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

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Doc. 13734
18 March 2015

Mass surveillance

Report[1]
Committee on Legal Affairs and Human Rights
Rapporteur: Mr Pieter OMTZIGT, Netherlands, Group of the European People's Party

Summary

The Committee on Legal Affairs and Human Rights is deeply concerned about mass surveillance and large-scale intrusion practices disclosed since June 2013 by Mr Edward Snowden. The disclosures have provided compelling evidence of the existence of far-reaching, technologically advanced systems put in place by US intelligence services and their partners in certain Council of Europe member States to collect, store and analyse communication data, including content, location and other metadata, on a massive scale. In several countries, a massive "Surveillance-Industrial Complex" has evolved, which risks escaping democratic control and accountability and threatens the free and open character of our societies.

The surveillance practices disclosed endanger fundamental human rights, including the rights to privacy (Article 8 of the European Convention on Human Rights), freedom of information and expression (Article 10), and the rights to a fair trial (Article 6) and freedom of religion (Article 9). The committee is also deeply worried about threats to Internet security by the practice of certain intelligence agencies of seeking out systematically, using and even creating "back doors" and other weaknesses in security standards and implementation, which could easily be exploited also by terrorists and cyberterrorists or other criminals.

The committee also recognises the need for transatlantic co-operation in the fight against terrorism and other forms of organised crime. But it considers that such co-operation must be based on mutual trust based on respect for human rights and the rule of law. In order to rebuild trust, a legal and technical framework must be put in place at the national and international level which ensures the protection of human rights, especially that which secures the right to privacy. An effective tool for the enforcement of such a legal and technical framework, besides enhanced judicial and parliamentary scrutiny, is credible protection extended to whistle-blowers who expose violations.

1. Reference to committee: Doc. 13288, Reference 4003 of 30 September 2013.

Contents **Page**

A. Draft resolution[2]

1. The Parliamentary Assembly is deeply concerned about mass surveillance practices disclosed since June 2013 by journalists to whom a former United States national security insider, Mr Edward Snowden, had entrusted a large amount of top secret data establishing the existence of mass surveillance and large-scale intrusion practices hitherto unknown to the general public and even to most political decision-makers.

2. The information disclosed so far in the Snowden files has triggered a massive, worldwide debate about mass surveillance by the United States and other countries' intelligence services and the lack of adequate legal regulation and technical protection at the national and international level, and/or its effective enforcement.

3. The disclosures have provided compelling evidence of the existence of far-reaching, technologically advanced systems put in place by United States intelligence services and their partners in certain Council of Europe member States to collect, store and analyse communication data, including content, location and other metadata, on a massive scale, as well as targeted surveillance measures encompassing numerous people against whom there is no ground for suspicion of any wrongdoing.

4. The surveillance practices disclosed so far endanger fundamental human rights, including the rights to privacy (Article 8 of the European Convention on Human Rights (ETS No. 5)), freedom of information and expression (Article 10) and the rights to a fair trial (Article 6) and freedom of religion (Article 9) – especially when privileged communications of lawyers and religious ministers are intercepted and when digital evidence is manipulated. These rights are cornerstones of democracy. Their infringement without adequate judicial control also jeopardises the rule of law.

5. The Assembly about also deeply worried about threats to Internet security by the practice of certain intelligence agencies, disclosed in the Snowden files, of seeking out systematically, using and even creating "back doors" and other weaknesses in security standards and implementation, which could easily be exploited also by terrorists and cyberterrorists or other criminals.

6. It is also worried about the collection of massive amounts of personal data by private businesses and the risk that these data may be accessed and used for unlawful purposes by State or non-State actors.

7. The Assembly is also deeply concerned about the extensive use of secret laws and secret courts, as well as secret interpretations of such laws, which are very poorly scrutinised.

8. The consequences of mass surveillance tools such as those developed by the United States and allied services falling into the hands of authoritarian regimes would be catastrophic. In times of crisis, it is not impossible for executive power to fall into the hands of extremist politicians, even in established democracies. High-technology surveillance tools are already in use in a number of authoritarian regimes and are used to track down opponents and to suppress freedom of information and expression.

9. In several countries, a massive "Surveillance-Industrial Complex" has evolved, fostered by the culture of secrecy surrounding surveillance operations, their highly technical character and the fact that both the seriousness of alleged threats and the need for specific counter-measures and their costs and benefits are difficult to assess for political and budgetary decision-makers without relying on input from interested groups themselves. These powerful structures risk escaping democratic control and accountability and they threaten the free and open character of our societies.

10. The Assembly notes that the law in most States provides some protection for the privacy of their own citizens, but not of foreigners. The Snowden files have shown that the United States National Security Agency (NSA) and their foreign partners, in particular among the "Five Eyes" partners (Australia, Canada, New Zealand, the United Kingdom and the United States) circumvent national restrictions by exchanging data on each other's citizens.

11. The Assembly recognises the need for effective, targeted surveillance of suspected terrorists or other organised criminal groups. Such targeted surveillance can be an effective tool for law enforcement and crime prevention. At the same time, it notes that, according to independent reviews carried out in the United States, mass surveillance does not appear to have contributed to the prevention of terrorist attacks, contrary to earlier assertions made by senior intelligence officials. Instead, resources that might prevent attacks are diverted to mass surveillance, leaving potentially dangerous persons free to act.

2. Draft resolution unanimously adopted by the committee on 26 January 2015.

12. The Assembly also recognises the need for transatlantic co-operation in the fight against terrorism and other forms of organised crime. But it considers that such co-operation must be based on mutual trust founded on respect for human rights and the rule of law. This trust has been severely damaged by the mass surveillance practices revealed in the Snowden files.

13. In order to rebuild trust among the transatlantic partners, among the member States of the Council of Europe and also between citizens and their own governments, a legal framework must be put in place at the national and international level which ensures the protection of human rights, especially the protection of the right to privacy. An effective tool for the enforcement of such a legal and technical framework, besides enhanced judicial and parliamentary scrutiny, is credible protection extended to whistle-blowers who expose violations.

14. The reluctance of the competent United States authorities and their European counterparts to contribute to the clarification of the facts, including their refusal to attend hearings organised by the Assembly and the European Parliament, as well as the harsh treatment of whistle-blower Edward Snowden, does not contribute to restoring mutual trust and public confidence.

15. The Assembly welcomes initiatives within the US Congress to review existing legislation in order to minimise abuses, as well as the German Bundestag's decision to set up a committee of inquiry into the repercussions of the NSA affair in Germany. It calls on the Bundestag committee to carry out its tasks of holding to account the executive and seeking the truth without regard to party-political considerations and encourages other parliaments to embark on similar inquiries.

16. The Assembly welcomes the thorough investigation carried out by the European Parliament leading to the adoption, on 12 March 2014, of a comprehensive resolution on the NSA affair and its repercussions for Euro-Atlantic relations. In particular, the Assembly strongly endorses:

16.1. the invitation addressed to the Secretary General of the Council of Europe by the European Parliament to use his powers under Article 52 of the European Convention on Human Rights to request information on the manner in which States Parties implement relevant provisions of the Convention;

16.2. the European Parliament's call to promote the wide use of encryption and resist any attempts to weaken encryption and other Internet safety standards, not only in the interest of privacy, but also in the interest of threats against national security posed by rogue States, terrorists, cyberterrorists and ordinary criminals.

17. The Assembly therefore urges the Council of Europe member and observer States to:

17.1. ensure that national law allows the collection and analysis of personal data (including so-called metadata) only with the consent of the person concerned or following a court order granted on the basis of reasonable suspicion of the target being involved in criminal activity; unlawful data collection and treatment should be penalised in the same way as the violation of the traditional mail secret; the creation of "back doors" or any other techniques to weaken or circumvent security measures or exploit their existing weaknesses should be strictly prohibited; all institutions and businesses holding personal data should be required to apply the most effective security measures available;

17.2. ensure, in order to enforce such a legal framework, that their intelligence services are subject to adequate judicial and/or parliamentary control mechanisms. National control mechanisms must have sufficient access to information and expertise and the power to review international co-operation without regard to the originator control principle, on a mutual basis;

17.3. provide for credible, effective protection for whistle-blowers exposing unlawful surveillance activities, including asylum in cases of threatened unfair prosecution in their home country;

17.4. agree on a multilateral "intelligence codex" for their intelligence services, which lays down rules governing co-operation for the purposes of the fight against terrorism and organised crime. The codex should include a mutual engagement to apply to the surveillance of each other's nationals and residents the same rules as those applied to their own, and to share data obtained through lawful surveillance measures solely for the purposes for which they were collected. The use of surveillance measures for political, economic or diplomatic purposes among participating States should be banned. Participation should be open to all States which implement a legal framework at national level corresponding to the specifications enumerated in paragraphs 16.1 to 16.3;

17.5. promote the further development of user-friendly (automatic) data protection techniques capable of countering mass surveillance and any other threats to Internet security, including those posed by non-State actors;

17.6. refrain from exporting advanced surveillance technology to authoritarian regimes.

18. The Assembly also invites the competent bodies of the European Union to make use of all the instruments at their disposal to promote the privacy of all Europeans in their relations with their counterparts in the United States, in particular in negotiating or implementing the Transatlantic Trade and Investment Partnership (TTIP), the Safe Harbour decision, the Terrorist Financing Tracking Program (TFTP) and the Passenger Name Records (PNR) agreement.

B. Draft recommendation[3]

1. The Parliamentary Assembly refers to its Resolution … (2015) on mass surveillance and invites the Committee of Ministers to make use of the tools at its disposal to uphold the fundamental right to privacy in all member and observer States of the Council of Europe.

2. In particular, the Assembly invites the Committee of Ministers to consider:

2.1. addressing a recommendation to member States on ensuring the protection of privacy in the digital age and Internet safety in the light of the threats posed by the newly disclosed mass surveillance techniques (see Resolution … (2015), paragraphs 16.1 to 16.3);

2.2. launching an initiative aimed at negotiating an "intelligence codex" addressed to the intelligence services of all participating States, which lays down rules governing co-operation in the fight against terrorism and organised crime (see Resolution … (2015), paragraph 16.4);

2.3. strengthening co-operation with the competent bodies of the European Union involved in negotiating trade and data protection issues with the United States and other third countries, with a view to bringing to bear the principles laid down in the European Convention on Human Rights (ETS No. 5) in the interest of all member States of the Council of Europe.

3. Draft recommendation unanimously adopted by the committee on 26 January 2015.

C. Explanatory memorandum by Mr Omtzigt, rapporteur

"Our freedom is built on what others do not know of our existences", Alexandr Solzhenitsyn

1. Introduction and procedure

1. Since June 2013, disclosures by journalists to whom Mr Edward Snowden, a former employee of the CIA and of a private contractor working for the United States National Security Agency (NSA), had entrusted a large amount of top secret data concerning mass surveillance carried out by the NSA and others have triggered a massive public debate on privacy in the Internet age. The extent of mass surveillance programmes conducted all around the world by the NSA and other countries' intelligence agencies is stunning. The disclosures have confirmed the need for the Council of Europe to encourage its member and observer States to reassess their own surveillance programmes, assess loopholes which enable such programmes to target their own citizens by foreign services, and consider possible redress, including through legislative means, international agreements and the promotion of mass encryption. This is a matter not only of the protection of our fundamental rights, but also a matter of national security, which is under threat from rogue States, terrorists, cyberterrorists and ordinary criminals who can do enormous damage by making use of weaknesses in encryption and other Internet security measures deliberately created by intelligence agencies in order to facilitate mass surveillance.

2. The manner in which Mr Snowden has made these disclosures possible has also reignited the discussion on the protection of whistle-blowers. Both discussions have given rise to motions in the Parliamentary Assembly.

3. On 6 November 2013, the Committee on Legal Affairs and Human Rights appointed me as rapporteur for two interrelated subjects, namely: "Massive Eavesdropping"[4] and "Additional Protocol to the European Convention on Human Rights on protection of whistle-blowers".[5] After a first round of discussions on 6 November 2013, the committee decided, at its meeting on 27 January 2014, on the basis of my introductory memorandum,[6] to change the title of the future report from "Massive eavesdropping" to "Mass surveillance" and to organise a hearing with the participation of Mr Snowden during the Assembly's spring part-session, on 8 April 2014.

4. Unfortunately, it was not possible to receive the necessary assurances which would have allowed Mr Snowden to come safely to Strasbourg and to freely travel to a country of his choosing after the hearing. The committee therefore had to content itself with hearing Mr Snowden via a live video link from his temporary place of asylum in Moscow, whilst his German lawyer, Mr Wolfgang Kaleck, followed the discussions by a standing telephone line enabling him to provide advice to his client, if needed.

5. I should like to thank Mr Snowden for his readiness to address the committee and to answer questions "live", despite possible legal risks. His courage and dedication to the cause of Internet freedom and privacy, despite the obvious danger for his personal safety and freedom, commands the highest respect.

6. I should also like to thank the two other experts who participated in the hearing on 8 April 2014, namely Mr Hansjörg Geiger, former head of the German Bundesnachrichtendienst (BND), and Mr Douwe Korff, Professor of International Law, London Metropolitan University.[7]

7. I had already agreed that this would not be a report about Mr Snowden, but about the practices he has helped to disclose. But we cannot close our eyes to the fact that it was Mr Snowden whose courageous action triggered the public debate on the protection of privacy. His case also provides a particularly interesting example of the kind of balancing of interests which underlies the rules on the protection of whistle-blowers, which I have been mandated to look into in a second, separate report.

4. Motion for a resolution, Doc. 13288.
5. Motion for a resolution, Doc. 13278.
6. Document AS/Jur (2014) 2 of 23 January 2014.
7. The recording of the hearing is available on the website of the Parliamentary Assembly. A summary is included in the minutes of the meeting of 8 April 2014.

2. Nature and extent of mass surveillance

8. The Snowden disclosures have revealed a stunning array of mass surveillance programmes by the NSA, but also by the intelligence services of other countries. These secret programmes directly threaten the protection of human rights and international co-operation.

2.1. No communication methods spared: the NSA's mass surveillance programmes

9. All types of communications are intercepted through a multitude of tools and programmes that the NSA, as well as other intelligence agencies around the world, has developed. Targeted surveillance has always been used for legitimate law-enforcement measures and for protecting States from threats against their national security. But the disclosures on the NSA have raised serious concerns about the indiscriminate collection and analysis of data from citizens who are not suspected of having links to terrorism or other forms of crime. The following is now known about the various methods intelligence agencies use to intercept, store, and analyse data.

