

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

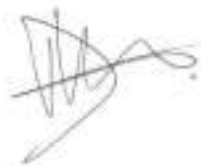
This paper seeks to provide answers to the questions put to me by the Committee of Inquiry, under the heading “‘Leitfragen’ für die Sachverständigengutachten – Anhörung 3, Teil 2 – Rechtslage Völker- und Europarecht” (Guiding Questions for the Expert Opinions – Annexe 3, Part 2 – Public international- 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.

Overall, I hope my Opinion 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.

CONTENTS

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. <u>Subjects</u>
A.2. <u>Substantive law</u>
A.3. <u>Remedies</u>
B. International and European human rights law
B.1. <u>Subjects</u>
B.2. <u>Substantive law</u>
B.3. <u>Remedies</u>
C. International and European human rights law
B.1. <u>Subjects</u>
B.2. <u>Substantive law</u>
a. Substantive international human rights standards applicable to Internet and electronic communications surveillance
b. The principle of non-discrimination
c. The extra-territorial application of international human rights law
d. "Positive obligations" of states
e. The EU Charter of Fundamental Rights and the exclusion of "national security" from EU competence
B.3. <u>Remedies</u> (ICCPR, ECHR, EU)
D. International and European data protection law
D.1. <u>Subjects</u>
D.2. <u>Substantive law</u>
D.3. <u>Remedies</u>
2) To what extent are there public international legal standards regulating spying by states?

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?

The *Leitfragen* ask me to address the above in terms of customary law, general (multilateral or bilateral) [conventional] law, as well as international human rights treaties (in particular, the European Convention on Human Rights, but I shall also mention the the International Covenant on Civil and Political Rights and the EU Charter of Fundamental Rights); to discuss whether these standards differentiate between data of private- and public-sector users; and whether international law (in any of the above-mentioned forms) contains requirements that there be remedies that private users of e-communications and the Internet can use against state entities or against corporations providing the e-communications- and Internet infrastructure.

Below, I have tried to address these issues in a structured way. In this, I use the phrase "**Internet and electronic communications surveillance**" (or just "**surveillance**") to cover the totality of the activities listed in the question (collecting, storing, "just-in-case" retention, analysis and exchanges of [personal] data relating to electronic communication and the use of the Internet), making distinctions between the various different activities as appropriate. Furthermore, as discussed in the text, in trying the answer the question of whether such surveillance is legal in terms of the different sets of legal rules, I focus on surveillance activities that are typically **illegal** under the domestic law of the targeted state, such as "interference with computer systems without right", and "interception of communications without right".

Applicable sources of law

Internet and electronic communications surveillance is subject to a range of different, albeit overlapping, international legal norms, in particular:

- A. general public international law;
- B. international and European human rights law; and
- C. international and European data protection law.

These sources of law apply to different subjects, set out different substantive standards, and provide for different kinds of remedies. I will briefly deal with each of these.

A. General public international law

A.1. Subjects

As its traditional name, the law of nations (*Völkerrecht*), already indicates, general public international law is the law that regulates the relations between states. It is firmly founded on the principle of respect for national sovereignty: in principle, and with only very limited exceptions, states are their own masters; no other state may interfere in matters that lie within the sovereign power of another state.

A.2 Substantive law

Although sovereign, states are subject to law, in particular to treaty law and to customary international law. The latter includes peremptory norms of international law, *ius cogens*. States are bound by their treaty obligations: *pacta sunt servanda*. States can depart from ordinary customary law by treaty, but they cannot set aside *ius cogens*, such as the prohibition of aggression, and the prohibition of the use of torture.

There is probably a rule of customary law that allows states involved in an international (i.e., an inter-state) armed conflict to spy on each other.¹ States can of course also target non-state entities within their own borders, with which they are engaged in a non-international armed conflict: this does not affect the sovereignty of any other nation.

However, as explained in my answer to Question 2, the customary rule allowing spying on an enemy state cannot be invoked by a state claiming to be involved in an armed conflict with an internationally operating non-state group (such as the USA claims to be with al Qaeda),² to carry out Internet and electronic communications surveillance in another country (such as Germany) that is far removed from any actual battlefield and that does not regard itself to be involved as a belligerent party in this armed conflict.

States are especially not allowed to carry out, on the territory of another state, acts that are typically the preserve of states and state agencies (*Hohheitsakte*); that would amount to an unlawful exercise of "enforcement jurisdiction". The basic, fundamental principle in that regard is that a state "*cannot take measures on the territory of another state by way of enforcement of national laws without the consent of the latter.*"³ As the International Law Commission said:⁴

¹ See the Legal Authorities Supporting the Activities of the National Security Agency described by the President, attached to the Communication from the US Attorney-General to Congress of 19 January 2006, referred to in footnote 18, below.

² Note that, if the USA can indeed be said to be involved in an "armed conflict" with al Qaeda and its affiliates (as it claims), this would still be a "non-international armed conflict", since "international armed conflicts" are by definition conflicts between two or more states. See the ICRC Opinion Paper "How is the Term "Armed Conflict" Defined in International Humanitarian Law?", March 2008, available at: <http://www.icrc.org/eng/assets/files/other/opinion-paper-armed-conflict.pdf>

As the ICRC points out there, this summary reflect the strong prevailing legal opinion.

³ Ian Brownlie, *Principles of Public International Law*, 6th ed., 2006, at p. 306. The classic expression of the principle can be found in the award of the sole arbitrator in the Palmas Island case, Max Huber:

"Sovereignty in the relations between states signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other state, the functions of a state. The development of the national organization of states during the last few centuries and, as a corollary, the development of international law, have established this principle of the exclusive competence of the state in regard to its own territory in such a way as to make it the point of departure in settling most questions that concern international relations."

Island of Palmas Case (Netherlands/United States of America), Award of 4 April 1928, UNRIIAA, vol. II (1928), pp. 829-871, at p. 838, available at: http://legal.un.org/riaa/cases/vol_II/829-871.pdf.

The same principle was also unambiguously expressed in what is still the leading case in this regard, the judgment of the Permanent Court of International Justice (the forerunner of the International Court of Justice) in the *Lotus* case:

Now the first and foremost restriction imposed by international law upon a State is that - failing the existence of a permissive rule to the contrary - it may not exercise its power in any form in the territory of another State. In this sense jurisdiction is certainly territorial; it cannot be exercised by a State outside

With regard to the jurisdiction to enforce, a State may not enforce its criminal law, that is, *investigate* crimes or arrest suspects, in the territory of another State without that other State's consent.

Rather than states acting by themselves in these ways, the proper channel for cross-border action in such matters is to go through so-called Mutual Legal Assistance Treaties or MLATs. These can be bi- or multilateral.

A fortiori, agents of any state that operate on the territory of another state, including diplomats, are required to abide by the domestic law of the latter country. They are not allowed to indulge in forms of "intelligence gathering" that violate those laws – such as illegal interference with computer systems or illegal interception of communications.

To put it simply: 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 by agents of the first state perpetrated 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.

This is also the case if the activities in question are undertaken by diplomats of the first country in the second (target) country, and/or from diplomatic premises of the first country in the second country: although they cannot be prosecuted because diplomatic immunity, diplomats are not exempt from the law of the host country.⁵

This would apply for instance to any tapping into any of the main Internet exchanges in Germany (such as the Frankfurt DE-CIX exchange)⁶ by a foreign state or foreign state

its territory except by virtue of a permissive rule derived from international custom or from a convention [i.e., a treaty].

PCIJ, *The Case of the S.S. "Lotus"*, judgment of 7 September 1927, pp. 18-19, emphasis added, available at http://www.icj-cij.org/pcij/serie_A/A_10/30_Lotus_Arret.pdf

⁴ See the 2006 Report of the International Law Commission (58th session), *Annex E – extraterritorial jurisdiction*, para. 22, on p. 526, available at:

<http://legal.un.org/ilc/reports/2006/2006report.htm> (emphasis added).

⁵ Whether it applies to agents of a spying state (non-diplomats) based on military bases in the target state who are there with the consent of the target state, depends on the terms of the agreements between those two states that cover the activities of such agents/those bases. I discuss that question in my answer to Question 3.

⁶ See:

<http://www.spiegel.de/international/world/secret-documents-nsa-targeted-germany-and-eu-buildings-a-908609-2.html> (1 July 2013)

This says the following (but does not name the DE-CIX exchange by name): "According to insiders familiar with the German portion of the NSA program, the main interest is in a number of large Internet hubs in western and southern Germany. The secret NSA documents show that Frankfurt plays an important role in the global network, and the city is named as a central base in the country. From there, the NSA has access to Internet connections that run not only to countries like Mali or Syria, but also to ones in Eastern Europe."

DE-CIX is mentioned as a specific target by the FT a few days later, on 4 July:

<http://www.ft.com/cms/s/0/a3e573ce-e3fd-11e2-91a3-00144feabdc0.html#axzz330IT41Hg>

On the widely reported surveillance of Chancellor Merkel's mobile phone, and the mobile communications of others in the Berlin government district, see, e.g.:

<http://www.spiegel.de/spiegel/print/d-118184380.html>

agencies, and to the interception, by foreign officials or agents (including diplomats) of mobile phone communications in Germany, from German soil.⁷ If this happened as alleged (and documented) by Edward Snowden, it is a clear violation of German sovereignty – *unless of course Germany consented to this* (as discussed in my answer to Question 3).

Nota Bene: My answer above may seem to contradict the opinion of my esteemed colleague, Prof. Aust, who writes in his statement to the Committee⁸ that it is generally assumed from the absence of general rules about espionage in time of peace (i.e., outside of an armed conflict) that "*in international law, espionage is neither permitted nor prohibited.*" (para. 38) However, I believe this is largely a question of semantics: Prof. Aust addresses the issue of "intelligence gathering" generally, whereas I focus on acts that involve violations of the domestic law of the targeted state, such as, especially, interference with computer systems and interception of electronic communications (acts that are generally regarded as criminal offences, and that must indeed be criminalised by parties to the Cybercrime Convention: see my answer to Question 3). Prof. Aust agrees that "*it is accepted in international law that spies can commit criminal offences under the laws of a relevant national state.*" (i.e., that when spies do this kind of thing, it still counts as criminal) (para. 39). If we limit the question put by the Committee to the legality of acts such as those just mentioned, which are criminal under the laws of most, if not all, countries (and certainly under German law), then Prof. Aust and I agree: states that are targeted in this way can criminalise such illegal intelligence gathering.

What is more, as I argue in my answer to Question 3, if agents of one state (the spying state) deliberately commit criminal offences in another state (the targeted state) that harm the interests of the targeted state and its citizens and officials, that constitutes an **internationally unlawful act** on the part of the spying state. In that sense, illegal spying of the kind just mentioned – spying that involves illegal interference with computer systems in the targeted state, or that involves illegal interception of communications in the targeted state – in my opinion clearly *is* illegal under general public international law.

The above applies to illegal interference with computer systems and illegal interception of communications by a spying state on the territory of a target state. However, we should also address the question of whether the above rule also applies if the first state carries out such surveillance over the Internet activities and electronic communications of citizens and officials of the other state, *but without this involving activities of the first state within the territory of the other state.*

This would cover the tapping into – or the full "splitting" – of the major undersea Internet cables that form the "backbone" of the Internet and that carry most of the world's (including Germany's) electronic communications, not in Germany, but on the territory of the states performing this interception. It is reported that such interception is performed on

⁷ Note that diplomatic premises remain territory of the state where they are located; they are not territory of the state using those premises – although of course they benefit from extensive protections and immunities under international law. But those immunities do not extend to freedom to violate the law – and in particular the criminal law – of the host country.

⁸ Dr Helmut Philipp Aust, *Stellungnahme zur Sachverständigenanhörung am 5. Juni 2014.*

the main Europe to USA undersea cable where this lands in the UK, at Bude, in Cornwall, UK, in a facility operated jointly by the UK and the USA.⁹

In my opinion, such interception of German (and other continental-European and other) communications data as they pass through structures outside Germany (or the other countries) probably does not constitute a violation of the sovereignty of Germany (or the other states), because the activities do not take place on German territory (or the territory of those other states), but on the territory of the state (on *in casu*, of one of the states) that perpetrates the interception.

However, such Internet and electronic communications surveillance can still constitute an **internationally wrongful act**, entailing the responsibility and liability of the state(s) perpetrating the acts, if the surveillance is unlawful in some other way – in particular, if the interception were to be in breach of any international obligations of the state carrying out the interception *vis-à-vis* the state that is (or whose officials or citizens are) affected by the act.¹⁰

As further explained below, under the heading "*International and European human rights law*", the untargeted mass surveillance perpetrated by the USA and the UK (and probably others, in particular their partners in the "5EYES" group) against essentially all "NON-USPERS[ons]" is in blatant violation of international human rights law – and of international human rights treaties to which both the spying states (the USA and the UK) and the spied-on states (such as Germany) are a party – and affects the fundamental rights of citizens of the targeted countries as well as officials of those countries, and the institutions they represent, irrespective of where the acts of interference and/or interception take place.

In my opinion, 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, but which violates the obligations of the latter state party under that treaty, 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.

⁹ See:

<http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa>

¹⁰ See the Draft Articles on the Responsibility of States for Internationally Wrongful Acts, drawn up by the International Law Commission (ILC) in August 2001, which are largely a codification of existing customary law in this regard, and have been cited by the International Court of Justice. For the text of the Draft principles, see:

http://legal.un.org/ilc/texts/instruments/english/draft%20articles/9_6_2001.pdf

A.3 Remedies

Because states are sovereign, they cannot generally be forced to submit to the authority of any outside agency, including international courts, unless they consent to this (either in general terms or *ad hoc*, in relation to a particular inter-state issue).¹¹

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

International human rights law is, as the name indicates, a special branch of public international law. However, modern, post-WWII human rights law shows one crucial departure from traditional public international law, in that for the first time in history – and as a clear response to the atrocities of the Nazi and Stalinist dictatorships of the mid-20th Century – it treats individuals as not just object but also *subjects* of international law. Under the post-WWII human rights treaties, individuals are directly granted important rights as individuals: modern rights are *human* rights, granted to all individuals by virtue simply of being a human being. See section B.2.b, below.

Moreover, although some states – including, regrettably, the USA – still have to catch up with this, in the modern world human rights must be granted to everyone within the control of a state, rather than just to citizens of the state (as the earlier human rights instruments such as the French Declaration of Human Rights and the US Bill of Rights suggested). I will discuss this below, at B.2.c.

Also, under current international human rights law, individuals are increasingly granted *standing* in international human rights fora (as discussed further under the heading "*Remedies*", below).

B.2 Substance

International human rights law is mainly treaty-based. Some of the norms laid down in these treaties, like the prohibition on torture, have become customary law (and indeed, in that case, *ius cogens*). We need not address here, however, the question of the extent to which this applies to other human rights principles, because all the countries reportedly

¹¹ There is an exception in international law, in that states are subject to the authority of the UN Security Council if the latter acts under Chapter VII of the UN Charter in relation to an actual or threatened breach of international peace and security – but that is not relevant here.

involved in global surveillance, including the "5EYES" are parties to at least the main global human rights treaty, the International Covenant on Civil and Political Rights (ICCPR). The UK is also a party to the main European human rights treaty, the European Convention on Human Rights (ECHR) and, through the Lisbon Treaty, and subject to some important limitations of that treaty and EU law generally, subject to the EU Charter of Fundamental Rights.

We should note that, in terms of inter-state relations, the obligations of the USA and the UK (and the other "5EYES") under these treaties are *reciprocal*: if the USA or the UK (or any of the other "5EYES") violate their obligations under the ICCPR and/or (for the UK) the ECHR, then that involves not only a violation of the rights of the individuals concerned (who therefore are granted certain individual remedies), but it also constitutes a violation of a reciprocal treaty obligation *vis-à-vis* the other state-parties. That means that those other state parties – such as Germany – too have special remedies (as also discussed further under the heading "*Remedies*", below).

