stiftung | neue verantwortung

Interparliamentary Committee Meeting
European Parliament – National Parliaments
Conference on the democratic oversight of intelligence services in the European Union
Brussels, 28-29 May 2015

Dr. Thorsten Wetzling
stiftung neue verantwortung
twetzling@stiftung-nv.de

How to deal with the collection of digital data?

1. Backdrop:

- The increased digitalisation of modern communication as well as significant advances in computing power enable our security services to collect and use an unprecedented amount of communication data in a cheaper, faster and more reliable manner.

- Most European intelligence agencies subject national and non-national communication data to different treatments. With regard to the former, regulations and safeguards tend to be in place on the authorisation to collect data, its subsequent use, control, oversight and *ex post* notifications. By contrast, the rules and regulations on the collection of non-national communications data are – at best – work in progress.

- It is difficult and costly to identify, tag and filter intercepted communication data according to whether it involves national citizens or not. This may be due to the "routing" and "packaging" of data but also to the popularity of foreign communication tools that may further obfuscate the foreign/national data distinction. Filtering and minimisation procedures may be used to approximate an ideal situation – unattainable in practice - where all data is readily identified as national, partly domestic –partly foreign or purely non-national and then subjected to different follow-up treatment regimes.

- The practical difficulties in separating domestic from non-domestic communication data, as well as the non-existent rules and regulations governing the collection of non-national communication data, is a cause of legal, technical, economic and diplomatic problems.

2. Propositions

Many EU member states are currently contemplating ways to further democratise and professionalise the governance of signals intelligence. Apart from the continued need to make the oversight and accountability mechanisms fit for the 21st century when it comes to domestic communication data collection, gaping holes exist in most European countries regarding the rules and regulations on the collection of the communications data of non-nationals. Hence, my focus on two basic propositions:

1) *The collection of non-national communication data should be subject to detailed legislation and democratic control.*

2) *Intelligence services of EU member states should be enjoined to handle communication data of EU citizens in the same way as "domestic" data. Provisions and safeguards that are currently in place to protect the data of national citizen from undue privacy infringements ought to be extended accordingly.*

About Proposition (1)

The recent report by the Venice Commission provides an excellent commentary on the standards of democratic governance to which signals intelligence agencies in Europe ought to adhere. It favourably discusses the Swedish and the German model for the authorisation, the collection and the subsequent handling of domestic data by national intelligence services.

Important reservations about the performance of the existing German system aside,[1] it remains clear that intense reform is still needed. The remit and resources of the review bodies need to be "supersized".

Why? The complex data protection scheme that exists in Germany on the authorisation and use of national data does not apply to the very core business of Germany's foreign intelligence service (Bundesnachrichtendienst – BND). The vast majority of cable and satellite communication data that the BND intercepts, stores, analyses and transfers has its origin and destination beyond Germany's territorial borders. The equipment and measures used for strategic foreign-to-foreign communication data surveillance, however, are operated by German personnel using German interception devices at German transit hubs (for cable).

[1] Just to name one criticism: The members of the German G-10 commission only receive information about communication interception measures on the very day when authorisation is being sought. This gives them insufficient time to consider the scope and the implications of the measures they are asked to sign off.

All state power is bound by the rules of the constitution. The practice and the secret legal interpretations by the government arguing that Art. 10 GG (right to privacy) can be territorially restricted so as to protect only German citizens was deemed unconstitutional by prominent legal scholars in the Bundestag's inquiry committee.

Currently, there are no safeguards or democratic control, let alone notification requirements in place. That means that the core function of the German intelligence service is administered in secret without judicial or parliamentary involvement as was first noted by Bertold Huber in his excellent article. This has meant that for years, the inner circle of power within the executive has solely determined both the strategic and legal decisions on the practice of foreign-foreign communication surveillance.

Recently the German government announced that it is working on changes to the current intelligence law but it keeps the matter very close to its chest. Unlike, for example, the Dutch government which consults with other governments as regards the future legal and institutional design of its communications interception governance system. Apparently, there will be an "internet consultation process" so as to allow external feedback, which will also include input from foreigners.

Benchmark: The executive should not solely interpret the legality of all intelligence practice. All public authorities/measures must be bound by the rules of the constitution.

- New legislation is needed in order to make sure that the full scope of agency conduct is placed under the remit of oversight bodies and subject to accountability
- Clearer depiction in surveillance laws of the role and involvement of the executive branch in the process of requesting and controlling strategic surveillance measures
- Institutional changes to existing oversight and judicial review structures (human and technical resources)
- More transparency on authorisation decisions and collection priorities

→ A complex and consequential question then arises: What needs to be considered when making amendments in keeping with propositions(1) and (2)?