2.1.1. Accessing Internet company data: "front-door" and "back-door" access

10. NSA files revealed that the agency accessed Internet companies' customer data with or without their consent, and Special Source Operations (SSO), the division inside the agency dealing with collection programmes through private companies, was described in leaked documents as the "crown jewels" of the NSA. With its PRISM programme, said to be the biggest single contributor to the NSA's intelligence collection effort, the NSA has "front-door" access to data from nine Internet firms, including Google, Microsoft and Yahoo. The NSA has access to the customer data held by the companies through a (secret) court-approved process and could collect email, chat logs, stored data, voice traffic file transfers, or social networking data from them. The companies in question first denied having had any knowledge of this programme and later insisted that any co-operation with the intelligence agencies was compelled by law.[8] Subsequent disclosures also showed that the NSA and its British counterpart, the General Communications Headquarters (GCHQ), had "back-door access" too: the agencies were able to intercept data from those companies, without their knowledge, via a secret programme codenamed "MUSCULAR", in addition to the data they gathered with the companies' knowledge.[9]

2.1.2. Tapping fibre-optic cables

11. The United Kingdom was said to tap into fibre-optic cables carrying global communications and share the data with the NSA. Because much of the world's communication traffic passes through the United States or the United Kingdom, both States' agencies have a "home-field advantage" to intercept traffic flowing into and across their countries. While the Internet as a "virtual" electronic communications system is transnational, even global, by its very nature, its infrastructure (all sorts of switches, routers, servers and cables) is physical and located in real places. At present, many of these places are in the United States and in the United Kingdom.[10] In this way, the GCHQ has been able to access at least 200 fibre-optic cables, giving it the ability to monitor up to 600 million communications every day. Information on Internet and phone use was allegedly stored up to 30 days in order for it to be sifted and analysed.[11]

2.1.3. Collecting and analysing metadata: "less" data is more

12. "Metadata" is information about the time and location of a phone call or email, as opposed to the actual content 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 telecom providers. Those who defend unfettered metadata collection[12] 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".

---

8. *The Guardian*, 6 September 2013, "Revealed: how US and UK spy agencies defeat Internet privacy and security".
9. *The Washington Post*, 30 October 2013, "NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say".
10. "The rule of law on the Internet and in the wider digital world", Issue Paper prepared by Professor Douwe Korff (one of the experts invited to our committee hearing in April) published by the Council of Europe Commissioner for Human Rights in December 2014 (p. 8) (hereafter "The rule of law on the Internet").
11. *The Guardian*, 21 June 2013, "GCHQ taps fibre-optic cables for secret access to world's communications".
12. For example US Senator Dianne Feinstein, chair of the Senate intelligence committee (quoted by USA Today).

In fact, the Court of Justice of the European Union observed that communications metadata "taken as a whole may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained".[13] The Office of the United Nations High Commissioner for Human Rights has taken the same position – namely that the distinction between metadata and data is not persuasive – in its June 2014 report on data privacy, thus concluding that "any capture of communications data is potentially an interference with privacy and, further, that the collection and communications data amounts to an interference with privacy whether or not those data are subsequently consulted or used".[14] I find this convincing, even more so in light of former NSA and CIA chief General Michael Hayden's unrepenting admission that "we kill people on the basis of metadata".[15]

13. Because metadata allows agencies to get a much more concise representation of the huge amount of communication that it intercepts and still includes personal information that can be used to build an even more detailed "profile" of a person than through listening to the actual content, the NSA has extensively relied on metadata collection. In March 2013, the NSA was said to have collected up to 97 billion pieces of intelligence or metadata from computer networks worldwide. More than 14 billion were from Iran, 13.5 billion from Pakistan, and 12.7 billion from Jordan, and European States were not spared. According to NSA presentation slides about "Boundless Informant", a tool used by the NSA to analyse the metadata it holds, and to know what information is currently available about a specific country, the agency may have been collecting metadata also from European allies. The slide showed the amount of metadata associated with a country, with over 70.3 million items from France, 471 million from Germany, 45.9 from Italy and 60.5 from Spain, among others. The Norwegian and German Governments claimed that numbers labelled for the metadata collection for their countries on the presentation slides referred to metadata that they themselves had collected in Afghanistan and shared with the NSA. But the journalist Glenn Greenwald has contested this explanation, referring to the NSA's own FAQ slide for "Boundless Informant", which explains that the "tool allows users to select a country on a map and view the metadata volume and select details about the collection *against* the country", not *from* the country.[16]

2.1.4. Eavesdropping on phones, collecting text messages, bugging faxes

14. In January 2014, it was revealed that the NSA stores data on hundreds of millions of mobile phones worldwide. In particular, it stocked about 5 billion sets of localisation data per day, which the NSA can access even when a smart phone's GPS function is turned off by simply following the movement of a phone from one "cell tower" (local emitter) to another.[17] The NSA collects such location and travel habit data for "target development", for example to find unknown associates of "targets" it already knows.

15. More details on the numerous other programmes used by the NSA and its British counterpart to intercept phone text messages, phone calls and fax messages are now available. GCHQ documents revealed, and the NSA later confirmed, that a system codenamed "DISHFIRE" can be used to process and store SMS message data, collecting "pretty much everything it can" rather than merely storing the communications of existing surveillance targets. An NSA presentation from 2011 showed that the programme collected an average of 194 million text messages a day in April of that year, adding that the content was shared with the GCHQ. The NSA has used its vast text message database to extract information on people's travel plans, contact lists, financial transactions and more, including of individuals under no suspicion of illegal activities.

16. The NSA also developed the "MYSTIC" voice interception programme to gather mobile calls placed in countries with a combined population of more than 250 million people. It was later disclosed that the United States was able to conduct one such operation, codenamed SOMALGET, in the Bahamas and record every single phone call in the entire country without its government's knowledge or consent, processing around 100 million call events per day concerning the Bahamas and a second, unnamed country. The NSA collected this huge amount of data that was accessed by the US Drug Enforcement Administration (DEA), which can request legal wiretaps of foreign phone networks as part of international law-enforcement co-operation. With 80 offices worldwide, the DEA is the most widely deployed US agency around the world. But foreign States do not realise

13. Court of Justice of the European Union, judgment in joined cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others*, judgment of 8 April 2014, paragraphs 26-27 and 37.
14. Report of the Office of the United Nations High Commissioner for Human Rights, 20 June 2014, "The right to privacy in the digital age".
15. Video recording of a conference at Johns Hopkins University on 1 April 2014.
16. *The Guardian*, 8 June 2013, "Boundless Informant: NSA explainer – full document text".
17. *The Washington Post*, 4 December 2013, "NSA tracking cellphone locations worldwide Snowden documents show".

that its mandate includes collecting intelligence beyond fighting drug trafficking. Edward Snowden testified in his hearing before the committee on the method of "parallel construction," whereby (secret) intelligence information is (unlawfully) used for law-enforcement purposes, whilst it remains concealed from the courts dealing with the cases in question. This deprives the accused party of the right to challenge the legality of the initial surveillance.[18] Mr Snowden noted that the initial intelligence information in such cases is often gathered without a judicial warrant, as would be required in a traditional law-enforcement setting. This unlawful use of secret evidence, whose existence or source has been concealed from both the defendant and the court, is a serious threat to both the right to a fair trial and the right to face one's accusers. Moreover, many countries, including the Bahamas, use private contractors to install and maintain intercept equipment on their telecommunications infrastructures in order to facilitate taps. A senior technologist at the American Civil Liberties Union noted that these systems always introduce vulnerabilities into communications networks.[19]

17. The NSA can not only intercept phone calls from entire countries, but can also go back in time and listen to phone calls recorded during previous months, allowing for "retrospective retrieval", that is figure out what targets said during calls that occurred even before the targets were identified as such.[20] In contrast to its previous remarks that the NSA only intercepted metadata on calls, "RETRO" was found to be the NSA's programme with which analysts can even rewind and retrieve phone conversations as long as a month after they take place.[21] Analysts are said to listen to only a fraction (about 1%) of the calls, but the absolute numbers remain high. Although Presidential Policy Directive 28 issued by President Obama instructed the NSA and other agencies that bulk acquisition may be used only to gather intelligence related to one of six specific threats, including nuclear proliferation and terrorism, it noted that limits on mass collection do not apply to intelligence that is "temporarily acquired to facilitate targeted collection". The White House had tasked an independent group to review US surveillance policies, but President Obama refused the group's recommendation that agencies should, as a rule, purge incidentally collected calls and emails involving US citizens upon their detection. US officials interviewed for the *Washington Post* instead acknowledged that large numbers of conversations involving Americans would be gathered from countries where "RETRO" operated, and that the NSA did not attempt to filter out their calls, since the communications were incidentally acquired as a result of collection directed against appropriate foreign intelligence targets.

18. With the "PREFER" programme, the NSA could extract each day on average more than 5 million missed-call alerts to use in contact-chaining analysis (that is working out someone's social network from who they contact, and when), details of 1.6 million border crossings a day, more than 110 000 names from electronic business cards (including the ability to extract and save images), over 800 000 financial transactions (by text-to-text payments or linking credit cards to phone users), and extract geolocalisation data from more than 76 000 text messages a day. Documents suggest that communications from US phone numbers were removed from the database, but that those of other countries were retained.

2.1.5. Collecting millions of faces from web images

19. In addition to written and oral communications, the NSA has collected millions of faces from web images every day to develop the large untapped potential of using facial images, fingerprints, and other identifiers to track suspected terrorists and other intelligence targets.[22] One of its broadest efforts to obtain facial images is through its programme called "WELLSPRING", which strips out images from emails and other communications, and those that might contain passport images. In conjunction with programmes that it has developed itself, the NSA also relies in part on commercially available facial recognition technology; both government and private sector have been investing billions of dollars into face recognition research and development. According to the *New York Times*, it is unclear how many images the agency has acquired and the NSA said it had no access to US States' drivers license or passport photos, but it declined to confirm whether the agency had access to the State Department database of photos of foreign visa applicants or

18. Edward Snowden's testimony at the Parliamentary Assembly of the Council of Europe on 8 April 2014.
19. *The Intercept*, 19 May 2014, "Data Pirates of the Caribbean: the NSA Is Recording Every Phone Call in the Bahamas".
20. *The Washington Post*, 18 March 2014, "NSA surveillance program reaches 'into the past' to retrieve, replay phone calls".
21. *Russia Today*, 19 March 2014, "Rewind and Play: NSA storing '100 percent' of a nation's calls".
22. James Risen and Laura Poitras, "NSA Collecting Millions of Faces From Web Images", *The New York Times*, 31 May 2014.

whether the agency collected facial images of Americans from Facebook, other social media, or by other means. The US Congress has largely ignored the issue, with Senator El Franken stating that American "privacy laws provide no express protections for facial recognition data".[23]

2.2. Working with Five Eyes and more: collaboration between the NSA and intelligence agencies around the world

20. The Snowden disclosures revealed details of the "Five Eyes" collaboration, as well as the extensive partnerships that the NSA has with other States, including members of the Council of Europe.

2.2.1. Five Eyes: United States, United Kingdom, Australia, New Zealand and Canada

21. The "Five Eyes" intelligence sharing alliance is based on the 1946 UKUSA Signals Intelligence Agreement, which was later extended to Australia, New Zealand, and Canada. For instance, the Five Eyes share "ECHELON", a global intelligence-gathering network operated on behalf of the Five Eyes Alliance with a focus on intercepting private and commercial (rather than military) communications. The system is alleged to be able to intercept any "telephone, fax, Internet, or email message sent by any individual".

22. Mr Snowden's files have also unveiled the United Kingdom's individual and collective surveillance efforts. In addition to sharing data collected with the help of "TEMPORA", a programme established in 2011 to intercept large amounts of phone and Internet traffic by tapping into fibre-optic cables, with its American counterpart, the GCHQ also had some level of access to the NSA's "PRISM" programme since June 2010 and during the Olympics, and has requested further unsupervised access to data collected by the NSA. As of April 2013, the GCHQ had successfully lobbied for increased access to the data trove "supervised" by the NSA.

23. According to *The Guardian*, the programme "OPTIC NERVE" could collect still images of Yahoo webcam chats in bulk and save them to agency databases, regardless of whether individual users were an intelligence target or not. Substantial quantities of sexually explicit communications were included and in one six-month period of 2008 alone, the agency collected webcam pictures from more than 1.8 million Yahoo user accounts globally. The programme saves one image every five minutes from the users' feeds, partly to comply with human rights legislation and also to avoid overloading GCHQ's servers. *The Guardian* explained that the agency did make efforts to limit analysts' ability to see webcam images, restricting bulk searches to metadata only. Yahoo has denied prior knowledge of the programme.

24. The Joint Threat Research Intelligence Group (JTRIG), GCHQ's previously secret unit, engaged in cyber-offensive missions against people who had nothing to do with terrorism or national security threats. For example, JTRIG used DDoS (Distributed Denial of Service) tactics to shut down Internet chat rooms used by members of the "hacktivist" group known as Anonymous, also affecting others using the same servers or network (a form of "collateral damage").

25. Meanwhile, in Canada, Communications Security Establishment Canada (CSEC) used information from the free Internet access at a major Canadian airport to track wireless devices of thousands of ordinary airline passengers for days after they had already left the terminal. Canada legally prohibits the targeting of Canadians or anyone in Canada without a judicial warrant, and the agency is supposed to be collecting foreign intelligence by intercepting overseas phone and Internet traffic. The CSEC's written statement retorted however that it was "legally authorized to collect and analyse metadata" that apparently identified the travellers' wireless devices, but not the content of calls made or emails sent from them. CBC reported that this programme was a trial run of a powerful new software programme the Canadian agency was developing with the NSA's help, and that the technology tested in 2012 has since become fully operational.

2.2.2. More eyes in Europe too

26. More information on US-European collaboration and European States' own individual efforts for mass surveillance programmes have come into the public domain. In France, *Le Monde* revealed that the *Direction générale de sécurité extérieure* relied on free and total access to the networks and flow of data transiting through the French telecommunications company Orange, including information on foreigners as well as

23. Ibid.

French citizens.[24] Unlike the US Prism programme, however, France has not formalised co-operation between the DGSE and France Telecom-Orange, relying instead on informal connections made by engineers who have "shuttled" between the two institutions for the last 30 years at least.

