National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies

ESTONIA

Version of 1 October 2014

Institute of Baltic Studies
Kari Käsper

SUMMARY

Description of the surveillance framework

[1]. The specific term mass surveillance does not exist in Estonian law, and there is no specific authorisation in Estonian law for mass surveillance measures undertaken by state security or surveillance authorities.

[2]. The only measure, according to which information about the whole population or large groups of the population is collected and retained, is so-called metadata retention by telecom and internet companies according to Article 111^1 of the Electronic Communications Act (*Elektroonilise side seadus* , hereinafter ECA), which incorporated into Estonian law Directive 2006/24/EC (Data Retention Directive). The requirements set for the telecom and internet companies by ECA are in some ways stricter than required by the now invalid Data Retention Directive, establishing that the data must be retained in an EU Member State and certain data only in the territory of Estonia. The data collected according to the ECA by internet and telecom service providers must be retained by them for a period of one year. These telecom and internet companies must then provide access to the retained metadata not only to the security authorities, but also to a wide range of governmental law enforcement and investigative authorities. ECA art 111^1(11) lists the authorities who are entitled to request the stored metadata:

1) an investigative body, a surveillance agency, the Prosecutor's Office or a court pursuant to the Code of Criminal Procedure;
2) a security authority;
3) the Data Protection Inspectorate, the Financial Supervision Authority, the Environmental Inspectorate, the Police and Border Guard Board, the Security Police Board and the Tax and Customs Board pursuant to the Code of Misdemeanour Procedure;
4) the Financial Supervision Authority pursuant to the Securities Market Act;
5) a court pursuant to the Code of Civil Procedure;
6) a surveillance agency in the cases provided for in the Organisation of the Defence Forces Act, the Taxation Act, the Police and Border Guard Act, the Weapons Act, the Strategic Goods Act, the Customs Act, the Witness Protection Act, the Security Act, the Imprisonment Act and the Aliens Act.

[3]. However, this access is provided only on a case-by-case basis according to a specific proceeding and based on specific authorisations that relate to that specific proceeding. According to ECA art 114^1, telecom and internet companies must provide the civil court on its written request on a case to case basis with data collected in the framework of the ECA. According to the Code of Criminal Procedure (hereinafter CCP), data collected within the scope of ECA art 111^1 may be requested by the surveillance agencies (The Police and Border Guard Board, the Security Police Board, the Tax and Customs Board, the Military Police and the Prisons Department of the Ministry of Justice and prisons, see CCP § 126^2 sec 1) to collect information particularly in the context of the prosecution of a criminal offence as well as for the purpose of the detection and prevention of a possible future criminal offence (CCP § 126^2 sec 1 p 1 and 4). Data collected on grounds of ECA art 111^1 may also be requested for prosecution of certain misdemeanours. Other regulations concerning the public authorities´ rights to request respective data can be found i.a. in the Securities Market Act, the Imprisonment Act and the Aliens Act (see above, ECA art 111^1 (11) p 6).

[4]. The other potential possibilities for surveillance outside of specific proceedings are regulated by the Security Authorities Act (*julgeolekuasutuste seadus*, hereinafter SAA). The Security Authorities Act (*Julgeolekuasutuste seadus* , hereinafter SAA) provides specific authorisation for the two security authorities, Estonian Internal Security Service (*Kaitsepolitseiamet* , EISS) and Information Board (*Teabeamet* , IB), to overcome a person's right to the confidentiality of messages sent or received by him or her by post, telegraph, or telephone. It also restricts a person's right to the inviolability of home, family or private life in specific instances. However, the scope of these activities does not include the authorization for mass surveillance activities.[1]

[5]. The main function of EISS is to secure national security using inter alia surveillance and data collection methods.The IB collects intelligence concerning foreign countries. The functions and powers of these agencies are regulated in the SAA, according to which "the objective of the activity of security authorities is to ensure national security by the continuance of constitutional order through the application of non-military means of prevention, and to collect and process information necessary for formulating security policy and for national defence". SAA allows security authorities to "collect and process information, including personal data, insofar as this is necessary for performing its functions." However, both the EISS and IB have explicitly denied that they have legal authority to conduct mass surveillance.[2] According to clause 27 (1) of the SAA (1) in the case of a need to restrict a person's right to the confidentiality of messages or to the inviolability of home, and family or private life in the manner specified in clause 26 (3) 5) of this Act, the head of a security authority shall submit to the chairman of an administrative court or an administrative judge appointed by the chairman a reasoned written application for the corresponding permission. The application shall set out the manner of restriction of the corresponding right. The special parliamentary oversight committee of security authorities Security Authorities Surveillance Committee has also denied having any knowledge of mass surveillance measures by security authorities.[3]

