Douwe Korff*
Emeritus Professor of International Law
douwe@korff.co.uk

EXPERT OPINION

prepared for the Committee of Inquiry of the *Bundestag*
into the "5EYES" global surveillance systems revealed by Edward Snowden

Committee Hearing, Paul-Löbe-Haus, Berlin, 5 June 2014

My full Opinion seeks to provide answers to the questions put to me by the Committee of Inquiry, under the heading "*'Leitfragen' für die Sachverständigengutachten – Anhörung 3, Teil 2 – Rechtslage Völker- und Europarecht*" (Guiding Questions for the Expert Opinions – Annexe 3, Part 2 – Public international- and European-legal situation).

In addressing the questions, I have tried to be systematic, distinguishing between different areas of (international) law, and between subjects of the law involved, substantive standards and remedies (both individual and inter-state). I have done this almost entirely under the rubric of Question 1, with the special issue of the question of international law on spying kept separate in my answer to Question 2.

The issue raised by Question 3 – whether Germany can have consented to spying by others – is an issue I am not best to address *in concreto*, but I have provided some comments on the legal position and some complications in my answer to Question 2, under the sub-heading "*Spying with the consent of the targeted state (and agreements not to spy)*".

I believe I have answered Questions 4, 5 and 6 in my answers to the sub-issues I identified under Question 1; and I believe the distinctions I make there also cover the ones I was asked to make in Question 7.

This short paper only contains a summary of the above answers.

Overall, I hope my Opinion (and this Summary) will contribute to the debates in the Committee of Inquiry and beyond.

Douwe Korff (Prof.)
Cambridge/London, 3 June 2014

---

* Douwe Korff is a Dutch comparative and international lawyer specialising in human rights law (in particular, the ECHR) and data protection. After earlier academic work in Florence, Freiburg im Breisgau, Heidelberg, Essex and Maastricht, he was Professor of International Law at London Metropolitan University, London, UK, until May 2014. He is currently an Associate of the Oxford Martin School of the University of Oxford, and a member of the cybersecurity working group (legal) of the OMS Global Cybersecurity Centre: http://www.oxfordmartin.ox.ac.uk/cybersecurity/people/578.

From July 2014, he will be a visiting fellow at Yale University.

Professor Korff has been closely involved with the legal responses to the Edward Snowden revelations of mass surveillance by the USA and the UK and others, and was called as an expert on those issues before the relevant committees of the European Parliament and the Parliamentary Assembly of the Council of Europe. He works closely with human and digital rights groups such as EDRi, EFF, Statewatch, FIPR, Article 19 and Privacy International.

Douwe Korff
Emeritus Professor of International Law

Expert Opinion prepared for the Committee of Inquiry of the *Bundestag*into the "5EYES" global surveillance systems revealed by Edward Snowden, Committee Hearing, Paul-Löbe-Haus, Berlin, 5 June 2014

SUMMARY OF ANSWERS

1. What international-legal norms apply to the collecting, storing, "just-in-case" retention, analysis and exchanges of [personal] data relating to electronic communication and the use of the Internet?	
A. General public international law	
A.1 Subjects	Only states (and international organisations) are subjects of general public international law. It rests on the concept of sovereignty.
A.2 Substantive law	**Surveillance by one state over the Internet activities and electronic communications of citizens and officials of another state with which the first state is not at war at that time, without the express consent of the other state, and which involve illegal activities (such as "interference with computer systems without right" or "interception of communications without right") by agents of the first state perpetrated from within the territory of the other state, is a violation of the sovereignty of the targeted state. This is a rule of primary international law.** **In casu*, in my opinion, the electronic communications surveillance reportedly perpetrated by the USA (and the UK?) against Germany, from USA diplomatic premises (and US and UK military bases?) in Germany, violates German sovereignty (unless Germany consented to this: see my answer to Question 3).*** **Surveillance of citizens and officials of one state-party to an international human rights treaty by agents of another state-party to that treaty, from the territory of the latter state, does not violate the sovereignty of the targeted state. However, if it involves acts which violate the obligations of the latter state party under that treaty, this not only violates that treaty but (since it harms the interests of the targeted state and its officials and citizens) also constitutes an internationally unlawful act against the state whose citizens and officials are affected. That is a rule of secondary international law.** **In casu*, in my opinion, the Internet and electronic communications surveillance reportedly perpetrated by the USA and the UK (et al.) against Germany and many other countries, from the territory of the USA and the UK (et al.), constitutes a whole series of internationally unlawful acts against Germany and those other countries.***
A.3 Remedies	It would be highly appropriate for Germany and, or with, other (European and other) states, to seek to have the issue of Internet and electronic communications surveillance by the USA and the UK (*et al.*) put before the International Court of Justice, in a contentious case. However, this would require the agreement of the USA and the UK,