27. The Netherlands has reportedly intercepted vast amounts of Somali telephone traffic and shared it with the NSA.[25] The Dutch authorities argued that they were not collecting information as per US requests, but to support the Dutch navy's own mission in the Gulf of Aden in order to combat piracy. The *NRC Handelsblad* suggested that the United States could have used the information for drone attacks against terrorism suspects.[26]

28. Denmark also collaborated closely with the United States on surveillance in the late 1990s. Secret documents revealed that Denmark was under "significant pressure" from the United States to change its laws and allow tapping of communication in order to stay within "the good company", also known as the "Echelon Network" or the "9-eyes" working closely with the NSA. During the 1998-2000 period described in the secret documents, the Danish national defence intelligence service allegedly received "technical assistance" to decrypt codes on tapped communication and surveillance techniques to tap the Internet and "identify illegal downloads on the Internet".[27] The Director of the Danish Defence Intelligence Service has neither confirmed nor denied the partnership with the NSA.[28]

29. The Snowden disclosures also revealed extensive collaboration between Germany and the United States. In June 2014, *Der Spiegel* revealed that the NSA was more active in Germany than anywhere else in Europe and described the increasingly intimate relationship that the American agency had developed over the past thirteen years with the *Bundesnachrichtendienst* (*BND*), the German foreign intelligence agency that reports directly to the Chancellor's Office.[29] Many sites of collaboration and surveillance were identified. The NSA's European headquarters in Stuttgart focuses closely on Africa and some intelligence documents state that the intelligence insights allowed for the "capture or killing of over 40 terrorists and has helped achieve GWOT (Global War on Terror) and regional policy successes in Africa" by passing on information to the US military's European Command or individual African governments. An agreement between Germany and the United States in 2004 established the now-named European Cryptologic Centre (ECC), currently the most important listening station in Europe. The office collects, processes, analyses, and distributes information and is presumed to be used for military purposes, but a presentation from 2012 suggests that European data streams are also monitored on a broad scale. The ECC targets Africa, as well as Europe, because ""most terrorists stop thru Europe" according to NSA slides.[30] The European Technical Centre in Wiesbaden is also said to serve as a "primary communications hub" of the NSA, with huge amounts of data intercepted and forwarded to NSA agents and fighters, and to foreign partners in Europe, Africa, and the Middle East. Last but not least, the Special Collection Service in the US Consulate General in Frankfurt was at the centre of a German investigation for tapping Chancellor Merkel's phone. Agents operating in this listening post, in addition to the one in the US Embassy in Berlin, are said to be protected by diplomatic accreditation, even though their job is not covered by the international agreements guaranteeing diplomatic immunity. As regards the co-operation between the BND and the NSA in Bad Aibling, based on a Memorandum of Understanding dating back to 2002, the Bundestag committee of inquiry on the NSA affair[31] has already held a number of public hearings with witnesses describing these activities, which were terminated in 2012.

2.2.3. Collusion for circumvention

30. These partnerships between US and allied services allow governments to easily engage in what could be termed "collusion for circumvention". For example, Britain's GCHQ intelligence agency is allowed to spy on anyone but British nationals, the NSA anyone but Americans, and Germany's BND anyone but Germans. Information-sharing partnerships allow each agency to circumvent its respective national restrictions protecting their own countries' citizens, since they are able to access the data collected by others.[32]

24. *Le Monde*, 20 March 2014, "Espionnage: comment Orange et les services secrets coopèrent".
25. *NRC Handelsblad*, "The secret role of the Dutch in the American war on terror".
26. Ibid.
27. Andreas Jakobsen, "Spying programs with NSA goes back years", *The Copenhagen Post*, 30 June 2014.
28. Anton Geist, Sebastian Gjerding, Henrik Moltke and Laura Poitras, 19 June 2014, www.information.dk/501280.
29. *Der Spiegel*, 18 June 2014, "New NSA Revelations: Inside Snowden's Germany File".
30. Ibid.
31. Paragraph 77.
32. *Der Spiegel*, 1 July 2013, "Cover Story: How the NSA Targets Germany and Europe".

31. This "collusion for circumvention" has important ramifications on the domestic level if it is strategically used to circumvent domestic legislation and limits on the government's ability to tap its own citizens' communications. The former President of the Federal Constitutional Court, Hans-Jürgen Papier, a former Constitutional Court judge, Mr Wolfgang Hoffmann-Riem, and another eminent expert, Professor Matthias Bäcker, stated that the BND is potentially violating the German Constitution by working with data received from the NSA. Furthermore, they argued that basic constitutional rights such as the privacy of correspondence, post and telecommunications apply to Germans abroad and to foreigners in Germany and that secret agreements between intelligence services cannot provide a legal basis for any interference with these rights. That would mean that this type of co-operation on surveillance between the BND and the NSA would be unconstitutional.[33]

32. In view of Mr Snowden's allegations in this respect at our hearing in June 2014, I addressed the following questions to the German, British and US authorities:

> *1. Is it true that the relevant US services (in particular the NSA) have obtained information on US citizens collected by their counterparts in Germany [in the United Kingdom] that they were not legally entitled to collect themselves?*
>
> *2. Is it true that in turn, the relevant US services provided their German [British] counterparts information on German [British] citizens that the German services were not legally entitled to collect themselves?*

33. The German answer is short and crisp: "German intelligence services respect the law. Personal data are transmitted to foreign intelligence services according to relevant statutory provisions. These provisions are not circumvented in any way."[34]

34. The British answer includes a helpful presentation of applicable legislation and review mechanisms[35] and stresses that "the gathering of information using State surveillance should be carried out in a proportionate and non-arbitrary manner, with legitimate purposes, in accordance with the rule of law and subject to effective oversight." Regarding my question, the letter says: "You have asked whether the strong working relationship between the GCHQ in the UK and NSA in the United States has been used to circumvent domestic legal regulations on the collection of information. The answer is emphatically no."

35. The US authorities have not replied to my letter and the reminder sent on 18 December 2014.

36. The strict wording of the German reply covers only the transmission of personal data to foreign intelligence services. Personal data of German residents are well-protected in law and there are no grounds to doubt that this protection is applied, as indicated in the letter. The public hearings in the Bundestag Committee of Inquiry concerning the so-called "set of issues relating to Bad Aibling" even provide some anecdotal evidence that the co-operation between the BND and the NSA using US and German facilities in this town, which was based on a Memorandum of Understanding of April 2002, was terminated in 2012 by the US side because it became frustrated with the German partners' insistence on (tediously) filtering out all data concerning Germans because of legal requirements based on Article 10 of the German Constitution (*Grundgesetz*). But the reply does not, at least not explicitly, refer to data concerning Germans received *from* foreign co-operation partners; and the Article 10-based protections for German data do not apply to foreigners, for example US citizens, whose data could thus indeed have been transmitted to their home country's intelligence services. In my understanding of the reports on the public hearings, the legal objections raised by the German partners which so "frustrated" their NSA colleagues concerned only German data.

37. The British reply regarding the circumvention issue is so strongly worded that I dare not put it into question. But it seems to me that since the (very) urgent adoption of the Data Retention and Investigatory Powers Act (DRIPA) in July 2014[36] and the rejection of the USA Freedom Act in September 2014, the real question is whether the relevant domestic legal regulations (in the United Kingdom and the United States) governing the retention and use of personal data are sufficiently narrowly drafted and assorted with sufficiently effective oversight in order to protect the privacy of British and US individuals. As I understand the new law, read in conjunction with the Regulation of Investigatory Powers Act (RIPA) adopted in 2000 and the interpretation given by the NSA to existing rules in the United States[37] allow for the wide-ranging collection,

33. *Der Spiegel*, 18 June 2014 (footnote 29).
34. Reply dated 26 September 2014 (translation by the secretariat).
35. Available from the secretariat.
36. Paragraph 74.
37. Paragraphs 44-52.

usage and transmission of personal data, in particular metadata, so that there seems to be little need for circumvention any more. This is confirmed by the ruling of the Investigatory Powers Tribunal (IPT) dated 5 December 2014,[38] which saw no problem in sharing intelligence with the NSA, or accessing information obtained through the NSA's PRISM programme, relying on secret government policies in reaching this decision.[39]

2.3. No one and nothing spared from surveillance

38. Despite strong partnerships and collaboration, if not collusion, between the NSA and intelligence agencies of certain allied countries, the Snowden files have shown that no States, individuals, or organisations – regardless of their ties with the United States – were exempt from surveillance.

2.3.1. US approval of surveillance over all but four countries in the entire world

39. In June 2014, the *Washington Post* revealed that the Foreign Intelligence Surveillance Court (FISC) allowed the NSA to intercept information "concerning" all but four countries in the entire world (namely the other four States of the Five Eyes coalition, except their sovereign territories, such as the British Virgin Islands) as well as international organisations such as the World Bank, the International Monetary Fund and the International Atomic Energy Agency.[40] The NSA is not necessarily targeting all targets identified in the certification at all times, but was granted the authority to do so.

2.3.2. Refusal to enter into "no-spy agreements" with any country

40. In spite of the exclusive relationship between the Five Eyes, an apparent disconnect surfaced between the understanding by the United States and the other four States as to whether their partnership included a "no-spy agreement" among themselves. Classified documents stated that the "NSA does not target its 2nd party partners, nor requests that 2nd parties do anything that is inherently illegal for NSA to do," underscoring the privileged relations the United States maintains with the Five Eyes.[41] Yet, the United States has repeatedly emphasised that it had no "no-spy agreement" with any country, not even the Five Eyes partners, and in fact, the text of the UK/USA agreement does not explicitly mention such an arrangement. The administration has instead clarified its position that while there are "no such formal agreements … [w]ith a very small number of governments, however, there are bilateral arrangements or understandings (which include, in appropriate cases, intentions, strictures, and limitations with respect to collection). These bilateral relationships are based on decades of familiarity, transparency, and past performance between the relevant policy and intelligence communities".[42]

41. This said, a draft memorandum leaked by Mr Snowden, entitled "Collection, Processing and Dissemination of Allied Communications", shows that even these long-standing trusting relationships have limits. The leaked memorandum 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 paragraph – 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, when it is in the best interests of the US and necessary for US national security".

2.3.3. A "European Bazaar": the watchers being watched

42. European countries, even those closely involved in the NSA's efforts, were not spared from US surveillance. Through the RAMPART-A programme, the NSA relies on foreign partners who provide access to communication cables and host US equipment to transport, process, and analyse the intercepted data. Once the partner country taps an international cable at an access point located in its territory, it sends the data to a

38. Paragraph 75.
39. Jennifer Baker, "Nothing illegal to see here: Tribunal says TEMPORA spying is OK", *The Register*, 5 December 2014.
40. *The Washington Post*, 30 June 2014, "Court gave NSA broad leeway in surveillance, documents show".
41. *Der Spiegel*, 1 July 2013, "How the NSA Targets Germany and Europe".
42. Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies (12 December 2013), p. 175.

processing centre, with the equipment provided by the NSA, before forwarding it to an NSA site located in the United States. As a result, States collaborate to collect and process the content of phone calls, faxes, emails, Internet chats, data from virtual private networks, and online video calls. At least 13 RAMPART-A sites were said to exist, with nine active in 2013. Thirty-three third party countries were revealed, and included Austria, Belgium, Croatia, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Italy, "the former Yugoslav Republic of Macedonia", the Netherlands, Norway, Poland, Romania, Spain, Sweden and Turkey among others.[43] These partnerships operate on the condition that the host country does not use the NSA's spy technology to collect any data on US citizens. In exchange, the NSA also agrees not to collect data of the host countries' citizens, subject to certain exceptions not described in the disclosed documents. Nevertheless, the bilateral agreements between the US and third party States not to spy on one another are meaningless and easily circumvented, resulting in what Mr Snowden called a "European bazaar". As Mr Snowden explained, the US can simply access communications of country A as it transits through country B, which would technically not violate its agreement with country A not to access A's communications. In fact, the NSA boasted in its own internal presentation that "we can, and often do, target the signals of most third party foreign partners" despite being supported by and working with those partner States.

43. Recent revelations about the NSA's repeated and continuous surveillance of Germany shows the extent of secretive monitoring the NSA carries out of its own allied States, whose activities and data seem at best tenuously related to US efforts to protect its own people from terrorist or other national security threats. Chancellor Angela Merkel, along with 121 other heads of States and government, was on the "Target Knowledge Base", the central agency database of individual targets that employees could use to analyse "complete profiles" of targeted people. In March 2013, the NSA also obtained a top-secret court order against Germany as part of US government efforts to monitor communications related to the country, while the GCHQ targeted three Germany companies in a clandestine operation that involved infiltrating the companies' computer servers and eavesdropping on the communications of their staff. Following the scandal of the NSA tapping the phone of Chancellor Merkel, a student named Sebastian Hahn has been identified as the second German citizen known to be under surveillance by the American agency. Hahn, based in Bavaria, was targeted by the US because he lawfully operated a server as part of Tor, a network for users trying to preserve the privacy of their activities on the Internet. Two of Germany's major public broadcasting channels, NDR and WDR, reported simultaneously that the NSA was spying specifically on individuals who use encryption and anonymisation procedures to hide data flows. Merely searching the web for software that encrypts data and provides further security to one's data caused the NSA to mark and track the IP address of the individuals conducting the search, regardless of where they were around the world. As of 10 July 2014, German Federal law-enforcement agencies are investigating two persons suspected of spying for the United States, one in the Federal Intelligence Service (BND) and another in the Defence Ministry in Berlin. The former was allegedly arrested when trying to sell some of the information he had been collecting for the US for two years to Russian intelligence.[44] In a country where surveillance is a particularly sensitive issue due to memories of abusive surveillance by the Gestapo (Nazi secret police) and the Stasi (East German State security police), such revelations contributed to considerably cooling relations with the United States.

2.3.4. Americans under surveillance, too

44. The US Government has repeatedly emphasised that it distinguished its treatment of Americans and foreigners for its surveillance programmes. For example, to obtain a court order to wiretap an American, the government must convince a judge that there is "probable cause" to believe the target is engaged in a crime on behalf of a foreign power; non-Americans need only be "suspected" of being foreign agents. But even Americans were not spared from their own government's surveillance. A few days after the Privacy and Civil Liberties Oversight Board approved of programmes operating under the authority of Section 702 that mainly targets foreigners,[45] the *Washington Post* reported that nine out of ten communications intercepted under these programmes were not direct targets of the NSA's surveillance measures and that ordinary Internet users, whether American or non-American, far outnumbered legally targeted foreigners.[46] For four months, the newspaper investigated an estimated 22 000 surveillance reports collected by the NSA between 2009 and

43. Algeria, Ethiopia, India, Israel, Japan, Jordan, Korea, Pakistan, Saudi Arabia, Singapore, Taiwan, Thailand, Tunisia, and the United Arab Emirates were the remaining third parties. See *Russia Today*, 19 June 2014, "NSA uses 33 countries to intercept web traffic – Snowden Files".

44. *Russia Today*, 7 July 2014, "Merkel's mad: German leader indignant over 'serious' US spying allegations".

45. See more in section 2.6.

46. *The Washington Post*, 5 July 2014, "In NSA-intercepted data, those not targeted far outnumber the foreigners who are".

2012, Obama's first term during which the NSA's domestic collection of data exponentially increased. The files leaked by Mr Snowden comprised a large number of emails, messages, photos, and documents that had valuable contents on a secret overseas nuclear project, identities of aggressive hackers into US computer networks, and military calamities affecting an unfriendly power. But the data also included "startlingly intimate, even voyeuristic" communications between more than 10 000 account holders who were not targeted but whose information was recorded nonetheless. In this sample, roughly nine in ten communications were not the direct targets of the NSA's surveillance, and based on numbers of a "transparency report" dated 26 June 2014 by the Office of the Director of National Intelligence, 89 238 people were targets of last year's collection under FISA (the Foreign Intelligence Surveillance Act, a US federal law authorising surveillance of "foreign intelligence information" between "foreign powers" and "agents of foreign powers") section 702. On the basis of the ratio found in Mr Snowden's sample, the Office's figure would amount to nearly 900 000 accounts, targeted or not, which were subjected to surveillance. Furthermore, nearly half of the surveillance files contained names, email addresses or other details that the NSA marked as belonging to US citizens or residents.

