffic by tapping into fiber-optic cables. GCHQ shares most of its information with the NSA.

3.1.2.4. "Five Eyes" and beyond: an almost trusting intelligence sharing partnership

13. The "Five-Eyes" intelligence sharing alliance (including the United States, the United Kingdom and Australia, New Zealand and Canada), based on the 1946 UKUSA Signals Intelligence Agreement foresees that the allied intelligence agencies do not spy on one another's citizens without permission. Such permission was generally limited to persons suspected of wrongdoings. A 2007 secret agreement between the United States and the United Kingdom (according to documents leaked by Mr Snowden[7]) changed the rules: the NSA was allowed to analyse and retain any British citizen's mobile phone and fax numbers, emails and IP addresses "swept up" by its "dragnet". The NSA can look up to three "hops" away from a target of interest – i.e. examine the communications of a friend of a friend of a friend.[8] Previously, such "by-catch" (i.e. incidentally collected data on individuals who were not the initial targets of surveillance and thus not suspected of wrongdoing) had to be deleted from the NSA databases ("minimized").

14. A (separate) draft memorandum leaked by Mr Snowden, entitled 'Collection, Processing and Dissemination of Allied Communications', has different classification levels, paragraph by paragraph. A paragraph, cleared to be shared with the Five-Eyes partners ("second party" countries), refers to the common understanding that both governments will not target each other's citizens. But the next – classified as not to be shared with foreign partners ("noforn") – states that governments "reserved the right" to conduct intelligence operations against each other's citizens "when it is in the best interests of each nation." The draft memorandum continues that "under certain circumstances, it may be advisable and allowable to target second party persons and second party communications systems unilaterally,

---

sounds-like-it-was-horribly-awkward/; http://www.spiegel.de/politik/deutschland/merkel-verlangt-von-usa-aufklaerung-der-nsa-affaere-a-934229.html; http://www.focus.de/politik/ausland/spaehaffaere-merkel-weitet-sich-aus-nsa-dementiert-obama-sprach-mit-nsa-chef-alexander-nie-ueber-merkel-ausspaehung_aid_1141205.html).

[6] For example U.S. Senator Dianne Feinstein, chair of the Senate intelligence committee (quoted by USA Today http://www.usatoday.com/story/opinion/2013/10/20/nsa-call-records-program-sen-dianne-feinstein-editorials-debates/3112715/).

[7] See James Ball, "US and UK struck secret deal to allow NSA to 'unmask' Britons' personal data", The Guardian, 20 November 2013.

[8] According to the Guardian's analysis, "three hops" for a typical Facebook user could pull the data of more than 5 million people into the dragnet.

when it is in the best interests of the US and necessary for US national security." Neither the leaked document itself nor officials contacted by "The Guardian" have indicated whether the draft memorandum has actually been implemented. But it has been revealed that communications of top leaders of traditional US allies such as German Chancellor Angela Merkel were indeed intercepted.[9]

3.1.2.5. Downstream collection: the NSA's PRISM programme

15. PRISM – according to the Snowden documents the biggest single contributor to the NSA's intelligence reports – is a "downstream" programme, which means that the NSA collects the data from US internet companies such as Google, Facebook, Apple, Yahoo and others. When "The Guardian" and the "Washington Post" revealed the existence of PRISM, the companies denied all knowledge of it and insisted that any cooperation with the intelligence agencies was compelled by law. The above-mentioned "Guardian" website[10] features a leaked document revealing the number of intelligence records being generated per company (Yahoo ranking at the top, followed by Microsoft and Google, for the period from June to July 2010).

3.1.2.6. "Brute force", "backdoors", "Trojans" and compromised hardware: how NSA and GCHQ defeat internet privacy and security[11]

16. According to documents leaked by Mr Snowden and revealed by "The Guardian" and others, NSA and GCHQ have successfully circumvented encryption protocols relied on by internet users to protect their personal data, online transactions and email traffic. The methods used include insuring NSA control over international encryption standards, the use of "brute force" by applying supercomputers for code breaking and collaboration with technology firms and internet service providers providing "backdoors", i.e. secret vulnerabilities, to subvert commercial encryption software. According to the leaked documents, an NSA programme against encryption made a major breakthrough in 2010, making "vast amounts" of data collected through internet cable taps "exploitable". The leaked briefing refers to consumers as "adversaries": it notes that the "design changes make the systems in question exploitable through Sigint collection […]. To the consumer and other adversaries, however, the systems' security remains intact." Technology companies insist that they work with the intelligence agencies only when legally compelled to do so.[12] According to the information leaked to "The Guardian", total spending on "Sigint enabling" since 2011 has topped USD 800 million. By comparison, PRISM comes cheap, at a cost of USD 20 million per year.

17. Another NSA programme disclosed by Mr Snowden (through the "Washington Post"[13]) called GENIUS run by an NSA unit called TAO (Tailored Access Operations) involves "implants" of software capable of being run from the outside in order to copy data or otherwise use the infected computer system. It could be used, for example, to download compromising material onto a target's computer – without leaving any trace. According to the "Washington Post", at least 85 000 computer systems world-wide are to be turned into a sort of "bot-net" in the service of the NSA, piloted by an automated system code-named TURBINE. According to the leaked documents, "only 8448" of 69 000 computer systems infiltrated by 2011 could be fully exploited, due to staff limitations, though 1870 persons were employed for this project at the time.