Overall, five issues need to be discussed in this context:

- a. the question of whether the Internet and electronic communications surveillance revealed by Edward Snowden is compatible with the general substantive requirements of the main human rights treaties, in particular the ICCPR and the ECHR;
- b. the question of whether, under these main treaties, in carrying out Internet and electronic communications surveillance, states are allowed to distinguish (discriminate) between their own nationals and others (foreigners) and/or between purely domestic communications (communications between parties that are both in their territory) and communications where at least one of the communicating parties is outside their territory;
- c. the question of whether states (and in particular the states involved in this surveillance) are, under these main treaties, bound by their international human rights obligations in respect of surveillance activities carried out outside their geographical jurisdiction, i.e., outside of their own territory;
- d. the question of whether, and if so when, states have a "positive obligation" to protect their citizens (and perhaps even citizens of other countries) from Internet and electronic communications surveillance by third states; and
- e. the special case of the EU Charter of Fundamental Rights and the limitation of EU law in relation to "national security" in particular.

NB: A sixth issue is what remedies both states and individuals have, or should have, under each of these instruments (ICCPR, ECHR and CFR) against alleged violations of their rights (or their citizens' rights) by states carrying out Internet and electronic communications surveillance, in either domestic or international fora. As already noted, this is addressed under a separate heading.

a. Substantive international human rights standards applicable to Internet and electronic communications surveillance¹²

A preliminary observation: the wide effects of surveillance on human rights

Surveillance of Internet activities and electronic communications of individuals, and of the patterns of their interactivity, affects a whole range of human rights protected by international (global and regional) human rights treaties. It of course directly impacts on the right to privacy (or "private life") and correspondence. But it also has a clear effect on other rights, including freedom of expression, freedom of information, and freedom of association. As the German Constitutional Court put it in its famous *Census* judgment: if someone must at all times wonder whether any "unconventional" behaviour on her part may be registered and permanently kept on record, she is likely to try to avoid such "coming to notice". That would not only affect that one person's right, but would damage the very foundations of a democratic society that is based on the active participation of its citizens.¹³

Basic human rights principles and case-law

The provisions in the ECHR and the ICCPR on the above-mentioned rights (private life, freedom of expression, freedom of information, and freedom of association) all stipulate or imply that those rights can only be restricted or interfered with on the basis of "law"; and that such restrictions or interferences must serve a "legitimate aim", and must be

¹² This section draws heavily on several notes, submissions and analyses I have written earlier, or which I helped to write, including in particular:

Douwe Korff, *Note on European & International Law on Trans-National Surveillance, prepared for the Civil Liberties Committee of the European Parliament to assist the Committee in its enquiries into USA and European states' surveillance*, August 2013, full text available at:

http://www.europarl.europa.eu/meetdocs/2009_2014/organes/libe/libe_20131014_1500.htm

See also the *Submission to the United States Congress, the European Parliament and Commission & the Council of the European Union, & the Secretary-General & the Parliamentary Assembly of the Council of Europe on the surveillance activities of the United States and certain European States' national security and "intelligence" agencies*, which I drafted for the European Digital Rights Initiative (EDRI) and the Fundamental Rights European Experts group (FREE), available at:

http://edri.org/files/submission_free_edri130801.pdf

Also the *Legal Analysis* supporting the *International Principles on the Application of Human Rights to Communications Surveillance*, issued by a global consortium of civil society organisations, of which I wrote the original draft:

<https://en.necessaryandproportionate.org/text>

<https://necessaryandproportionate.org/LegalAnalysis>

¹³ German Constitutional Court judgment of 15 December 1983 (the Court's famous "*Census*" judgment), Section II, at 1a). The original paragraph, paraphrased in the text, reads as follows:

"Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist."

"necessary" to achieve that aim. Each of these terms has been clarified in important ways in the case-law of the bodies implementing the treaties; and the case-law of the different treaty bodies in these regards is fully in agreement with each other, as noted below.

"Law"

According to the European Court of Human Rights, the following are two of the requirements that flow from the expression "prescribed by law":¹⁴

Firstly, the law must be adequately accessible: the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case. Secondly, a norm cannot be regarded as a "law" unless it is formulated with sufficient precision to enable the citizen to regulate his conduct: he must be able - if need be with appropriate advice - to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail. Those consequences need not be foreseeable with absolute certainty: experience shows this to be unattainable. Again, whilst certainty is highly desirable, it may bring in its train excessive rigidity and the law must be able to keep pace with changing circumstances. Accordingly, many laws are inevitably couched in terms which, to a greater or lesser extent, are vague and whose interpretation and application are questions of practice.

Secret rules, or secret guidelines on or interpretations of the rules, that an affected person cannot know, are not "law".¹⁵ Neither are laws or rules that give the authorities excessive discretion: such laws do not protect against arbitrary exercise of the powers in question. The scope and manner of exercise of any discretion granted must therefore be indicated (in the law itself, or in binding, published guidelines) with "reasonable clarity", so that, again, individuals can reasonably foresee how the law will be applied in practice.¹⁶

Moreover:¹⁷

Especially where a power of the executive is exercised in secret, the risks of arbitrariness are evident -

Such secret powers must therefore be subject to especially clear and precise, strict rules and especially close and strong oversight.

The Human Rights Committee takes the very same approach. To quote from one of its most recent General Comments, on Article 19 ICCPR (freedoms of opinion and expression):¹⁸

Restrictions must be provided by law. Law may include laws of parliamentary privilege¹⁹ and laws of contempt of court.²⁰ Since any restriction on freedom of expression

¹⁴ Judgment in *The Sunday Times v. The United Kingdom*, Application no. 6538/74, Judgment of 26 April 1979, para .49. This has become the standard interpretation.

¹⁵ *Siver v. the UK, Petra v. Romania*, 1998.

¹⁶ *Petra v. Romania*. In *Malone v. the UK*, the Court used the expression "sufficient clarity": para. 68.

¹⁷ *Malone v. the UK*, para. 67.

¹⁸ General Comment No. 34, CCPR/C/GC/34, 12 September 2011, paras. 24 – 26, available at: http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2fGC%2f34&Lang=en

¹⁹ See communication No. 633/95, *Gauthier v. Canada*. [original footnote]

²⁰ See communication No. 1373/2005, *Dissanayake v. Sri Lanka*, Views adopted on 22 July 2008. [original footnote]

constitutes a serious curtailment of human rights, it is not compatible with the Covenant for a restriction to be enshrined in traditional, religious or other such customary law.²¹

For the purposes of paragraph 3, a norm, to be characterized as a "law", must be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly²² and it must be made accessible to the public. A law may not confer unfettered discretion for the restriction of freedom of expression on those charged with its execution.²³ Laws must provide sufficient guidance to those charged with their execution to enable them to ascertain what sorts of expression are properly restricted and what sorts are not.

Laws restricting the rights enumerated in article 19, paragraph 2, including the laws referred to in paragraph 24, must not only comply with the strict requirements of article 19, paragraph 3 of the Covenant but must also themselves be compatible with the provisions, aims and objectives of the Covenant.²⁴ Laws must not violate the non-discrimination provisions of the Covenant. Laws must not provide for penalties that are incompatible with the Covenant, such as corporal punishment.²⁵

"Necessary [and proportionate]" in relation to a "legitimate aim"

Restrictions on the exercise of the main Convention rights set out in Articles 8 – 11 ECHR are only compatible with the Convention if they are "necessary" for a legitimate aim, which for these rights must be one of the aims specifically listed in the article in question. These aims are quite broadly phrased: they include public safety, prevention of crime, protection of morals and of the rights of others, and national security. It is notable, however, that the right to manifest one's religion or beliefs may not be limited or interfered with on grounds of national security.²⁶

The Court has clarified the meaning of the term "necessary" as follows:²⁷

... whilst the adjective "necessary" ... is not synonymous with "indispensable" ..., neither has it the flexibility of such expressions as "admissible", "ordinary" ..., "useful" ..., "reasonable" ... or "desirable".

For a measure that interferes with a right to be "necessary", it has to correspond to a "pressing social need", and it must be "proportionate" to that need.²⁸ Subject to the "margin of appreciation" doctrine, discussed under the next heading, the Court makes it

²¹ See general comment No. 32. [original footnote]

²² See communication No. 578/1994, *de Groot v. The Netherlands*, Views adopted on 14 July 1995. [original footnote]

²³ See general comment No. 27. [original footnote]

²⁴ See communication No. 488/1992, *Toonen v. Australia*, Views adopted on 30 March 1994. [original footnote]

²⁵ General comment No. 20, *Official Records of the General Assembly, Forty-seventh Session, Supplement No. 40 (A/47/40), annex VI, sect. A*. [original footnote]

²⁶ Note that the actual holding of beliefs may not be limited or interfered with at all: this is part of a person's "inner sanctum", into which the state may not intrude. Only "manifestations" of a religion or belief may be limited (to the extent necessary).

²⁷ *Handyside v. the UK*, para. 48.

²⁸ *Idem*, paras. 48 and 49.

assessment of the necessity and proportionality of a measure "in the light of all the circumstances". However, some measures deserve closer scrutiny than others. Therefore:²⁹

Powers of secret surveillance of citizens, characterising as they do the police state, are tolerable under the Convention only in so far as **strictly necessary** for safeguarding the democratic institutions. (emphasis added)

Once again, the approach of the Human Rights Committee fully concurs with this. On the general approach to necessity and proportionality, this is well reflected in its General Comment on Article 12 ICCPR (freedom of movement), that again reflects its general approach to the issue:³⁰

Article 12, paragraph 3, provides for exceptional circumstances in which rights under paragraphs 1 and 2 may be restricted. This provision authorizes the State to restrict these rights only to protect national security, public order (*ordre public*), public health or morals and the rights and freedoms of others. To be permissible, restrictions must be provided by law, must be necessary in a democratic society for the protection of these purposes and must be consistent with all other rights recognized in the Covenant (...).

The law itself has to establish the conditions under which the rights may be limited. State reports should therefore specify the legal norms upon which restrictions are founded. Restrictions which are not provided for in the law or are not in conformity with the requirements of article 12, paragraph 3, would violate the rights guaranteed by paragraphs 1 and 2.

In adopting laws providing for restrictions permitted by article 12, paragraph 3, States should always be guided by the principle that the restrictions must not impair the essence of the right (cf. article 5, paragraph 1); the relation between right and restriction, between norm and exception, must not be reversed. The laws authorizing the application of restrictions should use precise criteria and may not confer unfettered discretion on those charged with their execution.

Article 12, paragraph 3, clearly indicates that it is not sufficient that the restrictions serve the permissible purposes; they must also be necessary to protect them. Restrictive measures must conform to the principle of proportionality; they must be appropriate to achieve their protective function; they must be the least intrusive instrument amongst those which might achieve the desired result; and they must be proportionate to the interest to be protected.

The principle of proportionality has to be respected not only in the law that frames the restrictions, but also by the administrative and judicial authorities in applying the law. States should ensure that any proceedings relating to the exercise or restriction of these rights are expeditious and that reasons for the application of restrictive measures are provided.

²⁹ Klass v. Germany, para 42.

³⁰ General Comment No. 27, 1999, CCPR/C/21/Rev.1/Add.9, reproduced in Human Rights Instruments, Volume I, Compilation of General Comments and General Recommendations adopted by Human Rights Treaty Bodies, HRI/GEN/1/Rev.9 (Vol. I), 2008, pp. 223 – 227, paras. 11 – 16, available at: http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2f21%2fRev.1%2fAdd.13&Lang=en

States have often failed to show that the application of their laws restricting the rights enshrined in article 12, paragraphs 1 and 2, are in conformity with all requirements referred to in article 12, paragraph 3. The application of restrictions in any individual case must be based on clear legal grounds and meet the test of necessity and the requirements of proportionality.

The "margin of appreciation" doctrine

In assessing whether a measure that interferes with a Convention right is "necessary" and "legitimate", the European Court of Human Rights leaves to the state a certain "margin of appreciation". Under this doctrine (which as first developed in relation to the derogation clause, Article 15),³¹

... it is for the national authorities to make the initial assessment of the reality of the pressing social need implied by the notion of "necessity" in [the context of the specific case].

However:

The Court ... is empowered to give the final ruling on whether a "restriction" or "penalty" is reconcilable with [the right in question]. The domestic margin of appreciation thus goes hand in hand with a European supervision. Such supervision concerns both the aim of the measure challenged and its "necessity"; it covers not only the basic legislation but also the decision applying it, even one given by an independent court.

In Europe, the width of the margin of appreciation depends on various factors. In some contexts, such as morals and national security, the Court tends to grant states a wide margin of appreciation, while in others the margin can be quite narrow. The latter is especially the case if the issue is largely objective, or if there is a large measure of convergence in law and practice in the European states, or if there are accepted global or Europe-wide standards in the relevant area.

The doctrine has not been adopted as broadly in the case-law of the other international human rights bodies, in spite of occasional references to such a margin in the case-law of both the Inter-American Court of Human Rights and the Human Rights Committee; and has been criticised for potentially undermining both the principle of universality of human rights and the standing of the international human rights bodies.³²

The above general principles, as applied to surveillance by the ECtHR

Since the 1978 case of Klass v. Germany, the European Court of Human Rights (ECtHR) has consistently held that interception of telephone communications by State bodies, including national security agencies, constitutes an "interference" with the right to private and family life, home and correspondence, that is guaranteed by Article 8 of the Convention. There is no doubt that the same applies equally to other forms of electronic communications surveillance (Cf. Liberty and Others, para. 56). Indeed:

³¹ Handyside v. the UK, para. 48.

³² See Eyal Benvenisti, Margin of Appreciation, Consensus, and Universal Standards, JIL&P, Vol. 31 (1999), p. 843ff (with detailed references to case-law), available at: http://www.pict-pcti.org/publications/PICT_articles/JILP/Benvenisti.pdf

the mere existence of legislation which allows a system for the secret monitoring of communications entails a threat of surveillance for all those to whom the legislation may be applied. This threat necessarily strikes at freedom of communication between users of the telecommunications services and thereby amounts in itself to an interference with the exercise of [individuals'] rights under Article 8, irrespective of any measures actually taken against them. (Weber and Saravia, para. 78, emphasis added)

The Court is also particularly concerned that if intercept data are destroyed and the persons concerned are not notified of the fact that they were under surveillance, "this may serve to conceal monitoring measures which have been carried out by the authorities" (*idem*, para. 79). Such surveillance must therefore be "in accordance with law", serve a "legitimate aim in a democratic society", be "necessary" and "proportionate" in relation to that aim.

The first of these requirements is crucial. In particular, the Court accepts that safeguarding national security, preventing disorder and preventing and fighting crime are of course "legitimate aims" of a democratic State (Klass, para. 46, cf. Weber and Saravia, para. 104) - although it is notable that in the latter case the Court did not repeat the reference to "the economic well-being of the country" that was mentioned as a further aim of the relevant surveillance law by the German Government (see para. 103).

Moreover, while the Court grants States "a fairly wide margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security" (as discussed separately, below), it adds that:

Nevertheless, in view of the risk that a system of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there exist **adequate and effective guarantees against abuse**. This assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of **remedy** provided by the national law.

(Weber and Saravia, para. 106, with reference to Klass, Leander, Malone and other cases; emphases added.)

In other words, in judging whether secret surveillance is "necessary" and "proportionate", the Court looks mainly at the **nature and quality of the law** in question, and at the **available safeguards** and **domestic remedies** against abuse.

On the point of whether surveillance is "in accordance with law", the Court has developed a number of "minimum safeguards", which we shall examine below. First, however, it should be noted that the Court says that "these safeguards should be set out in **statute law**" (Weber and Saravia, para. 95). In other words, these matters are so fundamental that they may not be left to subsidiary rules or –legislation. This reflects the German constitutional concept of *Gesetzesvorbehalt*, according to which certain restrictions on fundamental rights may only be imposed by statute law, i.e., by a formal law adopted by the democratic representatives of the people. It goes beyond the normal Convention requirement that interferences with fundamental rights must be based on legal rules that are "accessible" to those (potentially) affected (cf. the fourth bullet-point, below).