45. The NSA defended its practice by insisting that it only aims for valid foreign intelligence targets and the only possible conclusion from the *Washington Post*'s coverage was that such a target talks to an average of nine people. The NSA insists that incidental collection of information on untargeted individuals is inevitable and in other contexts, the US Government also strives to limit and discard irrelevant data (for example, for criminal wiretaps, the FBI is supposed to stop listening to a call if a suspect's wife or child is using the phone). Yet, it is worth noting that while some incidental collection happened because the individuals communicated directly with a target, others had a more tenuous link. For example, the NSA collected words and identities of every person who, regardless of subject, was posting or just reading in a chat room which the target had entered. Presumptions that senders of emails written in a foreign language or anyone on a chatroom "buddy list" of a foreign national is also a foreigner, or the fact that someone connects to a computer address that seems to be from overseas (though very simple tools called proxies can be used to redirect a user's data traffic around the world) were all grounds to meet the requirement that analysts have a "reasonable belief" that the targets have information of value about a foreign government, a terrorist organisation or the spread of non-conventional weapons under PRISM and Upstream rules.

46. This disclosure came only a few days after the Privacy and Civil Liberties Oversight Board's conclusion that the NSA's policy of intercepting communications, which the agency said was based on Section 702, included efforts to "minimize" so-called "by-catch" data that the Board had found to be largely effective.[47] Mr Snowden's sample shows that a high number of unintended targets' communications are still caught in the Agency's net. Moreover, this disclosure was significant because General Keith Alexander had repeatedly denied that Mr Snowden could have passed the actual content of the intercepted communications to a journalist – which he in fact did – because he did not have access to such data. Mr Snowden claims that his position as contractor for Booz Allen in the NSA's Hawaii operations centre gave him "unusually broad, unescorted access to raw SIGINT [signals intelligence] under a special 'Dual Authorities' role".

47. Additionally, the Snowden files revealed that US intelligence agencies monitored prominent American Muslim activists, lawyers, and politicians under laws intended to target terrorists and foreign spies.[48] According to documents disclosed, the NSA and FBI covertly monitored emails of prominent American Muslims, whose names were in a list of 7 485 email addresses monitored between 2002 and 2008, alongside foreigners long accused of terrorist activities. One of them was Mr Faisal Gill, a lawyer and former intelligence policy adviser in the Department of Homeland Security who had authorisation to access sensitive compartmented information, a classification level reserved for the country's most closely guarded secrets. He served in the US Army and worked in the George W. Bush Administration from late 2001 until 2005. Yet the NSA began monitoring his account in 2006, after he left his government job and co-founded a law firm with Asim Ghafoor, a Muslim rights advocate who represented foreign governments and Middle Eastern organisations in US courts, and who was also targeted by US intelligence according to the report. He was once again monitored by the NSA from March 2005 until at least March 2008, while he was suing the government over its prior, illegal surveillance of his personal communications.

48. In order to conduct surveillance over an American citizen, agencies have to show probable cause to believe that the American targets are agents of a foreign power or an international terrorist organisation, and that they "are or may be" engaged in or abetting espionage, sabotage, or terrorism. US officials insist that

47. *The New York Times*, 6 July 2014, "Officials Defend NSA After New Privacy Details Are Reported".
48. *The Intercept*, 9 July 2014, "Meet the Muslim-American Leaders the FBI and NSA Have Been Spying On".

internal checks in the current procedure prevent any abuses. The Justice Department's Office of Intelligence has various "gatekeepers" that frequently (in at least half the cases) reject applications or send them back for further review. Finally, before the Foreign Intelligence Security Court (FISC), the agent wishing to carry out surveillance of a US citizen must establish probable cause that the target is an agent of a foreign power and is engaged in, or about to engage in, one of the "three crimes" included in the FISA statute, namely an actual or potential attack or other grave hostile act, sabotage or international terrorism, or clandestine intelligence activities. Nearly all of the cases that reach the FISC get permission to proceed with surveillance, but the intelligence officials claim that only the strongest applications reach the court in the first place.

49. Yet, according to *The Intercept*, there is no adversarial process before the FISC and it is not known what the exact standard is to establish "probable cause". A former law-enforcement official said in an interview that judges often simply relied on the claims of the agents seeking the authorisation, and that he had obtained many warrants signed by a judge – in his pyjamas, in his living room – at 2am.

50. These disclosures are a disturbing reminder of past surveillance practices against civil rights activists like Martin Luther King – even more troubling given the more effective surveillance tools now in the hands of the government. One of the leaked NSA documents described a potential target of FISA surveillance as a "raghead"[49] and some law-enforcement officials involved in counterterrorism efforts have expressed bigoted and conspiratorial views about Americans of Muslim descent. *The Intercept* mentioned John Guandolo, a former counterterrorism agent who candidly described a Muslim lawyer as "major player in the Muslim Brotherhood in the US" or a "jihadi" who was "directly linked to Al Qaeda guys," simply because he represented Middle Eastern Foundations or governments. Guandolo's anti-Islamic views were even incorporated in basic training materials within the Bureau. This shows that people can become victims of intrusive surveillance on the basis of stereotypes and questionable evidence.

51. A joint response from the Office of the Director of National Intelligence and the Justice Department stated that "it is entirely false that US intelligence agencies conduct electronic surveillance of political, religious or activist figures solely because they disagree with public policies or criticise the government, or for exercising constitutional rights".[50] This response does not exclude that religion and criticism is used as an important factor in initiating surveillance and is in any case difficult to assess due to the lack of transparency regarding the standards used by government to initiate surveillance.

52. Meanwhile, a new whistle-blower came forward, John Napier Tye, the former section chief for Internet freedom in the State Department's Bureau of Democracy, Human Rights and Labor from January 2011 to April 2014, where he had clearance to receive top-secret and "sensitive compartmented" information. On 18 July 2014, Mr Tye revealed through the *Washington Post* that while discussions on mass surveillance have focused on collections that happened under Section 215 of the Patriot Act, the latter is only a small part of the picture and "does not include the universe of collection and storage communications by US persons authorised under Executive Order 12333" that has much more problematic implications for Americans than Section 215.[51] Executive Order 12333, issued by President Reagan in 1981, has no protections even for US citizens if the collection occurs outside US borders. Agents must get a court order to individually target someone under Order 12333, but if the contents of a US person's communications (both content and metadata) are "incidentally" collected while lawfully targeting another (foreign) individual, then Section 2.3.*c* of Order 12333 explicitly authorises the retention of such data, without any conditions or limits. Mr Tye stated that President Obama's own Review Group on Intelligence and Communication Technologies had Executive Order 12333 in mind when it advised in Recommendation 12 of its public report that the government immediately purge "incidentally" collected US communications, which the White House has refused to do.

2.4. Actual and/or potential politically-motivated abuses of mass surveillance

53. Recent disclosures have shown that mass surveillance has been used to undermine opposition politicians, human rights activists or journalists. As indicated in my introductory memorandum, the NSA monitored the use of pornographic websites by six Muslim men considered to be Islamist hate mongers in order to undermine their credibility and reputation.[52] Mr Snowden confirmed at the hearing before our committee that

49. A racist slur for a person wearing an (Islamic) headcover.

50. Joint Statement by the Office of the Director of National Intelligence and the Department of Justice on Court-ordered Legal Surveillance of U.S. Persons, 9 July 2014.

51. *The Washington Post*, 18 July 2014, "Meet Executive Order 12333: The Reagan rule that lets the NSA spy on Americans".

52. Document AS/Jur (2014) 02, 23 January 2014, paragraph 20.

the NSA has even used surveillance against human rights organisations. It is hard to imagine how spying on the likes of Amnesty International or Human Rights Watch can be justified by "national security interests". To the contrary, these organisations' activities, which are highly valued for their contribution to the promotion of our common values, are seriously undermined when victims and witnesses of acts of human rights violations no longer dare to communicate freely with those who try to help them because they must fear surveillance.

2.4.1. Targeted spying for political and economic purposes

54. The Snowden files have confirmed that States spy on one another or engage in surveillance that at best tenuously relates to anti-terrorism efforts. *Le Monde* reported that with its Upstream programme, the NSA was able to intercept communications of a variety of targets, including two Filipino leaders, Jejomar Binay and Manual Roxas, who are not known for any anti-American stance, a resort in Honduras that hosts international conferences, the International Centre for Theory of Physics in Italy, AT&T, the Saudi Telecom Company, the Austrian Internet company Chello, the Pakistani online security company Tranchulas and the Libyan International Telecom Company.[53]

55. Other examples of the NSA's targeted surveillance include those described in an internal NSA presentation from 2010. The slides showed that the GCHQ's "Royal Concierge" operation involved monitoring at least 350 upmarket hotels around the world for more than three years "to target, search and analyse reservations to detect diplomats and government officials". The agency listened in on telephone calls and tapped hotel computers, in addition to sending intelligence officers to observe the targets in person at the hotels.[54] *The Guardian* also revealed that the NSA used a programme called Dropmire to bug security-enhanced fax machines and access documents that passed through encrypted fax machines based in other countries' foreign embassies.[55]

56. The British intelligence agency collaborated with its American counterpart to extract information from "leaky" smartphone apps, such as the game Angry Birds. They were able to obtain the age, gender, location, phone model, screen size and, in some instances, sensitive information like sexual orientation through their mass surveillance tools.

57. The *New York Times* revealed that the NSA monitored an American law firm representing a foreign government in trade disputes against the United States[56] as well as other countries' preparations for the Copenhagen Climate Summit, including those by the host country, Denmark.[57] The NSA also engaged in targeted surveillance of the United Nations, the European Union, and other international organisations in a variety of ways, including bugging embassy phones and faxes, copying hard disks, and tapping into the internal computer cable network used by collaborators.[58] To cite a few examples out of the many that were revealed, the NSA used operation Blackfoot to gather data from French diplomats' offices at the New York United Nations headquarters.[59] Operation Perdido targeted the European Union's offices in New York and Washington, while Powell was a codename for the NSA's scheme to eavesdrop on the Greek UN offices in New York. The NSA's internal document indicated that its spying had a key influence on "American negotiating tactics at the UN" in connection with the Iraq War. Thanks to the intercepted conversations, the NSA was allegedly able to inform the US State Department and the American Ambassador to the UN with a high degree of certainty that the required majority had been secured before the vote was held on the corresponding UN resolution.[60] While the inclusion of traditional ideological adversaries and sensitive Middle Eastern countries could be "expected" and more easily explained in light of US anti-terrorism efforts, the inclusion of traditional allies discredits the contention that the purpose of surveillance is the protection of national security.

53. *Le Monde*, 8 May 2014, "Révélations sur les écoutes sous-marines de la NSA".
54. *Der Spiegel*, 17 November 2013, "'Royal Concierge': GCHQ Monitors Diplomats' Hotel Bookings".
55. *The Guardian*, 30 June 2013, "New NSA leaks show how US is bugging its European allies".
56. *The New York Times*, 15 February 2014, "Spying by N.S.A. Ally Entangled in Law Firm".
57. *The Guardian*, 30 January 2014, "Snowden revelations of NSA spying on Copenhagen climate talks spark anger".
58. *The Guardian*, 30 June 2014, "New NSA leaks show how US is bugging its European allies".
59. *Der Spiegel*, 1 September 2013, "'Success Story': NSA Targeted French Foreign Ministry".
60. *Der Spiegel*, 26 August 2013, "Codename 'Apalachee': How America Spies on Europe and the UN".

2.4.2. Blatant propaganda attacks

58. The United States and the United Kingdom have been shown to resort to propaganda attacks to support their own agenda. The US Agency for International Development conducted a secret programme called ZunZuneo to gather private data from Cuban Internet users, which it hoped to use in order to manipulate users and foment dissent against the Cuban Government.[61]

59. Additional disclosures showed similar British offensive efforts unrelated to terrorism or national security threats. Leaked slides showed that the British agency published false material via the Internet in order to destroy the reputation of targeted individuals and companies, while also trying to manipulate online discourse and activism in order to generate outcomes that it considered desirable. It engaged in false flag operations (i.e. posting material online and falsely attributing it to someone else) and posted fake blog entries, pretending to be a victim of the individual whose reputation they wanted to destroy.[62] *The Intercept* also revealed that the GCHQ has developed numerous covert tools to manipulate and distort online political discourse and disseminate State propaganda. Tools included programmes to manipulate the results of online polls, artificially inflate pageview counts on websites, "amplif[y]" sanctioned messages on YouTube, censor video content judged to be "extremist", monitor the use of the UK auction site eBay, and even connect two target phones together in a call.[63]

60. It is obvious that such manipulation techniques represent a serious threat to the rule of law in that they allow for the fabrication of evidence in criminal cases, for example against journalists or human rights activists accused of aiding and abetting terrorists.[64] At the same time, the existence of such manipulations makes it harder, if not impossible, to use genuine digital evidence in court against real criminals.

2.4.3. Lack of internal accountability in intelligence agencies

61. In an interview with *The Guardian* in July 2014, Mr Snowden testified that privacy violations by NSA agents who had access to intercepted private communications were "routine enough":[65]

> *"You've got young enlisted guys, 18-22 years old. They've suddenly been thrust into a position of extraordinary responsibility where they now have access to all of your private records. During the course of their daily work they stumble upon something that is completely unrelated to their work in any sort of necessary sense -– for example, an intimate nude photo of someone in a sexually compromising situation, but they're extremely attractive. So what do they do? They turn around in their chair and show their co-worker – and their co-worker says 'hey, that's great, send it to Bill down the way.' And then Bill sends to George, George sends it to Tom, and sooner or later this person's whole life has been seen by all of these other people."*[66]

62. A similar accusation came up in 2008, when NSA employees were said to be sharing within the agency sexually explicit phone calls they had intercepted,[67] but such abuses have gone largely undetected and unreported because of weak internal controls. There have been reports of NSA officers using the agency's surveillance techniques to snoop on love interests, "a practice common enough that it has its own spycraft label: LOVEINT".[68]

2.5. Installing "back doors", breaking encryption and sending malwares: how the NSA and its partners undermine Internet privacy and security

63. Almost all online communications are encrypted in some way to protect our private lives, communications and bank accounts from cyberattacks, thieves, or nosy neighbours. The NSA openly admits that it is its vital job to counteract its adversaries' use of encryption. But in this quest, the agency has resorted

61. *The Guardian*, 3 April 2014, "US secretly created 'Cuban Twitter' to stir unrest and undermine government".
62. *The Intercept*, 24 February 2014, "How Covert Agents Infiltrate the Internet to Manipulate, Deceive, and Destroy Reputations".
63. *The Intercept*, 14 July 2014, "Hacking Online Polls and Other Ways British Spies Seek to Control the Internet".
64. This is by no means a hypothetical danger. In a number of recent cases against journalists in Turkey, the defence alleges that fake emails were "planted" on their clients' computers by the authorities (see for example Dexter Filkins, Showtrials on the Bosphorus, *The New Yorker*, 13 August 2013.
65. *The Guardian*, 17 July 2014, "Edward Snowden urges professionals to encrypt client communications".
66. *The Washington Post*, 17 July 2014, "Snowden: NSA employees share sexts".
67. ABC News, 9 October 2008, "Exclusive: Inside Account of U.S. Eavesdropping on Americans".
68. *The Washington Post*, ibid. (footnote 66).

to methods that experts warn have the counterproductive consequence of undermining online security and leaving users vulnerable to intrusions into their private lives and data. 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 to install "back doors", that is secret vulnerabilities, to subvert commercial encryption software.

