Ad hoc information request: National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies

FRANET Guidelines

Deadline: 18 August 2014

INTRODUCTION

Background

Following Edward Snowden's disclosures, in June 2013, about surveillance programmes in the United States, the United Kingdom and EU Member States, the EU institutions promptly reacted. A number of political declarations, resolutions and reports have been issued since June 2013. In particular, the European Parliament decided to conduct an in-depth inquiry on the US National Security Agency (NSA) surveillance programme. The inquiry's results served as a background to the European Parliament *Resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights*, which called on the Fundamental Rights Agency to "undertake in-depth research on the protection of fundamental rights in the context of surveillance, and in particular on the current legal situation of EU citizens with regard to the judicial remedies available to them in relation to those practices".[1]

The scope of large-scale surveillance in the European Parliament Resolution covers to the "collect[ion], stor[age] and analys[is] of communication data, including content data, location data and metadata of all citizens around the world, on an unprecedented scale and in an indiscriminate and non-suspicion-based manner" as carried out by Member States' intelligence services.[2]

This FRA project focuses on safeguarding the following two fundamental rights in the context of large-scale communication surveillance conducted by intelligence services: the respect for private and family life (e.g. privacy) and the protection of personal data (Article 7 and Article 8 of the Charter of Fundamental Rights of the EU). The scope of the project is limited to the role played by State actors. It analyses the way national institutions that are in charge of upholding fundamental rights ensure democratic oversight over intelligence authorities and enable effective remedies against fundamental rights violations in line with Article 47 of the Charter of Fundamental Rights of the EU.

FRANET contractors are encouraged to visit the FRA project webpage (http://fra.europa.eu/en/project/2014/national-intelligence-authorities-and-surveillance-eu-fundamental-rights-safeguards-and?tab=links), which lists relevant documents on international and European standards and other important resources addressing the issues linked to this project.

Furthermore, before drafting the report, FRANET contractors should take into account the following documents, which provide relevant comparative law elements:

- European Commission for Democracy through Law (Venice Commission) (2007), *Report on the Democratic oversight of the Security Services adopted by the Venice Commission at its 71st Plenary Session (Venice, 1-2 June 2007)*, Study no. 388 / 2006, CDL-AD(2007)016-e, Strasbourg, 11 June 2007;[3]

[1] www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0230
[2] *Ibid*. paragraph 1.
[3] www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2007)016-e

- European Commission for Democracy through Law (Venice Commission) (1998), *Internal security services in Europe: Secretariat memorandum based on the opinions of Mr John Lundum, Mr Joseph Said Pullicino & Mr Antti Suviranta*, Study no. 039 / 97, CDL(1998)011-e, Strasbourg, 19 February 1998;[4]
- European Commission for Democracy through Law (Venice Commission) (1998), *Internal Security Services in Europe*, Study no. 039 / 97, CDL(1998)011-e, Strasbourg, 19 February 1998;[5]
- European Parliament, DG for Internal Policies (2013), *National Programmes for mass surveillance of personal data in EU Member States and their compatibility with EU Law*, PE 493.032, Brussels, October 2013; [6]
- Parliamentary Assembly of the Council of Europe (2014), "*Massive Eavesdropping" and "Additional Protocol to the ECHR on Protection of whistleblowers",* AS/Jur (2014) 02, Strasbourg, 23 January 2014.[7]

Objective

The objective of this deliverable is to collect information on fundamental rights compliance in the area of privacy and data protection as well as information on available remedies in the Member States in the context of large-scale surveillance by State actors.

The data provided by the contractors will help to map fundamental rights safeguards and remedial procedures in a comparable manner in the 28 Member States.

Delivery deadline

The deadline for this deliverable is **18 August 2014**.

Reference period

Analysis and information provided should **reflect the most recent situation** and include developments over the past three and half years (2011-2014) that would contribute to a better understanding of the current situation.

General description of the service

FRANET contractors are requested to present in a summary, and by filling the tables included in annexes 1 to 5, information on policies, legal frameworks and case law linked to surveillance practices by national authorities and their compliance with respect for fundamental rights, and in particular the right of privacy and the protection of personal data. Completion of annex 6 will provide key bibliographical references.

---

[4] www.venice.coe.int/webforms/documents/?pdf=CDL(1998)011-e
[5] www.venice.coe.int/webforms/documents/?pdf=CDL-INF(1998)006-e
[6] www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET(2013)493032_EN.pdf
[7] website-pace.net/documents/19838/419003/AS-JUR-2014-02-EN.pdf/2c9ba3c3-d456-4471-a39d-087987ef1208

Style, language and size

The FRA Style Guide must be strictly followed. **The size of the deliverable should be one to three A4 page summary** (excluding annexes).

Sources of information should be fully referenced. If the information is available online, please provide the internet addresses (with date accessed); where data is available in both English and the national languages Please provide the address of the English version.

When completing the annexes, please indicate for each source:

- the **title** in the original language,
- the **author**,
- the **main findings** focussing on those that are relevant to one or more specific topic points,
- the **locations** referred to (where relevant),
- the **national authorities** mentioned,
- and the web **link** or publication details.

If the same source can be listed under more than one of the five thematic areas, please repeat the link in each area.

CONTENTS

Summary

The summary shall provide information on the following three issues:

1. Description of the surveillance legal framework in your country, including different laws governing surveillance by State actors and on-going legislative reforms. The summary should include the following aspects:

    a. types of security services and bodies involved,
    b. the extent of their powers incase of surveillance of individuals and also vis-a-vis private sector (right to acccess to data held by telecom or internet providers, right to refuse access),
    c. control/oversight mechanisms,
    d. geographical scope of surveillance
    e. conditions under which intelligence services can conduct surveillance and for which purpose(s) (such as national security, investigation or prevention of crimes, etc.)
    f. different stages of surveillance procedure (collection, analysis, storing, destruction).