Minimum safeguards

The "**minimum safeguards** that according to the Court should be set out in statute law in order to avoid abuses of power" relate to the following:

- the nature of the offences in relation to which electronic surveillance may be ordered;
- the definition of the categories of people who are liable to be placed under surveillance;
- the limits on the duration of the surveillance;
- the procedure to be followed for ordering the examination, use and storage of the data obtained; these "should be set out in a form which is open to public scrutiny and knowledge";
- the precautions to be taken when communicating the data to other parties; and
- the circumstances in which the intercept data may or must be erased or destroyed.

These principles, which were first listed in this way in Weber and Saravia (para. 95, with references to earlier case-law), apply not just to "strategic monitoring" of communications based on "catchwords", but to all interceptions of and surveillance over (e-)communications (Liberty and Others, para. 63; the quote in the fourth bullet-point is from para. 67).

The systems in Germany and the UK compared

It is very instructive to contrast the findings in relation to these tests in Weber and Saravia v. Germany on the one hand, with those in Liberty and Others v. the UK on the other hand.

In Weber and Saravia, the Court found that the German surveillance law (the "amended G 10 Act"), as further restricted by the German Constitutional Court:

- "**defined the offences**" which could give rise to an interception order "**in a clear and precise manner**". (para. 96);
- **indicated which categories of persons** were liable to have their telephone tapped with **sufficient precision** (para. 97);
- limited interception orders to a period of **three months** (renewable as long as the statutory conditions for the order were met) (para. 98);
- set out **strict procedures** for the imposition of surveillance (in particular, for automated "strategic monitoring" through "catchwords"), including **prior authorisation** from an **independent commission** (the G10 Commission) that is appointed by **Parliament** (in consultation with the Government);
- contained sufficient "**safeguards against abuse**", including **strict purpose- (use-) limitation-, data disclosure- and data destruction rules**, and close oversight over surveillance by a Parliamentary Board and by the G10 Commission (cf. paras. 116, 120ff, and *passim*); and
- "effectively ensured that **the persons monitored were notified** in cases where notification could be carried out without jeopardising the purpose of the restriction of the secrecy of telecommunications." (para. 136).

In its judgment in Liberty and Others v. the UK, the Court held that surveillance in the UK, too, had a basis in domestic law, i.e., in the Interception of Communications Act 1985 (ICA) and the Regulation of Investigatory Powers Act 2000 (RIPA). However, in contrast to the case of Weber and Saravia, above, the Court held that in the UK the law:

- “allowed the executive an **extremely broad discretion** in respect of the interception of communications passing between the United Kingdom and an external receiver ... The **legal discretion** granted to the executive for the physical capture of external communications was ... **virtually unfettered**;
- the detailed “arrangements” for surveillance were contained in “**internal regulations, manuals and instructions**” that were **not contained in legislation or otherwise made available to the public**;
- the **supervision** provided by the Interception of Communications Commissioner (further discussed below), **did not contribute towards the accessibility and clarity** of the scheme, since he was not able to reveal what the “arrangements” were; consequently, the procedures to be followed for examining, using and storing intercepted material were not “set out in a form which is open to public scrutiny and knowledge”; and
- the fact that “extensive extracts” from the Code of Practice on surveillance had belatedly been made public “suggests that it is possible for a State to make public certain details about the operation of a scheme of external surveillance without compromising national security.”

The Court concluded that:

the domestic law at the relevant time [did not indicate] with sufficient clarity, so as to provide adequate protection against abuse of power, the scope or manner of exercise of the very wide discretion conferred on the State to intercept and examine external communications. In particular, it did not, as required by the Court’s case-law, set out in a form accessible to the public any indication of the procedure to be followed for selecting for examination, sharing, storing and destroying intercepted material. The interference with the applicants’ rights under Article 8 was not, therefore, “in accordance with the law”.

It follows that there has been a violation of Article 8 in this case.

(Liberty and Others, paras. 69-70)

The European Court of Human Rights considerations and minimum requirements relating to State surveillance, adduced above, are summarised overleaf.³³

³³ The Court will soon be able to rule specifically on the mass surveillance programmes of the UK in the case of *Big Brother Watch, Open Rights Group, English PEN and Kurz v. the United Kingdom*, now pending. Application 58170/13, 30 September 2013. The full text of the application, as well as important expert witness statements from Cindy Cohn (EFF) and Ian Brown (OII), is available at:

<https://www.privacynotprism.org.uk/news/2013/10/03/legal-challenge-to-uk-internet-surveillance/>

The Court has fast-tracked the case and a judgment may, unusually, be handed out still this year.

See also my recommendation as concerns the bringing of an inter-state case on the issue under the heading “Remedies”, below.

ECtHR CONSIDERATIONS & MINIMUM REQUIREMENTS RELATING TO SURVEILLANCE:

The case-law of the ECtHR shows the following considerations and requirements of European human rights law relating to surveillance:

- A system of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it.
- The mere existence of legislation which allows a system for the secret monitoring of communications entails a threat of surveillance for all those to whom the legislation may be applied.
- In view of these risks, there must be adequate and effective guarantees against abuse.
- The first of these is that such systems must be set out in statute law, rather than in subsidiary rules, orders or manuals. The rules must moreover be in a form which is open to public scrutiny and knowledge. Secret, unpublished rules in this context are fundamentally contrary to the Rule of Law; surveillance on such a basis would *ipso facto* violate the Convention.

The following are the "minimum safeguards" that should be enshrined in such (published) statute:

- the offences and activities in relation to which surveillance may be ordered should be spelled out in a clear and precise manner;
- the law should clearly indicate which categories of people may be subjected to surveillance;
- there must be strict limits on the duration of any ordered surveillance;
- there must be strict procedures to be followed for ordering the examination, use and storage of the data obtained through surveillance;
- there must be strong safeguards against abuse of surveillance powers, including strict purpose/use-limitations (e.g., preventing the too-easy disclosure of intelligence data for criminal law purposes) and strict limitations and rules on when data can be disclosed by NSAs to LEAs, etc.;
- there must be strict rules on the destruction/erasure of surveillance data to prevent surveillance from remaining hidden after the fact;
- persons who have been subjected to surveillance should be informed of this as soon as this is possible without endangering national security or criminal investigations, so that they can exercise their right to an effective remedy at least *ex post facto*; and
- the bodies charged with supervising the use of surveillance powers should be independent and responsible to, and be appointed by, Parliament rather than the Executive.

Under the ECHR, these principles must be applied to anyone who is affected by surveillance measures taken by any Council of Europe Member State.

In addition, European States have a "positive obligation" to protect their citizens from surveillance contrary to the above, perpetrated by any other State. *A fortiori*, they are under a legal obligation not to actively support, participate or collude in such surveillance by a non-European State.

Assessment of the global surveillance systems revealed by Edward Snowden in terms of the European Convention on Human Rights

In my opinion, the global surveillance operations and –systems revealed by Edward Snowden grossly, manifestly – “screamingly”, as someone put it – fail to meet the “minimum standards” for surveillance adduced by the European Court of Human Rights (as summarised on the previous page). Specifically:

- the offences and activities in relation to which this surveillance is carried out is not spelled out in a clear and precise manner, in either US or UK law;
- neither US nor UK law clearly indicates which categories of people may be subjected to surveillance;
- under neither US nor UK law are there strict limits on the duration of any ordered surveillance;
- under neither US nor UK law are there strict procedures to be followed for ordering the examination, use and storage of the data obtained through surveillance;
- there are not adequate (let alone strong) safeguards in place, either in the USA or in the UK, against abuse of surveillance powers; there are no strict purpose/use-limitations (e.g., preventing the too-easy disclosure of intelligence data for criminal law purposes); and there are no strict limitations and rules on when data can be disclosed by national security agencies to law enforcement agencies, etc.;
- there are no strict rules on the destruction/erasure of surveillance data to prevent surveillance from remaining hidden after the fact;
- persons who have been subjected to surveillance are almost never informed of this, not even when this can be done without endangering national security or criminal investigations; they therefore cannot effectively challenge their surveillance, even in such cases, *ex post facto*; and
- in both the USA and the UK, the bodies nominally charged with supervising the use of surveillance powers are not independent from the Executive.

If the European Court of Human Rights declares the case of *BBW, ORG et al. v. the UK*, currently pending,³⁴ to be admissible, I expect that it will confirm that the surveillance operations and systems of the UK indeed fails to meet these standards (the US surveillance is not, and cannot be, tested in this case as the USA are not a party to the ECHR; however, their surveillance actions have already been assessed under the ICCPR, albeit not [yet] in a contentious case: see under the next heading).

Assessment of the global surveillance systems revealed by Edward Snowden in terms of the International Covenant on Civil and Political Rights

As noted earlier, the Human Rights Committee applies the same general standards of “law”, “legitimate aim”, “necessity” and “proportionality” to issues arising under the ICCPR as the European Court of Human Rights applies to similar issues under similar provisions of the

³⁴ See the previous footnote.

ECHR. The Committee has not yet been able to rule specifically on the US and UK mass surveillance programmes in individual or inter-state cases (see "*Remedies*", below). However, it has quite clearly expressed its views on the US programmes in its Concluding Observations on the 4th USA periodic report under the Covenant.³⁵

The Committee is concerned about the surveillance of communications in the interests of protecting national security, conducted by the National Security Agency (NSA) both within and outside the United States through the bulk phone metadata program (Section 215 of the PATRIOT Act) and, in particular, the surveillance under Section 702 of Amendments to the Foreign Intelligence Surveillance Act (FISA) [introducing s.1881a – DK] conducted through PRISM (collection of the contents of communications from U.S.-based companies) and UPSTREAM (tapping of fiber-optic cables in the U.S. that carry internet traffic) programs and their adverse impact on the right to privacy. The Committee is concerned that until recently, judicial interpretations of FISA and rulings of the Foreign Intelligence Surveillance Court (FISC) have largely been kept secret, thus not allowing affected persons to know the law with sufficient precision. The Committee is concerned that the current system of oversight of the activities of the NSA fails to effectively protect the rights of those affected. While welcoming the recent Presidential Policy Directive (PPD-28) that will now extend some safeguards to non-US persons "to the maximum extent feasible consistent with the national security", the Committee remains concerned that such persons enjoy only limited protection against excessive surveillance. Finally, the Committee is concerned that those affected have no access to effective remedies in case of abuse ...

The Committee urged the USA to bring its surveillance in line with international human rights law in terms of legality and proportionality, surveillance and remedies.³⁶

The Committee added that the USA should "refrain from imposing mandatory retention of data by third parties."³⁷ The latter, though only comprising one line in the Committee's Observations, is notable because it ties in with an almost concurrent ruling of the Court of Justice of the EU, which held that the EC Data Retention Directive – which mandated precisely such compulsory retention, of electronic communications data, without suspicion – was invalid *in toto* and *ab initio*.³⁸

It is if anything an understatement to say that the above strongly suggests that the Committee regards the US surveillance programmes as contrary to the ICCPR.

b. The principle of non-discrimination

As the *Leitfragen* rightly note, there are several issues that need to be looked at that concern the making of distinctions by states in their surveillance activities. Below, I will look at the compatibility with international human rights law of the following distinctions:

³⁵ Human Rights Committee *Concluding Observations on the Fourth USA Report* (advance unedited version, March 2014), para. 4 (p. 2), available from:

http://tbinternet.ohchr.org/_layouts/treatybodyexternal/SessionDetails1.aspx?SessionID=625&Lang=en

³⁶ *Idem*, para. 22, at (a), (b) and (e) (see there for details).

³⁷ *Idem*, para. 22, at (d).

³⁸ Judgment in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others*, of 8 April 2014, available at:

<http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=12322>

- legal rules that allow for surveillance of non-nationals or non-residents of the state carrying out the surveillance that are less strict than the rules on surveillance of nationals or residents; and
- legal rules that allow for surveillance of communications that take place wholly or partly outside the territory of the state carrying out the surveillance that are less strict than the rules on surveillance of communications that take place entirely within the state.

In terms of international human rights law, such differentiating rules raise issues of discrimination.

Note: The *Leitfragen* raise another question, i.e., whether international human rights law only protects individuals and private entities against surveillance, or whether public entities could also invoke international human rights law in this respect. That is not a question of discrimination, but of the scope of human rights law and, especially, of standing. I will deal with that issue under the heading “*Remedies*”.

In this respect, there is a clear disjunction between the basic principle, discussed next, and what seems to be widespread state practice: from an admittedly very limited survey, it would appear that, to the extent that there are [published] laws on the activities of national security agencies at all, those laws often tend to make the above-mentioned kinds of distinctions: they allow surveillance of “foreigners” and/or “foreign communications” (including communications to or from “foreign” countries) on much more relaxed terms than they apply to domestic communications surveillance. I therefore address both.

The basic – and crucial – principle

It is one of the hallmarks, and one of the greatest achievements, of modern, post-WWII international human rights law that human rights must be accorded to “everyone”, to all human beings. That is a departure from previous practice, in which such rights were still often seen as pertaining only to citizens of a state, and not to foreigners (except perhaps foreign residents), and/or based on reciprocity. That approach was explicitly rejected in the mother of all post-WWII human rights treaties, the Universal Declaration of Human Rights:

All human beings are born free and equal in dignity and rights. ...

Everyone is entitled to all the rights and freedoms set forth in this Declaration, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status. Furthermore, no distinction shall be made on the basis of the political, jurisdictional or international status of the country or territory to which a person belongs, whether it be independent, trust, non-self-governing or under any other limitation of sovereignty.

(Articles 1 and 2 of the Universal Declaration of Human Rights, emphases added)

This is not just aspirational. On the contrary, this approach was confirmed by, and under, the binding international human rights treaties adopted to implement the UDHR, including both the UN ICCPR and the ECHR:³⁹

³⁹ Note that the ECHR, too, is expressly inspired by the Universal Declaration of Human Rights: see the first two preambular considerations.

In general, the rights set forth in the Covenant apply to everyone, irrespective of reciprocity, and irrespective of his or her nationality or statelessness.⁴⁰

Subject to the quite separate question of when a person who is entitled to the enjoyment of a right can be said to be under the “jurisdiction” of a state (as further discussed at c, below) and to the very limited exception with regard to restrictions on the political activities of non-nationals (“aliens”), which are not relevant to this Opinion,⁴¹ the application of the human rights guarantees in the ECHR and the ICCPR to “everyone”, irrespective of nationality or national status, has been consistently affirmed by both the European Court of Human Rights and the Human Rights Committee. To quote the latter:⁴²

As indicated in general comment No. 15 ..., the enjoyment of Covenant rights is not limited to citizens of States parties but must also be available to all individuals, regardless of nationality or statelessness, such as asylum-seekers, refugees, migrant workers and other persons, who may find themselves in the territory or subject to the jurisdiction of the State party.

This is absolutely fundamental to the modern, post-WWII international human rights edifice. It does not mean that states may not make distinctions in the way they guarantee rights to different people or groups of people – rather, it means that if they make any such distinctions, those distinctions must (i) serve a “legitimate aim” in a democratic society and (ii) be “necessary” and “proportionate” in relation to that legitimate aim. What is more, given the crucial importance of non-discrimination to modern human rights law, states will only be granted a very limited “margin of appreciation” in the making of such distinctions (if any).

Surprisingly, and regrettably, although the Court noted in *Weber and Saravia* that under the German law on communications surveillance (the so-called “G10 Law”):⁴³

⁴⁰ Human Rights Committee, General Comment No. 15 on The position of aliens under the Covenant, adopted 11 April 1986 (UN Document HRI/GEN/1/Rev.9 (Vol. I)), para. 1, available at:

http://ccprcentre.org/doc/ICCPR/General%20Comments/HRI.GEN.1.Rev.9%28Vol.I%29%28GC15%29_en.pdf

⁴¹ The ECHR contains a provision, Article 16, that stipulates that “Nothing in Articles 10 [freedom of opinion and expression], 11 [freedom of association] and 14 [prohibition of discrimination] shall be regarded as preventing the High Contracting Parties from imposing restrictions on the political activity of aliens.” However, this provision has been criticised as being in essence contrary to Articles 1 and 14 of the ECHR (guaranteeing equal rights for all); and the Parliamentary Assembly of the Council of Europe has called for its revocation (Recommendation 799 (1977)). Moreover, there is no comparable provision in the ICCPR (except that it allows states to limit the right to participate in elections to citizens: see Art. 25 ICCPR). This means not only that state-parties to the ECHR that are also parties to the ICCPR cannot invoke Article 16 to impose restrictions that would not be permissible under the ICCPR (see Art. 53 ECHR), unless they entered a declaration to the contrary upon ratification of the ECHR, but also supports the contention that Article 16 ECHR should be very narrowly interpreted, so as to allow only restrictions by European states on the rights of non-nationals that are manifestly reasonable and imposed for objective, legitimate purposes. See Ruma Mandal, Political Rights of Refugees, UNHCR Legal and Protection Policy Research Series, PPLA/2003/04, November 2003, available at:

<http://www.refworld.org/pdfid/3fe820794.pdf>

⁴² General Comment No. 31 (footnote 48, above), para. 10. For General Comment No. 15, see footnote 39, above.

