European Parliament LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens

European Parliament, Brussels, 14 October 2013

PRESENTATION BY DOUWE KORFF

Professor of International Law

London Metropolitan University, London (UK)

d.korff@londonmet.ac.uk

THE EU, COE & GENERAL INTERNATIONAL LEGAL FRAMEWORK

European Parliament LIBE Committee Inquiry
on Electronic Mass Surveillance of EU Citizens
European Parliament, Brussels, 14 October 2013

Presentation by Douwe Korff:
"The EU, COE and general international legal framework"

Overview

Five main topics:

(A)The ECHR requirements that must be met by European States undertaking surveillance of electronic communications, both in terms of substantive law and in terms of oversight and remedies; and the application of the ECHR requirements to surveillance by European States of electronic communications outside their territory. (slides (A)(i) – (A)(iii))

(B)Reflection of the ECHR requirements in EU law (to the extent that EU applies: see below, at E). (slides (B)(i) and (B)(ii))

(C)European data protection requirements. (slides (C)(i) – (C)(iv))

(D)The international-legal requirements that must be met by non-European States undertaking surveillance of electronic communications, both in terms of substantive law and in terms of oversight and remedies; and general international law on extra-territorial activities. (slides (D)(i) and (D)(ii)).

(E)And a crucial preliminary issue for the EU: the extent to which such activities by EU Member States are covered by the "national security" exemption in the Treaties and in the data protection directives. (slides (E)(**ADD**)

European Parliament LIBE Committee Inquiry
on Electronic Mass Surveillance of EU Citizens
European Parliament, Brussels, 14 October 2013

Presentation by Douwe Korff:
"The EU, COE and general international legal framework"

(A)(i) The **substantive ECHR requirements** that must be met by European States undertaking surveillance of electronic communications

ECtHR case-law on the scope of national security surveillance:

- The **offences and activities** in relation to which national security 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 such surveillance; and
- There must be strict limits on the **duration** of any ordered surveillance.
- (Cf. Weber and Saravia v. Germany, Liberty and Others v. UK. For details, see the Korff Note, sections I & II, with a summary on p. 6)

Note: ***indiscriminate mass surveillance of everyone's e-communications, without any individualised suspicion of criminal or subversive activities, and effectively without time-limit, is fundamentally contrary to these principles.***

Moreover, under the ECHR:

- European States also 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 any other, European or non-European State.

(Korff Note, section V)

European Parliament LIBE Committee Inquiry
on Electronic Mass Surveillance of EU Citizens
European Parliament, Brussels, 14 October 2013

Presentation by Douwe Korff:
"The EU, COE and general international legal framework"

(A)(ii) The **procedural ECHR requirements** that must be met by European States undertaking surveillance of electronic communications

ECtHR case-law on procedures, safeguards and remedies:

- States must impose **strict procedures** on when, how and by whom surveillance can be authorised;
- States must lay down **strict time-limits** on surveillance;
- There must be **strong and effective safeguards against abuse** of surveillance powers, including **strict purpose-limitation rules** and **rules against unwarranted disclosure** of data to other agencies (at home and abroad); and *ex post facto* **informing** of people who have been put under surveillance whenever possible;
- These procedures and rules should be based on **statute** and set out in a form which is **open to public scrutiny and knowledge**; and
- There must be **strong independent (preferably parliamentary) oversight**.

(Cf. again Weber and Saravia v. Germany, Liberty and Others v. UK. For details, see the Korff Note, sections I & II, with a summary on p. 6)

Note: ***UK law governing the activities of GCHQ appears to be seriously deficient in these terms.***

(See the detailed summary of the law and the arguments of the applicant in this regard in the recently filed ECHR application Big Brother Watch and Others v. the UK , Appl. Nr. 58170/13, submitted on 4 October 2013, in particular paras. 53-88 and 119-139)

European Parliament LIBE Committee Inquiry
on Electronic Mass Surveillance of EU Citizens
European Parliament, Brussels, 14 October 2013

Presentation by Douwe Korff:
"The EU, COE and general international legal framework"

(A)(iii) The application of the **ECHR requirements** to surveillance by European States of electronic communications **outside their territory**

ECtHR case-law:

- Under the ECHR, the principles set out in slides (A)(i) and (A)(ii) must be applied to "**everyone**" who is "**within the jurisdiction**" of the State carrying out the surveillance (Art. 1 ECHR)
- The concept of jurisdiction is increasingly applied in a **functional**, rather than purely territorial way because, as the Court has said:

"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. ... 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." (Issa and Others v. Turkey, paras. 68 and 71, emphasis added)

- In any case, if a State explicitly **legislates** to authorise and regulate surveillance by its agencies over "foreign" communications, it is thereby undoubtedly exercising its "jurisdiction" in that respect.