	which is unlikely to be forthcoming. The USA and the UK (*et al.*) are also unlikely to agree to arbitration on the issue. **This means that, regrettably, states affected by the unlawful surveillance have few legal remedies available in public international law other than the inter-state procedures under international human rights law, noted below. However, as we shall see, these are not without promise.**
B. International and European human rights law	
B.1 Subjects	In modern human rights law, individuals are made subjects of international law, and are granted rights and remedies in their own right.
B.2 Substantive law	*In this regard, I address five issues:*
a. general principles	**In my opinion, the UK's involvement in the global surveillance operations and –systems revealed by Edward Snowden grossly, manifestly – "screamingly", as someone put it – fails to meet the "minimum standards" for surveillance adduced by the European Court of Human Rights under the ECHR (as summarised on p. 17 of my full opinion).** **The Human Rights Committee has already clearly indicated that it regards the USA's involvement in (and leadership of) these operations and –systems as equally in breach of the ICCPR.**
b. discrimination	**The prohibition of discrimination in international human rights law is absolutely fundamental to that already fundamental area of law. Any state laws or practices that appear *prima facie* to be in violation of that principle must be subject to the most rigorous assessment as to the necessity of the apparent distinctions. If, and to the extent that there is, a clear and objective reason to treat "foreign communications" differently from purely-internal domestic ones, for national security purposes, such a distinction can be justified. But the mere fact that a person who is to be spied upon is a "foreigner", or that the communications that are to be intercepted occur outside the spying state's territory, can in my opinion not be a sufficient reason to make such a distinction.** **In other words, historical laws that contain such distinctions (often at their very heart) must be fundamentally re-written. This must be done in and by Germany as much as in and by the states accused of having established a global surveillance system.**

c. extra-territorial application of human rights law	**In my opinion, a state that uses its legislative and enforcement powers to interfere with computer systems, or intercept the communications, of individuals and officials outside its own territory, e.g., by using the physical infrastructure of the Internet and the global e-communications systems to extract those data from servers, personal computers or mobile devices in another state, or by requiring private entities that have access to such data abroad to extract those data from the servers or devices in another country and hand them over to the spying state, is bringing those data, and in respect of those data, the data subjects, within its "jurisdiction" in the sense in which that term is used in the ECHR and in the ICCPR.** **It follows from the recent developments in the case-law of the international human rights courts and –fora that such a spying state must, in this extraterritorial activity, comply with the obligations under the international human rights treaties to which it is a party.** ***Re the USA position on this issue:*** **In my opinion, the US Government's view (categorically rejected by the Human Rights Committee, and contrary to the views of all other international human rights fora), that the USA's obligations under the ICCPR do not apply (at all) to any extraterritorial activities of US agents or agencies, is incompatible with the modern approach to human rights as pertaining to everyone, irrespective of who or where they are, without discrimination, and with the view that states must comply with their international human rights obligations whenever and wherever they are exercising their sovereign powers.** **In view of the predominance of the USA (and of US corporations) in the digital environment, this poses a serious threat to the effective protection of the human rights of "non-US-persons" and their global communications.**
d. "positive obligations"	**In my opinion, all state-parties to the ECHR, including Germany and the UK, have not just a right but a duty – a "positive obligation" – to limit the involvement of private entities that are subject to their jurisdiction in global surveillance systems that can violate the rights of their citizens. That includes foreign private entities when they operate in such a way as to bring themselves within the jurisdiction of the state concerned, e.g., by having establishments there, or by targeting individuals there.** **They must establish a legal framework that clearly and "foreseeably" regulates the actions of such private entities, and limits the private entities' involvement to what is "necessary and proportionate".** **They also have a "positive obligation" to ensure that any surveillance,**