⁴³ Weber and Saravia v. Germany, (in)admissibility decision, para. 32, with reference to §3(2), third sentence of the G10 Law.

[certain restrictions on surveillance] did not apply to telephone connections situated abroad if it could be ruled out that connections concerning German nationals or German companies were deliberately being monitored -

the issue of discrimination between nationals/residents and non-nationals/non-residents was not pursued by the applicants, and not further examined by the Court.

However, in my opinion, any crude distinction in surveillance laws between "nationals" and "non-nationals" (or residents and non-residents), or between communications taking place (wholly or partly) outside or wholly inside a country, without any more specific justification, is contrary to the highly-protected principle of non-discrimination in international human rights law.

However, such distinctions are common, as we shall note next.

The laws and practices of states

From a very limited survey, it would appear that national laws on surveillance by national security agencies⁴⁴ often allow for surveillance of non-nationals or non-residents of the state carrying out the surveillance, or for surveillance of communications that take place wholly or partly outside the territory of the state carrying out the surveillance, on the basis of legal rules that are less strict than the rules on surveillance of nationals or residents, or on surveillance of communications that take place entirely within the state.

This is the case in the UK, under the Regulation of Investigatory Powers Act (RIPA). Thus, when the European Court of Human Rights approved RIPA's regime for authorising interception of *internal* communications (within the UK) in *Kennedy v. UK*, it explicitly mentioned that in this regime:⁴⁵

the warrant itself must clearly specify, either by name or by description, one person as the interception subject or a single set of premises as the premises in respect of which the warrant is ordered. Names, addresses, telephone numbers and other relevant information must be specified in the schedule to the warrant. Indiscriminate capturing of vast amounts of communications is not permitted under the internal communications provisions of RIPA (...).

However, RIPA's legal provisions on the issuing of warrants for the interception of *external* communication (i.e., of "communication[s] sent or received outside the British Islands"),⁴⁶ which were not examined by the Court in that case, expressly do not require any such details: see RIPA, s.8(4). All that is needed in respect of such interceptions is a certificate from the Secretary of State in which he (in fact, now a she) certifies:⁴⁷

- (i) the descriptions of intercepted material the examination of which (s)he considers necessary [e.g., a specified submarine Internet cable – DK]; and

⁴⁴ Apparently, in some countries, these matters are not regulated by law at all. In the UK, the very existence of the main intelligence agencies was not even admitted by the authorities until the late 1980s. This is of course in manifest breach of international human rights law: see the discussion under the heading "Law" in the text, above.

⁴⁵ European Court of Human Rights, *Kennedy v. UK*, 26839/05, 18/05/2010, par. 160, effectively summarising the requirements set out in RIPA, s.8(1) and (2).

⁴⁶ s.20.

⁴⁷ s.8(4)(b)(i) and (ii). For further details, see the Opinion provided to the Committee by Dr. Ian Brown.

- (ii) that (s)he considers the examination of material of those descriptions necessary as mentioned in section 5(3)(a), (b) or (c).

In other words, a s.8(4) certificate can permit indiscriminate capture of UK-external communications data, in bulk, by reference only to its means of transmission – something which is expressly not allowed in relation to purely domestic (UK-internal) communications. As a recent opinion from a leading UK lawyer notes, after summarising and contrasting the legal provisions (s.8(1)-(3) vs. s.8(4)):⁴⁸

Accordingly, a warrant to intercept the contents of **internal** communications cannot sanction the collection and retention of bulk electronic data of the sort envisaged in scenario (a). Such a warrant has to be precisely targeted to a particular person or premises.

The position is different in relation to '**external**' warrants. Under section 8(4)(a) of RIPA, a warrant to intercept external communications only has to specify the 'communications to which the warrant relates'. For example, it might be simply that the warrant relates to interception of communications containing certain keywords. Or communications between a large number of named individuals. **At the most extreme end of the spectrum, it is conceivable that an external warrant might specify 'all communications entering and leaving the British Isles', or all such communications carried on a particular cable.** It may be that such broad warrants are wanted in order subsequently to carry out [keyword analysis].

In short 'external' warrants allow for interception of bulk or mass data, 'internal' warrants do not.

The situation in the USA is even worse, partly for historical reasons. Specifically, many of the human rights guarantees in the US Constitution and in various US laws relating to the digital environment only apply to US citizens and non-US citizens residing in the USA. This includes both the First Amendment, covering free speech and freedom of association⁴⁹ and the Fourth Amendment, protecting US citizens from "unreasonable searches".⁵⁰ This appears to

⁴⁸ Jemima Stratford QC, *Advice In the Matter of State Surveillance*, 22 January 2014, paras. 13-15, emphasis in bold added, available at: [http://www.brickcourt.co.uk/news-attachments/APPG_Final_\(2\).pdf](http://www.brickcourt.co.uk/news-attachments/APPG_Final_(2).pdf). See the full text of this advice for further detailed analyses of the relevant RIPA provisions in relation to the ECHR requirements. Also the Opinion of Dr Ian Brown, provided to the Committee.

Note that RIPA ss.15 and 16 impose some very high-level restrictions, that limit copying and/or sharing or access to data of intercepted data to limited groups of people. Crucially, however, they do not in any way limit the data collection, or any other forms of processing, such as lifestyle/social graph analysis or other forms of data mining. Rather, apart from a prohibition of the use of intercepted data in court (s. 17), such rules (or "arrangements", as they are called in these sections of RIPA) as there are on what the authorities can do with the captured data (i.e., what kinds of analyses they can perform, or what they can share with whom) are set out in internal, secret interpretations of RIPA (NB: this is not addressed in the QC's advice referred to in the previous footnote.). The Act even expressly allows the Secretary of State to waive or relax any such restrictions or safeguards as there may be, when intercepted data are passed on to "authorities of a country or territory outside the United Kingdom", such as the NSA.

⁴⁹ "[T]he interests in free speech and freedom of association of foreign nationals acting outside the borders, jurisdiction, and control of the United States do not fall within the interests protected by the First Amendment." (*DKT Memorial Fund Ltd. v. Agency for Int'l Dev.*, 1989, quoted in *Chevron Corporation v. Steven Donziger et al.*, US District Judge Kaplan order of June 25, 2013).

⁵⁰ The Fourth Amendment does not apply if the person affected by a "search" (which includes an online search) does not have a "significant voluntary connection with the United States": *US v. Verdugo-Urquidez*, 1979. This was also confirmed to the *Ad-hoc EU-US Working Group on Data Protection*, established to investigate the US surveillance activities exposed by Snowden: see the [Report on the Findings by the EU Co-](#)

be the result of the fact that the Constitution was written at a time when human rights were still seen mainly as "citizens' rights".

However, this has also allowed the uncritical exclusion of "NON-USpers[ons]" from the (in any case limited) protections against excessive surveillance in the FISAA and PATRIOT Acts.⁵¹ Essentially, FISAA allows for the indiscriminate surveillance of the Internet activities and electronic communications of non-US citizens and –residents, with little or no substantive or formal constraints, whenever this is deemed by the NSA and other US agencies to be useful in providing "foreign intelligence" – a concept that is so wide as to allow almost unfettered political, economic and diplomatic espionage.⁵²

However, the laws of other countries are little better. German law, too, apparently also contains much more relaxed rules on the interception of "foreign" communications than on entirely internal ones; and the same is apparently the case in other (Western) countries.⁵³

Historical explanation

I believe that there are two explanations for the apparently manifest clash between the very clear principle and the equally clear laws and practices. The first is the historical roots of the modern spying agencies in the context of war. The second is the historical view – now abandoned, as we shall see at c., below – that human rights only accrue to citizens of the state (or at most to lawful residents), and not to "foreigners".

On the first point, we should note that many modern spying agencies trace their history to (the run-up to) the First World War, and to the Bolshevik Revolution: e.g., the UK's Secret Service Bureau, founded in 1909, of whose nineteen military intelligence departments MI5 and MI6 still survive; the French *Deuxième Bureau*, founded in 1871 but significantly reformed in the First World War, and its internal twin, the *Renseignements Généraux*, founded in 1907 and operating until 2008 (now merged into CDRI);⁵⁴ and the Soviet *Cheka* that became the KGB, which after the fall of the Soviet empire became the current FSB. The US CIA was born out of its WWII Secret Operations Service, the SOS.

This background is important because it informs the framework for the operations of the present-day agencies. They were conceived as part of a war effort, against external military threats and foreign spies, *saboteurs* and infiltrators connected to those threats, and associated traitors and fellow-travellers in their own countries. During the wars, they operated in contexts in which many legal safeguards of their citizens (and even more so of aliens) were suspended. They were not subject to the kinds of legal restraints that were imposed on civil police forces.

chairs of the ad hoc EU-US Working Group on Data Protection, 27 November 2013, section 2, second paragraph.

⁵¹ See the report by Caspar Bowden et al. to the European Parliament, *Fighting Cybercrime and Protection Privacy in the Cloud*, 2012, and the subsequent article by him and Judith Rauhofer, *Protecting their own: Fundamental rights implications for EU data sovereignty in the cloud*, 2013, available at, respectively:

<http://www.europarl.europa.eu/committees/en/studiesdownload.html?languageDocument=EN&file=79050>
<http://ssrn.com/abstract=2283175>

⁵² *Idem.*

⁵³ See Joseph Foschepoth, *Überwachtes Deutschland*, 3rd ed., 2013, *passim*.

⁵⁴ See:

https://en.wikipedia.org/wiki/Direction_centrale_des_reenseignements_g%C3%A9n%C3%A9raux

The mind-set of these agencies remained essentially unchanged in the Cold War: they still saw themselves as the frontline defenders of their respective nations, against ruthless adversaries threatening the very survival of their countries and political systems. Unlike the better kind of civil policemen, they did not feel morally bound by the constraints of the ordinary law:⁵⁵

For five years we bugged and burgled our way across London at the State's behest, while pompous bowler-hatted civil servants in Whitehall pretended to look the other way.

Until the collapse of the Soviet empire, both the KGB and the Western intelligence agencies essentially behaved in lawless ways, murdering and kidnapping, engaging in sabotage and supporting unconstitutional *coups d'états*, at least abroad. Surveillance of the "enemy"'s communication was but a minor matter in this context, and basically accepted, at least *de facto*, by all sides as part of life in the international arena. *De iure*, all states involved protested strongly, however, whenever they managed to expose the surveillance activities of the other side: there was, and is, certainly no *opinio iuris* to the effect that these practices are in accordance with international law.

The point to be made here is that this historical situation and mindset is no longer acceptable.

In simple terms: 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. The extra-territorial application of international human rights law

Historical background

Historically, human rights were *citizens'* rights, as is indeed clear from the very title of the "grandmother" of all modern human rights instruments, the *Déclaration des droits de l'homme et du citoyen* (1789). The almost contemporaneous US Bill of Rights (drafted in the summer of 1789 and adopted in 1791) similarly was conceived first and foremost as "a list of limits on government power",⁵⁶ and hence aimed at protecting the US citizens from their (federal) government.

⁵⁵ Peter Wright, *Spycatcher*, 1987, p. 54.

⁵⁶ The quote is from:

However, when the Universal Declaration of Human Rights was drafted, the term "universal" was deliberately chosen to emphasise a fundamental change in this respect.⁵⁷ As already noted under the heading "*Discrimination*", at **b**, above, it was felt that "human" rights should pertain to every human being, by virtue of every human being being a member of the new, global, post-WWII society.

However, as we shall discuss next, the instruments created to give binding legal effect to the civil and political rights set out in the Declaration, the UN's International Covenant on Civil and Political Rights and the Council of Europe's European Convention on Human Rights,⁵⁸ contain somewhat ambiguous wording.

The treaty texts and recent developments in interpretation

The texts of the ICCPR and the ECHR appear to qualify the duty of the state-parties to those instrument to guarantee the rights in those instruments:

Each State Party to the present Covenant undertakes to respect and to ensure to **all individuals within its territory and subject to its jurisdiction** the rights recognized in the present Covenant, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.

(Article 2(1) ICCPR, emphasis added)

The High Contracting Parties shall secure to **everyone within their jurisdiction** the rights and freedoms defined in [the substantive part of] this Convention.

(Article 1 ECHR; the non-discrimination requirements are spelled out separately in Article 14, emphasis added)

On their face, these provisions may seem to suggest that states are only required to "respect", "ensure" or "secure" the rights in the international human rights treaties on their own territory. However, in the case-law of the European Court of Human Rights, and in the case-law of other international human rights adjudicating bodies, it has become clear that the concept of "jurisdiction" should be read as a more "functional" than territorial one, at least in special cases, such as when agents of a state are acting outside the state and exercise control outside the state:⁵⁹

It follows from Article 1 [ECHR] that Contracting States must answer for any infringement of the rights and freedoms protected by the Convention committed against individuals placed under their "jurisdiction".

<http://billofrightsinstitute.org/founding-documents/bill-of-rights/>

⁵⁷ Stéphane Hessel explains in his famous essay *Indignez-vous!* that: "*C'est à René Cassin que nous devons le terme de droits 'universelle' et non 'internationaux' comme le proposaient nos amis anglo-saxon.*" *Indignez-vous!*, pp. 6-7, available at:

http://www.millebords.org/IMG/pdf/INDIGNEZ_VOUS.pdf

⁵⁸ See footnote 39, above.

⁵⁹ *Issa and Others v. Turkey*, Application no. 31821/96, judgment of 16 November 2004, paras. 66–71, references to other cases in brackets omitted. The *Lotus judgment* of the Permanent Court of International Justice (footnote 3, above) also stressed that sovereignty and jurisdiction were, at that time, still primarily seen as territorial concepts – but of course, that was in 1927.

The exercise of jurisdiction is a necessary condition for a Contracting State to be able to be held responsible for acts or omissions imputable to it which give rise to an allegation of the infringement of rights and freedoms set forth in the Convention (...).

The established case-law in this area indicates that the concept of "jurisdiction" for the purposes of Article 1 of the Convention must be considered to reflect the term's meaning in public international law (...).

From the standpoint of public international law, the words "within their jurisdiction" in Article 1 of the Convention must be understood to mean that a State's jurisdictional competence is primarily territorial (...), but also that jurisdiction is presumed to be exercised normally throughout the State's territory.

However, the concept of "jurisdiction" within the meaning of Article 1 of the Convention is not necessarily restricted to the national territory of the High Contracting Parties (...). In exceptional circumstances the acts of Contracting States performed outside their territory or which produce effects there ("extra-territorial act") may amount to exercise by them of their jurisdiction within the meaning of Article 1 of the Convention.

According to the relevant principles of international law, a State's responsibility may be engaged where, as a consequence of military action – whether lawful or unlawful – that State in practice exercises effective control of an area situated outside its national territory. The obligation to secure, in such an area, the rights and freedoms set out in the Convention derives from the fact of such control, whether it be exercised directly, through its armed forces, or through a subordinate local administration (...).

It is not necessary to determine whether a Contracting Party actually exercises detailed control over the policies and actions of the authorities in the area situated outside its national territory, since even overall control of the area may engage the responsibility of the Contracting Party concerned (...).

Moreover, a State may also be held accountable for violation of the Convention rights and freedoms of persons who are in the territory of another State but who are found to be under the former State's authority and control through its agents operating – whether lawfully or unlawfully - in the latter State (...). Accountability in such situations stems from the fact that Article 1 of the Convention cannot be interpreted so as to allow a State party to perpetrate violations of the Convention on the territory of another State, which it could not perpetrate on its own territory (...).