18. Last but not least, it was revealed at the end of 2013 that the NSA is also intercepting shipments from hardware manufacturers to "targets" and compromising hardware during transit, by embedding "malware". This is a particularly serious threat to privacy and data safety because, as I have been told by an expert in the field, no tools exist today to detect such modifications.

3.1.2.7. Geolocalisation of hundreds of millions of mobile phones

19. According to documents leaked by Mr Snowden and published by the Washington Post on 4 December 2013[14], the NSA stores data on hundreds of millions of mobile phones, world-wide, and stocks

[9] See note 5 above.
[10] note 3 above.
[11] See The Guardian of 6 September 2013, "Revealed: how US and UK spy agencies defeat internet privacy and security".
[12] Reportedly, Microsoft is now defending against 'duties of cooperation' before US courts (see DIE WELT of 5 December 2013, Microsoft zieht gegen die NSA vor Gericht).
[13] See Washington Post of 30 August 2013, "US spy agencies mounted 231 offensive cyber operations in 2011 documents show"..
[14] See Washington Post of 4 December 2013, "NSA tracking cellphone locations worldwide Snowden documents show, available"

about 5 billion sets of localisation data per day. This works even when the GPS function of a smart phone is turned off, by following the movement of a phone from cell tower (local emitter) to cell tower. The NSA collects such location and travel habit data in order to carry out "target development", i.e. to find unknown associates of "targets" it already knows about (so-called "co-travelers"). According to the Washington Post, officials say that they do not purposely collect US phone locations in bulk, but a large number are swept up "incidentally". The bulk collection of mobile phone users' locations is performed "upstream" (see above, 3.1.2.2.), by tapping into the telephony links of major telecommunications providers.

3.1.2.8. NSA observing the use of pornographic websites by Islamists

20. An October 2012 document leaked by Mr Snowden[15] discusses the surveillance of six Muslim men considered by the NSA as Islamist hate mongers and explains how "personal weaknesses" can be detected by digital surveillance and used to undermine the credibility and reputation of the person in question.

21. What has me worried most is that such tools (or those available under the GENIUS programme[16]) can also be used to undermine, for example, opposition politicians, human rights activists or journalists. Until recently, there has been very little public debate in any country about whether and to what extent mass surveillance is acceptable. Such a debate is now overdue, and it should be held on the basis of openly available information.

3.1.2.9. NSA infiltrating online videogames

22. According to documents revealed by Mr Snowden[17], both U.S. and UK agents infiltrated such online games as "World of Warcraft" and "Second Life". In a 2008 document entitled "Exploiting terrorist use of Games & Virtual Environments" the NSA described online games as "target-rich communication networks" where terrorists and criminals hang out. These games may provide potentially interesting metadata such as "buddy lists", photos and location data. But whose? Playful teenagers'? Should they now worry that an elf or an orc they are fighting on screen is a real-life secret agent out to fish for data or recruit informers?[18] I was unsure whether to include this information in my paper, as it may deflect from the very serious nature of other attacks on the privacy of all of us. But this example shows the NSA's determination to infiltrate everything and anything.

3.1.3. Some reactions to the disclosures on mass surveillance to date

23. The discussion triggered by these disclosures is ongoing. There has been a large number of negative reactions both from citizens and leading politicians. The latter were particularly outraged when they learned that they too had been the object of surveillance. The disappointment about "friends spying on friends" expressed most pungently by Angela Merkel[19] has undermined mutual trust considerably.

24. On 10 July 2013, the European Parliament's Civil Liberties (LIBE) Committee has launched a large-scale "Inquiry on Electronic Mass Surveillance of EU Citizens"[20]. So far it has held 11 hearings with experts and activists and has reportedly[21] also resolved to hear out Mr Snowden himself. On 18 December 2013, the LIBE committee tabled its preliminary conclusions drafted by Claude Moraes (United Kingdom, S&D)[22]. The preliminary conclusions advocate consenting to a trade deal with the United States

---

[15] See Huffington Post of 26 November 2013: "Top-Secret Document Reveals NSA Spied On Porn Habits As Part Of Plan To Discredit 'Radicalizers'"; BBC news of 27 November 2013, "NSA planned to discredit radicals over web-porn use",; Spiegel online 27 November 2013: NSA beobachtet Porno-Nutzung islamischer Zielpersonen.

[16] See above, item 3.1.2.6.

[17] See http://www.theguardian.com/world/2013/dec/09/nsa-spies-online-games-world-warcraft-second-life (published simultaneously on 9 December 2013 by "The Guardian" and the "New York Times").

[18] I am probably oversimplifying in that it is doubtful that agents participating this kind of monitoring would actually be "playing" or using the ordinary game interface, as monitoring transaction histories and chats does not require graphical interactions. Also, an expert I consulted pointed out that some monitoring of transactions on "SecondLife" or the like by law enforcement agencies may well be a legitimate and effective way to curb money laundering by organised criminals via the exchange of virtual goods.

[19] See for example AFP of 18 November 2013, Merkel urges explanation over 'grave' US spy claims.

[20] See http://www.europarl.europa.eu/news/en/news-room/content/20130701IPR14770/html/Parliament-to-launch-in-depth-inquiry-into-US-surveillance-programmes.