	not just by their own intelligence agencies, but also by the intelligence agencies of other countries operating on their territory, equally meets the ECHR "minimum requirements" (set out on p. 17 of the full opinion).
e. EU law, the CFR & "national security"	It would appear, at least *prima facie*, that the national laws (and case-law) allowing for surveillance by these states for such wide-ranging ends cannot be said to be limited to national security purposes in the sense in which that concept must be understood in international human rights- or EU law. **In my opinion, the Court of Justice of the EU has the right, first of all, to determine what can (and what cannot) be reasonably said to be covered by the concept of "national security" as used in the TEU. In my opinion, it is likely to be guided in this by developing international standards on the issue, in particular the Johannesburg Principles.** **If a Member State were to claim to be acting in relation to "national security", but in matters that cannot properly be regarded as pertaining to national security – such as, say, purely economic spying, or spying on the institutions of the EU itself (as Snowden says has been done, also by the UK) – and if the actions of the Member State in that regard touch on matters within the competence of the EU (e.g., if this affects the operation of the Single Market/the e-Privacy Directive, or the functioning of the spied-on institutions), then the Court has the right to hold that the activity in question is *not* covered by the Art. 4(2) TEU exemption. And in such a case, it can hold such actions to be contrary to Union law and unlawful.** **Moreover, secondly, even if a Member State were to act in a matter that does genuinely pertain to its national security, the Court would still have the power to assess whether the actions of the state concerned are compatible with the state's other duties under the treaties, including in matters of shared competence. And in such a case, too, it can hold that such actions are not thus compatible, and thus unlawful.**
B.3 Remedies	ICCPR: Although it is not possible for individuals or groups of individuals to take a case to the Human Rights Committee under the ICCPR, EU countries including Germany should seriously consider bringing an inter-state complaint against the USA and the UK under Art. 41 of the Covenant over the USA-UK (*et al.*) surveillance programmes. ECHR: A strong and well-argued individual application against the UK (*BBW, ORG et al. v. the UK*) is already pending before the European Court of

	Human Rights. However, the bringing of a separate, inter-state case under Art. 33 ECHR against the UK, by Germany and any other willing Council of Europe Member State, is still fully warranted. Such an inter-state case would raise the issue to a higher level – which I believe is entirely justified in the circumstances, given the enormous implications of the UK surveillance operations for all other Council of Europe Member States. Quite separately from this, it would, in my opinion, be highly appropriate for the Committee of Inquiry to call on the German Government to support the call for the Secretary-General of the Council of Europe to use his power under Art. 52 ECHR to demand that the UK provide full information on its surveillance programmes <u>EU law</u>: "National security" activities of the EU Member States are outside of EU jurisdiction – but this does not mean that Member States have a *carte blanche* whenever they invoke national security. Rather, two crucial issues remain judiciable: whether any particular measure that touched on issues within EU competence (such as e-communications privacy), but that a Member State claims to be in pursuit of "national security", actually served that purpose; and whether, even if such a measure did pursue that aim, the actual measures taken are compatible with the other obligations of that State under EU law (in particular, in relation to other "security" issues that clearly are within EU competence) and/or with the EU *acquis*. In my opinion, these matters should be judicially clarified in proceedings brought before the Court of Justice of the EU, either by other EU Governments affected by the UK programmes (including Germany), or by the European Commission. Again, I believe that it would be appropriate for the Committee of Inquiry to urge the German Government to explore these possibilities.
C. International and European data protection law	
C.1 Subjects	International data protection law does not only also treat individuals as subjects of the law, but it also provides then with protection and remedies against those who control data on them – be these public (state) entities or private ones, such as corporations. The latter – providing protection under international rules for individuals against other individuals and private entities – is the special feature of data protection law.