(emphases added)

It is notable that the Court, in the final paragraph just quoted, expressly refers, not only to its own earlier case-law, but also to a decision of the Inter-American Commission of Human Rights, *Coard et al. v. the United States*;⁶⁰ and to the views adopted by the Human Rights Committee in the cases of *Lopez Burgos v. Uruguay* and *Celiberti de Casariego v. Uruguay*.⁶¹ This shows that the "functional" approach to the human rights obligations of states has broad support in the international human rights fora.

⁶⁰ Decision of 29 September 1999, Report No. 109/99, case No. 10.951, §§ 37, 39, 41 and 43.

⁶¹ Case nos. 52/1979 and 56/1979, both of 29 July 1981, at §§ 12.3 and 10.3 respectively.

This is confirmed by the Human Rights Committee in its General Comment on *The Nature of the General Legal Obligation Imposed on States Parties to the Covenant*, where it says:⁶²

States Parties are required by article 2, paragraph 1, to respect and to ensure the Covenant rights to all persons who may be within their territory and to all persons subject to their jurisdiction. **This means that a State party must respect and ensure the rights laid down in the Covenant to anyone within the power or effective control of that State Party, even if not situated within the territory of the State Party.** As indicated in General Comment 15 adopted at the twenty-seventh session (1986), the enjoyment of Covenant rights is not limited to citizens of States Parties but must also be available to all individuals, regardless of nationality or statelessness, such as asylum seekers, refugees, migrant workers and other persons, who may find themselves **in the territory or subject to the jurisdiction of the State Party.** This principle also applies to those within the power or effective control of the forces of a State Party acting outside its territory, regardless of the circumstances in which such power or effective control was obtained, such as forces constituting a national contingent of a State Party assigned to an international peace-keeping or peace-enforcement operation.

(emphases added)

Most of the cases concern the exercise of state power by state agents such as soldiers on the soil of other states. If soldiers of a state that is party to the ICCPR, the I-ACHR or the ECHR exercise "effective control" of an area in another country, and put a person in that area under their authority, e.g., by detaining him or killing or injuring him, then the state under whose control they are operating is responsible for those actions under international human rights law: such victims are "within the jurisdiction" of the state concerned.⁶³

However, in recognition of the broad principle quoted above, that states should not be allowed to perpetrate violations of international human rights law on the territory of another state, which it could not perpetrate on its own territory, the concept of "extra-territorial acts" that come within the "jurisdiction" of a State is wider than just covering physical acts on permanently or temporarily occupied foreign soil.

As Prof. Martin Scheinin, the first United Nations Special Rapporteur on human rights and counter-terrorism (2005 – 2011), put it in his analysis of the Human Rights Committee's case-law, presented to the US *Privacy and Civil Liberties Oversight Board's* hearing on the NSA surveillance programme on 19 March 2014:⁶⁴

As [the Human Rights Committee cases] demonstrate, in respect of human rights violations such as discrimination or preventing someone from leaving a country, the

⁶² General Comment No. 31 (footnote 48, above), para. 10.

⁶³ For more European Court's cases, see the very recent European Court of Human Rights [Factsheet on Extra-territorial jurisdiction of ECHR States Parties](http://www.echr.coe.int/Documents/FS_Extra-territorial_jurisdiction_ENG.pdf) (December 2013), available at: http://www.echr.coe.int/Documents/FS_Extra-territorial_jurisdiction_ENG.pdf

⁶⁴ Martin Scheinin, presentation to the US *Privacy and Civil Liberties Oversight Board's* hearing on the NSA surveillance programme on 19 March 2014, available at: <http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0085>

See also Martin Scheinin and Mathias Vermeulen, [Unilateral Exceptions to International Law: Systematic legal Analysis and Critique of Doctrines that seek to Deny or Reduce the Applicability of Human Rights Norms in the Fight against Terrorism](http://projects.essex.ac.uk/ehrr/V8N1/Scheinin_Vermeulen.pdf), section 3.7, *Denial of Extraterritorial Effect of Human Rights (Treaties)*, available at: http://projects.essex.ac.uk/ehrr/V8N1/Scheinin_Vermeulen.pdf

relationship between the violating state and the individual need not amount to effective control over a territory or a person. It is sufficient that a state has control over someone’s rights, or authority over a person or context. The situation is the same with privacy. ...

Moreover, it would be perverse to argue that if a state explicitly legislates to authorise surveillance of “foreigners” outside its territory, and/or of “foreign” communications, it is not exercising its “jurisdiction” in that respect: bringing certain matters (such as electronic communications or Internet- or social network activities) within the legal rules of a country, making those activities subject to the legal order of a country, is perhaps the most conspicuous way to exercise a country’s jurisdiction. In international-legal terms, such a country is exercising “enforcement jurisdiction” over the data.

This is the case, even if the exercise of that jurisdiction would violate the sovereignty of another state, e.g., because it concerned data physically located in another country (cf. the discussion at **A**, above): the fact that the act was contrary to international law of course does not mean that the State perpetrating the act is not bound by its human rights obligations; that too would be perverse.

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.

The contrary position of the USA

The US Government has consistently maintained that “the obligations assumed by a State Party to the International Covenant on Civil and Political Rights (Covenant) apply only within the territory of the State Party”;⁶⁵ and that it is therefore not legally required to comply with the ICCPR in relation to its surveillance over non-US communications or Internet activities.

⁶⁵ The United States stated this position in the first, second, and third periodic reports under the ICCPR (submitted in 1995 and 2005), as well as in its 2007 Observations regarding the Human Rights Committee’s General Comment 31, and reiterated it in its latest, fourth periodic report (2011), although it acknowledged in the last of these that its position is at odds with the views of the Human Rights Committee, the International Court of Justice, and “positions taken by other States parties” (para. 505). See the documentation relating to the latest (2011-2014) review of the USA, at: http://tbinternet.ohchr.org/_layouts/treatybodyexternal/SessionDetails1.aspx?SessionID=625&Lang=en

In the context of the discussions on the (then draft) UN General Assembly Resolution on *Privacy in the Digital Age*, submitted in response to the Snowden revelations,⁶⁶ a briefing note was leaked that confirms that the USA still believes that it is not under any legal duty to comply with international human rights law outside its own geographical territory. Indeed, it considered this to be a "red line" which it will not cross. Its very first instruction was that the US negotiators should:⁶⁷

Clarify that references to privacy rights are referring explicitly to States' obligations under ICCPR and **remove suggestion that such obligations apply extra-territorially.**

(emphasis added)

The Human Rights Committee firmly rejected this position in its Concluding Observations on the 4th USA report, listing the issue first under the heading "Principal matters of concern and recommendations".⁶⁸

Applicability of the Covenant at national level

4. The Committee regrets that the State party continues to maintain its position that the Covenant does not apply with respect to individuals under its jurisdiction but outside its territory, despite the contrary interpretation of article 2(1) supported by the Committee's established jurisprudence, the jurisprudence of the International Court of Justice and state practice. The Committee further notes that the State party has only limited avenues to ensure that state and local governments respect and implement the Covenant, and that its provisions have been declared to be non-self-executing at the time of ratification. Taken together, these elements considerably limit the legal reach and the practical relevance of the Covenant (art. 2).

The State party should:

(a) Interpret the Covenant in good faith, in accordance with the ordinary meaning to be given to its terms in their context, including subsequent practice, and in the light of its object and purpose and review its legal position so as to acknowledge the extraterritorial application of the Covenant under certain circumstances, as outlined inter alia in the Committee's general comment No. 31 (2004) on the nature of the general legal obligation imposed on States parties to the Covenant; ...

(original emphasis in bold)

The Committee added a little later, under the heading "NSA surveillance":

The State party should:

(a) take all necessary measures to ensure that its surveillance activities, both within and outside the United States, conform to its obligations under the Covenant, including article 17; in particular, measures should be taken to ensure that any interference with the right to privacy complies with the principles of legality,

⁶⁶ The debates led to the adoption, on 18 December 2013, of UNGA Resolution 68/167, *The right to privacy in the digital age*, available at: http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/167

⁶⁷ *Right to Privacy in the Digital Age – US Redlines*, available at:

<http://columlynch.tumblr.com/post/67588682409/right-to-privacy-in-the-digital-age-u-s>

⁶⁸ Human Rights Committee Concluding Observations on the 4th USA report (advance unedited version, March 2014), para. 4 (p. 2), available from the webpage mentioned in footnote 65, above.

proportionality and necessity regardless of the nationality or location of individuals whose communications are under direct surveillance;

(original emphasis in bold, underlining added)

In my opinion, the US Government's view, 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.

At the end of this section, I will discuss the avenues available to individuals and states to counter this stand of the USA, under the heading "*Remedies*".

d. "Positive obligations" of states⁶⁹

Treaties are agreements between states. It is a basic principle of treaty law that a treaty binds the parties (the state-parties to the treaty), but not other states.⁷⁰ Also, the human rights obligations laid down in human rights treaties primarily concern the actions (or omissions) of public authorities: private entities are not bound by them.

This is problematic in relation to global surveillance, because in the borderless digital environment individuals (and state officials) can be subjected to surveillance by states that are not party to the human rights treaties that their own governments are subject to, in ways that seriously undermine the rights supposedly guaranteed by those treaties. Furthermore, the technologies and infrastructures involved in electronic communications and the Internet are mainly managed by private-sector entities, including the main US-based "Internet giants", such as Microsoft, Google, Yahoo, etc.. Snowden has revealed that much of the global surveillance perpetrated by the USA in particular focuses on the servers and other infrastructure of these companies; and that these companies have either "voluntarily" cooperated with the US authorities in this respect, or have been forced to cooperate (in particular, through [secret] orders of the FISA Court).

Sometimes, specific requirements in human rights treaties – in particular, the ECHR – are given what is somewhat mistakenly referred to as "horizontal effect" (*Drittwirkung*), in that they are applied, indirectly, in relation to actions (or omissions) of private actors. But even

⁶⁹ This sub-section in part draws on Ian Brown and Douwe Korff, *Digital Freedoms in International Law*, Global Network Initiative (GNI), 2012, available at:

<https://globalnetworkinitiative.org/sites/default/files/Digital%20Freedoms%20in%20International%20Law.pdf>

See also the recent EDRI booklet, *Human Rights and privatised law enforcement: Abandoning rights - abandoning democracy - abandoning law*, EDRI, February 2014, available at:

http://edri.org/wp-content/uploads/2014/02/EDRI_HumanRights_and_PrivLaw_web.pdf

⁷⁰ *Vienna Convention on the Law of Treaties*, Art. 34. This can be different if a treaty requirement either codifies existing customary law, or becomes so widely accepted that it itself becomes customary law. However, even in that case, it is the (old or new) rule of customary law that binds the states that are not party to the treaty in which the norm is codified or expressed; the other states are still not otherwise bound by the treaty.

then, the relevant obligations still rest on the state. The state has, in such cases, a **"positive obligation"** to regulate the actions of the private entities. If it fails to do this, the state can be held responsible for this failure to regulate the relevant private entities concerned.⁷¹

Three issues arise in this respect. First of all, states (such as Germany) and supranational entities such as the EU (within its competences: see at e, below) undoubtedly have a **right** to regulate the acts of private entities that are established in or operate within their territory and jurisdiction, and this includes the right to regulate – or indeed forbid – such entities from cooperating with foreign – *in casu*, US and/or UK – national security agencies. Germany, like other states, and indeed the EU (within its competences: see again at e, below) may indeed have a **duty** – a "positive obligation" – to do so, if without such regulation the fundamental rights of their citizens (and others) would be put at risk.

In my opinion, state-parties to the ECHR have a "positive obligation" to regulate the activities of private entities (such as the US "Internet giants" and the major electronic communication service providers) to ensure that these entities do not cooperate with foreign national intelligence agencies in ways which lead to surveillance practices by those foreign agencies that are not in accordance with the "minimum standards" for surveillance, adduced by the European Court of Human Rights (as summarised on p. 19). In my opinion, the EU has a similar "positive obligation" (within its competences: see at e, below).

States such as the UK (but also others), which by contrast have not just not restricted such cooperation but actually collude in it and encourage and support it, are in my opinion *a fortiori* in breach of their "positive obligations" under the ECHR by not regulating the involvement of the private entities over which they have jurisdiction in an appropriate (ECHR-compliant) manner.

Indeed, in my opinion, the concept of "positive obligations" under the ECHR can be extended to a duty on the part of state-parties to the Convention to regulate the actions of third countries that are not party to the Convention (such as the USA), when those third countries act on the territory of state parties in ways that lead to violations of the rights of individuals within the ECHR area.

In other words: 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

⁷¹ See Harris, O'Boyle & Warbrick, Law of the European Convention on Human Rights, 2nd ed. (2009), Chapter 1, section 5, *Negative and Positive Obligations and Drittwirkung*, in particular pp. 19 – 21.

I will not discuss here the UN *Guiding Principles on Business and Human Rights*, drafted by the United Nations Secretary-General's Special Representative for Business and Human Rights, Professor John Ruggie (the "Ruggie Principles"), contained in his report to the UN Human Rights Council:

Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, John Ruggie: Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework, UN Human Rights Council Document A/HRC/17/31, 21 March 2011, available at:

http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

Important though they are as emerging principles, they are not yet firm enough to be taken into consideration here.

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 "lawfully" 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. 19, above).

I believe that the German legal framework – like most countries' legal frameworks – needs to be reviewed in this light (see also my answer to Question 3).

More importantly, Germany as a state-party can raise this issue as concerns the UK in inter-state proceedings under the ECHR, and individuals can do the same through individual applications (see below, under the heading "Remedies").

e. The EU Charter of Fundamental Rights and the exclusion of "national security" from EU competence⁷²

From the mid-70s, the Court of Justice of the EC (now EU) began to uphold human rights as "general principles of Community [now Union] law", mainly in response to rulings by the German and Italian constitutional courts that threatened to refuse to give EC law precedence over national law unless human rights were protected at at least the level of those constitutions.⁷³

More recently, fundamental rights were codified within the EU in the form of the Charter of Fundamental Rights of the European Union (the Charter or CFR), adopted in 2007.⁷⁴ It was

⁷² This section expands on a series of slides used for my presentation on the law relating to the surveillance issues to the European Parliament's LIBE Committee on 14 October 2013.

⁷³ The Court of Justice of the EC first recognised that "...respect for fundamental rights forms an integral part of the general principles of Community law" in the *Internationale Handelsgesellschaft* case (Case 11/70 [1970] ECR 1161). It developed this further, and more emphatically and explicitly in *Nold v. Commission* (Case 4/73 [1974] ECR 491), in which the Court cited the inspiration for these general principles as comprising both the common national constitutional traditions of the Member States and international human rights agreements in the drafting of which they had cooperated, i.e., in particular, the ECHR. This case was a clear response to the so-called "*Solange-I*" decision of the German Constitutional Court, BVerfGE 37, 271, available at: <http://www.servat.unibe.ch/dfr/bv037271.html>

In later decisions (in particular "*Solange-II*", BVerfGE 73, 339), the Constitutional Court modified this stance in response to the CJEU's upholding of human rights through "general principles", to the effect that the German court would normally leave the protection of human rights to the European Court. However, the basic threat of not applying EC or EU law unless it meets the human rights requirements of the German Constitution remains.

⁷⁴ Available at:

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:en:PDF>

given legally binding status with the coming into force of the Lisbon Treaty in 2009.⁷⁵ The Charter includes all the rights in the ECHR (and those rights must be interpreted in the same way as the ECHR rights),⁷⁶ but also adds further rights. In particular, the CFR contains a specific provision on data protection which, as we shall see below, at C, is given increasingly strong support by the Court of Justice of the EU (CJEU).

In principle, EU law can therefore provide a strong means to protect human rights in relation to matters subject to Union law. However, here we must note one particular problematic aspect of EU law: the seemingly complete exclusion of EU competence from matters relating to “national security”. As it is put in Article 4(2) of the treaty on European Union (TEU): “[N]ational security remains the sole responsibility of each Member State.”