Example Germany:

According to the G10 law, the Commission must do three basic things for each government request for surveillance authorization: 1) judge whether or not to authorise based on legal criteria and the facts of the case; 2) set limits on the operation (i.e. how much data, over how long, how often it must be re-authorised ,and whether they can share data); and 3) determine what, if any, notification of targets is necessary.

	Safeguards for German citizen as regards infringements of their right to privacy (Art. 10 GG)	Safeguards in place for the protection of non-national communication data in strategic surveillance
Authorisation procedure	G-10 law / G-10 commission	-/-
Data handling	G-10 law / G-10 commission	-/-
Notification requirements	G-10 law / G-10 commission	-/-

Implications / consequences of extending the remit of the G-10 Commission to all surveillance measures

(a) Ex ante authorisation of ALL surveillance

Core Reform Proposals:

- ✓ **All surveillance** must be authorised by the G-10 Commission and subjected to parliamentary control. This includes foreign-foreign communications.

- ✓ G10 decisions should be documented in a **written statement** -- like a court judgement-- explaining the reasoning and the facts of the case. Non-classified versions of these judgments should be published. The un-redacted versions should go to the parliamentary control panel.[2]

- ✓ **Special Advocate in G10** -- there should be an opposition counsel representing public privacy interests in the G-10 Commission. He/she would work alongside the government lawyers that bring surveillance requests to the G10 Commission. The special advocate should be able to appeal decisions that he/she finds objectionable to the parliamentary control panel.

Implications:

This would require a major expansion of the power and capability of the G10 Commission -- including more staff, lawyers, technicians, and a more resourceful secretariat to draft reports of their decisions (similar to a court ruling). The law would set the criteria under

[2] These are all parallels to recommendation 28 in the White House Review Group in the US. Some of the declassified FISA Court decisions are available here. An example of a published decision with some moderate redaction is available here:

which surveillance MAY be authorized, but the G10 members will judge whether the proposals of the BND are necessary and proportionate.

Bureaucratic time and effort will doubtlessly increase manifold. Having to provide an account of the rationale for all envisaged surveillance measure will certainly serve as an in-built *correctif to curb unnecessary and costly surveillance*: If no convincing argument for a surveillance measure can be fathomed, it probably does not deserve to be put into action.

The nationality of the targets will have considerable influence over whether surveillance measures are determined to be necessary and proportionate.

With the G10 Commission authorising ALL surveillance, it is plausible to assign the same standard to Germans, EU citizens, and everyone else in this important phase in the SIGINT cycle. In so doing, the reformed systems would meet the basic criteria of domestic, European and International law.

(b) Data handling and the safeguards for different strategic surveillance measures

(c) Notification requirements for some surveillance measures

As concerns (b) and (c), higher standards can be afforded to Europeans than the rest of the world. Here one may find guidance from other bodies of law and draw on the case law of the German constitutional court (BVerfGE 92 26/42) where the court considered acceptable reasons for a de facto diminution of basic right protection standards under certain conditions.

About proposition (2):

This, too, is an ambitious goal that will encounter many technical, administrative and legal hurdles. Progress will be incremental. A few progressive states may take the lead and in so doing will convince their partners that it is possible to safeguard the basic rights of fellow Europeans without disabling the important mission of our national intelligence services. National lawmakers are key in this regard. They are the ones that can extent the remit of existing laws.

Because of Article 4(2) TEU, the institutions of the European Union will not be able to compel individual member states into action. Still, they can facilitate the dialogue and promote best practices as a means to *nudge* member states to adopt better intelligence legislation and to perform better oversight.

Yet:

(a) What minimal standards should be in place throughout EU member states as regards the authorisation, the collection, the use, the storage and the transferal of communications data of EU member state citizens?

I very much hope that intelligence governance stakeholders in European capitals are attentively reading the recent report of the Council of Europe's Venice Commission. It provides an excellent commentary on the standards of democratic governance to which signals intelligence agencies in Europe ought to adhere. The report uses the case law of the European Court of Human Rights to give further gravitas to these important standards and provides a critical discussion of individual oversight arrangements of some countries.

Mid-to-Long-term policy advantages

> foreign policy credibility; paradoxically US Presidential Policy Directive 28 remains sole "high water mark", ordering the NSA and other US intelligence agencies to consider the privacy of non-nationals

> clear and consistent standard that is in keeping with constitutional and international human rights law and that will provide much-needed guidance to the intelligence services

> helps to build trust in IT-solutions made in Europe