[21] The Guardian of 8 December 2013, "Edward Snowden to give evidence to EU parliament, says MEP" But there has been no agreement yet on the format of such a hearing, which is why it cannot take place before the end of 2013, as initially planned (see http://www.welt.de/politik/ausland/article122863850/Snowden-Anhoerung-vor-EU-Parlament-geplatzt.html?config=print#).

[22] See press release of 18.12.2013: NSA inquiry: lead MEP presents preliminary conclusions.

only if it makes no reference to data protection, suspending the "Safe Harbour" principles (data protection standards to be met by US companies when transferring EU citizens' data) and TFTP (Terrorist Finance Tracking Programme) agreement, with a view to renegotiating more appropriate data protection standards; the draft also calls for the creation of an EU data storage "cloud". In parallel, the EU Commission has also engaged in a dialogue with the US authorities.[23]

25. A draft UN General Assembly resolution criticizing mass surveillance of online communications jointly introduced by Germany and Brazil was adopted unanimously at committee level on 26 November 2013[24] - but not before it was considerably watered down under pressure of the United States and other members of the "Five Eyes" alliance. Interestingly, so far,

> "most of the political responses from governments have criticized Washington and London and called for an end to their surveillance practices. But few have held up their own systems as examples to follow."[25]

26. Part of civil society is also up in arms. Edward Snowden is a hero for internet freedom activists and whistleblowers. In an "open letter to intelligence employees after Snowden"[26], well-known whistleblowers urge civil servants to follow their conscience and join Edward Snowden in helping to hold "crooked politicians accountable". The signatories include Daniel Ellsberg, who, after leaking the "Pentagon papers", was unsuccessfully prosecuted for treason and is now widely credited for having contributed to shortening the Vietnam war.[27] Also, on 10 December 2013, 560 authors from all over the world, including five Nobel prize winners, have launched an appeal against mass surveillance of the internet and in favour of a "Charter of Digital Rights".[28]

27. The NSA scandal has also damaged the reputation of the US-based internet giants such as Microsoft, Cisco and Google. The Snowden revelations show that they and others have voluntarily or under coercion – colluded with the NSA by giving access to customer data or even by compromising commercial data security measures. According to a study by the Information Technology & Innovation Foundation in Washington, D.C., Mr Snowden's disclosures may cost US companies up to USD 35 billion in lost turnover[29]. US technology firms may not have been too concerned with the privacy of commercial data, but their public image in Europe and elsewhere is badly bruised by the Snowden revelations[30]. When 'official' Washington tries to justify the NSA programmes as targeting only foreigners, this does not help global companies – which are now lobbying for secret service reform[31]. Foreign competitors are encouraging economic nationalism to cash in on fears that US-based technology companies are threatening customer privacy.[32] As we will see, this may well threaten not only US players, but the future viability of the internet as we know it, no less!

28. Having reviewed initial reactions in the political sphere, civil society and business to the disclosures summed up before, I should now like to begin preparing for a contribution to the Council of Europe's response to the disclosures on mass surveillance.

3.1.4. Contributing to a Council of Europe response to mass surveillance

29. As "Europe's leading human rights organisation"[33], the Council of Europe should approach mass surveillance from a human rights perspective. As a platform for dialogue and cooperation in Europe, it should also be concerned with the impact of mass surveillance on international cooperation in the internet age.

---

[23] See for example Le Point of 19 November 2013: "Surveillance de la NSA: rencontre "constructive" entre UE et Etats-Unis.
[24] See for example "Süddeutsche Zeitung" of 26 November 2013: "Deutsche UN-Resolution gegen Spionage einstimmig verabschiedet".
[25] Georg Mascolo and Ben Scott, Lessons from the summer of Snowden, the hard road back to trust, Open Technology Institute, Wilson Center, New America Foundation, October 2013 (page 9).
[26] "The Guardian" of 11 December 2013: Former whistleblowers: open letter to intelligence employees after Snowden.
[27] See for example the detailed description available at: http://law2.umkc.edu/faculty/projects/ftrials/ellsberg/ellsberghome.html.
[28] See http://www.change.org/petitions/a-stand-for-democracy-in-the-digital-age-3.
[29] See DIE WELT of 27 November 2013, "NSA-Skandal kostet die USA bis zu 35 Milliarden Dollar".
[30] See Mascolo and Scott (ibid.), page 11.
[31] See DIE WELT of 18 December 2013: "Internet-Bosse fordern Reform der Geheimdienste",
[32] See for example DIE ZEIT online, 11 November 2013, "Ein Schlandnet würde nur der Telekom nützen",
[33] See Washington Post of 4 November 2005 "US faces scrutiny over secret prisons",

3.1.4.1. A human rights perspective on mass surveillance

30. Any surveillance of communications is *a priori* an interference with Article 8 ECHR:

> "Everyone has the right to respect for his private and family life, his home and his correspondence." (Article 8 para. 1 ECHR)

31. There can be little doubt that the term "correspondence" also includes electronic means of communication, whose interception can encroach upon "private life" in the same way as the interception of letters, whose secrecy enjoys elaborate protection also in national constitutions and criminal codes. The change in the technology for the transmission of messages cannot have the legal consequence of reduced protection of privacy.

32. Article 8 paragraph 2 provides for an important exception from the protection of privacy:

> "There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

33. This exception clearly covers the original form of surveillance, i.e. as authorised by evidence-based court orders against suspect individuals. But to what extent does it also allow for mass surveillance, without court orders and even without any grounds for suspicion against the multiple "targets"?