In sum: ***EU Member States must apply the ECHR principles to surveillance by them of both their own citizens and of foreigners, even if the latter are outside the State in question, certainly when this is within the EU or the Council of Europe area.***

(See section III of the Korff Note)

European Parliament LIBE Committee Inquiry
on Electronic Mass Surveillance of EU Citizens
European Parliament, Brussels, 14 October 2013

Presentation by Douwe Korff:
"The EU, COE and general international legal framework"

(B)(i) Reflection of the **ECHR requirements** in **EU law** (see also slides (D))

EU Charter of Fundamental Rights:

- Reflects ECHR guarantees, and indeed updates them and expands on them in certain ways, in particular in relation to "communications" and data protection (Arts. 7 and 8 CFR). **The Charter is now binding law for the EU.**

However, ***the CJEU cannot use the Charter to rule on the compatibility of any UK (or Polish) law or practice with the Charter: see Protocol No. 30 to the revised Treaties.***

EU is to become a party to the ECHR - but of course that will only be in respect of EU competences: see slides (E)(i)-(x) on excluded matters.

CJEU Case-law:

- The CJEU applies largely the same principles as the ECtHR on basic matters such as "law", "necessity", "proportionality", "fair balance" and "effective remedies".
- With one exception (noted in slide (E)(i)), there is as yet no specific case-law on data processing for "national security" purposes.
- However, in a different context (copyright infringement), the CJEU has stressed the **prohibition on "general monitoring"** and the overall need to strike a **"fair balance"** between competing interests: see the next slide.

European Parliament LIBE Committee Inquiry
on Electronic Mass Surveillance of EU Citizens
European Parliament, Brussels, 14 October 2013

Presentation by Douwe Korff:
"The EU, COE and general international legal framework"

(B)(ii) Reflection of the **ECHR requirements** in **EU law** (*continued*)

CJEU Judgment in Case C-70/10 of 24 November 2011 (SABAM):

- A filtering system that allows for the **active, preventive monitoring of all the data** that are transmitted, relating to all the customers of designated ISPs, without time limit:

- constitutes "**general monitoring**, something which is prohibited by Article 15(1) of Directive 2000/31";
- "may also **infringe the fundamental rights** of that ISP's customers, namely their right to protection of their personal data and their freedom to receive or impart information, which are rights safeguarded by Articles 8 and 11 of the Charter respectively"; and
- may "**not** be respecting the requirement that **a fair balance** be struck between [the legitimate aim to be pursued by the monitoring], on the one hand, and the freedom to conduct business, the right to protection of personal data and the freedom to receive or impart information, on the other."

Of course, ***the "fair balance" will be struck differently in relation to national security than in relation to intellectual property, and it cannot be deduced from the SABAM judgment that the CJEU would necessarily find "general monitoring" for national security purposes to be unlawful. However, the reference to the prohibition of such monitoring in Directive 2000/31 and to the rights of individuals protected by the Charter, suggest that the CJEU [if it had jurisdiction: see slides (E)] would apply to such monitoring tests similar to those applied by the Strasbourg Court, and perhaps even stricter ones, given the special emphasis on data protection in EU law and the Charter.***

European Parliament LIBE Committee Inquiry
on Electronic Mass Surveillance of EU Citizens
European Parliament, Brussels, 14 October 2013

Presentation by Douwe Korff:
"The EU, COE and general international legal framework"

(C)(i) European data protection law

General basic principles and the General Data Protection Regulation:

- In terms of general human rights law, data protection is based on the **right to privacy** (Art. 8 ECHR, Art. 17 ICCPR), and data protection is given increasing protection under that broader right in the case-law of the ECtHR and the HRCtee.
- However, data protection is also increasingly give express, enhanced protection as a ***sui generis* right**, especially in Europe, through CofE Convention No. 108 (and important subsidiary rules such as Recommendation R(7)15 on police data) and the EC Directives on data protection and other EU data protection rules.
- Crucially, data protection is now also explicitly recognised as a distinct *sui generis* right in the **Charter of Fundamental Rights (Art. 8)**.
- Data protection centres on a set of core principles including **fairness**, **legality** (cf. "law" in the ECHR), **transparency**, **purpose-limitation**, **data minimisation**, and **data subject rights**. It also provides for special **enforcement mechanisms**, and lays down important **restrictions on transborder data transfers**.
- EU data protection law will hopefully be **reinforced** through the General Data Protection Regulation, currently in the process of being adopted (rather than weakened, as the U.S. Government and industry want). **The GDPR should in particular reinstate the so-called "Anti-NSA clause". More importantly, it should stress that transfers of personal data from agencies subject to the Regulation to agencies (at home or abroad, in the EU or outside it) that are not subject to the Regulation must conform to the data disclosure requirements of the Regulation** (see slides (E)).

European Parliament LIBE Committee Inquiry
on Electronic Mass Surveillance of EU Citizens
European Parliament, Brussels, 14 October 2013

Presentation by Douwe Korff:
"The EU, COE and general international legal framework"

(C)(ii) European data protection law

e-Communications data retention, -interception and –"buffering":

- The **compulsory retention of e-communications data on everyone, without any individualised suspicion of criminal or subversive behaviour**, is ***highly dubious*** in terms of the basic data protection principles set out in slide (C)(i); national laws implementing the Data Retention Directive have been found to be **unconstitutional** in several countries, and the **compatibility of the DR Directive with the Charter** is under consideration by the CJEU. At the very least, such retention must be **strictly time-limited** and access to the data must be **very tightly controlled**, also and especially in terms of **purpose-limitation** (cf. the German Constitutional Court judgment on the German law implementing the DR Directive).

(See: E Kosta, The Way to Luxemburg: National Court Decisions on the Compatibility of the Data Retention Directive with the Rights to Privacy and Data Protection, (2013) 10:3*SCRIPTed* 339 http://script-ed.org/?p=1163)

- **Continuous interception and "buffering" of all traffic going through the fibre-optic cables carrying large portions of European (and global) Internet traffic (as is apparently done by NSA and GCHQ), for ill-defined purposes, without any individualised suspision or targetting, is impossible to square with the basic data protection principles set out in EC- and EU law, in the CJEU's SABAM judgment, and in the judgments of several MSs' constitutional courts (including Germany).** ***Put simply, any such activity that falls within EU competence (as to which, see slides (E)) is in violation of general principles of EU law and the Charter of Fundamental Rights.***

European Parliament LIBE Committee Inquiry
on Electronic Mass Surveillance of EU Citizens
European Parliament, Brussels, 14 October 2013

Presentation by Douwe Korff:
"The EU, COE and general international legal framework"

(C)(iii) European data protection law

"Key-word searches", data mining and profiling:

- The purpose of the "buffering" of e-communications data is to allow **searches** of the vast data "mine" (after an initial "Massive Volume Reduction" (MVR) technique, to weed out "spam" and peer-to-peer music downloads, etc.), by means of **keywords, email [IP] addresses, names or aliases, phone numbers, etc**.. This results in tens of thousands of "**selectors**", further augmented by **artificial intelligence** (the computers "learning" from the results, to generate new selectors or combinations of selectors). (See: Witness statement of Ian Brown in the ECHR case of Big Brother and Others v. the UK, at: https://www.privacynotprism.org.uk/assets/files/privacynotprism/IAN_BROWN-FINAL_WITNESS_STATEMENT.pdf

- Essentially, this means that individuals are selected for intrusive surveillance on the basis of what in the end is a largely automated, self-correcting and -improving ("dynamic") algorithm. **I.e., in effect, "targets" of PRISM and TEMPORA are selected on the basis of a mathematical "profile".**

- **Automated profiles are dangerous**, especially if used to identify rare phenomena (like finding a [potential] terrorist in a large population): they lead to large numbers of "**false positives**" or "**false negatives**" (or both); they can reinforce **discriminatory societal views and practices**; and because of the sophistication of the algorithms they become **effectively unchallengeable**. (See the section on "*Profiling"* in the EDRi booklet All you need to know (about data protection), at: [ADD]

- **In sum**: ***The use of data mining/"profiling" technologies in the reported PRISM and TEMPORA programmes pose an especially grave risk to the fundamental rights and freedoms of European (and non-European) citizens.***