[6]. Parliamentary control over the activities of the security authorities is exercised by the Security Authorities Surveillance Committee of the Riigikogu (*Riigikogu Julgeolekuasutuste järelevalve erikomisjon,* SCOSA). SAA states that the principal function of SCOSA is the supervision of authorities of executive power in matters relating to the activities of the security authorities and surveillance agencies, including questions on fundamental rights guarantees and efficiency and supervision of the security authorities' and surveillance agencies' work. There are eight members of the SCOSA who are members of parliament while the other two are parliamentary officials. The disclosure of large-scale surveillance programs such as PRISM and TEMPORA however did not result in investigations being initiated or relevant enquiries being made by SCOSA.[4] The effectiveness of the oversight of SCOSA has been widely criticized, most remarkably by its previous chairman of the committee in an interview given to the Estonian Internet Society in which he claimed that the committee is technically and legally ill-equipped to provide meaningful oversight due to lack of resources and expertise.[5] The former chairman also stated that Members

---

[1] Estonia, Information Board, Reply to request for clarification, 8 August 2014.
[2] Estonia, Estonian Internal Security Service, Reply to request for clarification, 8 August 2014 and Estonia, Information Board, Reply to request for clarification, 8 August 2014.
[3] Estonia, Security Authorities Surveillance Committee, Reply to request for clarification, 8 August 2014.
[4] Kukk, U. and Väljataga, A. (2014), 'Right to respect for family and private life', *Human Rights in Estonia 2013*, available at: http://humanrights.ee/en/annual-human-rights-report/human-rights-in-estonia-2013/right-to-respect-for-family-and-private-life/
[5] *Eesti Interneti Kogukond* (Estonian Internet Society), *'Eksklusiivne usutlus "KAPO-komisjoni" endise aseesimehega: komisjonil puudub ülevaade luure ja vastuluure tegevusest'* ('Exclusive interview with the former vice-chairman of KAPO-committee: committee has no overview of intelligence and counter-intelligence actitivities'), 25 June 2013, Available at: http://kogukond.org/2013/06/eksklusiivne-usutlus-kapo-komisjoni-endise-aseesimehega-komisjonil-puudub-ulevaade-luure-ja-vastuluure-tegevusest/

of Parliament lack the security clearances needed to be able to access relevant information and they are generally uninterested in conducting effective oversight. Furthermore, the committee only has two persons in staff compared to many more in the security authorities and thus they capacities are much more asymmetric compared to other countries.

[7]. Information regarding the cooperation of Estonian security authorities with foreign authorities is a state secret and thus there is no information regarding the usage of information provided by other states or to other states.[6]

[8]. In terms of safeguards, there is only one specific safeguard in place. The SAA requires that the person whose privacy rights were restricted should be notified of this "immediately, if this does not threaten the purpose of the restriction, or after the end of such threat". Similar requirement of notification is provided also by other legal acts, such as Code of Criminal Procedure and Police and Border Guard Act.

[9]. In the ECA, there are safeguards related to the data that the telecom and internet companies have to retain. The ECA requires that retained data is held securely, respecting the rules regarding data protection, that access to the data is limited and that no content data is retained. There is a notification requirement to the Technical Regulatory Authority (*Tehnilise Järelevalve Amet*), which gathers the annual data and sends it to the European Commission. An additional safeguard comes from Electronic Communications Act § 1111 (5), according to which data has to be saved in the EU (and in special cases in the territory of Estonia).

[10]. When analysing the data on requests made for retained data, it is remarkable that a significant percentage of requests by the different authorities are not granted. For example, in 2013 47.6% of the 4068 requests for regular telephony service were denied by the telecom companies.[7] The same statistics regarding internet services show a higher rate of approval for requests (only 10.4% of 2202 requests were refused).