Art. 73 TFEU adds that “[MSs may] organise between themselves and under their responsibility such forms of cooperation and coordination as they deem appropriate between the competent departments of their administrations responsible for safeguarding national security.” – but if anything, this merely underscores that the matter is the responsibility of the States, and not of the Union.

In other words, on the face of these texts, it would appear that the EU has no competence at all on matters relating to national security; that those matters remain the sole responsibility of the States; and that the Member States are also free to organise any cooperation between themselves – and with third countries – as they deem fit.

Moreover, since national security is outside EU competence and thus outside EU law, it would appear to follow:

- that the Charter FR (which is EU law) does not apply to anything the MSs do (either by themselves or in some form of cooperation, be that within the EU or with third countries) in relation to national security; and
- that the ECJ also has no jurisdiction over such matters at all.

However, that is an over-statement of the legal position. In particular, Article 4(2) TEU applies to Member States’ action in relation to [their] “national security”. However, that begs the question of what exactly is covered by the term “national security”, and whether it is solely left to the Member States to define this concept as they like.

In that context, it is important to note that as part of the EU’s Common Foreign and Security Policy (CFSP) the Union is required to “safeguard its [i.e., the Union’s] values, fundamental interests, [internal] security, independence and integrity” and to “strengthen international security” (Art. 21(2)(a) & (c) TEU); and that Article 4(2)(j) TFEU provides for “shared competence” between the Union and the MSs in respect of the area of “freedom, security and justice”, covered by Part Three, Title V, of the treaty on the Functioning of the European Union (TFEU), including in relation to the fight against crime, racism and xenophobia (see Art. 67(3) and against “terrorism and related activities” (see Art. 75).

⁷⁵ Note that the special protocol to the Lisbon Treaty, adopted for the UK and Poland, contrary to what one might think on first reading, does not amount to an “opt out” from the legally binding nature of the Charter for those countries. See:

<http://www.headoflegal.com/2013/11/21/whos-right-about-the-eu-charter-of-fundamental-rights/>

⁷⁶ See Art. 52(3) CFR.

In other words, Member States may have sole competence in relation to their own national security, BUT the Union has shared competence with the Member States when it comes to the Union’s own internal security, and in relation to crime and terrorism, and under the CFSP the Union also has competences in relation to international security. There are clearly considerable overlaps between these matters – and that has implications for the scope of the “national security” exemption.

Specifically, “national security”, each Member State’s “internal security”, the Union’s “internal security”, and “international security” cannot be separated from each other, nor from *Justice and Home Affairs* or *Justice and Freedom* action (i.e., police and judicial cooperation), in particular in relation to “terrorism and related activities” (or international crime, or extremism or xenophobia). The duties and responsibilities that Member States have in relation to the latter matters impact on the autonomy of Member States in relation to the first.

Thus, it follows from general law on treaties (VCLT) that Member States may not invoke Art. 4(2) TEU in such a way as to negate or undermine the shared competences of the EU in relation to internal security, crime and terrorism. Member States’ “autonomous” actions to protect their own national security must respect, and tie in with, their joint or cooperative or coordinated actions with other Member States in relation to the EU’s own internal security, the joint security of all the Member States, and the joint fight against international crime and terrorism.

Moreover, just as Member States may not invoke Art. 4(2) to negate or undermine the shared competences of the EU in relation to internal security, crime and terrorism, they may also not use their powers in the exempt area to negate or undermine the Union’s general *aquis*:⁷⁷

National measures which seek to maintain national security may not interfere with the fundamental freedoms and, insofar as they fall within the scope of EU law, must respect fundamental rights as understood in the EU legal order.

Of course, the *caveat* “insofar as [the measures] fall within the scope of EU law” largely begs the question. However, as we shall see at **C**, below, the surveillance exposed by Snowden directly affects matters that are tightly regulated by EU law, i.e., privacy in electronic communications. What is more, it is clear from the CJEU judgment on data retention (also further discussed at **C**) that a Member State’s activities in the context of an exception to an EU (or EC-)regulated matter also falls “within the scope of EU law”.

At the most basic level, the question of what is, and what is not, a matter of “national security”, is a legal question. The term is a word that is used in the treaties, and the meaning of that term in that context may – indeed, must – therefore be determined by the Court.

There is little explicit guidance on the meaning of the term “national security” in the case-law of the human rights treaty bodies. However, the Johannesburg Principles, issued by the civil society group Article 19 has gained some authority, in that it has been repeatedly

⁷⁷ Diamond Ashiagbor, Nicola Countouris, Ioannis Lianos (Eds.), The European Union After the Treaty of Lisbon, CUP, 2012, p. 57, emphases added.

endorsed by UN special rapporteurs in particular.⁷⁸ They stipulate the following in Principle 2:

(a) A restriction sought to be justified on the ground of national security is not legitimate unless its genuine purpose and demonstrable effect is to protect a country's existence or its territorial integrity against the use or threat of force, or its capacity to respond to the use or threat of force, whether from an external source, such as a military threat, or an internal source, such as incitement to violent overthrow of the government.

(b) In particular, a restriction sought to be justified on the ground of national security is not legitimate if its genuine purpose or demonstrable effect is to protect interests unrelated to national security, including, for example, to protect a government from embarrassment or exposure of wrongdoing, or to conceal information about the functioning of its public institutions, or to entrench a particular ideology, or to suppress industrial unrest.

The Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, expressly referred to the Johannesburg Principles in his 2011 report, in relation to the use of defamation law.⁷⁹

The Special Rapporteur would like to reiterate that defamation should be decriminalized, and that protection of national security or countering terrorism cannot be used to justify restricting the right to expression unless the Government can demonstrate that: (a) the expression is intended to incite imminent violence; (b) it is likely to incite such violence; and (c) there is a direct and immediate connection between the expression and the likelihood or occurrence of such violence.

Without a further express reference to the Principles, but in terms clearly echoing the above, the Rapporteur also, in the same report, expressed his "*deep concern*" over "*actions taken by States against individuals communicating via the Internet, frequently justified broadly as being necessary to protect national security or to combat terrorism*"⁸⁰ He clearly doubts whether such actions can always be justified by reference to these purposes.

Overall, one can conclude that the concept of national security as used in the international human rights treaties, and thus, I believe, in the EU treaties, must be narrowly interpreted – it certainly does not constitute a "blank cheque", under which states are allowed to do

⁷⁸ Johannesburg Principles on National Security, Freedom of Expression and Access to Information, 1996, adopted on 1 October 1995 by a group of experts in international law, national security, and human rights convened by ARTICLE 19, the International Centre Against Censorship, in collaboration with the Centre for Applied Legal Studies of the University of the Witwatersrand, in Johannesburg, available at: <http://www.article19.org/data/files/pdfs/standards/joburgprinciples.pdf>

As noted by UNHCHR, the Principles have been endorsed by Mr. Abid Hussain, the UN Special Rapporteur on Freedom of Opinion and Expression, in his reports to the 1996, 1998, 1999 and 2001 sessions of the United Nations Commission on Human Rights, and were referred to by the Commission in their annual resolutions on freedom of expression every year since 1996.

⁷⁹ Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, to the Human Rights Council, 16 May 2011, A/HRC/17/27, para. 36, available at: http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

⁸⁰ *Idem*, para. 54. Note also more broadly the emphasis placed by the Special Rapporteur in the subsequent paragraphs on the need for states to comply with the general human rights principles discussed earlier ("law", "necessity", "proportionality", etc.) in their national security/ant-terrorism surveillance.

whatever they like as long as they invoke the phrase. On the contrary, as a term used in the treaties it is subject to legal interpretation, and because it allows for limitations, it must be restrictively interpreted.

Even if one were to feel that the limitation in the Johannesburg Principle 2(a), above – allowing the invocation of national security essentially only in relation to the use or threat of force by either foreign or domestic opponents – is too limited, it is clear that the concept can only be invoked in relation to very major threats against a state’s crucial political structures, or essential interests. Gaining a political advantage in diplomatic negotiations, or an economic advantage for the state itself or for the country’s industries, are clearly not included in the concept of national security.

Indeed, the use of special national security powers for such purposes that cannot be reasonably said to relate to “national security” interests would constitute *abus de pouvoir* or *détournement de pouvoir* in terms of international human rights- and/or general treaty law, and would therefore be in violation of the relevant human rights treaties.⁸¹

By contrast, the main surveillance agencies of the two states that appear to be at the forefront of global Internet and communications surveillance operate on the basis of much wider concepts. The NSA can essentially look for any information on non-US individuals that “relates to the conduct of the foreign affairs of the United States”;⁸² and the UK’s GCHQ’s mandate, too, stretches beyond “national security” in any narrow sense to matters such as pandemics, cyberthreats, energy security, serious crime and the economic well-being of the country.⁸³

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.

⁸¹ See Art. 18 ECHR. With regard to the ICCPR and other international human rights treaties, the same would apply under general treaty law, as codified in the VCLT.

⁸² FISA Act §1801(a) & (e). For details, See again the report by Caspar Bowden et al. to the European Parliament, *Fighting Cybercrime and Protection Privacy in the Cloud*, 2012, and the subsequent article by him and Judith Rauhofer, *Protecting their own: Fundamental rights implications for EU data sovereignty in the cloud*, 2013, already noted in footnote 51, above.

⁸³ See the application by *BBW, ORG et al. v. the UK* (note 39, above).

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.

Finally, in view of the strong recent positions taken by the Court on data protection matters, I believe that the Court would not hesitate to reach such conclusions in relation to the utterly unrestrained surveillance by the UK. This means that, in my opinion, there are good prospects for a challenge to the UK's surveillance activities in the Luxembourg Court (as further noted below, under the heading "*Remedies*").

B.3 Remedies

I believe that the above sub-sections (B.2.a – e.) have shown categorically that the mass surveillance systems and operations of the USA and the UK (and others, in particular the other countries in the "5EYES" club) are in manifest violation of these countries' obligations under the relevant international human rights treaties, i.e., in relation to all of them, under the ICCPR (to which all the "5EYES" are party) and, as concerns the UK, also under the ECHR.

Moreover, as I have shown in the last sub-section, e, in spite of the "national security" exemption clause in Art. 4(2) TEU, the Court of Justice of the EU is competent to rule (i) on whether the UK can, in relation to specific matters, honestly invoke the exemption (and it cannot do so in relation to purely economic spying or spying on the institutions of the EU); and (ii) on whether the UK, even in matters in which it can in principle rely on the exemption, is exercising its discretion and competences in that matter in a way that does not unduly conflict with its other obligations under EU law, or with the EU *acquis*.

This means that there is a range of remedies available to individuals and states, including German citizens and the Federal Republic – but with some distinctions, as follows:

ICCPR:

As Prof. Scheinin, the former UN Special Rapporteur on human rights and counter-terrorism, observed in his testimony to the European Parliament's LIBE Committee investigating the Snowden revelations:⁸⁴

The short answer to the question of [the lawfulness of the surveillance programmes exposed by Snowden, in terms of the ICCPR] is that both the United States and the United Kingdom have been involved, and continue to be involved, in activities that are in violation of their legally binding obligations under the International Covenant on Civil and Political Rights of 1966. ...

⁸⁴ LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens Hearing, European Parliament, 14 October 2013, *Statement by Professor Martin Scheinin (EUI)*, available at: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/scheinin/_scheinin_en.pdf (emphasis added).

Neither the United States nor the United Kingdom have accepted the right of individual complaint under the Covenant, which would allow the pertinent quasi-judicial body of independent experts, the Human Rights Committee, to assess whether the country violated the Covenant in respect of a specific individual. There are, nevertheless, two other mechanisms through which the same Committee can address treaty compliance by these two countries. Both have accepted the procedure for inter-state complaints under article 41 of the Covenant. Even if this procedure has never been resorted to, **the current context of two Western democracies involved in what appears to be a massive interference with the privacy rights of EU citizens (and others), coupled with the unavailability of individual redress, would provide an instance where EU countries should seriously consider triggering the inter-state complaint procedure.**

I can only wholeheartedly concur, and would call on the Committee of Inquiry to recommend such action to the German Government.

Prof. Scheinin also noted that *"independently of that option, both countries are subject to the single mandatory monitoring mechanism under the Covenant, the duty to submit periodic reports for the consideration by the Human Rights Committee"*. As we have seen, the Human Rights Committee has already issued its "Concluding Observations" on the latest report from the USA, and clearly indicated that it considers the surveillance programmes of the USA to be in violation of the Covenant.⁸⁵ The UK is up for its review later this year, and it would be highly surprising (to say the least) if the Committee were not to indicate the same view in respect of that country's surveillance programmes.

ECHR:

Unlike the situation under the ICCPR, since the coming into force of the 11th protocol to the ECHR in 1988, states can no longer "opt out" of either the system for inter-state complaints or individual applications under the ECHR. This means that both individuals, or groups of individuals, and states can raise the issue of mass surveillance as perpetrated by the UK before the European Court of Human Rights.

As we have seen, an important, well-argued individual application on the issue, *BBW, ORG et al. v. the UK*, is already before the Court.⁸⁶ If the Court accepts that the case is not inadmissible (in particular, over the issue of exhaustion of domestic remedies),⁸⁷ the Court will be able to rule authoritatively on the mass surveillance programmes still this year. That would be a crucial, judicial and binding international-legal ruling that could settle many of the core issues definitively.

German citizens, or groups representing German citizens, could bring similar cases (or they could wait to see the outcome of the *BBW, ORG et al.* case).

⁸⁵ See footnote 35, above, and the text to which that footnote relates.

⁸⁶ See footnote 33, above.

⁸⁷ Unlike some other groups, such as the UK NGO *Liberty*, *BBW* and *ORG* decided not to first submit their complaint to the Investigatory Powers Tribunal, because in their view this tribunal did not afford an "effective remedy" against the surveillance. The *Liberty* case is likely to be heard soon, but may then have to be appealed through the UK legal system. See:

<http://www.theguardian.com/world/2014/feb/14/court-challenge-mass-surveillance>

The situation of the German Government is different. It is harmed not only because its citizens' rights are trampled on by the UK Government (and by the US Government, but that is outside of the jurisdiction of the Strasbourg Court). Rather, it is harmed because the UK surveillance is a serious violation of its rights as an equal party to the UK to the Convention: through its programmes of surveillance of German citizens, and officials, and institutions, the UK is, in my opinion, in serious contractual breach of its reciprocal duties towards its other European treaty partners.

In my opinion, that warrants 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. 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

In that context, it is worth noting that under Article 52 of the Convention, the Secretary-General of the Council of Europe has the right to demand of any state-party to the ECHR that it furnishes the Council of Europe and the other state-parties with "*an explanation of the manner in which its internal law ensures the effective implementation of any of the provisions of the Convention.*" To date, the Secretary-General has not used this power, but several bodies, including the Parliamentary Assembly of the Council of Europe (PACE) have called upon him to use this power in relation to the Snowden revelations.

In my opinion, it would be highly appropriate for the German Government to support the call for the Secretary-General to use this power; and the Committee of Inquiry should in my opinion request the Government to do that.

EU remedies

As explained in section B.2, sub-section e, above, "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, large parts of the surveillance operations carried out by the UK security services (GCHQ in particular) are *not* directed at protecting national security within the proper international- (and EU-) legal meaning of that term; and others, that might be said to fall within that ambit, are so disproportionate and unnecessary to that aim, and so much in conflict with other EU principles, that they too are incompatible with EU law.

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.

D. International and European data protection law

D.1. Subjects

If international human rights law is a special branch, with special features, of general public international law, in particular in terms of individuals being subjects of that branch of the law, then international data protection law is a special further offshoot, with further special features. Specifically, international data protection law does not only also treat individuals as subjects of the law, but it also provides them 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.

D.2 Substantive law

Data protection laws were first introduced into many European countries, including Germany, during the 1970s and 80s.⁸⁸ Data protection was first given explicit international recognition and protection in the 1981 Council of Europe Data Protection Convention (hereinafter the 1981 Convention or Convention No. 108), the "mother" document of all international data protection instruments.⁸⁹ In 1995, the first (and still the main) EC directive on data protection was adopted,⁹⁰ followed by a specialised, subsidiary directive on privacy and electronic communications in 2002 (the "e-Privacy Directive"),⁹¹ and, in 2006, by the so-called "Data Retention Directive", which is technically an amendment to the e-Privacy Directive.⁹² The e-Privacy Directive and the Data Retention Directive (which has now been declared null and void: see below) are the most important ones in relation to Internet and electronic communications surveillance, but the main directive is also important because it spells out the main, "core" data protection principles (in line with the 1981 Convention, with some additions).