34. The case law of the European Court of Human Rights ("the Court"), so far, seems to be relatively protective of privacy rights. In the leading case of *Klass and others v. Germany*[34], the Court found that

> "Powers of secret surveillance of citizens, characterising as they do the police state, are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions. […] The Court, in its appreciation of the scope of the protection offered by Article 8, cannot but take judicial notice of two important facts. The first consists of the technical advances made in the means of espionage and, correspondingly, of surveillance; the second is the development of terrorism in Europe in recent years. Democratic societies nowadays find themselves threatened by highly sophisticated forms of espionage and by terrorism, with the result that the State must be able, in order effectively to counter such threats, to undertake the secret surveillance of subversive elements operating within its jurisdiction. The Court has therefore to accept that the existence of some legislation granting powers of secret surveillance over the mail, post and telecommunications is, under exceptional conditions, necessary in a democratic society in the interests of national security and/or for the prevention of disorder or crime"(§42, 48).

35. As to the conditions for surveillance, the Court allows member states wide discretion. But the Court stresses that

> "this does not mean that the Contracting States enjoy an unlimited discretion to subject persons within their jurisdiction to secret surveillance. […] The Court must be satisfied that, whatever system of surveillance is adopted, there exist adequate and effective guarantees against abuse. This assessment has only a relative character: it depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering such measures, the authorities competent to permit, carry out and supervise such measures, and the kind of remedy provided by the national law" (§49, 50).

36. The Court, when it passed this judgment in 1978, could not even imagine the technological progress, which would in time allow for the extent of surveillance that we are discussing here. Meanwhile, it has had the opportunity to spell out in some more detail the conditions under which it finds surveillance measures acceptable under the Convention.

37. In *Kruslin v. France*[35], the Court found a violation of Article 8, because French law governing telephone wiretapping was not sufficiently "foreseeable" in that it did not define the categories of people

[34] Application no. 5029/71, judgment of the Plenary Court of 6 September 1978.
[35] Application no. 11801/85, judgment of 24 April 1990.

liable to have their phones tapped by judicial order and the nature of the offences which might give rise so such an order.

38. In *Halford v. the United Kingdom*[36], the Court confirmed that telephone calls made from business premises as well as from the home may be covered by the notions of "private life" and "correspondence" in Article 8. It found a violation because internal calls within the police headquarters were intercepted without there being a statutory basis.

39. In *Lambert v. France*[37], the Court found a violation of Article 8 because the applicant was refused the possibility to challenge the manner in which the duration of the monitoring of a third person's telephone line was extended. The Court's argument is particularly interesting in our context:

> "this could lead to decisions whereby a very large number of people were deprived of the protection of the law, namely all those who had conversations on a telephone line other than their own. That would in practice render the protective machinery largely devoid of substance" (§38).

40. This argument would appear to apply even better to mass surveillance of the kind disclosed by Mr Snowden.

41. In *Amann v. Switzerland*[38], the Court found a violation of Article 8 because the interception of a phone call was not covered by a law which satisfied the requirement of foreseeability and the Government could not establish that the safeguards provided for in the law had been complied with. This case is, again, particularly interesting in our context because the applicant became subject of surveillance by accident: because a woman had called him from the Soviet embassy in Berne to order an appliance sold by the applicant, he ended up in an anti-espionage surveillance database. Arguably, in the context of mass surveillance, the vast majority of people whose communications are intercepted in today's surveillance "dragnet" end up in the database by accident, like Mr Amann, as "by-catch".

42. In *Copland v. the United Kingdom*[39], the Court made it clear that email correspondence and internet usage fall in the ambit of Article 8, in the same way as telephone or postal communications. In finding a violation, the Court did not consider relevant that the data obtained had not been disclosed to third parties or used against the applicant in any way. Interestingly, in our context, the Court found that the mere

> "collection and storage of personal information relating to the applicant's use of the telephone, e-mail and internet, without her knowledge, therefore amounted to an interference with her right to respect for her private life and correspondence" (§44).

43. In the absence of any domestic law regulating monitoring at the material time, the interference was not "in accordance with the law".

44. The case of *Liberty and others v. the United Kingdom*[40] deals with the interception by the Ministry of Defence of the foreign communications of civil liberties organisations. Under the Interception of Communications Act 1985, warrants could be issued in respect of (internal or external) communications linked to a particular address or person or to external (foreign) communications generally, with no restriction on the persons or premises concerned. The Act required the Secretary of State to make such arrangements as he considered necessary to ensure safeguards against abuses of power, and established a special tribunal to investigate complaints and a Commissioner with reporting and review powers. The precise details of the "safeguards" were not disclosed in the interests of national security. The Court found a violation of Article 8 because the Act allowed the British authorities "a virtually unlimited discretion to intercept any communications between the United Kingdom and an external receiver", and "in principle, any person who sent or received any form of telecommunication outside the British Islands during the period in question could have had their communications intercepted", whilst the nature of the "arrangements" to prevent abuse had not been contained in legislation or otherwise made available to the public".