European Parliament LIBE Committee Inquiry
on Electronic Mass Surveillance of EU Citizens
European Parliament, Brussels, 14 October 2013

Presentation by Douwe Korff:
"The EU, COE and general international legal framework"

(C)(iv) European data protection law

Examples of data protection restrictions on processing of personal data for national security purposes (from the Law on the Intelligence Service of Schleswig-Holstein , *LVerfSchG*):

- The application of the basic data protection principles to **national security agencies** is ***difficult*** since special exceptions are clearly required - ***but it is not impossible***, as these ***examples*** from the Schleswig-Holstein law show:
- **Relatively clear purpose-specification and -limitation**: countering [actual] threats to the free and democratic legal order of the State; to the existence or security of the State; or to the proper functioning of the organs of the State; spying by foreign States; use of violence or the preparation of violent acts aimed at endangering the external interests of the State; acts against international peace and co-operation. (§ 5 LVerfSchG) (Cf. Slide (E)(x))
- **Activities must be targetted**. E.g.: "In relation to [the fight against] political extremism, personal data may only be stored in a [structured] database if there are factual indications to suspect that the person concerned is involved in activities [threatening the free and democratic legal order of the State] and provided that this [the storing of the data] is necessary for the monitoring of these activities." (§ 7 Abs. 2, § 11 Abs. 1 Nr. 1 LVerfSchG).
- **Targetting must be based on individual, factual suspicions** ("*tatsächliche Anhaltspunkte*", § 7 Abs. 1 LVerfSchG)
- **Etcetera.**

The Schleswig-Holstein Law would clearly not allow any suspicionless mass surveillance of the kind inherent in the PRISM and TEMPORA programmes.

European Parliament LIBE Committee Inquiry
on Electronic Mass Surveillance of EU Citizens
European Parliament, Brussels, 14 October 2013

Presentation by Douwe Korff:
"The EU, COE and general international legal framework"

(D)(i) The substantive and procedural requirements that must be met by **non-European States** undertaking surveillance of electronic communications

ICCPR & other UN principles:

- The UN standards will be presented by Prof. Martin Scheinin. Here, it will suffice to note, first, that they are fully in accordance with the ECHR standards set out in the earlier slides, both as regards the substantive requirements and the procedural ones; and second, that the USA is a party to the ICCPR in particular.
- The views of the Human Rights Committee also show an increasing trend towards a functional, rather than a purely territorial approach to the question of "jurisdiction" (and thus to the applicability of the ICCPR to extra-territorial acts by States).

(Cf. *Attachment 2* to the EDRi/FREE submission on surveillance, at:
http://www.edri.org/files/submission_free_edri130801.pdf

In sum: ***In principle, the USA, as a party to the ICCPR, is bound to comply with essentially the same international human rights principles as apply in Europe, also in respect to surveillance over "NON-USPERSONS". The non-application of U.S. Constitutional and statutory guarantees to non-US citizens would appear to be in clear breach of modern international human rights standards generally and the ICCPR in particular.***

(Note that the fifth U.S. "Understanding" submitted to the UN when it ratified the ICCPR does not affect this, as far as matters are concerned over which the U.S. Federal authorities "exercise jurisdiction" - as they undoubtedly do over PRISM, etc.)

European Parliament LIBE Committee Inquiry
on Electronic Mass Surveillance of EU Citizens
European Parliament, Brussels, 14 October 2013

Presentation by Douwe Korff:
"The EU, COE and general international legal framework"

(D)(ii) General international law on extra-territorial surveillance of electronic communications

- It can be strongly argued that surveillance by one State over the communications of citizens and organisations - and indeed of public institutions - in another State constitutes the exercise of jurisdiction (more specifically: enforcement jurisdiction) in a way that contravenes the sovereignty of the other State. Cf. PCIJ, The Case of the S.S. "Lotus", judgment of 7 September 1927, which is still the leading case, at pp. 18-19.
- This is also the view of the vice-president of the EU's European Commission, Viviane Reding, who issued a statement on 25 July 2013, saying:

"The [EU's new General Data Protection Regulation] will also provide legal clarity on data transfers outside the EU: **when third country authorities want to access the data of EU citizens outside their territory, they have to use a legal framework that involves judicial control. Asking the companies directly is illegal. This is public international law.**"
See: http://techcrunch.com/2013/07/25/ireland-prism/ (emphasis added)

In sum: ***The surveillance of global communications by the USA, and of vast amounts of non-UK communications data by the UK (and similar actions by other States), is strongly arguably illegal under general public international law.***

- The proposal for an *Additional Protocol* to the COE Cybercrime Convention that would legalise such extraterritorial data gathering is dangerous and would undermine national sovereignty.