[11]. In terms of remedies and according to a reply received from the Ministry of Justice, each person has tje right to inquire from the surveillance authorities the processing of his or her personal data. Additionally, the person has the right to turn to an administrative court to check the legality of such activity as well as possibility of turning to the Chancellor of Justice as general institution of petition. The Ministry also pointed out that a person could turn to the relevant authorities in case he or she is of the opinion that a criminal act against him or her has been committed.[8] These are, however, general remedies that are unlikely to be used in practice.

[12]. In terms of remedies related to data retained according to the ECA by telecom and internet companies, the availability of solutions is hampered by the lack of a notification requirement.

As of 17 August 2014, the Estonian regulations on the collection, retention, processing and distribution of so-called metadata are in force. However, Minister of Justice Andres Anvelt has publicly stated[9] that a review of the provisions of ECA has to be made in order to ensure the conformity of the Estonian legal order with the recent CJEU decision in joined cases Digital

---

[6] Estonia, Estonian Internal Security Service, Reply to request for clarification, 8 August 2014 and Estonia, Information Board, Reply to request for clarification, 8 August 2014.
[7] Estonia, Technical Regulatory Authority, Reply to request for information, 18 August 2014.
[8] Estonia, Ministry of Justice, Reply to request for clarification, 27 August 2014.
[9] *ERR uudised* (2014), '*Anvelt: sideandmete kasutamine ei tohi tulla isikute põhiõiguste arvelt*' (Anvelt: use of communication data cannot lessen fundamental rights protection'), 7 June 2014, available at: http://uudised.err.ee/v/eesti/ff1a9de1-2865-4b0d-8163-0c9d8f1a2e35

Rights Ireland and Seitlinger and Others. The Chancellor of Justice has received one complaint by a private individual in April 2014, which asked for review of the constitutionality of Art 111^1 of the ECA in light of the invalidity of the Data Retention Directive. The Chancellor of Justice has started a proceeding based on the complaint and sent letters of inquiry to the Ministries of Justice, the Interior and Economic Affairs and Communications asking their opinion on the constitutionality of this specific provision of ECA.[10] In a preliminary analysis, the Chancellor of Justice has concluded that "it cannot be excluded in light of the arguments put forward by the European Court of Justice that regulation of ECA that was adopted for the implementation of the directive is at least partially incompatible with the Constitution,"[11] specifically referring to the fact that information is collected and retained about all users of the communications services provided by the telecom and internet companies.

[10] Estonia, Õiguskantsler (Chancellor of Justice), 'Teabe nõudmine, Elektoonilise side seaduse § 111^{1}' (Request for information, Electronic Communications Act § 111^1), 15 July 2014, Available at http://adr.rik.ee/okk/dokument/3764037

[11] Estonia, Õiguskantsler (Chancellor of Justice), 'Teabe nõudmine, Elektoonilise side seaduse § 111^{1}' (Request for information, Electronic Communications Act § 111^1), 15 July 2014, Available at http://adr.rik.ee/okk/dokument/3764037

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)?
Electronic Communications Act *Elektroonilise side seadus* Act of Parliament	All users of services of telecom and internet companies.	Using communication services provided by telecom and internet companies, including geographic location.	A wide range of purposes ranging from national security to investigation of illegal fishing or tax fraud.[12]	An individualised authorisation is required.	Collecting and retaining data is done by the telecom and internet companies, this data can be accessed based on individualised electronic or written requests (which can	Data is retained for one year or for two years in case a specific request has been made (and its log).	No.

1)The data is provided to 1) an investigative body, a surveillance agency, the Prosecutor's Office or a court pursuant to the Code of Criminal Procedure;
2) a security authority;
3) the Data Protection Inspectorate, the Financial Supervision Authority, the Environmental Inspectorate, the Police and Border Guard Board, the Security Police Board and the Tax and Customs Board pursuant to the Code of Misdemeanour Procedure;
4) the Financial Supervision Authority pursuant to the Securities Market Act;
5) a court pursuant to the Code of Civil Procedure;
6) a surveillance agency in the cases provided for in the Organisation of the Defence Forces Act, the Taxation Act, the Police and Border Guard Act, the Weapons Act, the Strategic Goods Act, the Customs Act, the Witness Protection Act, the Security Act, the Imprisonment Act and the Aliens Act.