C.2 Substantive law	Data protection is seen, in Europe, as a new fundamental right, *sui generis*, linked to but not limited to the protection of privacy, that has the wider purpose of protecting "human identity" (*l'identité humaine*) or – as in Germany – the protoright to [respect for one's] "personality" (*das allgemeine Persönlichtkeitsrecht*). This is most clearly expressed in the EU's *Charter of Fundamental Rights*, in which data protection is guaranteed as a separate right from private life (Article 8). In Europe, data protection is seen as an essential pre-requisite for the protection of other freedoms, including freedom of thought and freedom of expression. This is especially so in relation to surveillance. Privacy law in the USA is not based on such a broad, fundamental view, and provides much less protection even for US citizens – and hardly any for "non-US-persons". **Even if the USA were to be prepared to extend absolutely all the privacy rights accorded to US citizens to European citizens – which it does not even appear to be willing to consider – this would still leave European citizens with a level of protection against US agencies that fell far below what European courts, and the German Constitutional Court, would regard as an absolute minimum in terms of fundamental rights. The *Bundestag* (and the other national parliaments, and the European Parliament) should be most wary of any proposed "EU-USA Umbrella Agreement" that fails to secure data protection rights for European citizens at the minimum level required by European and national-constitutional laws.** European data protection law is firmly based on a number of core princples including purpose-specification and –limitation (*Zweckbindung*), data retention-limitation, fairness, transparency, etc.. These principles are strongly asserted in the Council of Europe Data Protection Convention and in the EC/EU data protection directives – except for the EC Data Retention Directive which, however, has been declared null and void *in toto* and *ab initio* by the Court of Justice of the EU, exactly because it failed to properly adhere to the core principles, by disproportionally departing from them. ***The considerations of the CJEU in the Data Retention case strongly suggest that, as civil society has long argued, compulsory indiscriminate retention of data for law enforcement purposes should be replaced with a system of targeted data retention (also referred to as "data deep-freeze"), under which the communication data of persons "of interest" could be ordered to be retained. Such an order should in principle be a judicial one, with allowance for urgent measures subject to* ex post facto *judicial review.***

	Moreover, it is in my view clear from the Data Retention judgment that the suspicionless mass surveillance programmes of the US NSA and the UK GCHQ (*et al.*) are manifestly – I would again say, "screamingly" – contrary to the basic data protection principles set out in the EU Charter of Fundamental Rights as applied by the CJEU in this case (as well as protected, albeit indirectly, by the ECHR), even if one takes full account of the exception- and derogation clauses in the main data protection directive and in the e-Privacy Directive.
C.3 Remedies	The above leaves the UK in particular with the only option of arguing that the EU rules simply do not apply, and that no EU institution, including the Court, can rule on these matters. However, as I have explained at **B.3**, above, in my opinion that is simply wrong. To repeat: in my opinion, the Luxembourg Court has jurisdiction to assess, in matters which touch on issues within EU competence – such as privacy and e-communications – whether a Member State claims to be in pursuit of "national security", actually served that purpose; and whether, even if such a measure did pursue that aim, the actual measures taken are compatible with the other obligations of that State under EU law (in particular, in relation to other "security" issues that clearly are within EU competence) and/or with the EU *acquis*. **In other words, the remedies noted at B.3, above, are in my opinion available in particular in relation to EU data protection law – including the question of whether the UK's surveillance practices are indeed really in pursuit of "national security", or also served other non-exempt purposes (as I believe is the case), and even to the extent that they might be aimed at protecting national security, whether they do not unduly – i.e., disproportionately – impact on matters within EU competence.** Moreover, the question of competence quite simply does not arise in relation to the Council of Europe, either in terms of the European Convention on Human Rights or the 1981 Data Protection Convention. In my opinion, the drafting of, for a start, non-binding but still authoritative guidance on the processing (including the collecting) of personal data by national security agencies is now a matter of urgency. Beyond that, in my opinion, the fact that the UK surveillance operations so clearly breach the standards applied by the CJEU in the Data Retention case strongly reinforces the likelihood of those operations also being regarded as in violation of the ECHR. The same would apply to any inter-state case over the issue.