As the EDPS said to this Committee last week: ***We should do our utmost to ensure that this additional protocol will not be adopted.***

European Parliament LIBE Committee Inquiry
on Electronic Mass Surveillance of EU Citizens
European Parliament, Brussels, 14 October 2013

Presentation by Douwe Korff:
"The EU, COE and general international legal framework"

(E)(i) The "national security" exemption in the Treaties

"[N]ational security remains the sole responsibility of each Member State" (Art. 4(2) TEU)

- 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 MSs 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: see the next slides

European Parliament LIBE Committee Inquiry
on Electronic Mass Surveillance of EU Citizens
European Parliament, Brussels, 14 October 2013

Presentation by Douwe Korff:
"The EU, COE and general international legal framework"

(E)(ii) The "national security" exemption in the Treaties

- **Article 4(2) applies to MSs' 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 MSs to define this concept as they like.
- In that context, it is important to note that as part of the EU's **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, 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).
- In other words:

- **MSs** may have sole competence in relation to their own **national security**, **BUT**
- **the Union** has shared competence with the MSs 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.**

European Parliament LIBE Committee Inquiry
on Electronic Mass Surveillance of EU Citizens
European Parliament, Brussels, 14 October 2013

Presentation by Douwe Korff:
"The EU, COE and general international legal framework"

(E)(iii) The "national security" exemption in the Treaties

The implications of the overlapping issues and competences:

- "National security", each MS's "internal security", the Union's "internal security", and "international security" cannot be separated from each other, nor from JHA action, in particular in relation to "terrorism and related activities" (or international crime, or extremism or xenophobia). The duties and responsibilities that MSs have in relation to the latter matters impact on the autonomy of MSs in relation to the first:
- **It follows from general law on treaties (VCLT) that MSs 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. MSs' "autonomous" actions to protect their own national security must respect, and tie in with, their joint or cooperative or coordinated actions with other MSs in relation to the EU's own internal security, the joint security of all the MSs, and the joint fight against international crime and terrorism.**

The "national security" exemption and the Union's *acquis*:

- Just as MSs may also 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*:
- **"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.**"

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

European Parliament LIBE Committee Inquiry
on Electronic Mass Surveillance of EU Citizens
European Parliament, Brussels, 14 October 2013

Presentation by Douwe Korff:
"The EU, COE and general international legal framework"

(E)(iv) The "national security" exemption in the Treaties

- The EP has competence, and the CJEU has jurisdiction, in relation to several legal matters:

- First of all, since the term "national security" is part of the Treaties, the EP can discuss and if needs be make a determination (subject to the supervisory powers of the CJEU) as to the meaning to be given to the term - and thus as to the scope of the exemption in Art. 4(2) TEU. (Although of course, in this the EP and the Court should show due respect to the intention of the drafters of the Treaties, to the fundamental principles underpinning the Union - including both respect for fundamental rights and the Charter and respect for the principle of subsidiarity and for the sovereignty of the Member States in areas where they have not handed over or are sharing their sovereignty - and to the general rules on the interpretation of treaties, in accordance with the Vienna Convention on the Law of Treaties).

- Secondly, the compatibility of actions of MSs with the principles adduced in the previous slide can be assessed by the EP (subject to the supervision of the CJEU): they can assess whether the actions of a MS in the exempt area unduly affect actions lawfully taken by the Union (or by its MSs acting jointly under Union law) in relation to internal or international security, and/or in relation to the fight against terrorism.