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)?
					also be oral) or by providing a continuous connection to the network of the provider.		
Security Authorities Act (*Julgeolekuasutus te seadus*)[13] Act of Parliament	No limit on categories of individuals.	No limit on circumstances.	1. prevention and combating of changing the constitutional order or territorial integrity of the state by force 2. prevention and combating of intelligence	Need to apply for court permission for restriction a person's right to the confidentiality of messages or for covert entry in the person's dwelling, other building or property in the person's possession, database, place of	Depending on the surveillance, court permission (by written application of the head of security authority) or an order by the head of security authority (or an official authorised by him or her) has to be applied for. Notification of a person whose fundamental rights	An order shall be valid for the term indicated therein but for no longer than two months. Court permission may be granted for a period of up to two months or extended for the same period at a time. An order by the head of security authority shall be valid for the term	The law does not specifically regulate or allow mass surveillance.

[13] Mass surveillance is not legally possible under the SAA, according to the authorities. The law itself is less clear.

			activities directed against the state 3. prevention and combating of terrorism and terrorist financing and support; 4. prevention and combating of corruption endangering national security; 5. combating of those criminal offences the pre-trial investigation of which is within the competence of the Estonian Internal Security Service; 6. pre-trial investigation of criminal offences in the cases	employment or vehicle for the purposes of covert collection or recording of information or installation of technical aids necessary for such purposes. Restriction of a person's right to the inviolability of home, and family or private life shall be decided, by an order, by the head of a security authority or an official authorised by him or her.	are restricted immediately of the measures used and the circumstances relating to the restriction of fundamental rights if this does not endanger the aim of the restriction, or after such danger ceases to exist.	indicated therein but for no longer than two months.	

			prescribed by law; 7. collection and processing of information concerning foreign states, or foreign factors or activities, which is necessary for the state in formulating the foreign, economic and national defence policy and for national defence; 8. conduct of counter-intelligence for the protection of the foreign missions of the state and such structural units or staff of the Defence Forces which are outside				

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)?
			the territory of the state; 9. conduct of counter-intelligence for the protection of the staff of the Information Board, persons recruited for co-operation, and property in the possession of the Information Board; 10. organisation and verification of INFOSEC				

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)**
Põhiseadus (Constitution)	No specific safeguards, a general provision of protection of private and family life (including data protection).	Estonian nationals and all persons who are present in Estonia	Only inside the country.
Isikuandmete kaitse seadus (Personal Data Protection Act)	Right to be informed, right to rectification/deletion/blockage, right to challenge, right of access, etc. The activities of the surveillance authorities are not expressly excluded from the scope of the Act, but activities that relate to state secrets are and this is interpreted by the Data Protection Inspectorate as not having an oversight capacity over security authorities.	Estonian nationals and all persons who are present in Estonia	Only inside the country.
Julgeolekuasutuste seadus (Security Authorities Act)	Right to be informed.	No limitations specified, thus available to all.	No limitations specified, thus available for all.

Annex 2 – Oversight bodies and mechanisms

Name of the body/mechanism	Type of the body/mechanism	Legal basis	Type of oversight	Staff	Powers
Special Committee on Oversight of Security Authorities of *Riigikogu* *(Riigikogu Julgeolekuasutuste järelvalve erikomisjon)*	Parliamentary	*Riigikogu kodu- ja töökorra seadus*	Supervision over authorities of executive power in matters relating to the activities of the security authorities and surveillance agencies, including guarantee of fundamental rights and efficiency of the work of the security authorities and surveillance agencies, and also in matters relating to supervision exercised over the security authorities and surveillance agencies. Deliberates the draft budget of a security authority	Currently 8 Members of Parliament (two from each fraction), supported by 2 officials. The number of MPs is not set in a law and thus can be changed.[14]	Hears a report by the Prime Minister and other relevant ministers on the activities of the security authorities at least every six months, reports to the full parliament at least once a year, and has the right to summon persons and require documents for examination. In case of offenses, can refer the matter to the investigative body or Chancellor of Justice.