2. To what extent are there public international legal standards regulating spying by states?	
Scope	**In this opinion refer to spying as covering activities aimed at obtaining information on a state, state institutions or state officials, by means that are *unlawful* under the law of the targeted country**. This typically includes bribing or blackmailing officials to provide information, burgling houses or offices to search for documents or other information, placing hidden microphones or cameras in private or official buildings – and "*access[ing] the whole or any part of a computer system without right*" or "*intercept[ing] without right, ... by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data*", i.e., the kinds of activities that Snowden has revealed are carried out on a massive, global scale by the US's NSA, the UK's GCHQ, and their allies. Indeed, the acts put in quotation marks just now *must* be made criminal offences under the Cybercrime Convention, to which, interestingly, both the UK and the USA are parties (since 2011 and 2007, respectively).
Substance	***In principle* any official or agent of a state who accesses public- or private-sector computer systems, or who intercepts electronic communications, in another country is subject to the criminal-legal provisions of the target country: if a US or UK official or agent perpetrates any of the above acts in Germany, he or she commits a crime, just like any other person committing such acts on German territory would be guilty of a crime.** Diplomats are not exempt from this. In my opinion, there are basically only two exceptions to this in-principle prohibition: <u>Exceptions in war</u>: **In my opinion – and as I understand her, also in the opinion of Anne Peters of the MPI – to the extent that spying by a nation at war can be lawful, this legality is limited to spying on the enemy in the enemy's own country (and of course on agents of the enemy country in the spying country, including spying on suspected spies from the other side). The historical acceptance of the legality of spying noted by Greenspan (and the other authors cited by the US A-G) does not extend to acceptance of the legality of spying in countries that are not involved in an armed conflict with the spying state.**

	<u>Spying with the consent of the targeted state (and agreements not to spy)</u>: The basic answer to this question in terms of international law is deceptively simple: states can consent to other states doing things that would otherwise be unlawful *vis-à-vis* the consenting state, and that will render the conduct lawful. States can, indeed, not argue that their "consent" was not freely given. But the situation is actually more complex. **Any surveillance, by any state that is a party to any of the main human rights treaties (in particular, the ICCPR and the ECHR) would be in violation of those treaties if it carried out surveillance (over anyone, anywhere: see my remarks on "discrimination" and the extra-territorial application of human rights law) on the basis of secret rules.** ***In my opinion, this now fundamental rule of international human rights law applies equally to secret treaties (or secret annexes or secret interpretations of treaties) as it does to secret laws: it would be preposterous if states could carry out acts that they could not carry out on the basis of their own laws, on the basis of secret international agreements with other countries that the individuals involved cannot even be aware of. Yet it would seem that to some extent that is exactly what is happening. If that is so, it is high time the rule of* law was brought to bear on this murky area of state activity.** **In my opinion, this area is still unacceptably opaque. In addition to the suggestion I made in my answer to Question 1, that the Committee urges the German Government to ask the Secretary-General of the Council of Europe to demand that the UK furnish a complete overview of its laws and practices – and treaties! – relating to its surveillance activities, also in relation to its cooperation with the USA, I would also recommend that the *Bundestag* ask the German government:** **i. to provide a complete overview of all international agreements, and all annexes or "understandings" related to such agreements, with all other states, bilaterally and multilaterally, including through NATO;** **ii. to ask the former Occupying Powers – the USA, the UK, France and Russia (as the successor state to the USSR) – whether they agree with the German government's view that they have no remaining powers of information gathering and export in Germany (or in relation to Germany). For the German government alone to be convinced of this is of little use if these countries actually take a different view;**

	iii. to inform the *Bundestag* if German officials or agencies have in the last (say) ten years been "helped" by lawyers from the UK and US national security agencies in the drafting and/or interpreting of any German laws or treaties to which Germany is a party; **and in the light of the answers to these questions:** **iv. to review all domestic German laws, and all such international agreements and "arrangements" as may still be found to exist in he light of international, and in particular European, human rights law, and to amend all laws and treaties and agreements that fail to meet international human rights and data protection standards.** In this regard, I would like to point out the important presentation made to the Parliamentary Assembly of the Council of Europe by the former head of the BND, Dr. Hansjörg Geiger, who has proposed a "codex" to regulate intelligence activities between friendly states. I strongly endorse that call.

- O – o – O -

Douwe Korff (Prof.)
Cambridge/London, 3 June 2014