All these directives have been implemented by the EU Member States (including Germany) in the form of national laws and/or subsidiary statutory instruments. The main directive is soon to be replaced by a General Data Protection Regulation, which will further strengthen European data protection law.⁹³ As a regulation, it will be directly applicable in the Member

⁸⁸ The Data Protection Law of the German *Land* of Hesse was the first data protection law in the world.

⁸⁹ Full title: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No. 108 (hence the reference to 'Convention 108').

⁹⁰ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 23 November 1995, OJ L.281, p. 31ff (**the main directive**).

⁹¹ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications, commonly referred to as **the e-Privacy Directive**), 31 July 2002, OJ L 201, p. 37ff (as amended by the Data Retention Directive, references in the next footnote).

⁹² Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, 13 April 2006, OJ L105, p. 54ff (**the Data Retention Directive**).

⁹³ Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Brussels, 25.1.2012, COM(2012) 11 final (original Commission proposal). An

States, without the need for "transposition" (which has led to significant divergencies between the current laws implementing the directives). However, the e-Privacy Directive is likely to remain in place for a while yet.

Below, I will briefly address three issues before drawing some broader conclusions in relation to surveillance:

- what European data protection law is about;
- the "core" data protection principles; and
- the special exceptions, including the issue of compulsory data retention.

What European data protection is about

The rights which the data protection laws and this convention seek to protect *include* the right to privacy - or "private life" as it is called in the European Convention on Human Rights (Article 8). However, the laws and the European data protection instruments aim at more than that: in the view of legislators and constitutional courts in many European countries, data protection as applied to "natural persons" has the wider purpose of protecting "human identity" (*l'identité humaine*)⁹⁴ or – as in Germany – the protoright to [respect for one's] "personality" (*das allgemeine Persönlichkeitsrecht*).

Data protection is therefore seen, in Europe at least, as a new fundamental right, *sui generis*, linked to but not limited to the protection of privacy. 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 other words, 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. As the German Constitutional Court put it in its famous *Census* judgment: if someone must at all times wonder whether any "unconventional" behaviour on her part may be registered and permanently kept on record, she is likely to try to avoid such "coming to notice". That would not only affect that one person's right, but would damage the very foundations of a democratic society that is based on the active participation of its citizens.⁹⁵

informal version of the latest text, containing the amendments proposed by the European Parliament, is available here:

<http://www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf>

Note however that, apparently, at the time of writing, Germany is leading the opposition to the GDPR, because reportedly it feels that the Regulation is not strict enough.

⁹⁴ Cf. Art. 1 of the French data protection law, the *Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*:

"L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques." (emphasis added)

⁹⁵ German Constitutional Court judgment of 15 December 1983 (the Court's famous "*Census*" judgment), Section II, at 1a). The original paragraph, paraphrased in the text, reads as follows:

"Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und

It is relevant to the Snowden issues to note that although the leading advocate of a "right to be left alone", Louis Brandeis, saw privacy in a similar way,⁹⁶ the law in the USA has not adopted such a broad view.⁹⁷ Rather, privacy law in the USA is a disparate patchwork of Federal and State-, common- and statute law. In some areas covered by federal law (such as cable tv), and in some State Constitutions and -laws, there are some protections that come somewhere near to the European standards. However, even in the better-protected areas (which mostly relate to private-sector controllers), standards do not really meet the European ones, especially when it comes to the (to us Europeans, absolutely core) requirement of "purpose-limitation". These laws also tend to contain sweeping exemptions in respect of disclosure of data by private-sector entities to law enforcement and anti-terrorist agencies.

Such protections are US law provided were already severely limited by the PATRIOT Act, as well as largely limited to US citizens and lawful US residents ("US persons").⁹⁸ As we have since learned, the FISA Act, as amended, effectively removed all privacy protection from "non-US-persons".⁹⁹

The fundamental difference of the weight given to data protection/informational privacy as viewed from Europe and the USA, and the different ways in which they are balances against freedom of expression on the one hand and the rights of law enforcement- and national security agencies on the other hand, will make it very difficult to reach an EU-USA agreement on these matters. 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

als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist."

⁹⁶ Louis Brandeis and Samuel Warren, *The Right to Privacy*, Harvard Law Review, 15 December 1890, available at:

<http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm>

Later, as a Supreme Court judge, he defined the "right to be let alone" in his famous dissenting opinion in *Olmstead v. United States* (1928) as "the most comprehensive of rights, and the right most valued by civilized men."

⁹⁷ See the [EDRI/FREE submission on the surveillance activities of the United States and certain European States' national security and "intelligence" agencies](#), sent to various European and U.S. bodies in August 2013, in particular Section III (paras. 10 and 11) and [Attachment 3: Summary of United States standards on national security surveillance](#) (with further references), available at:

http://www.edri.org/files/submission_free_edri130801.pdf

⁹⁸ *Idem.*

⁹⁹ *Idem.* See also again the report by Caspar Bowden et al. to the European Parliament, *Fighting Cybercrime and Protection Privacy in the Cloud*, 2012, and the subsequent article by him and Judith Rauhofer, *Protecting their own: Fundamental rights implications for EU data sovereignty in the cloud*, 2013, already noted in footnote 51, above.

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.

the “core” data protection principles

All the European data protection instruments stipulate as their core principles, with minor variations, that all personal data must be:

- processed fairly and lawfully (Art. 5(a) of the 1981 Convention; Art. 6(1)(a) of the main EC Directive);
- collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes (Art. 5(b) of the 1981 Convention; Art. 6(1)(b) of the main EC Directive) (German: *Zweckbindung*);
- adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed (Art. 5(c) of the 1981 Convention; Art. 6(1)(c) of the main EC Directive);
- accurate and, where necessary, kept up to date (Art. 5(d) of the 1981 Convention; Art. 6(1)(d) of the main EC Directive); and
- kept in identifiable form for no longer than necessary for the purposes for which the data were collected or for which they are further processed (Art. 5(e) of the 1981 Convention; Art. 6(1)(e) of the main EC Directive).

The e-Privacy Directive adds specific, strict rules on the use of traffic- and location data, i.e., on the kinds of data typically generated in relation to electronic communications. In principle, such data may only be used for the purpose of the transmission of a communication, or for the purposes of subscriber billing and interconnection payments or, with the consent of the subscriber, for the provision of “value-added services”.¹⁰⁰

the special exceptions, and the CJEU judgment on the Data Retention Directive

Article 13 of the main EC data protection directive allows for exceptions to its rules and principles, including its provisions on purpose-limitation and data retention-limitation, and Art. 15 of the e-Privacy Directive makes clear that these also apply to the rules in that directive. However, as it is put in the latter article, any such an exception to the normal rules and principles must be:

a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system ...

In a crucial recent judgment, the Court of Justice ruled that the Data retention Directive failed to meet these requirements, because it imposed departures from the core data protection principles that were not proportionate to the stated aim of the Directive, the

¹⁰⁰ See Arts. 6 and 9 of the e-Privacy Directive.

prevention, investigation, detection and prosecution of serious crime, such as organised crime and terrorism.¹⁰¹

In reaching this conclusion, the Court first of all noted that the "metadata" that were to be compulsorily retained:

taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them. (para. 27)

It continued:

In such circumstances, even though, ..., the directive does not permit the retention of the content of the communication or of information consulted using an electronic communications network, it is not inconceivable that the retention of the data in question might have an effect on the use, by subscribers or registered users, of the means of communication covered by that directive and, consequently, on their exercise of the freedom of expression guaranteed by Article 11 of the Charter. (para. 28)

This of course echoes the view of the German Constitutional Court in the *Census* judgment.¹⁰²

The Court expressly rejected the view (often put forward in the UK) that data protection should be limited to data that is particularly sensitive or touches on particularly private matters: there was an interference with the fundamental right to privacy, even if the data were not sensitive and even if the persons concerned were not inconvenienced in any way (para. 33). The mere fact that communication metadata were compulsorily retained constituted an interference with the fundamental right to privacy (para. 34).

In this, the Court also expressly rejected the view (put forward especially by the USA, in particular in relation to the NSA surveillance operations) that there is only an interference with the right to privacy when data are *accessed* by state agencies. The Court expressly rejected this view, holding that such access constitutes a further, separate interference, over and above the interference created by the compulsory data retention (para. 35).

The interference allowed by the Data Retention Directive was, indeed, "wide-ranging" and "particularly serious" (para. 37). The Court agreed with the Advocate General that:

the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance. (para. 37)

¹⁰¹ Judgment in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others*, of 8 April 2014, available at: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=12322>

For an early analysis, see:

<http://eulawanalysis.blogspot.co.uk/2014/04/the-data-retention-judgment-cjeu.html>

¹⁰² See footnote 95, above.

Somewhat inconsistent with its finding about the intrusiveness and revealingness of metadata, quoted above, the Court held that because the Directive did not require the retention of communication content, it did not adversely affect "the essence" of data protection rights (the untouchable core of a fundamental right never being permitted to be compromised) (para. 39). It therefore had to assess the question of whether compulsory data retention served "an objective of general interest" (the EU equivalent of the "legitimate aim" required by the ECHR); and if so, whether the measure was "necessary", "appropriate" and "proportionate" to that aim.

On the first point, the Court held that "*data relating to the use of electronic communications are particularly important and therefore a valuable tool in the prevention of offences and the fight against crime, in particular organised crime*"; and that the retention of data therefore did serve an objective of general interest (paras. 43 – 44). Data retention was also not "inappropriate" (read: unsuited to achieving the stated purpose; German: *geeignet*), just because people could evade being caught by the retention measures (para. 50).

The Court also held that because of the seriousness of the interference with a fundamental right posed by compulsory data retention, "*the EU legislature's discretion is reduced, with the result that review of that discretion [by the Court] should be strict*" (para. 48). Indeed, the Court stressed that because protection of private life constitutes a fundamental right, according to its settled case-law, "*derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary*" (para. 52, with reference to further case-law).

Consequently:

the EU legislation in question must lay down **clear and precise rules** governing the scope and application of the measure in question and imposing **minimum safeguards** so that the persons whose data have been retained have **sufficient guarantees to effectively protect** their personal data against the risk of abuse and against any unlawful access and use of that data (para. 54, with extensive reference, interestingly, to ECHR case-law; emphasis added)

In undertaking this review, the Court was critical of a large number of aspects of the data retention regime established by the Data Retention Directive:

... [T]he directive requires the retention of all traffic data concerning fixed telephony, mobile telephony, Internet access, Internet e-mail and Internet telephony. It therefore applies to all means of electronic communication, the use of which is very widespread and of growing importance in people's everyday lives. Furthermore, in accordance with Article 3 of Directive 2006/24, the directive covers all subscribers and registered users. It therefore entails an interference with the fundamental rights of practically the entire European population.

... Directive 2006/24 covers, in a generalised manner, all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime.

Directive 2006/24 affects, in a comprehensive manner, all persons using electronic communications services, but without the persons whose data are retained being, even

indirectly, in a situation which is liable to give rise to criminal prosecutions. It therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime. Furthermore, it does not provide for any exception, with the result that it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy.

Moreover, whilst seeking to contribute to the fight against serious crime, Directive 2006/24 does not require any relationship between the data whose retention is provided for and a threat to public security and, in particular, it is not restricted to a retention in relation (i) to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or (ii) to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences.

Secondly, not only is there a general absence of limits in Directive 2006/24 but Directive 2006/24 also fails to lay down any objective criterion by which to determine the limits of the access of the competent national authorities to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions concerning offences that, in view of the extent and seriousness of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, may be considered to be sufficiently serious to justify such an interference. On the contrary, Directive 2006/24 simply refers, in Article 1(1), in a general manner to serious crime, as defined by each Member State in its national law.

Furthermore, Directive 2006/24 does not contain substantive and procedural conditions relating to the access of the competent national authorities to the data and to their subsequent use. Article 4 of the directive, which governs the access of those authorities to the data retained, does not expressly provide that that access and the subsequent use of the data in question must be strictly restricted to the purpose of preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating thereto; it merely provides that each Member State is to define the procedures to be followed and the conditions to be fulfilled in order to gain access to the retained data in accordance with necessity and proportionality requirements.

In particular, Directive 2006/24 does not lay down any objective criterion by which the number of persons authorised to access and subsequently use the data retained is limited to what is strictly necessary in the light of the objective pursued. Above all, the access by the competent national authorities to the data retained is not made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions. Nor does it lay down a specific obligation on Member States designed to establish such limits.

Thirdly, so far as concerns the data retention period, Article 6 of Directive 2006/24 requires that those data be retained for a period of at least six months, without any distinction being made between the categories of data set out in Article 5 of that directive on the basis of their possible usefulness for the purposes of the objective pursued or according to the persons concerned.

Furthermore, that period is set at between a minimum of 6 months and a maximum of 24 months, but it is not stated that the determination of the period of retention must be based on objective criteria in order to ensure that it is limited to what is strictly necessary.

(paras. 56 – 64)

In view of these defects in the Directive, the Court held that:

It follows from the above that Directive 2006/24 does not lay down clear and precise rules governing the extent of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter. It must therefore be held that Directive 2006/24 entails a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary. (para. 65)

Moreover, the Directive also did not provide “*sufficient safeguards, as required by Article 8 of the Charter, to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of that data*”:

In the first place, Article 7 of Directive 2006/24 does not lay down rules which are specific and adapted to (i) the vast quantity of data whose retention is required by that directive, (ii) the sensitive nature of that data and (iii) the risk of unlawful access to that data, rules which would serve, in particular, to govern the protection and security of the data in question in a clear and strict manner in order to ensure their full integrity and confidentiality. Furthermore, a specific obligation on Member States to establish such rules has also not been laid down.

[The Directive also] does not ensure that a particularly high level of protection and security is applied by those providers by means of technical and organisational measures, but permits those providers in particular to have regard to economic considerations when determining the level of security which they apply, as regards the costs of implementing security measures. In particular, Directive 2006/24 does not ensure the irreversible destruction of the data at the end of the data retention period.

In the second place, it should be added that that directive does not require the data in question to be retained within the European Union, with the result that it cannot be held that the control, explicitly required by Article 8(3) of the Charter, by an independent authority of compliance with the requirements of protection and security, as referred to in the two previous paragraphs, is fully ensured. Such a control, carried out on the basis of EU law, is an essential component of the protection of individuals with regard to the processing of personal data (see, to that effect, Case C-614/10 Commission v Austria EU:C:2012:631, paragraph 37).

(paras. 66 – 68)

Having thus found that the Directive was fundamentally flawed because it both lacked sufficiently “clear and precise rules” to circumscribe the capturing of data, and “sufficient safeguards against abuse”, the Court concluded that in adopting the Data Retention Directive in the form it did, “the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality” (para. 69). The Directive was therefore invalid, *in toto* and *ab initio* (para. 71).

The implications of the EU data protection rules and the CJEU judgment on the Data Retention Directive for surveillance generally

The judgment of the Court on the Data Retention Directive has clear and direct implications for surveillance generally (subject only to the question of EU competence, already noted, to which I will return).

First of all, the Luxembourg Court made it very clear that the main reason why it felt the Data Retention Directive violated the Charter was the indiscriminate nature of the measure, covering the communications data of "practically the entire European population", without any differentiation, and thus affecting "even ... persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime", and "persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy" (such as lawyers, priests, imams and journalists), as well as "all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception".

In particular, the Court criticised the fact that the Data Retention Directive "[did] not require any relationship between the data whose retention is provided for and a threat to public security and, in particular, it is not restricted to a retention in relation (i) to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or (ii) to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences."

These considerations 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. In the EU, I believe this is the only way to overcome the debacle of the Data Retention Directive. Personally, I do not see any other way in which the EU could comply with the judgment.