2. Safeguards put in place by the legal framework (described under 1 above) to ensure respect for privacy and data protection during surveillance measures (judicial warrant, right to be informed, right to rectification/deletion/blockage, right to challenge the surveillance, etc.)

3. Judicial or non-judicial remedies available to an individual subject to surveillance at different stages of surveillance procedures.

Annex 1 – Legal Framework relating to mass surveillance

A- Details on legal basis providing for mass surveillance

Name and type of the mass surveillance-related law	**A definition of the categories of individuals liable to be subjected to such surveillance**	**Nature of circumstances which may give rise to surveillance**	**List purposes for which surveillance can be carried out**	**Previous approval / need for a warrant**	**List key steps to be followed in the course of surveillance**	**Time limits, geographical scope and other limits of mass surveillance as provided for by the law**	**Is the law allowing for mass surveillance in another country (EU MS or third countries)?**
Full name in English and national languages indicating its type – Act of the parliament, Government order, etc.			*National security, economic well-being, etc.…*	*Indicate whether any prior/ex post judicial warrant or a similar permission is needed to undertake surveillance and whether such approval/warrant needs to be regularly reviewed*	*See for example the principles developed by the European Court of Human Rights in the case of Weber and Saravia v. Germany*, (dec.) n°54934/00, 29 June 2006, para. 95 *Steps could include collecting data, analysing data, storing data, destroying data, etc.*	*Clearly state if there are any existing limitations in terms of nationality, national borders, time limits, the amount of data flow caught etc.*	*Please, provide details*

B- Details on the law providing privacy and data protection safeguards against mass surveillance

Please, list law(s) providing for the protection of privacy and data protection against unlawful surveillance	**List specific privacy and data protection safeguards put in place by this law(s)**	**Indicate whether rules on protection of privacy and data protection apply:** **only to nationals or also to EU citizens and/or third country nationals**	**Indicate whether rules on protection of privacy and data protection apply:** **only inside the country, or also outside (including differentiation if EU or outside EU)**
Include a reference to specific provision and describe their content	*e.g. right to be informed, right to rectification/deletion/blockage, right to challenge, etc.*	*Please, provide details*	*Please, provide details*

Annex 2 – Oversight bodies and mechanisms

Name of the body/mechanism	**Type of the body/mechanism**	**Legal basis**	**Type of oversight**	**Staff**	**Powers**
in English as well as in national language	*e.g. parliamentary, executive/government, judicial, etc.*	*name of the relevant law, incl. specific provision*	*ex ante / ex post / both/ during the surveillance/etc. as well as whether such oversight is ongoining/regularly repeated*	*including the method of appointment of the head of such body **AND** indicate a total number of staff (total number of supporting staff as well as a total number of governing/managing staff) of such body*	*e.g. issuing legally binding or non-binding decisions, recommendations, reporting obligation to the parliament, etc.*

Annex 3 – Remedies[8]

[Name of the law as per Annex 1]				
Stages of surveillance process	**Is the subject informed?**	**Does the subject have a right of access to the data collected on him/her?**	**List remedies available to an individual concerned**	**Legal basis for using the available remedies**
	Yes/No	*Yes/No, please provide details if needed*	*Please list the type of remedial action that can be taken: e.g.: claims lodged with court(s), claims lodged with the oversight body, request to the surveillance authority, etc.* ***AND*** *please specify also the name (e.g. Supreme Court) and type of the body (e.g. judicial, executive, parliamentary) providing such remedies.*	*Violation of data protection, private life, specific legislation, etc.*
Collection*				
Analysis*				
Storing*				
Destruction*				
After the whole surveillance process has ended				

[8] In case of different remedial procedures please replicate the table for each legal regime.

* For the definitions of these terms, please refer to the FRA/CoE (2014), *Handbook on European data protection law*, Luxembourg, 2014, pp. 46-47, available at: http://fra.europa.eu/en/news/2014/council-europe-and-eu-fundamental-rights-agency-launch-handbook-european-data-protection

Annex 4 – Surveillance-related case law at national level

Please provide a maximun of three of the most important national cases relating to surveillance. Use the table template below and put each case in a separate table.

Case title	
Decision date	
Reference details (type and title of court/body; in original language and English [official translation, if available])	
Key facts of the case (max. 500 chars)	
Main reasoning/argumentation (max. 500 chars)	
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	

Annex 5 – Key stakeholders at national level

Please list all the key stakeholders in your country working in the area of surveillance and divide them according to their type (i.e. public authorities, civil society organisations, academia, government, courts, parliament, other). Please provide name, website and contact details.

Name of stakeholder (in English as well as your national language)	**Type of stakeholder** *(i.e. public authorities, civil society organisations, academia, government, courts, parliament, other)*	**Contact details**	**Website**

Annex 6 – Indicative bibliography

Please list relevant reports, articles, studies, speeches and statements divided by the following type of **sources** ***(in accordance with FRA style guide)****:*

1. Government/ministries/public authorities in charge of surveillance

2. National human rights institutions, ombudsperson institutions, national data protection authorities and other national non-judicial bodies/authorities monitoring or supervising implementation of human rights with a particular interest in surveillance

3. Non-governmental organisations (NGOs)

4. Academic and research institutes, think tanks, investigative media report.