45. The subsequent case of *Kennedy v. the United Kingdom*[41] discusses the proportionality and safeguards foreseen in British legislation on interception of internal (domestic) communication. The Court

[36] Application no. 20605/92, judgment of 25 June 1997.
[37] Application no. 23618/94, judgment of 24 August 1998.
[38] Application no. 27798/95, judgment of 16 February 2000.
[39] Application no. 62617/00, judgment of 3 April 2007.
[40] Application no. 58243/00, judgment of 1 July 2008.
[41] Application no. 26839/05, judgment of 18 May 2010.

found no violation of the Convention because "the legislation underpinning the regime specified a number of safeguards for the protection of any data obtained", and "the regime was supervised by a body which enjoyed an adequate level of independence and which possessed sufficient powers." This judgment or more precisely, the legal regime of surveillance of internal communications in the UK in force in 2005 may in fact show a way forward: legislation establishing specific safeguards against abuse, and an independent supervisory body with sufficient powers. I intend to look more closely at what this means in actual practice in the further pursuit of this rapporteur mandate.

46. The Court will have the opportunity to further clarify its case law in the near future, as at least two new relevant applications were recently introduced: a Hungarian NGO has challenged Hungarian legislation allowing secret surveillance and data gathering by national security services solely based on ministerial approval[42]; and three UK NGO's have seized the Strasbourg Court with an application against the collection of vast amounts of data by the UK's GCHQ.[43] Meanwhile, Mr Bosjan Zupancic, judge at the European Court of Human Rights in respect of Slovenia, reportedly maintained, at a hearing before the European Parliament's committee of inquiry into the NSA affair, that mass surveillance is generally unacceptable and open to challenge before the courts.[44]

47. The legality of mass surveillance under international human rights law is also under scrutiny in the framework of the Inter-American Commission of Human Rights, which, in October 2013, has held a thematic hearing on "Freedom of expression and communication surveillance by the United States".[45]

48. A key question the courts will have to decide is whether the moment of infringement of privacy remains the collection or interception of the personal data, or shifts to their processing or use. Technology could shape the policy-makers' approach. I was told by an expert that it is usually technically easier to filter data transmitted in real time for specific targets, and only store the relevant data. Filtering is faster than storing, and filtering at the site of interception is easier than first transmitting "full take" to the storage site. But it is not currently technically possible to go back in time (e.g. find out what the Boston bombers did in 2011? with whom did they communicate before they appeared on the "radar"?) That can only be done after the data are intercepted, stored and searchable.[46] In order to make mass interception and storage legal, it has been argued that "surveillance" (as an infringement of privacy rights) no longer means merely intercepting data but only the actual processing and use of the data. Does this shift have to be accepted as a matter of technical necessity – for the sake of fighting terrorism? Or is it an unacceptable step onto the slippery slope towards George Orwell's "1984"?[47] And to the extent that such "drag-net fishing" (and storage) of huge amounts of data mostly belonging to non-suspects is actually taking place, can we at least ensure that the technologically unavoidable "by-catch" of data is speedily deleted ("minimised" in the NSA's terminology)?

3.1.4.2. A perspective of international cooperation: mass surveillance as a threat to the viability of the internet and possible answers

49. The internet as we know it (or believed we knew it) is a global platform for exchange of information, open and free debate and – why not? – commerce. This may well change after the Snowden revelations. One answer to perceived generalised surveillance by the NSA and others is "technological sovereignty", including regulations requiring that all data stored or processed for European consumers must be stored and processed inside Europe – or even inside each country.[48] This is both a political response to abuses and a marketing tool for European companies, as we have seen. But it is fraught with danger: the architecture of the internet is not designed for "national routing", and big changes to routing patterns might diminish overall network functionality.[49] Most importantly, in the Council of Europe's perspective,

[42] See MTI-EcoNews/Hungary of 29/11/2013: "NGO to turn to Strasbourg court over security services' secret surveillance."
[43] See Guardian of 3/10 /2013: "GCHQ faces legal challenge in European court over online privacy".
[44] See Heise online of 15/10/2013: "Rechtsexperten im EU-Parlament: NSA und GCHQ verletzen Menschenrechte und Souveränität".
[45] See the testimony of Emi MacLean of the Open Society Justice Initiative and of Alex Abdo on behalf of the American Civil Liberties Union (ACLU) as well as the submission of a group of other NGO (available from the secretariat).
[46] See Georg Mascolo and Ben Scott, Lessons from the summer of Snowden, the hard road back to trust, Open Technology Institute, Wilson Center, New America Foundation, October 2013 (page 7).
[47] See Mascolo and Scott, ibid., page 7.
[48] Reportedly, German Interior Minister Friedrich suggested that citizens worried about American espionage should avoid internet services that send data over US networks. Chancellor Merkel mentioned a Germany-only routing solution (see Mascolo and Scott, ibid., page 10). The draft conclusions of the European Parliament's LIBE Committee (see note 21 above) also advocate the creation of a "European data cloud".
[49] See Mascolo and Scott, ibid., page 12.

> "the purposes of national routing do not typically tend towards protecting civil rights, but rather the opposite. The localization of Internet traffic will intensify opportunities for national surveillance, censorship, and the kind of political persecution of online dissidents that the West has fought for years."[50]

50. I fully share this concern. The "Balkanisation of the internet"[51] does not look like a good the solution. I agree with Mascolo and Scott's conclusion:

> "Given the risks, it would be sensible to make an aggressive attempt at a political solution before falling back on economic and technological nationalism as a response to foreign surveillance."[52]

51. Another solution advocated in the wake of the Snowden disclosures is the negotiation, at least among friends and allies, of "no-spy" agreements[53], and generally the establishment of a more precise legal framework for surveillance activities, within and outside national borders. Such solutions obviously require a fair amount of trust, including of internet users that such agreements are meant seriously in the first place and that they will actually be respected by all partners.