64. The NSA paid companies to deliberately set weaker encryption standards as the default choice for their safety software clients. Using "supply-chain interdiction", the agency could intercept US-made products, such as routers and servers manufactured by American companies such as Cisco, and implant them with beacons before they are repackaged and shipped to unaware consumers around the world.

65. According to an intelligence budget document leaked by Mr Snowden, the NSA. spends more than US$250 million a year on its "Sigint Enabling Project" designed to undermine security standards and implementation.[69]

66. The NSA has also aggressively accelerated hacking initiatives that it had repeatedly criticised when the US was the victim of such attacks. Using "malwares", the agency can gain total control of an infected computer, which then enables agents to take over a targeted computer's microphone and record conversations taking place near the device, covertly take over a computer's webcam and snap photographs, or record logs of Internet browsing histories and collect login details and passwords used to access websites and email accounts. The NSA has also computerised processes for large-scale dispatches of such "malwares" and shared many of its files on the use of "implants" with its Five Eyes alliance members. For example, the TURBINE system, which carries out automated implants of malwares to targets, has been operated with the knowledge and support of other governments, some of which have even participated in malware attacks. The GCHQ has played a particularly important role in helping to develop the malware tactics: it operated the Menwith Hill satellite eavesdropping base (the NSA's European hub in North Yorkshire) and applied some tactics itself, like when it reportedly hacked computers of network engineers at Belgacom, the Belgian telecommunications providers whose customers include several EU institutions.[70] A new disclosure by *The Intercept* on 4 December 2014, based on the Snowden files, shows that in an operation codenamed "AURORAGOLD", it is shown that the NSA has hacked the networks of mobile phone operators world-wide.[71] Another spyware programme apparently jointly developed by the NSA and the GCHQ was named "REGIN" when it was discovered by Internet security firms; the latter have reportedly succeeded in developing countermeasures.[72]

67. The flagship programme for the surveillance of the Internet on a global scale would appear to be the joint NSA/GCHQ "TREASUREMAP" disclosed in September 2014[73] on the basis of documents leaked by Mr Snowden. It is described as a vast NSA campaign to map the global Internet, seeking to identify and locate every single device (computer, tablet, smartphone) that is connected to the Internet somewhere in the world – "anywhere, all the time", according to leaked NSA documents. Maps extracted from TREASUREMAP show that the agencies broke into private satellite companies such as German-based Stellar. These security breaches potentially have enormous consequences, including the capability to cut entire countries off the Internet.[74]

68. Installing back doors, deploying malwares and deliberately weakening encryption systems creates new vulnerabilities in the targeted systems that other non-benevolent third parties can discover and exploit. The targeted computers and users' information are left defenceless not only to the governments' surveillance, but

69. ProPublica, 5 September 2013, "Revealed: the NSA's Secret Campaign to Crack, Undermine Internet Security".
70. See for example *SPIEGELonline* (English edition), 11 November 2013, GCHQ targets engineers with fax LinkedIn pages.
71. "The Intercept": Operation Auroragold – How the NSA Hacks Cellphone Networks Worldwide".
72. The functioning of the "super-trojan" Regin is described by C. Stöcker and M. Rosenbach, Super-Trojaner Regin ist eine NSA-Geheimwaffe, *SPIEGELonline*, 25 November 2014.
73. Some elements of Treasure Map were disclosed in November 2013 by the *New York Times* ("NSA Report outlined Goals for More Power").
74. See for a detailed description of Treasure Map and its implications: Andy Müller-Maguhn, Laura Poitras, Marcel Rosenbach, Michael Sontheimer and Christian Grothoff, "Map of the Stars, the NSA and GCHQ campaign against German Satellite Companies", *The Intercept*, 14 September 2014.

also other hackers, thieves and dangers from which the encryption system is supposed to defend users. I am therefore somewhat surprised that the head of Europol's European Cybercrime Centre[75] has asked for encryption to be allowed only subject to back doors being installed for their benefit.[76]

69. Moreover, such programmes were not only used against those who pose a threat to national security or to individuals regarded as "extremist" by the NSA. Targets have included systems administrators working at foreign phone and Internet service providers, none of whom were related to terrorist or other criminal activities. They were targeted because by hacking an administrator's computer, the NSA could gain covert access to communications that are processed by the administrator's company. Finally, the NSA has repeatedly reaffirmed its position that Mr Snowden was not able to access the raw data resulting from the agency's surveillance activities. Yet, the agency has proven itself incapable of safeguarding the extremely sensitive data it gathered.[77] What if Edward Snowden were a terrorist? What if such data fell into the hands of a totalitarian regime? The deliberate weakening of encryption and other Internet safety standards by the NSA and its allies for purposes of facilitating mass surveillance presents a grave danger for national security. These weaknesses can be detected and exploited by rogue States, terrorists, cyberterrorists and ordinary criminals, and even individual researchers, who independently discovered such weaknesses and published their exploits as a warning. They can take advantage of the schemes implemented by those entrusted with ensuring our security in order to wreak enormous damage on our societies.

2.6. Legislative, judicial, and political responses in the United States and United Kingdom following the Snowden disclosures

70. Following the Snowden disclosures, the US Government has reviewed and implemented some changes in its surveillance practices. In January 2014, the Privacy and Civil Liberties Oversight Board[78] criticised telephone records programmes conducted under Section 215 of the USA PATRIOT Act ("United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001") and the functioning of the Foreign Intelligence Surveillance Court. It concluded that collecting phone records in bulk had provided only "minimal" benefits in stopping terrorism,[79] was illegal, and should be shut down. The Board found "no instance in which the programme directly contributed to the discovery of a previously unknown terrorist plot or the disruption of a terrorist attack".[80] In its first report, the Board also recommended that the government limit analysts' access to the call records of people to no further than two links removed from a suspect (currently three), create a panel of outside lawyers to serve as public advocates in major cases involving secret surveillance programmes, and delete data faster. President Obama, in his Presidential Policy Directive of 17 January 2014[81] ultimately decided to cease government bulk collection of phone data and required individual warrants from the FISC for the NSA to access the data henceforth collected by the phone companies.[82] He also forbade eavesdropping on leaders of allied countries unless there is a compelling national security purpose. But the administration did not address the issue whether the United States would spy on other top officials from those countries. Finally, scrutiny of phone calls was limited to lines two steps removed from a number associated with a terrorist suspect. But President Obama did not accept

75. https://www.europol.europa.eu/ec3.

76. *SPIEGELonline*, 13 October 2014, "Cybercrime – Europäische Internetpolizei fordert Hintertüren"; ironically, a criminal extortion malware virus named "European Cybercrime Centre" demands the payment of hefty "fines" in return for unfreezing the computer infected by the virus (see for example http://pcviruskiller.blogspot.fr/2013/07/removing-european-cybercrime-centre.html).

77. *The Atlantic*, 7 July 2014, "The Latest Snowden Leak Is Devastating to NSA Defenders".

78. A bipartisan agency in the US executive branch whose role includes the review of the executive branch's anti-terrorism efforts to ensure they are balanced with the need for privacy and civil liberties.

79. This finding by an official US oversight panel is confirmed by an extensive study conducted under the auspices of the European Union (SURVEILLE Paper Assessing Surveillance in the Context of Preventing a Terrorist Act, FP7-SEC-2011-284725) published on 29 May 2014. The study, co-authored by, *inter alia*, Martin Scheinin and Douwe Korff, concludes that in comparison with traditional surveillance techniques, mass Internet monitoring fares poorly in terms of usefulness in anti-terrorism investigations: "Internet monitoring techniques, with the exception of targeted social networking analysis, represent an unacceptable interference with fundamental rights to privacy and data protection, the deepest ethical risks of chill and damage to trust, intrusion and discrimination, while also violating moral norms of proportionality of methods and consent of the policed. Meanwhile these high moral and legal costs reflect a mostly middling to poor usability benefit, performing worse with regard to cost, efficiency and privacy-by-design than lower tech alternatives. The case for a mass Internet monitoring system is wanting" (p. 50).

80. *The New York Times*, 23 January 2014, "Watchdog report says N.S.A. Program is Illegal and Should End".

81. PPD28: www.whitehouse.gov/sites/default/files/docs/2014sigint_mem_ppd_rel.pdf.

82. *The New York Times*, 30 June 2014, "Sky Isn't Falling After Leaks by Snowden".

some of the further-reaching recommendations of his advisory board on surveillance practices (for example requiring court approval for so-called national security letters, a kind of subpoena allowing the FBI to obtain information about persons from their banks, cell phone providers and other companies).[83]

71. In contrast, in July 2014, the Privacy and Civil Liberty Oversight Board's second report upheld the NSA's Internet tapping programmes pursuant to Section 702 of the Foreign Intelligence Surveillance Act. Section 702 covers the PRISM programme, under which the NSA collects foreign intelligence from Google, Facebook, Microsoft, Apple and nearly every other major US technology firm. According to the Board, the Section 702 programme has enabled the government to "acquire a greater range of foreign intelligence than it otherwise would have been able to obtain – and to do so quickly and effectively" for purposes such as tracking nuclear proliferation and monitoring terrorist networks to understand how they operate.[84] The Board's report concluded that in some aspects, the programmes "push to the line of constitutional reasonableness" because of the "unknown and potentially large scope of the incidental collection of US persons' communications", and offered some policy proposals to take the programmes more "comfortably into the sphere of reasonableness".[85]

72. In July 2014, the US Senate Intelligence Committee passed new cybersecurity legislation called the Cybersecurity Information Sharing Act (CISA) that critics of the NSA say would further broaden the Agency's access to the data of Americans.[86] If passed by the Senate, the Act would grant permission to government agencies to retain and share data for "a cybersecurity purpose" and allow private firms to share information regarding cyberattacks "in real time", in addition to shielding them from lawsuits by individuals for sharing data with each other and with the US Government.[87]

73. A legislative effort to (somewhat) rein in the NSA – the USA Freedom Act introduced in 2013 to end the NSA collection of US phone data – was defeated in the US Senate in November 2014. The bill had received support from the President, senior congress members from both parties, and more reluctantly from most civil liberty groups and the NSA. It was stopped in the Senate after critics depicted the bill as a "gift to terrorists"; it also failed to rally support from civil libertarians (including NSA whistle-blowers Thomas Drake and Bill Binney), who feared that the wording of the bill was so vague that it could even inadvertently expand the NSA's powers, given the NSA's history of expansive interpretation of legal provisions intended to restrict its powers.[88] The last hope for civil libertarians is the fact that Section 215 of the Patriot Act, on which much of the metadata collection is based, will be timed out in June 2015. This will give rise to new debates.[89]

74. In the United Kingdom, in July 2014, the government passed controversial emergency laws through all its House of Commons stages within a single day in order to continue to force Internet and communications companies to store their customers' usage and location data for up to a year and hand it over to law-enforcement services when requested. The government claimed this legislation was necessary to protect national security in light of events in Iraq and Syria. The rush also came in reaction to the ruling of the Court of Justice of the European Union (CJEU) in April 2014[90] holding that the EU Data Retention Directive, which required communications providers to store the traffic and location records (though not content) of their customers for up to two years, was disproportionate in relation to individuals' right to privacy. The new bill also introduced new oversight tools, including the establishment of a Privacy and Civil Liberties Oversight Board, and the government was required to publish annual "transparency reports". In response, United Nations Human Rights Commissioner, Navi Pillay, criticised the decision to fast-track the emergency surveillance bill and echoed civil liberties groups' concerns that the rushed procedure failed to address key privacy concerns raised by the CJEU when it struck down the EU Directive.[91]

83. *The New York Times*, 17 January 2014, "Obama Outlines Calibrated Curbs on Phone Spying".
84. *The New York Times*, 2 July 2014, "U.S. Privacy Panel Backs N.S.A.'s Internet Tapping".
85. Ibid.
86. *The Guardian*, 12 July 2014, "The Senate is giving more power to the NSA, in secret. Everyone should fight it".
87. President Obama threatened to veto a similar proposal (CISPA) in 2013 and his administration indicated that the draft CISA needs to be strengthened in terms of privacy protection in order to qualify for presidential support, www.bankinfosecurity.com/white-house-hasnt-backed-cisa-a-7126.
88. Spencer Ackermann, "Senate Republicans block landmark NSA surveillance reform bill", *The Guardian*, 19 November 2014.
89. Sebastian Fischer, Republikaner stoppen NSA-Reform, *SPIEGELonline*, 19 November 2014.
90. http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf.
91. *The Guardian*, 15 July 2014, "UN commissioner criticizes decision to fast-track emergency surveillance bill".

75. The legal challenge against the GCHQ's surveillance activities that Amnesty International, the American Civil Liberties Union, Privacy International and Liberty, among others, brought before the Investigatory Powers Tribunal (IPT) descended into "pure farce", according to Amnesty International.[92] During the proceedings, the government insisted that it would neither confirm nor deny any of their surveillance activities[93] which illustrates the difficulty of challenging secret government surveillance programmes in court. In its ruling dated 5 December 2014,[94] the IPT rejected the complaints against, *inter alia*, the TEMPORA programme revealed by Mr Snowden, finding this programme (if it were to exist...) in compliance with the law. The plaintiffs have announced that they will take this case to the European Court of Human Rights.