- In other words, ***MSs do not have unfettered freedom to decide for themselves what is, and what is not, covered by the term "national security", or what thay can or cannot do in that area. MSs must limit any exemption they claim in that regard to what can reasonably be understood by the term "national security"; and their autonomous actions in the area of national security may not undermine Union security, or the internal security of other MSs, or joint actions under Union law, or the Union's fundamental freedoms. Parliament has the right to make its own assessments in this area, with the Court being the final judge on these matters.***

European Parliament LIBE Committee Inquiry
on Electronic Mass Surveillance of EU Citizens
European Parliament, Brussels, 14 October 2013

Presentation by Douwe Korff:
"The EU, COE and general international legal framework"

(E)(v) The "national security" exemption in the Treaties

What can legitimately be regarded as covered by the concept of "national security"

Johannesburg Principles:

Principle 2: Legitimate National Security Interest

(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.***

- (or, one could add, to gain an ***advantage in diplomatic negotiations, or an economic advantage for itself or the country's industries*** – DK)

- **Compare this to the excessively wide definitions given to "national security" and "foreign intelligence" in UK and US law, in the next slide.**

European Parliament LIBE Committee Inquiry
on Electronic Mass Surveillance of EU Citizens
European Parliament, Brussels, 14 October 2013

Presentation by Douwe Korff:
"The EU, COE and general international legal framework"

(E)(vi) The "national security" exemption in the Treaties

UK definition of "national security" and surveillance powers:

- There is no formal definition of 'national security' in any statute or judicial decision. However, it is acknowledged that the concept has been expanded and is now **very broad**, to include not just **military threats**, **espionage**, etc., but also **pandemics**, **cyberthreats**, matters relating to **energy securi**ty, etc. (Cf. Big Brother Watch and Others, paras. 105 – 112)
- GCHQ's surveillance powers go even beyond this: surveillance warrants such as those presumably used to legitimise TEMPORA can be issued when the Secretary of State "*believes*" they are necessary and proportionate:

(a) in the interests of **national security** [as widely defined: see above];
(b) for he purpose of preventing or detecting **serious crime**;
(c) for the purpose of safeguarding **the economic well-being of the United Kingdom** [provided the targets are outside "the British Islands"]; or
(d) [in relation to **mutual assistance in criminal matters**] (RIPA S. 5)

USA definitions of "national security" and "foreign intelligence":

- As Caspar Bowden in particular has shown in his excellent study for the EU, the definition of 'foreign intelligence information' in FISAA, as amended, now includes **any information with respect to a foreign-based political organization or foreign territory that "relates to the conduct of the foreign affairs of the United States"**. (See FISA §1801(a) & (e))

Consequently, it is lawful for the NSA under U.S. Law to conduct purely political or economic surveillance on foreigners' e-communications data and their data accessible in US Clouds.

European Parliament LIBE Committee Inquiry
on Electronic Mass Surveillance of EU Citizens
European Parliament, Brussels, 14 October 2013

Presentation by Douwe Korff:
"The EU, COE and general international legal framework"

(E)(vii) The "national security" exemption in the Treaties

General conclusion *re* EU competence concerning the UK's GCHQ's surveillance:

- **The EU institutions (including the EP and the Court) are legally allowed to assess, within their own competences:**

(i) **whether the UK's surveillance programmes, and its data exchanges/cooperation with the USA, are limited to the protection of "national security" in the sense in which that term must be understood in international and EU law;**

(ii) **even if they are so limited: whether they do not unduly affect actions lawfully taken by the Union (or by its MSs acting jointly under Union law) in relation to internal or international security, and/or in relation to the fight against terrorism; and/or whether they do not unduly affect the Union's fundamental freedoms;**

(iii) **to the extent that they are not limited to the protection of "national security" as understood in international and EU law: quite broadly, whether those programmes are compatible with Union law (since the Art. 4(2) TEU exemption does not apply);**

(iv) **specifically, the latter would include competence to assess whether the programmes meet the Union's privacy and data protection requirements; and**

(v) **In relation to the U.S.'s surveillance programmes, whether the USA is acting in contravention of the EU's data protection rules in any activity carried out in the EU; and whether the "Safe Harbor" and other EU-USA arrangements relating to personal data are actually safe and appropriate.**

European Parliament LIBE Committee Inquiry
on Electronic Mass Surveillance of EU Citizens
European Parliament, Brussels, 14 October 2013

Presentation by Douwe Korff:
"The EU, COE and general international legal framework"

Final remark:

To end this presentation, let me wholeheartedly endorse the view of the European Data Protection Supervisor, Peter Hustinx, expressed to the LIBE Committee at the last hearing, on 7 October 2013:

"We are facing an existential challenge to our fundamental rights and liberties. We must therefore be prepared to 'draw a line in the sand'".

The LIBE enquiry is a major opportunity to draw this line. I hope that my presentation will help it do that.