52. But trust, even among "friends", has been seriously eroded – not by Mr Snowden's revelations, but by the actions he has disclosed. The runaway surveillance machine is also the outcome of a loss of control by the political leadership over the activities of intelligence agencies that most politicians can no longer understand. James Clapper, Director of National Intelligence, famously replied "no sir, not wittingly" to the question of Senator Ron Wyden, member of the Senate Intelligence Committee, at an open congressional hearing on 12 March 2013 whether the NSA was collecting the data of hundreds of millions or hundreds of millions of Americans not suspected of any crime.[54] I do not want to believe that he lied. But he was at least not properly briefed by his own collaborators, who themselves may have lost control over the activities of the private businesses to whom much of the surveillance work has been outsourced (such as Mr Snowden's employer). Privatisation of surveillance carries a high risk of self-propelled growth fuelled by the providers' self-interest. Ever-increasing "needs" for surveillance spending can be justified so easily: if a terrorist attack was averted by surveillance, more surveillance is needed to avert more attacks.[55] If an attack could not be averted, the cause must have been insufficient surveillance… The parallel to the privatization of prisons in the United States is worrying: since privatization began in the early 1980s, the US prison population has at least tripled, whilst the crime rate has decreased.[56] The "rise of the prison industrial complex"[57] may find itself matched or even surpassed by the rise of the "surveillance industrial complex".

53. Advocates of mass encryption as an answer to mass surveillance insist that they can win an "arms race" with the NSA and others because of the technology-based "asymmetry" between the modest resources required from "code-makers" compared to the huge cost of breaking a relatively cheap code. Crypto-activists propose decentralising the internet far beyond country-by-country "Balkanisation". They believe that "atomisation" of the net - each user having his or her own well-encrypted server - is the answer. No known code can resist "brute force", the massive use of supercomputers to play out all

---

[50] Mascolo and Scott, ibid., page 12.
[51] See Eugene Kaspersky, "What will happen if countries carve up the internet?", in: The Guardian of 17 December 2013.
[52] Mascolo and Scott, ibid., page 12.
[53] See DIE WELT of 17 December 2013: "Ein Abkommen wird NSA-Spionage nicht verhindern". In sum: the New York Times had indicated that the US authorities refused to enter into a "no spy" – agreement with Germany, as proposed by Germany according to a reply of the Government to a parliamentary question of the Social democratic faction in the Bundestag (link: http://www.welt.de/themen/bundesregierung). Berlin confirmed that the negotiations continued. The author of the article puts in doubt the value of the possible future "memorandum of understanding". He recalls that in a "memorandum of agreement" between the NSA and the German BND dated 28 April 2002, the NSA declared itself ready to respect German laws on phone and other surveillance, whilst it now turned out that even Chancellor Merkel's mobile phone was targeted for years.
[54] See Fred Kaplan, "James Clapper lied to Congress about NSA surveillance", 11 June 2013.
[55] But the NSA stepped up surveillance well before September 11, 2001, and even at the current level of surveillance, terrorism has not been stopped. A report by a group of experts of the US Senate dated 12 December 2013 ("Liberty and security in a changing world, Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies" finds that metadata collection was not instrumental in preventing terrorist attacks (at page 104).
[56] See for example http://www.globalresearch.ca/the-prison-industry-in-the-united-states-big-business-or-a-new-form-of-slavery/8289.
[57] See John W. Whitehead, "Jailing Americans for profit: the rise of the prison industrial complex", Huffington Post of 4 October 2012.

combinations, but "brute force" is very resource-intensive and can therefore only be used against a limited number of well-chosen targets, such as terrorists, weapons traders, mafia bosses and the like. This clientele is what surveillance used to be reserved for, authorised by court orders based on concrete grounds for suspicion. I must admit that this is not without attraction, but I want to find out more about the feasibility and possible consequences of such a "mass encryption solution", especially how it would impact law enforcement.

54. We as politicians must be in any case aware of the political price tag of massive surveillance: the threat to the very existence of the Internet as we know it, with all its social and economic benefits, and the erosion of trust between friends and partners on the international scene.

55. Trust is the basis of any kind of international cooperation, and it must therefore urgently be rebuilt. The alternative, namely the "Balkanisation" or "atomisation" of the internet, and a cryptological arms race, does not look very attractive, at least at first glance. Even if it is difficult to trust that national and international legal regulations and agreements will be kept, we should not just forget about them – as some "techies" tend to do. We must ensure that the Convention and national laws are up to date in view of technological developments so that they can offer adequate protection against unnecessary intrusion in private life. The existence of a legal framework established after a democratic debate[58] provides legitimacy for those practices that remain legal whilst giving guidance to those on the "frontline". Not least, a proper legal framework provides an important safeguard for potential whistleblowers, whose action might well be the best possible enforcement mechanism for any present or future legal framework. In order for disclosures to be protected following relevant laws and principles, they must concern abuses, i.e. ideally, practices breaching an existing legal framework.[59]

56. The last consideration takes us straight to the next topic, the protection of whistleblowers.

3.2. Additional Protocol to the ECHR on the protection of whistleblowers (Improving the protection of whistleblowers)

57. For the second subject, I should also begin by suggesting a change of title, namely by dropping the reference to an "additional protocol to the ECHR". This is but one possible (and quite possibly not the most realistic) option for improving the protection of whistleblowers. As I said at the Committee meeting on 6 November 2013, I should like to look into other options, too.