76. By contrast, constitutional courts in Austria, Bulgaria, Cyprus, the Czech Republic, Germany, Romania, and Slovenia, like the CJEU, have all rejected blanket data retention as unconstitutional.[95]

77. In Germany, the Bundestag set up a Committee of inquiry on the NSA affair on 20 March 2014.[96] The Committee's work is still going on, which is why I should like to limit myself to the following comments, based on publicly available information:

i. Firstly, I should like to commend the *Bundestag* for setting up such a committee of inquiry at all. I am not aware of any other parliament of a member State of the Council of Europe which has taken a similar step.

ii. Secondly, I am a little worried that, as in previous instances, the parliamentarians accept all too readily the executive's tactics of refusing to provide information to the committee on the ground that it must be kept secret on national security grounds. In his report on "State secrecy as an obstacle to judicial and parliamentary scrutiny of serious human rights violations",[97] our colleague Dick Marty has already made a similar remark with respect to the Committee of inquiry on the BND's role in the CIA renditions programme. A judgment of the German Federal Constitutional Court[98] following a complaint lodged by opposition members clarified the scope of the parliamentary right to information in a spirit of openness, stressing that the protection of the State's security interest is not a monopoly of the executive, but that it is a responsibility shared by parliament. This judgment came too late for the BND/CIA committee, but the NSA committee could rely on it to assert its information rights in a more robust way.

iii. Thirdly, I regret that the committee has not been able to agree on inviting Mr Snowden to Berlin. He is obviously an important witness, and it is doubtful that he can speak freely in Moscow.[99]

3. Implications of mass surveillance for human rights

78. Mr Snowden's disclosures inevitably raise the question of the human rights implications of the large-scale collection of private data. Former BND chief Hansjörg Geiger aptly summed up the situation before our committee: "To put it bluntly, if we have unfettered massive data surveillance by intelligence services then this is simply incompatible with safeguarding human rights".[100] Similarly, the Council of Europe's Commissioner for Human Rights has stated that "suspicionless mass retention of communications data is fundamentally contrary to the rule of law, incompatible with core data-protection principles and ineffective".[101]

92. Amnesty International, 18 July 2014, "UK hearing on mass government surveillance wraps up after 'farcical' week".
93. BBC News, 14 July 2014, "Tribunal hearing legal challenge over GCHQ surveillance claims".
94. https://www.privacyinternational.org/temporaipt.pdf.
95. BBC News (footnote 93).
96. www.bundestag.de/bundestag/ausschuesse18/ua/1untersuchungsausschuss.
97. Doc. 12714, paragraph 32.
98. Decision of 17 June 2009 (2 BvE 3/07), available (in German) at: www.bundesverfassungsgericht.de/entscheidungen/es20090617_2bve000307.html.
99. The opposition members seized the Federal Constitutional Court against the majority's refusal to invite Mr Snowden to testify in Berlin. The Court rejected the complaint on procedural grounds: under the law governing the work of committees of inquiry, it is the Federal Supreme Court (in Leipzig) and not the Federal Constitutional Court (in Karlsruhe) which is competent to hear this case, which concerns "only" the modalities of the implementation of a decision to take evidence.
100. Testimony of Mr Geiger before the committee on 8 April 2014.
101. The rule of law on the Internet (footnote 10), recommendation II.6 (p. 22).

3.1. Right to privacy

3.1.1. Council of Europe standards

79. Mass surveillance is a prima facie interference with Article 8 of the European Convention on Human Rights (ETS No. 5, "the Convention"), by which all member States of the Council of Europe are bound. The European Court of Human Rights ("the Court") has ruled on a series of data protection and surveillance cases, including applications concerning the interception of communications,[102] various forms of surveillance[103] and protection against storage of personal data by public authorities.[104]

80. Article 8.1 ("Everyone has the right to respect for his private and family life, his home and his correspondence") affirms the right to privacy, which is also enshrined in other human rights conventions, such as Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights.[105] Communications intercepted and stored under mass surveillance programmes without the consent of the targeted individual clearly fall within the scope of "correspondence" and "private life" in Article 8.[106] Even if the interference affects information that is available in the public domain, the Court found in *Segerstedt-Wiberg and Others v. Sweden*[107] and *Rotaru v. Romania,*[108] and reaffirmed in *Shimovolos v. Russia*[109] that "public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities".[110] According to the Court, "private life is a broad term not susceptible to exhausting definition" and can include activities of a professional or business nature.[111] Because the protection of personal data is of fundamental importance to a person's right to privacy, the Court has consistently found that "the systematic collection and storing of data by security services on particular individuals constituted an interference with these persons' private lives, even if that data was collected in a public place or concerned exclusively the person's professional or public activities".[112]

81. Article 8.2 provides for narrow exceptions for which the Court has developed a set of principles that governments must comply with when engaging in conduct affecting people's privacy as protected in Article 8.1. There are two conditions which must be met as detailed below.

82. The first is that the interference must be in accordance with the law. The law must be accessible and the person concerned able to foresee its consequences for him/her, in other words the law must be formulated with sufficient clarity and precision to give citizens adequate notice of the conditions and circumstances under which the authorities are empowered to interfere with the right to privacy. The law must provide for minimum safeguards for the exercise of discretion by public authorities, that is it should have sufficiently detailed and clear rules on the nature of the offences that could give rise to an interception order. Effective supervision and review should be provided by competent authorities to prevent abuse. The Court stressed that "it would be contrary to the rule of law for the legal discretion granted to the executive to be expressed in terms of an unfettered power", especially since risks of arbitrariness are evident when it comes to a form of power that the executive exercises in secret.[113]

---

102. *Malone v. the United Kingdom* (Application No. 8691/79, judgment of 2 August 1984).
103. *Klass and Others v. Germany* (Application No. 5029/71, judgment of 6 September 1978).
104. *Leander v. Sweden* (Application No. 9248/81, judgment of 26 March 1987), *S. and Marper v. the United Kingdom* (Applications Nos. 30562 and 30566/04, judgment of 4 December 2008).
105. The ICCPR prohibits arbitrary or unlawful interference with anyone's privacy or correspondence; it establishes for all State 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 privacy actors; it protects specific private domain such as a person's body, family, home, and correspondence; and it restricts the collection, use and exchange of personal data about the individual, often referred to as information privacy.
106. "Telephone conversations are covered by the notions of 'private life' and 'correspondence' within the meaning of Article 8" in *Klass and Others v. Germany*, Application No. 5029/71, judgment of 6 September 1978.
107. Application No. 62332/00, judgment of 6 September 2006.
108. Application No. 28341/95, judgment of 4 May 2000 (Grand Chamber).
109. Application No. 30194/09, judgment of 28 November 2011.
110. *Rotaru v. Romania* (footnote 108), paragraph 43.
111. *Shimovolos v. Russia* (footnote 109), paragraph 64, referring to *Niemietz v. Germany*, Application No. 13710/88, judgment of 16 December 1992, paragraph 29, and *Halford v. the United Kingdom*, Application No. 20605/92, judgment of 25 June 1997, paragraphs 42-46.
112. *Shimovolos v. Russia* (footnote 109), paragraph 64; see also *S. and Marper v. the United Kingdom*, Application Nos. 30562/04 and 30566/04, judgment of 4 December 2008.
113. *Segerstedt-Wiberg and Others v. Sweden*, Application No. 62332/00, judgment of 6 September 2006, paragraph 76.

83. In *Khan v. the United Kingdom*[114] and *PG. and J.H. v. the United Kingdom*,[115] the European Court of Human Rights found that covert listening devices planted by the police in a private home violated Article 8. At the time of the events, such measures were only governed by Home Office Guidelines, which were neither legally binding nor directly publicly accessible. Similarly, in *Copland v. the United Kingdom*, the use of covert listening devices and the collection and storage of information on the applicant's use of phone, email, and Internet, was found not to be "in accordance with the law" because no domestic law existed at the relevant time to regulate such monitoring.[116]

84. In *Kruslin v. France*, the Court found a violation of Article 8 in a telephone tapping ordered by an investigating judge in a murder case, because French law did not indicate with sufficient clarity the scope and manner of exercise of the authorities' discretion in this area.[117] In *Amann v. Switzerland*, the Court also found an Article 8 violation when the public prosecutor's office intercepted a telephone call the applicant received from the former Soviet embassy (for an order of a depilatory appliance advertised by the applicant), since Swiss law was unclear as to the authorities' discretionary power in the creation and storage of intelligence files of the type drawn up about the applicant.[118] The Court found similar violations for lack of clarity in the legal provisions allowing the systematic recording of conversations in a visiting room for purposes other than prison security in *Wisse v. France*[119] and the use of recording devices against murder suspects in *Vetter v. France*.[120] In *A. v. France*, the Court found a violation of Article 8 because the recording of a private individual in the context of a preliminary police investigation was not carried out pursuant to a judicial procedure and had not been ordered by an investigation judge.[121]

85. The second condition for an interference to fall under the exception under Article 8.2 is that the interference with the right to privacy shall be "necessary in a democratic society" in the interest of one of the stated goals in the second clause (national security, public safety, economic well-being, etc.). In *Segerstedt-Wiberg and Others v. Sweden*,[122] the applicants complained about the storage of information about them in Swedish Security Police files and the latter's refusal to reveal the extent of the information stored. The Court found in 2006 that for one of the applicants, it was legitimate for the government to keep information relating to bomb threats against the applicant and certain other personalities, since it was justified by the police's goal of preventing disorder or crime. In contrast, it found no legitimate aims for the other applicants who had been affiliated with certain left-wing and communist political parties. One had allegedly advocated violent resistance against police during demonstrations in 1969, while others were party members of KPLM(r), which advocates the dominion of one social class over another by disregarding the law. Because of the historical nature of the relevant information, however, the Court found that its storage could not have pursued any relevant national security interest.

86. *Klass and others v. Germany*, despite being from 1978, accurately shows the different benefits and dangers at stake with surveillance tools of the kind revealed through the NSA files. The Court recognised that:

> *"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".*[123]

114. Application No. 35394/97, judgment of 4 October 2000.
115. Application No. 44787/98, judgment of 25 December 2001.
116. Application No. 62617/00, judgment 3 April 2007.
117. Application No. 11801/85, judgment of 24 April 1990.
118. Application No. 27798/95, judgment of 16 February 2000.
119. Application No. 71611/01, judgment of 20 December 2005.
120. Application No. 59842/00, judgment of 31 May 2005.
121. Application No. 14838/89, judgment of 23 November 1992.
122. Application No. 62332/00, judgment of 6 September 2006.
123. Application No. 5029/71, judgment of 6 September 1978, paragraph 48.

87. But it also emphasised that technical advances have made espionage as well as surveillance much more sophisticated, and the Court emphasised that the threat of terrorism

> *"does not mean that the Contracting States enjoy an unlimited discretion to subject persons within their jurisdiction to secret surveillance. The Court, being aware of the danger such a law poses of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate".*[124]

88. The guidelines and requirements laid down in *Shimovolos v. Russia* provide guidance on legislative safeguards that all States must have to protect privacy under Article 8. According to the Court,

> *"where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident. It is therefore essential to have clear, detailed rules on the application of secret measures of surveillance, especially as the technology available for use is continually becoming more sophisticated. The law must be sufficiently clear in its terms to give citizens an adequate indication of the conditions and circumstances in which the authorities are empowered to resort to any measures of secret surveillance and collection of data. In addition, because of the lack of public scrutiny and the risk of abuse intrinsic to any system of secret surveillance, the following minimum safeguards should be set out in statute law to avoid abuses: the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to permit, carry out and supervise them, and the kind of remedy provided by the national law".*[125]

89. This case is especially illustrative of the forms of mass surveillance discussed in this report: the applicant, a human rights activist, was placed in a secret surveillance security database – and his movements subsequently tracked, which led to his arrest – based on a ministerial order that had not been published and was not accessible to the public. The public could thus not know why individuals were registered in the database, what type of information was included, for what duration, how it was stored and used or who had control over the information. In another case, *Association "21 December 1989" and others v. Romania*,[126] the president of an association that defended the interests of participants and victims of the 1989 events (a crackdown on anti-government demonstrations in Romania) had been subjected to surveillance measures, mainly phone tapping, by the secret services. The intelligence services had gathered information on the applicant in 1990, which they stored for 16 years. The Court found a violation of Article 8.

90. The Court's assessment of the quality of the law and safeguards against abuses of surveillance programmes depends on the circumstances of each case, including "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".[127] In *Klass and others v. Germany*, the Court found no violation of Article 8, because it found the surveillance measures in question necessary in a democratic society in the interests of national security and for the prevention of disorder or crime and that there were sufficient safeguards ensuring the review of such measures before, during, and after the monitoring. It concluded that the review bodies foreseen in the law were independent from the authorities carrying out the surveillance and vested with sufficient powers to exercise effective and continuous control over the monitoring process.

91. Additionally, the Court has also accepted, in *Association "21 December 1989" and Others v. Romania*,[128] that an individual, under certain conditions, can claim to be the victim of a violation residing in the mere possibility of secret measures on the basis of legislation allowing for this, without having to establish that such measures were in fact applied to him or. Otherwise, Article 8 would be "reduced to a nullity". This would also contravene Article 13 of the European Convention on Human Rights that guarantees that "everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity".

124. Ibid., paragraph 49.
125. Application No. 30194/09, judgment of 28 November 2011, paragraph 68.
126. Applications Nos. 33810/07 and 18817/08, judgment of 24 May 2011.
127. *Klass and others v. Germany*, Application No. 5029/71, judgment of 6 September 1978, paragraph 50.
128. Applications Nos. 33810/07 and 18817/08, judgment of 24 May 2011.

92. The pending case of *Big Brother Watch and Others v. the United Kingdom* and other cases brought after the Snowden disclosures[129] will show the Court's position on the GCHQ's mass surveillance programmes.[130] The applicants in *Big Brother Watch* allege that they are likely to have been the subject of generic surveillance by the United Kingdom security services, which may have been in receipt of foreign intercept material relating to their electronic communications. They contend that these interferences are not "in accordance with the law" as required under Article 8, because there is no basis in domestic law for the receipt of information from foreign intelligence agencies and there was no legislative control and safeguards in relation to the circumstances in which the UK intelligence services can request foreign intelligence agencies to intercept communications and share access to the data obtained, and the extent to which the United Kingdom can use, analyse, disseminate, store, and destroy data solicited and/or received from foreign intelligence agencies. In another case pending since 2006, *Roman Zakharov v. Russia,*[131] a Russian book editor complains about the lack of legal guarantees against the surveillance of his mobile phone communications. On the basis of an unpublished executive order, his mobile phone operator had installed equipment allowing the Federal Security Service (FSB) to intercept any phone communication without prior judicial authorisation.

93. In the meantime, the Court of Justice of the European Union addressed the issue of data privacy and found in *Google Spain v. Gonzalez*[132] that an Internet search engine operator is responsible for the processing that it carries out of personal data that appear on web pages published by third parties. The CJEU essentially upheld a right for citizens to request erasure of such personal data listings.