But there are wider implications, in particular also for surveillance by national security agencies. Leaving aside the question of EU competence (to which I will return), **it is in my view clear 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.**

If one takes the same approach to the GCHQ surveillance as was taken by the Luxembourg Court to the Data Retention Directive – which was supposedly based on the same derogation clauses that also cover national security – it is clear that even under such clauses states do not have *carte blanche*. On the contrary, even in the fight against serious organised crime – and in the fight against terrorism – some basic standards must still be

met: the special rules must still be sufficiently **clear and precise** to be foreseeable (and thus also, at the most basic, published!); they must **not be indiscriminate**, but rather, targeted at people with some link (in time or place, or connections) to targeted issues and people; and they must contain **adequate safeguards** against abuse, including *independent supervision*.

The mass surveillance systems, rules, institutions and practices of the USA and the UK (et al.), exposed by Edward Snowden manifestly do not meet any of these requirements.

This 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, as noted next.

D.3 Remedies

To repeat what I said at **B.3**: 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. The latter does not have a judicial or quasi-judicial enforcement system attached to it, but it can address issues of the application of that Convention in particular areas. An important recommendation on the use of police data (Recommendation R(87)15) has become fundamental to all European (including EU) police cooperation matters.

In my opinion, the drafting of a similar – for a start, non-binding but still authoritative – set of guidance on the processing (including the collecting) of personal data by national security agencies is now a matter of urgency.

Beyond that, I believe that the fact that the UK surveillance operations are so manifestly in breach of EU and Council of Europe data protection standards will also have a major impact on the application of the ECHR to those operations: the Strasbourg Court tries to ensure that its application of the Human Rights Convention is consistent with other Council of Europe (and wider, global) standards. 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?

What is spying?

Before answering this question, it is first necessary to clarify "spying". The gathering of information on other countries, including "friendly nations", is a normal part of any country's activities, in particular its diplomatic services. Diplomats and other state agents in other countries legitimately try to understand the country and find out what is happening in the country. They read the papers, meet and mingle with officials, business leaders, trade unions, politicians, religious leaders and civil society people. That is normal and of course legal.

But in this opinion I will be referring 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).¹⁰³

When is spying that would otherwise be illegal permitted?

As the words "without right" in the above clauses already indicate, these acts can sometimes be permitted – typically, if the owner of the computer system in question consents to the access or interception (e.g., a telephone subscriber can ask to have his or her phone lines monitored to catch a "nuisance caller"), or if there is a special legal authorisation, such as can be found, for German law enforcement agencies, in the provisions on "special investigative measures" in the various *Länder*-laws (within the limits laid down by the Constitutional Court).¹⁰⁴ However, such typical domestic exceptions do not normally apply to officials or agents of a foreign state.

¹⁰³ Cybercrime Convention, CETS 185, Arts. 2 and 3. Note that neither the UK nor the USA has exempted their national security activities from the provisions of the Convention in their reservations or declarations; see:

<http://www.conventions.coe.int/Treaty/Commun/ListeDeclarations.asp?NT=185&CM=1&DF=27/05/2014&CL=ENG&VL=1>

Indeed, both the USA and the UK would undoubtedly regard hacking and interception of communications by agents of other countries in their territories as serious crimes.

¹⁰⁴ See BVerfG, 1 BvR 370/07 vom 27.2.2008.

The in-principle prohibition on spying

Leaving those domestic exceptions therefore aside, we can state quite categorically that ***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, by the way, are not exempt from this. Diplomatic immunity protects them from prosecution by the host nation; it does not give them the right to do things that are illegal under the law of that nation. Expulsions or declarations that they are *persona non grata* of diplomats that have been found guilty of such acts underline that those acts are not regarded as acceptable in international law.¹⁰⁵

Exceptions

There are basically only two exceptions to the above in international law; these relate to spying in times of war, and to spying with the consent of the targeted state.

Spying in times of war

As Prof. Aust rightly observes in his statement to the Committee, in (international-) legal terms there is no such thing as a "War Against Terrorism",¹⁰⁶ and in fact the Obama administration now rarely uses this Bush-era phrase.

Even so, the US Government has framed – and continues to frame – its responses to the "9/11" atrocity in terms of armed conflict; and this has also influenced its position on its global surveillance operations. Specifically, the US Government relies on the "Authorization for Use of Military Force" Act (AUMF), passed by Congress on 14 September 2001, as the formal legal basis for both its domestic and foreign surveillance programmes, including specifically the NSA global Internet and e-communications surveillance programmes discussed in this opinion.¹⁰⁷

Thus, the then US Attorney-General, Alberto R Gonzales, wrote to Congress that NSA surveillance as revealed in 2006 should be seen in the context of **"the ongoing armed conflict with al Qaeda and its allies"**. He argued, with reference to Morris Greenspan's 1959 treatise on *The Modern Law of Land Warfare*, that:¹⁰⁸

¹⁰⁵ Under Question x, we will note that such acts also violate the sovereignty of the targeted state, and that that is indeed the case also if the acts are perpetrated from abroad.

¹⁰⁶ Aust, *o.c.* (footnote 8, above), para. 38.

¹⁰⁷ The US courts have also consistently held that in any case the US President has quite generally "inherent authority to conduct warrantless searches to obtain foreign intelligence information". See in particular *United States v. Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980), since confirmed in this regard in other cases. However, the present section addresses the specific arguments made by US authorities under the international legal rules pertaining to armed conflict.

¹⁰⁸ Communication from the US Attorney-General to Congress of 19 January 2006, emphasis in bold added. The text quoted is from Part II, section B (pp. 21-22), of the enclosure with that letter, Legal Authorities Supporting the Activities of the National Security Agency described by the President, available at: https://www.fas.org/irp/congress/2006_rpt/hrpt109-384.pdf

Electronic surveillance is a fundamental tool of war that must be included in any natural reading of the AUMF's authorization to use "all necessary and appropriate force."

As one author [Greenspan] has explained:

It is essential in warfare for a belligerent to be as fully informed as possible about the enemy— his strength, his weaknesses, measures taken by him and measures contemplated by him. This applies not only to military matters, but . . . anything which bears on and is material to his ability to wage the war in which he is engaged. *The laws of war recognize and sanction this aspect of warfare.*

It is not necessary to engage with this in any depth: one can basically accept that in situations in which an "enemy" can be lawfully shot at and killed (subject to the laws of armed conflict and international humanitarian law), listening in to the enemy's communications or hacking into his computer systems may well also be lawful (subject to those same constraints). This can apply, for instance, in relation to US operations in Afghanistan against the Taliban enemy (although with the hand-over of sovereignty to the Afghan Government that would still require the latter's consent).

The real point for Germany and other countries at peace with the USA and the UK, is that all this is unacceptable to stretch this to cover the US and UK surveillance operations in Europe, in countries with which neither the USA nor the UK are in armed conflict.

As Anne Peters, Director at the Max Planck Institute for Comparative Public Law and International Law put it, with almost British understatement:¹⁰⁹

If the United States seek to justify their surveillance activities [in Germany] by pointing to the "global war on terror" or, to use the term employed by former US legal adviser Harold Koh, "armed conflict with Al Qaeda, as well as the Taliban and associated forces", the US would first have to show that there is indeed, in Germany, an armed conflict of this type. This seems difficult to demonstrate because the geographic and substantive nexus to the battlefield is lacking.

One *caveat* remains. The Attorney-General submitted to Congress that the NSA operations at the time "*target[ed] only the international communications of persons reasonably believed to be linked to al Qaeda, and [were] designed [only] to protect the Nation from a devastating attack*", and that they were "*proportional because they are minimally invasive*". It is because of this, that he claimed that the measures were "*consistent with the law of armed conflict principle that the use of force be necessary and proportional*".¹¹⁰

In fact, as I already noted in relation to Question 1, **the US (and UK) surveillance programmes in Europe, and in Germany in particular, are clearly not linked to any "battlefield", or limited to persons "reasonably believed to be linked to al Qaeda", or even to (suspected) terrorists in any wider sense. They cover communications mostly totally unrelated to, and between individuals mostly totally unrelated to, any party to any armed**

¹⁰⁹ Anne Peters, *Surveillance Without Borders? The Unlawfulness of the NSA-Panopticon, Part I*, available at: <http://www.ejiltalk.org/surveillance-without-borders-the-unlawfulness-of-the-nsa-panopticon-part-i/>

¹¹⁰ *Idem*, p. 21, footnote 4.

conflict with the USA (or the UK). To that extent, they are clearly not justified in terms of the rules of armed conflict.

But the question could be raised whether the "right to spy" that belligerent states can probably claim in relation to each other when they are at war also extends to spying on "the enemy" in third countries not involved in the conflict.

Such spying of course happened, in WWII, and in the Cold War – in Lisbon, Zurich and Havana, as depicted in many films. But that does not make it legal. On the contrary, in those contexts, too, the states in which the spying took place clearly took the view that it was not allowed, and if they found out (and had no contrary reasons to pretend to not have noticed), they would still arrest and possibly intern, prosecute or expell those involved.

In my opinion – and as I understand her, also in the opinion of Anne Peters – 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.

In particular, the fact that such spying is sometimes – perhaps even often – tolerated (to some extent) does not change this: for this toleration to be turned into a (new) legal norm, not just such a practice of toleration is required, but also *opinio iuris*: the acceptance by the states concerned that this practice has become a legal norm. That is quite manifestly not the case.

Rather, if a state involved in an armed conflict with another state wants to carry out surveillance activities on the territory of a third state not involved in the conflict, the first state would, in law, have to obtain the consent of that third state. Such consent can, in particular, be given in the form of an international agreement of treaty. I shall now turn to that possibility.

Spying with the consent of the targeted state (and agreements not to spy)

Disclaimer: I do not claim to be an expert on international treaties on intelligence matters generally, or in relation to Germany, and I gladly defer to the greater expertise of my colleague, Prof. Aust. My comments below are just my general observations on issues raised in this regard.

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 as I will discuss, the situation is actually more complex.

First, I should note that inter-state agreements relating to spying – or "intelligence cooperation" as it usually euphemistically called – are historically often set out in secret

treaties, or in secret annexes or "understandings" to treaties.¹¹¹ The original UKUSA treaty of 1946 (later expanded into the "5EYES" arrangement) was kept secret until 2010.¹¹²

Germany was forced to submit to intrusive powers by the occupying countries after WWII, and these continued under a secret "Memorandum of Understanding" when the FRG regained its sovereignty.¹¹³ Whether the increasingly close practical arrangements between the secret agencies of Western states are clearly based on treaty provisions or developed more *ad hoc* within a lax international legal environment is unclear, but not that it has happened.¹¹⁴ Similarly, it is unclear to what extent even the governments – let alone the parliaments – of the European states involved were fully aware of what has been going on.¹¹⁵

¹¹¹ For details, see the following two important comparative studies:

- Ira Rubinstein, Greg Nojeim and Ronald Lee, Systematic Government Access to Personal Data: A Comparative Analysis, Center for Democracy & Technology, 2013, and on the 14 reports on 13 countries prepared for that study, nine of which, on eight countries, were published in *International Data Privacy Law*, Vol. 2, Issue 4 (November 2012), i.e.:
 - Jane Bailey, Systematic government access to private-sector data in Canada;
 - Zhizheng Wang, Systematic government access to private-sector data in China;
 - Ian Brown, Government access to private-sector data in the United Kingdom;
 - Motohiro Tsuchiya, Systematic government access to private-sector data in Japan;
 - Stephanie K Pell, Systematic government access to private-sector data in the United States;
 - Fred H Cate and Beth E Cate, The Supreme Court and information privacy (USA);
 - Dan Jerker B Svatešson, Systematic government access to private-sector data in Australia;
 - Omer Tene, Systematic government access to private-sector data in Israel;
 - Sunil Abraham and Elonnai Hickok, Government access to private-sector data in India;

All available from:

<http://idpl.oxfordjournals.org/content/2/4.toc>

- Didier Bigo, Sergio Carrera, Nicholas Hernanz, Julien Jeandesboz, Joanna Parkin, Francesco Ragazzi, Amandine Scherrer, National programmes for mass surveillance of personal data in eu member states and their compatibility with EU law, study for the European Parliament, PE 493.032, October 2013, with five country reports on the UK, Sweden, France, Germany, and the Netherlands

Available from:

<http://www.statewatch.org/news/2013/oct/ep-study-national-law-on-surveillance.pdf>

¹¹² For the original text, see:

http://www.nsa.gov/public_info/files/ukusa/agreement_outline_5mar46.pdf

For the background and extensive further documentation, see:

http://www.nsa.gov/public_info/declass/ukusa.shtml

But note that this is still not complete; some (many?) documents relating to the 5EYES arrangements, including in particular subsidiary agreements or guidelines, remain secret.

The principle that 5EYES countries (or rather, initially, the USA and the UK) would not spy on each other may be derived from the clarification in footnote 3 to the 5 March 1946 text, which says that "the U.S., the British Commonwealth of Nations, and the British Empire" shall not be regarded as "foreign countries"; and that their communications therefore do not constitute "foreign communications". Note the deletion of one word from the de-classified text: the word may well be "diplomatic". If so, that would suggest that diplomatic communications of countries outside the 5EYES were (and still are?) specifically targeted under the treaty.

¹¹³ See Joseph Foschepoth, Überwachtes Deutschland, 3rd ed., 2013, chapter 2. The (German) text of the "Memorandum of Understanding" between the Western allies and the young FRG (full title in English: "Agreements affecting the Intelligence Situation in Germany after the Termination of the Occupation", 11.5.1955, ref. NACP, RG 84) can be found on pp. 291-292. It was only declassified in the last few years.

¹¹⁴ See Didier Bigo *et al.* (footnote 111, above), p. 24.

¹¹⁵ *Idem*, pp. 24-25.

Apparently, the different national agencies are trying to influence their governments and legislators to retain a lax system of laws, or even to relax the laws further. Thus, it was revealed that the UK signals intelligence agency GCHQ has been working with its European counterparts to "update" the latter's national legal frameworks to give them similar freedom of action to the British agencies.¹¹⁶

The point to be made here is that this combination of secret or vague rules, wide executive discretion on their application, discrimination between nationals/residents and non-nationals/non-residents, and "light" oversight regimes not seriously independent from the government flies in the face of the minimum requirements laid down by the European Court of Human Rights. At its most basic (as explained in my answers to various issues raised by Question 1), in modern human rights law secret rules can never constitute "law", and they can therefore never provide a legal basis for any interference with any fundamental right.

To put it simply: 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.

Professor Aust writes in his statement to the Committee of Inquiry that:¹¹⁷

The [German] federal government is of the view that with the reunification of Germany on 3 October 1990 and the entering into force of the Two-plus-Four Treaty of 15 March 1991, all allied reserved powers [i.e., the powers provided to the Allied States at the end of WWII, as occupying powers] have ceased to have effect. ... [and that the German government believes that] "There are [at present] no international treaties with the USA under which US entities in Germany can obtain data in Germany or pass data on"

He does not mention the UK, but I assume the position is the same.

That said, however, I feel this is not clear enough. The German government may believe that the Allies no longer have any power to carry out surveillance but – given that they had extremely wide powers to do exactly that under the various post-WWII agreements – it would be crucial to check if they too accept that all those powers have now ceased to be.

What is more, for foreign bases on a state's territory – such as the continued bases of the USA and the UK in Germany – there is always a "Status Agreement". In addition, I would be surprised if there were no NATO agreements on intelligence gathering and –sharing.

¹¹⁶ Julian Borger, *GCHQ and European spy agencies worked together on mass surveillance*, The Guardian, 1 November 2013.

¹¹⁷ Aust, *Stellungnahme zur Sachverständigenanhörung am 5. Juni 2014* (footnote 8, above), para. 48.

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 the 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.

If we Europeans want to tackle the illegal and unacceptable surveillance by the USA and the UK (and others, in particular the other parties to the “5EYES”), we must be prepared to also examine the laws and practices of our own states, and to review and revise the treaties – and the secret agreements and “understandings” that we ourselves have adopted.

- O - o - O -

Douwe Korff (Prof.)

Cambridge/London, 3 June 2014