58. Regarding this subject, we will be able to build on the Assembly's 2010 report[60] on the protection of whistleblowers. In preparing this report, I had the benefit of cooperation with a group of civil society stakeholders brought together by Transparency International, which drafted a set of guiding principles for the protection of whistleblowers. I also received information, through the ECPRD network of parliamentary research services, on existing whistleblowing legislation in member states, which turned out to be rather limited. Ironically, the most effective legal framework seemed to exist in the United States of America. In its Resolution 1729 (2010), the Assembly largely subscribed to the above-mentioned guiding principles and encouraged the Committee of Ministers to engage in a dialogue with civil society in order to devise ways and means to protect whistleblowers more efficiently.

---

[58] The report of the President's Review Group (note 54 above) acknowledges the damage done to US diplomatic and business interests by the NSA's exaggerations and proposes sweeping reforms of existing surveillance practices, including restrictions on the collection of metadata by the NSA, a rejection of compelled data security "backdoors" (proof of which the experts did not find, contrary to allegations based on documents leaked by Mr Snowden, see page 217) and treating the citizens of foreign countries with more respect (page 155). The Group also criticises the Foreign Intelligence Surveillance Court (FISC) for being too compliant with the intelligence agencies (page 207). The discussion of the Group's recommendations will begin in January.

[59] This explains why Mr Snowden reacted very positively to the recent ruling of a US Federal judge. Conservative activists challenged the NSA's surveillance programmes in court. Federal district court judge Richard J. Leon found that the massive collection of metadata and of millions of telephone conversations seemed to violate US citizens' privacy guaranteed in the 4th Amendment and invited the authorities to comment. The case is likely to end up in the US Supreme Court. But no matter what the final outcome, Judge Leon's preliminary findings are a boon to Mr Snowden, who argues that he believed that the NSA activities disclosed were unconstitutional. It will be difficult to find his belief unreasonable if it is shared by a US Federal judge. The case may also influence the debate about a possible conditional amnesty for Mr Snowden triggered by a proposal in this sense by a high-ranking NSA official, which was promptly refused by the White House; see DIE WELT of 17 December 2013, US-Bundesrichter setzt das Weisse Haus unter Druck; link to the judgment: https://ecf.dcd.uscourts.gov/cgi-bin/show_public_doc?2013cv0851-48; link to the statement of Mr Snowden published by the New York Times: http://www.nytimes.com/2013/12/17/us/politics/federal-judge-rules-against-nsa-phone-data-program.html).

[60] See Doc. 12006, adopted on 29 April 2010.

59. I will also be able to make use of the work by our colleague Arcadio Diaz Tejera on Access to Information and National Security.[61] The "Tshwane Principles" on Access to information and national security endorsed by the Assembly in Resolution 1954 (2013) include principles on whistleblower protection in the national security context that are very pertinent for the case of Mr Snowden. They have been widely supported in the Inter-American Commission on Human Rights during its Thematic Hearing on "Freedom of Expression and Communications Surveillance by the United States" at the end of October 2013.[62]

60. The Committee of Ministers reacted positively to the Assembly's recommendations[63] and, in particular, agreed on the need to elaborate further guidelines on the topic with a view to creating a common set of principles to which all member states should adhere. In June 2012, the European Committee on Legal Co-operation (CDCJ) tasked its Bureau together with its members from France, Ireland and the United Kingdom to prepare a preliminary draft legal instrument. In May 2013, a stakeholder conference was held in Strasbourg, in which I had the honour of representing the Parliamentary Assembly. The CDCJ has approved a draft Committee of Ministers Recommendation on protecting whistleblowers and adopted an explanatory memorandum[64] at its meeting on 16 December 2013, thereby preparing the ground for its adoption by the Committee of Ministers in the course of 2014.

61. Since the adoption of the last Assembly report in 2010, the European Court of Human Rights has issued two significant rulings with regard to whistleblowing, *Heinisch v. Germany* (2011)[65] and *Sosinowska v. Poland* (2011).[66] Furthermore, Transparency International[67] and other specialised international networks have worked on perfecting their guiding principles and sets of good practices, which could feed into the new report.

62. For this Rapporteur mandate, I intend to begin by taking stock of the follow-up given to the Assembly's relevant recommendations, both by the Committee of Ministers and in the Council of Europe's member and observer states.

63. I should also like to revisit the above-mentioned recommendations and guiding principles, including the pertinent "Tshwane Principles", in light of the NSA affair. I should like to subject the generally agreed principles to a "practice test", by applying them to recent, high-profile cases such as those of Mr Edward Snowden and Mr Bradley/Ms Chelsea Manning.[68] Besides the purely legal aspects, it should also be worth looking into the role and development of new international networks and platforms as additional safeguard mechanisms for the protection of whistleblowers.

64. An interesting proposal I also intend to look into is included in a recent report addressed to the European Parliament[69], namely that whistleblower protection measures could be taken at European level, including asylum rights for whistleblowers persecuted in their home countries because of disclosures they made in the public interest.

65. Taking into account these inputs and those that will be provided at our own future hearing, I plan to make concrete proposals, in the final report, for improving the protection of whistleblowers. The Assembly could address them to all member states of the Council of Europe and to the Committee of Ministers to take into account in its ongoing work on the subject.