94. The Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) grants additional protection for any data processing carried out by the private and the public sector, including data processing by judicial and other enforcement authorities. The convention defines "personal data" as "any information relating to an identified or identifiable individual", which includes communications intercepted by government surveillance programmes. As of April 2014, this convention was ratified by all EU member States; it was amended in 1999 to enable the European Union to become a Party. It is the only legally binding international instrument in the data protection field. The convention allows the processing even of "sensitive" data, such as information pertaining to a person's race, politics, health, religion, sexual life or criminal record, in the presence of certain legal safeguards. The convention provides for the free flow of personal data between States Parties to the convention, but it also imposes restrictions on flows to States where legal regulation does not provide equivalent protection. The convention is currently undergoing a modernisation exercise. I strongly agree with the recommendation of the Council of Europe Commissioner for Human Rights that "the review of Convention No. 108 should not lead to any lowering of European or global data-protection standards. On the contrary, it should lead to a clarification and better enforcement of the rules, especially … in relation to surveillance for national security and intelligence purposes".[133]

3.1.2. Discussions at United Nations level

95. The Snowden files have also given rise to discussions at United Nations level. In December 2013, the UN General Assembly adopted Resolution 68/167, which affirmed that people's rights protected offline should also be protected online and called on all States to respect and protect the right to privacy in digital communications. On 30 June 2014, the Office of the United Nations High Commissioner for Human Rights presented a report[134] on the serious human rights implications that mass surveillance programmes have in the context of the International Covenant on Civil and Political Rights (ICCPR), which has been ratified by 167 States and includes in its Article 17 similar guarantees for the right to privacy as the European Convention on Human Rights. The report raised several important points that States will have to address in order to maintain legislation and policies up to date with the evolving nature of digital communications. First, it called for surveillance measures to be "lawful" (that is that the interference be authorised by States on the basis of law,

129. MTI-EcoNews/Hungary, 29 November 2013, "NGO to turn to Strasbourg court over security services' secret surveillance".
130. Application No. 58170/13, case communicated on 7 January 2014.
131. Application No. 47143/06 (see press release of the European Court of Human Rights with a summary of the facts and proceedings to date, announcing the oral hearing on 24 September 2014, CEDH 241 (2014) dated 29 August 2014; see also the analysis by Philip Leach cited in *The Guardian*, 25 September 2014 ("Russia's eavesdropping on phone calls examined by Strasbourg Court").
132. Case C-131/12, Grand Chamber judgment on 13 May 2014.
133. The rule of law on the Internet (footnote 10), recommendation II.4 (p. 22).
134. The right to privacy in the digital age, Report of the Office of the United Nations High Commissioner for Human Rights.

which must itself comply with the Covenant), not "arbitrary", and be "reasonable" (proportional to the end sought and necessary in the circumstances of the case at hand). The report asserts that mandatory third-party data retention (for example when States require communications companies to store data about their clients' communications) was neither necessary nor proportionate, and that the collection of data for a legitimate aim and its subsequent use for another also violated proportionality. It stressed that secret rules and secret interpretations – even secret judicial interpretations of law – [to which certain States have referred in order to justify their surveillance programmes] do not possess the necessary qualities of "law" as they are not sufficiently precise and accessible to enable potentially affected persons to regulate their conduct with foresight of the consequences that a given action may entail. To address legal loopholes that allow for "co-operation for collusion", the report found that State obligations to protect privacy arise as soon as the surveillance involves the exercise of the State's "power or effective control in relation to digital communications infrastructure".

96. The United Nations report finally noted that the different treatment of foreign and non-foreign targets contravenes the principle of non-discrimination in the ICCPR – a key issue in my view also. It stressed the need to have an effective oversight process over surveillance programmes, a combination of administrative, judicial, and parliamentary oversight mechanisms that are truly impartial, independent and transparent. Finally, the report suggested that States make effective remedies available to those whose privacy was violated and that the business sector, to the extent that it has been entrusted with a role of "law-enforcement and quasi-judicial responsibilities [as] Internet intermediaries under the guise of 'self-regulation' or 'co-operation'",[135] should explicitly commit to respecting and protecting human rights.

3.2. Freedom of speech, right to information and freedom of association

97. Regardless of whether individuals are aware of being targets of mass surveillance, the indiscriminate interception and collection of data has important ramifications with regard to the freedoms of speech, information and association. The knowledge that States engage in mass surveillance has a chilling effect on the exercise of these freedoms. According to a November 2013 report by PEN International[136] on the effects of NSA surveillance, the vast majority of writers are not only worried about government surveillance, but are also engaging in self-censorship as a result. 85% of the 520 American writers who responded to the survey said they were worried about government surveillance.[137] 28% have curtailed or avoided social media activities, 24% have deliberately avoided certain topics in phone or email conversations, and 16% have avoided writing or speaking about a particular topic. When authors, journalists or civil society activists are reluctant to write, speak, or pursue research about certain subjects (for example the Middle East, criticisms of the government post-9/11, the Occupy movement, military affairs, etc.) or to communicate with sources or friends abroad for fear that they will endanger their counterparts by so doing, this does not only affect their freedom of speech, but also everyone else's freedom of information.

98. As mentioned above, the NSA has targeted individuals who had merely searched for certain words indicating their desire to protect their data, visited certain websites, or passively read an online forum where other suspected individuals were chatting. Awareness that governments are likely to target individuals who gather on certain websites affects people's freedom to navigate through the online world or communicate with people they think might raise the authorities' suspicions for one reason or another.

99. In October 2014, President Putin announced tougher surveillance of the Internet in Russia, to guard against hacker attacks and propaganda for violence and extremism.[138] As the latter term is known to be interpreted widely by Russian law enforcement, this announcement is ominous, even though the President vowed to uphold the democratic principles of freedom of expression and information.

3.3. Democracy

100. Indiscriminate mass surveillance also presents substantial dangers for democracy if intelligence agencies bypass democratic political and legal channels to implement programmes that intercept a large amount of private communications. Files disclosed by Mr Snowden show that States have made false claims of ignorance about their intelligence agencies' co-operation with the NSA in conducting various forms of mass surveillance nationally and internationally. In the United Kingdom, ministers have claimed to have been in

135. Ibid., p. 14.
136. An association of writers that promotes literature and freedom of speech worldwide.
137. www.pen.org/sites/default/files/Chilling%20Effects_PEN%20American.pdf.
138. *SPIEGELonline*, 1 October 2014, Internetüberwachung – Putin klagt über Hacker-Angriffe.

complete ignorance of TEMPORA, the largest GCHQ spying programme, while President Obama claimed he was kept unaware of the NSA's surveillance of Chancellor Merkel's personal cell phone. Top-ranking German politicians have expressed outrage following the disclosure of mass surveillance of the German population.[139] Subsequently, disclosures of extensive co-operation by German intelligence services in such surveillance have emerged.[140]

101. Such supposed or actual ignorance suggests that some parts of government, let alone the public that is directly affected by the surveillance programmes, was not properly consulted. In fact, a leaked NSA document revealed that: "Upon being asked whether political shifts within those nations affect the NSA's relationships, the SIGINT ['signals intelligence'] official explain[ed] why such changes generally have no effect: because only a handful of military officials in those countries are aware of the spying activities. Few, if any, elected leaders have any knowledge of the surveillance."[141] While it is of course not advisable or even possible to place all intelligence activities under full public scrutiny, constitutional political processes ensuring the services' accountability before democratically elected leaders must not be bypassed. Parliamentary oversight bodies must have sufficient access to information and resources in order to fulfil their mandate in a meaningful way. In my view, an idea I heard in Brussels earlier this month makes eminent sense: in order to give parliamentary oversight bodies teeth, they should be given a say in the budgetary appropriations for the services they oversee. In my own experience, budgetary responsibility is indeed a very effective form of political accountability.

102. As noted in my introductory memorandum,[142] the runaway surveillance machine is 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.[143] I still do not want to believe that he lied. But he was at the very 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;[144] if an attack is not be averted, the cause must have been insufficient surveillance… The parallel to the privatisation of prisons in the United States is worrying: since privatisation began in the early 1980s, the US prison population has at least tripled, despite a decrease in the crime rate during the same period.[145] The "rise of the prison industrial complex"[146] may find itself matched or even surpassed by the rise of the "surveillance-industrial complex".

3.4. Extraterritorial application of human rights and equal treatment of domestic and foreign residents

103. We have seen that national law provides more or less solid legal protections for the privacy rights of residents – fairly solid in Germany, somewhat less so in the United States[147] or the United Kingdom, whose populations lack the distrust of their respective intelligence agencies that Germans owe to the ravages of the Gestapo and Stasi. But these protections (and even the improvements under discussion in the United States and elsewhere) simply do not apply to foreigners, who are treated as fair game: only "US persons" (citizens and residents) benefit from the First Amendment (free speech and freedom of association), the Fourth Amendment (protection against "unreasonable searches") and from most of the (limited) protections under the

139. See references in the introductory memorandum (AS/Jur (2014) 02), paragraph 23.
140. See paragraph 29 above and footnote 31.
141. *The Intercept*, 13 March 2014, "Foreign Officials In the Dark About Their Own Spy Agencies' Cooperation with NSA".
142. Document AS/Jur (2014) 02, paragraph 52.
143. Fred Kaplan, "James Clapper lied to Congress about NSA surveillance", 11 June 2013.
144. But the NSA stepped up surveillance well before 11 September 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 has not been instrumental in preventing terrorist attacks (p. 104).
145. See, for example, www.globalresearch.ca/the-prison-industry-in-the-united-states-big-business-or-a-new-form-of-slavery/8289.
146. John W. Whitehead, "Jailing Americans for profit: the rise of the prison industrial complex", *Huffington Post*, 4 October 2012.

national security legislation.[148] The December 2014 report of the Council of Europe's Commissioner for Human Rights aptly sums up how this state of affairs runs counter to the general trend in international human rights law to broaden the scope of the extraterritorial application of the States' human rights obligations (including those under the ICCPR, which the United States has ratified) and why it constitutes a violation of the principle of equal treatment.[149] For the purposes of this report, the unique position of the United States (and the United Kingdom) with regard to the physical infrastructure of the Internet and the fact that private companies based in the United States collect and store huge amounts of data of persons residing anywhere in the world makes the exclusion of "non-US (and UK) persons" from any legal protection against mass surveillance simply intolerable – it may well lead to the destruction of the Internet as we know it, as we will see below.

4. Implications of mass surveillance on international co-operation and the future of the Internet

104. First, revelations that the NSA spied on even its closest allies have affected State-to-State relations. In Brazil, President Rousseff has strongly condemned NSA surveillance, stating, at an address before the United Nations General Assembly in September 2013, that: "We face … a situation of grave violation of human rights and of civil liberties; of invasion and capture of confidential information concerning corporate activities, and especially of disrespect to national sovereignty of my country."[150] Ms Rousseff even called off a visit to the United States after revelations that the NSA had intercepted emails and messages from her, as well as those of the State oil company Petrobras.[151] Brazil has since attempted to route Internet traffic around the United States in order to avoid surveillance. On 2 July 2014, India summoned a senior US diplomat over reports that the United States had authorised the NSA to spy on the ruling party, the BJP, in 2010 when it was in the opposition.[152]

105. US-German relations have also substantially soured over the surveillance affair. The German Government terminated its contract with US-based Verizon Communications Inc. on communication services to government agencies from 2015.[153] A public outcry followed revelations that the NSA was spying on Chancellor Merkel and other high-profile Germans. *Der Spiegel* accused the NSA of "turning the Internet into a weapons system", while the *New York Times* reported that Ms Merkel likened NSA wiretapping of her phone to Stasi eavesdropping. German Justice Minister Sabine Leutheusser-Schnarrenberger, who had strongly criticised the United States since the PRISM scandal, called US surveillance methods "reminiscent of methods used by enemies during the Cold War". Months of negotiations on a no-spy agreement between Germany and the United States ended unsuccessfully, as the two sides could not agree on its scope.[154] Although Ms Merkel advised against inviting Mr Snowden to testify before the above-mentioned Committee of Inquiry set up by the German Parliament, to avoid further damage to the relationship between the United States and Germany, relations were strained again following reports of two alleged double agents spying on Germany on behalf of the United States. These disclosures were made when the Bundestag Committee of Inquiry heard the testimony of two former NSA collaborators, Thomas Drake and William Binney, on the NSA's mass surveillance programmes and the German BND's alleged co-operative role. After cautiously asking for explanations from Washington, especially since President Obama had earlier ordered a complete review of spying on allies and other partners following the disclosure of the wiretap against Ms Merkel, Germany not only summoned US ambassador John B. Emerson to the Foreign Ministry on 4 July 2014, just before the American Embassy's

147. An excellent overview of the legal basis for surveillance activities in the United States under Section 702 FISA, Section 215 US Patriot Act and Executive Order 12333 is provided in the Report on Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection dated 27 November 2013. This document points out, *inter alia*, the fundamental difference between the European Union's definitions of data collection and processing and those used by the US side, which, contrary to EU law, does not generally consider the initial acquisition of personal data as "processing" of personal data within the meaning of the protections provided by law. The document also demonstrates that the main problem is not the illegality, under American law, of the NSA's surveillance activities, but the weakness of the existing legal provisions which appear to cover most of the practices disclosed by Mr Snowden.

148. The rule of law on the Internet (footnote 10), p. 11, and the Commissioner's recommendations under I.1 (p. 21).

149. The rule of law on the Internet (footnote 10), p. 48-50.

150. *USA Today*, 29 October 2013, "Global reaction to NSA spying reports" for a sample of reactions from leaders around the world to the disclosures about the NSA.

151. BBC News, 17 September 2013, "Brazilian President Dilma Rousseff calls off US trip".

152. Harmeet Shah Singh and Ben Brumfield, "India summons U.S. diplomat over report of NSA spying", CNN.com, 2 July 2014.

153. Anton Troianovski and Danny Yadron, "German Government Ends Verizon Contract: Interior Ministry Cites Security Concerns Amid U.S. Spying Disclosures", *Wall Street Journal*, 26 June 2014.

154. *The New York Times*, 2 May 2014, "Merkel Signals That Tension Persists Over U.S. Spying".

national holiday party for hundreds of guests,[155] but also invited the CIA Station Chief to leave Berlin, stopping short of formally expelling him from the country.[156] Certain Bundestag offices were even said to have seriously considered reverting to the use of typewriters for particularly sensitive communications in order to foil further NSA surveillance.[157]

106. Yet, some have called governments' initial responses to the revelation of the NSA's mass surveillance programmes as "surprisingly muted", because leaders have been generally aware that foreign intelligence agencies – as well as their own – routinely engage in such surveillance activities.[158] A representative example was the United Kingdom. Following the destruction of computers and files that journalists of *The Guardian* had received from Edward Snowden, Prime Minister Cameron even made a public announcement that "[i]f they [newspapers] don't demonstrate some social responsibility it will be very difficult for government to stand back and not to act", essentially warning British newspapers against reporting on the content of the Snowden files. In August 2013, David Miranda, the partner of Mr Greenwald who had been given access to the Snowden files, was even detained under anti-terrorism laws at Heathrow airport for nine hours on his way to Rio de Janeiro. The Brazilian citizen reportedly had his mobile phone, laptop, DVDs and other items seized. As Jonathan Marcus stated on BBC news,

> *"European governments friendly to the United States are somewhat upset and the Obama Administration is somewhat embarrassed. I say 'somewhat' because, as much of the commentary in the wake of these disclosures has indicated, there is a kind of shadow game going on here. It is a bit like that moment in the classic film 'Casablanca' when the police chief expresses his shock that gambling is going on in an establishment he well knows is a casino, only moments before being handed his own winnings by a clerk".*[159]

107. Or as US Defence Secretary Donald Rumsfeld once put it, "stuff happens". But the confirmation that close allies spy on one another puts political and economic co-operation in other areas at stake. The public's trust in their own country's government and companies has also eroded, because actors in both the public and private sectors were shown to have colluded with the NSA. Europe's Internet users have increasingly complained about the dominance of American tech companies, particularly when it comes to handling data, although they still heavily rely on those companies.[160] Google still maintains an 85% market share for search in the five largest European economies, including the United Kingdom, France and Germany, in contrast to the 65% Google has in the American market. Facebook has also more than doubled its number of European users to over 150 million in the last five years, and according to comScore statistics, American tech companies operate seven of the ten most visited websites.

108. In response to growing discontent with US surveillance, one political response has been to push for more "technological sovereignty" and "data nationalisation". The Snowden disclosures have therefore had serious implications on the development of the Internet and hastened trends to "balkanise" the Internet to the detriment of the development of a wide, vast and easily accessible online network. The Internet as we knew it, or believed we knew it, is a global platform for exchange of information, open and free debate, and commerce. But Brazil and the European Union, for example, have announced plans to lay a US$185 million undersea fibre-optic cable between them to thwart US surveillance. German politicians have also called for the development of a "German Internet" for German customers' data to circumvent foreign servers and the information to stay on networks that would be fully under Germany's control.[161] Russia passed a law obliging Internet companies to store the data of Russian users on servers in Russia.[162] After a six-month inquiry following the Snowden disclosures, the European Parliament adopted a report on the NSA surveillance programme in February 2014,[163] which argues that the European Union should suspend bank data and "Safe Harbour" agreements on data privacy (voluntary data protection standards for non-EU companies transferring EU citizens' personal data

155. *The New York Times*, 6 July 2014, "Ties Strained, Germans Press U.S. to Answer Spy Allegation".
156. *The Telegraph*, 10 July 2014, "Germany asks CIA station chief in Berlin to leave country over US spying row".
157. *Forbes*, 19 July 2014, "German NSA Inquiry Chief Proposes Ultimate Cybersecurity Move… Use a Typewriter".
158. Karen Kornbluh, Senior Fellow for Digital Policy, Council on Foreign Relations, "Global Responses to NSA Surveillance: 3 things to know".
159. BBC News, 26 October 2013, "NSA spying allegations: Are US allies really shocked?".
160. *The New York Times*, 6 July 2014, "Principles Are No Match for Europe's Love of US Web Titans".
161. Reuters, 25 October 2013, "Germany wants German Internet as spying scandal rankles".
162. Hogan Lovells, Chronicle of Data Protection, Russia Enacts Data Localization Requirement; New Rules Restricting Online Content Come into Effect (posted on 18 July 2014).
163. Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI)).

to the US) with the United States. MEPs added that the European Parliament should only give its consent to the EU-US free trade deal (TTIP) that is being negotiated if the US fully respects EU citizens' fundamental rights. The European Parliament is seeking tough new data protection rules that would place US companies in the difficult situation of having to check with EU authorities before complying with mandatory requests made by US authorities. The European Parliament's LIBE Committee also advocated the creation of a "European data cloud" that would require all data from European consumers to be stored or processed within Europe, or even within the individual country of the consumer concerned. Some nations, such as Australia, France, South Korea, and India, have already implemented a patchwork of data-localisation requirements, according to two legal scholars.[164]

109. In my view, the European Parliament's proposals to make use of all the instruments at the European Union's disposal in its relations with the United States in order to build up pressure in favour of protecting the privacy of European citizens deserves every support. Both in negotiating new agreements such as the Transatlantic Trade and Investment Partnership (TTIP) and in implementing existing ones such as the Terrorist Finance Tracking Programme (TFTP) or the Passenger Name Records (PNR) agreement and the Safe Harbour decision,[165] EU negotiators should make it clear that Europe does not accept to be spied on by its transatlantic partner. Equal protection in law and practice of European and US persons' privacy rights should be part and parcel of a partnership based on mutual respect and trust.[166]

110. By contrast, suggestions to "nationalise" Internet traffic are 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.[167] Furthermore, experts consider that the sophistication of defence measures, rather than the location of data, is what truly matters for communications security.[168] Most importantly, such re-nationalisation measures may well be counterproductive from the point of view of the principles upheld by the Council of Europe. National routing typically does not protect fundamental rights, but rather the opposite. It is abused for instance in China or Iran where governments seek to restrict the availability of information to their citizens: "The localisation 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."[169] Some member States of the Council of Europe may also be tempted.[170]

5. Possible solutions to minimise negative consequences of mass surveillance, and the role of the Council of Europe

111. The Snowden files have shown the need to establish a more precise legal framework for surveillance activities, within and outside of national borders. The Council of Europe has an important role to play in this respect, as it is not, contrary to the European Union, precluded from dealing with the national security aspects of human rights protection.

5.1. Reviewing national legislation with a view to adapting the protection of privacy to the challenges posed by technological advances enabling mass surveillance

112. Since July 2014, several new cases that directly involve mass surveillance programmes disclosed through the Snowden files are pending before the European Court of Human Rights. The Court's existing case law has already established that the States must establish a transparent process to ensure that only the requisite amount of surveillance takes place, for a clearly defined set of objectives that require and justify

164. *The Atlantic*, 25 June 2014, "The End of the Internet?".
165. Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU, 27 November 2013 (European Commission document COM(2013)847 final).
166. Communication from the Commission to the European Parliament and the Council, Rebuilding Trust in EU-US Data Flows, 27 November 2013 (European Commission document COM(2013)846 final).
167. 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 (p. 12).
168. *The Atlantic*, 25 June 2014, "The End of the Internet?".
169. Mascolo and Scott, *op. cit.*, p. 12.
170. See, for example, the report by Human Rights Watch on "Turkey: Internet Freedom Rights in Sharp Decline", 2 September 2014; regarding Azerbaijan, see overview by Freedom House, "Freedom on the Net/Azerbaijan" (2013).

affecting the right to privacy. Rather than awaiting findings of violations by the Court, the member States of the Council of Europe should proactively review their legislation to ensure that it is (still) adapted to the challenges posed by the technological advances enabling mass surveillance on the scale revealed by Mr Snowden.

113. National law should allow the collection and analysis of personal data (including so-called metadata) only with the consent of the person concerned or following a court order granted on the basis of reasonable suspicion of the target being involved in criminal activity. Unlawful data collection and treatment should be penalised in the same way as the violation of the traditional mail secret. The creation of "back doors" or any other techniques to weaken or circumvent security measures or exploit their existing weaknesses should be strictly prohibited. Given the particularly strong role played by private businesses in the collection and treatment of personal data, all private institutions and businesses collecting or holding such data should be held to stringent security standards.

114. In order to enforce such a legal framework, member States should also ensure that their intelligence services shall be subjected to adequate judicial and parliamentary control mechanisms. Control bodies shall be given sufficient access to information and expertise. They should also have the power to review international co-operation without regard to the so-called originator control principle (according to which the service with whom the information in question has originated has the right to determine with whom this information is shared). This shall be valid on a mutual basis, on the common understanding that in all States under the rule of law, intelligence services are subject to judicial or parliamentary controls.

5.2. An international "Intelligence Codex" laying down mutually accepted ground rules

115. The political problems caused by "spying on friends" and the possible collusion between intelligence services for the circumvention of national restrictions show the need for States to come up with a generally accepted "codex" for intelligence services that would put an end to unfettered mass surveillance and confine surveillance practices to what is strictly needed for legitimate security purposes. Such a codex would lay down precisely what is allowed and what is prohibited between allies and partners; it would clarify what intelligence agencies can do, how they can co-operate, and how allies should refrain from spying on each other. As explained at the committee's hearing on 4 April 2014 by Mr Hansjörg Geiger, former head of the German BND and State Secretary at the Ministry of Justice, such a codex would be a signal that governments are willing to provide some degree of transparency in the conduct of their surveillance programmes and guarantee citizens' rights to privacy to the extent possible.[171]

116. Mr Geiger suggested four simple rules. First, any form of mutual political, economic espionage must be prohibited without exception. Eavesdropping or wiretapping on allies erodes trust among "friendly" nations with a price tag that outweighs any benefits. Second, any intelligence activity on the territory of another member State may only be carried out with that State's approval and only taken within a statutory framework (for example for the specific goal of preventing terrorism or other very serious criminal acts). Third, in no event may mass data be tracked, analysed or stored, if it is data from non-suspected individuals from a friendly State. Only information pertaining to legitimately targeted individuals may be collected on an exceptional basis for specific individual purposes. Any data on individual citizens or economic data that is stored but is not needed for this clearly defined purpose must be deleted or destroyed without delay. And fourth, telecommunications and Internet companies cannot be forced by intelligence services to grant them unfettered access to their massive databases of personal data; this should only be possible on the basis of a court order. This limit would not jeopardise the security of contracting States, because in the case of a specific, realistic threat, such a court order can be obtained.

117. Even a voluntary intelligence codex would have a strong effect because those States that do not abide by it could be accused of wrongful actions by their allies, thus eroding their credibility as co-operation partners. But a multilateral binding agreement would be more effective to close loopholes States can currently exploit in order to circumvent legal limits placed on their intelligence programmes. As seen in previous sections, "collusion for circumvention" still allows intelligence agencies to push the boundaries of their data collection powers at home by relying on data collected by their allies or third parties. An intelligence codex would provide an opportunity to close loopholes and protect citizens not only from surveillance by their own government, but also from those of other contracting States.

171. Hearing of the Committee on Legal Affairs and Human Rights on "Mass surveillance" 8 April 2014. Full video of the hearing: http://clients.dbee.com/coe/webcast/index.php?id=20140408-1&lang=en.

118. Such a feat would of course be challenging and raise many key questions before the negotiation process is even initiated, such as determining who would be part of such a codex, how its enforcement would be monitored, and the precise terms of the agreement that would allow intelligence agencies to function properly for their legitimate missions while protecting civil liberties and human rights. But the challenge is worth taking up, given the stakes, and provides an opportunity for the Council of Europe to play an important role in line with its mandate to uphold the rule of law, human rights and democracy.

5.3. Pervasive encryption to strengthen privacy

119. Until States agree on and actually implement limits on their intelligence agencies' mass surveillance programmes, pervasive encryption to strengthen privacy remains the most effective fallback for people to defend their data. As explained by Mr Snowden during the April 2014 committee hearing, some encryption methods are not susceptible to any realistic brute-force attacks, because "properly implemented modern encryption algorithms backed by truly random keys, of significant length, can require the application of more energy to cryptanalyse, or basically to derive the solution to and decrypt, than exists in the known universe". Advocates of mass encryption as an answer to mass surveillance thus 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 for "codebreakers" of neutralising even a relatively cheap code.

120. Taking this suggestion a step further, some technical experts propose "decentralising" (rather than "Balkanising") the Internet, for example encouraging each user to set up his or her own well-protected server. This would exclude any form of mass surveillance. Legitimate targets, such as terrorists, organised criminals and the like (and their providers) would have to be court-ordered to relinquish their encryption keys. This type of "clientele" is in any event what traditional, targeted forms of surveillance used to be reserved for, which were authorised by specific court orders based on concrete grounds for suspicion.

5.4. Improving the protection of whistle-blowers

121. Mr Snowden's revelations have been essential for the public – and politicians – to become aware of intelligence agencies' mass surveillance programmes and have sparked the much needed discussion about the extent to which the public's civil rights and privacy should be sacrificed in the name of national security.

122. But even after appropriate legal limits and oversight mechanisms have been established on the national level and on the international plane in the form of a multilateral "intelligence codex", whistle-blowing will be needed as the most effective tool for enforcing the limits placed on surveillance. The activities of secret services are by nature difficult to scrutinise by any of the usual judicial or parliamentary control mechanisms. Access of any monitoring bodies to relevant information and capacity issues in view of the huge volume of activity to be monitored will always remain a problem for effective supervision. The "sword of Damocles" of the disclosure of any abuses by well-protected inside whistle-blowers may well constitute the most powerful deterrent against serious violations of the legal limits that should in our view be placed under surveillance. This assessment is particularly authoritative as it is shared by a senior former intelligence practitioner, Mr Geiger, whose experience as former head of the German BND carries special weight.

123. Consequently, we need to reassess whistle-blower protection measures in parallel with our recommendations concerning mass surveillance. These issues will be addressed shortly in the separate report under preparation on "Improving the protection of whistle-blowers".

6. Conclusions

124. The "Snowden files" have shown the extent of the threat mass surveillance represents for our privacy and other human rights whose effective exercise depends on privacy – such as freedom of expression and information, even freedom of religion, the right to a fair trial and the right to equal treatment. In sum, nobody and nothing is safe from snooping by our own countries' and even foreign intelligence services – unless we succeed in generalising the use of secure technologies.[172] The technological progress enabling the world's leading intelligence services to collect and store stunning amounts of data "anywhere, anytime" is in the process of being matched by equivalent technological leaps in the development of the filtering and analysing

172. Such as GnuPG, OTR (see *Der Spiegel*, 27 December 2014, revealing NSA documents assessing the effectiveness of various encryption standards).

tools needed to use these data. Before the ever-growing "surveillance-industrial complex" spins completely out of control, we must act, in order to subject surveillance to the rule of law. This will require a thorough review of the relevant national legislation in most, if not all member and observer States. In addition, ground rules must be laid down on the international plane. In order to be credible, the national and international legal framework must be enforced by credible control mechanisms – including the protection of whistle-blowers who disclose any violations. Also, parliamentary oversight bodies should be given the necessary teeth by giving them, *inter alia*, a say in the approval of the services' budgetary appropriations. Whilst waiting for such a legal framework to be actually in place and functioning, pervasive end-to-end encryption and decentralisation seems to be the only available defence against abuses that already now affect the integrity of the Internet.

125. Ultimately, we should bear in mind the political and human rights price tag of mass surveillance: the threat to the very existence of the Internet as we know it and of which we currently enjoy the socio-economic benefits; the erosion of trust between friends and partners on the international scene; and the privacy and civil liberties of our citizens. The Council of Europe should seize this opportunity to draw attention to the need for international standards to safeguard basic human rights, while ensuring that intelligence agencies continue defending our security using effective and proportional means. A good first step could be for the Secretary General of the Council of Europe to launch an inquiry under Article 52 of the European Convention on Human Rights requesting all member States to explain the manner in which their internal law ensures the effective implementation of the right to respect for private and family life protected by Article 8.

126. We have seen that mass surveillance is not even effective as a tool in the fight against terrorism and organised crime, in comparison with traditional targeted surveillance.[173] We have also seen that some aspects of mass surveillance, such as the deliberate weakening of encryption and other Internet safety standards for the purposes of facilitating data collection, present a grave danger for national security.[174] Such weaknesses can be detected and exploited by rogue States, terrorists, cyberterrorists and ordinary criminals to inflict enormous damage on our societies. It follows that there is no contradiction between the protection of privacy and of national security, on the contrary: data protection and Internet security are necessary for our safety!

127. The draft resolution and draft recommendation reflect the essence of these findings and conclusions.

173. Paragraph 70 above, with references to US and EU studies coming to the same conclusion.
174. Paragraphs 68 and 69 above.