4. Fact-finding proposals

66. In order to fulfil my two rapporteur mandates, I should like to organize two separate hearings before the Committee, one focusing on mass surveillance, the other on the protection of whistleblowers. Both hearings could take place at a Committee meeting during the Assembly's April 2014 part-session. Ideally,

---

[61] See Resolution 1954 (2013) based on the report by Mr Diaz Tejera (Spain/SOC), doc. 13293 of 3 September 2013.
[62] See in particular the testimony of Emi MacLean of the Open Society Justice Initiative, who was also involved in the formulation of the "Tshwane Principles" (text available from the secretariat).
[63] Doc. 12479 of 24 January 2011.
[64] Prepared by Ms Anna Myers, Expert Coordinator**,** *Whistleblowing* International *Network* (WIN), London.
[65] http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-105777.
[66] http://echr.ketse.com/doc/10247.09-en-20111018/view/.
[67] See International Principles for whistleblower legislation: best practices for laws to protect whistleblowers and support whistleblowing in the public interest, Transparency International 2013.
[68] See http://assembly.coe.int/nw/xml/News/News-View-EN.asp?newsid=4553&lang=2&cat=5.
[69] "National programmes for mass surveillance of personal data in EU Member States and their compatibility with EU law", study by the Directorate-General for Internal Policies of the European Parliament (Policy Department C, Citizens' Rights and Constitutional Affairs), 2013; authors: Didier Bigo, Sergio Carrera, Nicholas Hernanz, Joanna Parkin, Francesco Ragazzi and Amandine Scherrer; see in particular recommendation 8 on p. 46.

the hearings should be held on the same day, one in the morning and one in the afternoon, and be open to the public. This would enable the Committee to appreciate in real time the implications of contributions made in relation to one topic for the other, and the invited experts to follow the discussions on the related topic, whilst needing to travel to Strasbourg only once. As to the order of the two hearings, I suggest to start with the topic of mass surveillance, which provides a good illustration both for the opportunities and the risks inherent in whistleblowing and can therefore serve as a good background for the second hearing.

67. Usually, experts invited to hearings are simply chosen by the rapporteur. But in light of the discussion at the Committee meeting on 12 November 2013, I prefer submitting specific proposals to the Committee for its approval.

68. For both hearings, I should like to invite experts who do not share the same views so that we can enjoy a lively discussion and reach well-balanced conclusions.

69. Ideally, we should be able to hear a representative of the competent US authorities and Mr Snowden for both hearings.

70. In the hearing on mass surveillance, Mr Snowden could sum up his disclosures to date and possibly make additional ones, and a US representative (an appropriately high-ranking government official, perhaps) could take position both on the question whether Mr Snowden is telling the truth and, to the extent that he does, why the NSA is justified in carrying out such surveillance.

71. In the hearing on whistleblower protection, the US representative could be invited to make the case for treating Mr Snowden as a criminal, and Mr Snowden could explain why he made the choice of blowing the whistle on his former employer's activities.

72. For each of the hearings, we should also invite one or two other experts, who could provide additional perspectives on the facts and map out possible solutions.

73. For mass surveillance, I propose inviting, in addition to the US representative and Mr Snowden:

(1) Ben Scott, senior advisor to the Open Technology Institute at the New America Foundation and Director of the European Digital Agenda Program at the Stiftung Neue Verantwortung in Berlin. He had also served as an advisor on technology issues at the US Department of State, and

(2) Hansjörg Geiger, former head of the German Bundesnachrichtendienst (BND), author of a proposal for an "Intelligence Kodex" to be adopted by all NATO countries designed to restore trust among like-minded countries.

74. For whistleblower protection, I propose inviting as additional experts:

(1) Anna Myers, head of the UK-based whistleblowing network and adviser to the Council of Europe on the draft whistleblowing recommendation of the Committee of Ministers, and

(2) Brendan Howlin, Irish Minister for expenditure and reform, who has introduced legislation to promote the protection of whistleblowers in Ireland.

75. I am aware that the proposal to invite Mr Snowden is controversial. But I am convinced that he has interesting contributions to make, on both subjects. Inviting him will inevitably give Mr Snowden additional public exposure, but frankly, he is not lacking such exposure even without our invitation. As I explained in November, listening to what he has to say does not mean that we adopt his position or endorse his actions. Mr Snowden's statements will be counterbalanced by the presentations of the US representative and other experts, at least one of whom also has a strong intelligence background. The possibility of exchanging views with a controversial interlocutor without causing a strain on bilateral relations for one country or another is a particular strength of an international assembly such as ours, which we should exploit.

76. I am also aware that Mr Snowden may not be in a position to travel to Strasbourg. He is a wanted man in the United States. The U.S. might request his extradition from France, the Council's seat State, which may have certain obligations as such. It will be ultimately up to Mr Snowden, in agreement with his Russian hosts, to decide whether he feels confident to accept such an invitation. As fallback, we could invite Mr Snowden to participate in the hearing by way of teleconferencing, or the Committee could authorise me to visit him in Russia and report back to it.

77. In addition to the two committee hearings, I would also like to ask the committee for its authorisation to meet with an IT expert specializing in internet security and with a legal expert with a view to advising me on the technical and legal viability of proposals I intend to make in my final report on mass surveillance.