[14] See more: http://www.riigikogu.ee/index.php?op=ems&page=view_pohiandmed&pid=90617&u=20070514094002

			concurrently with the deliberation of the draft state budget In case of offenses, can refer the matter to the investigative body or Chancellor of Justice.		
Ministry of Defence, Ministry of Internal Affairs, Ministry of Justice, Ministry of Economic Affairs and Communications	executive/government	*Vabariigi Valitsuse seadus* (Law on the Government of the Republic)	Ongoing, repeated, both	Each Ministry has internal oversight departments that can conduct oversight. The staff of these vary between ministries. Ad hoc oversight can also be organised.	Can conduct administrative supervision over an authority under its competence. For example, the Ministry of Internal Affairs conducts administrative supervision over the Internal Security Service and Ministry of Defence over the Information Board.
Chancellor of Justice (*Õiguskantsler*)	Ombudsman / constitutional rights oversight body	Õiguskantsleri seadus (*Chancellor of Justice Act*)	*Ex post* in case of complaints which can be submitted by anyone, can also be own initiative	Head appointed by *Riigikogu* according to recommendation by the President; there were 38 officials, 11 support employees in 2013.	Can make recommendations to amend laws, if recommendation is not followed in can refer the matter to the Supreme Court for it to declare the law or legal act invalid, in case of non-legal act, it can issue a non-binding opinion and refer the matter to executive oversight bodies,

					reporting obligation to the parliament
Tehnilise Järelevalve Amet (*Technical Regulatory Authority*)	Government	*Elektroonilise side seadus* (Electronic Communications Act)	Ongoing, yearly	Head appointed by Minister of Economic Affairs and Communication; total of 83 public officials.	Collecting statistics for requests made under ECA. No other specific powers for oversight of surveillance.
Courts	Court	Constitution, Personal Data Protection Act	*Ex post*	Judges appointed by President	Make binding judgments; gives grants to access, i.e. conduct *ex ante* control.

Annex 3 – Remedies[15]

Electronic Communications Act				
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*	No, but it is public knowledge that data is retained as it is required by law.	Yes, under the Data Protection Act.	Claim to administrative court or criminal court depending on the proceeding, complaint to the data protection inspectorate, complaint to the Chancellor of Justice.	Violation of Constitution.
Analysis*	No.	Yes, but in practice it is difficult since there is no notification.	Claim to administrative court or criminal court depending on the	Violation of specific legislation that was the basis of access to the data.

[15] 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

			proceeding, complaint to the data protection inspectorate.	
Storing*	No.	Yes, under the Data Protection Act.	Claim to administrative court or criminal court depending on the proceeding, complaint to the data protection inspectorate.	Violation of Constitution.
Destruction *	No.	Yes, under the Data Protection Act.	Claim to administrative court or criminal court depending on the proceeding, complaint to the data protection inspectorate.	Violation of Constitution.
After the whole surveillance process has ended	N/A	Yes, in principle, but in practice not possible since there is no notification.	Claim to administrative court or criminal court depending on the proceeding, complaint to the data protection inspectorate.	Violation of specific legislation that was the basis of access to the data.
Security Authorities Act				
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*	Yes, unless threat to purpose for investigation	Possibility to request information under general freedom of information rules.	Claim to administrative court, complaint to the Chancellor of Justice.	Violation of SAA, Constitution.
Analysis*	No.	Possibility to request information under general freedom of information rules.	Claim to administrative court, complaint to the Chancellor of Justice.	Violation of SAA, Constitution.
Storing*	No.	Possibility to request information under general freedom of information rules.	Claim to administrative court, complaint to the Chancellor of Justice.	Violation of SAA, Constitution.
Destruction*	No.	Possibility to request information under general freedom of information rules.	Claim to administrative court, complaint to the Chancellor of Justice.	Violation of SAA, Constitution.
After the whole surveillance process has ended	Yes.	Possibility to request information under general freedom of information rules.	Claim to administrative court, complaint to the Chancellor of Justice.	Violation of SAA, Constitution.

* 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.

No lawsuits have been initiated based on or since Snowden revelations or related to mass surveillance.

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** (Address, telephone, e-mail)	**Website**
Õiguskantsler (Chancellor of Justice)	ombudsman	Kohtu 8, 15193 Tallinn (+372) 693 8404 info@oiguskantsler.ee	www.oiguskantsler.ee
Riigikogu julgeolekuasutuste erikomisjon (Special Committee on Oversight of Security Authorities of *Riigikogu)*	parliament	Lossi plats 1a, 15165 Tallinn (+372) 631 6690 kapokom@riigikogu.ee	www.riigikogu.ee
Justiitsministeerium (Ministry of Justice)	government	Tõnismägi 5a, 15191 Tallinn (+372) 620 8100 info@just.ee	www.just.ee

Majandus- ja kommunikatsioonimi nisteerium (Ministry of Economic Affairs and Communications)	government	Harju 11, 15072 Tallinn (+372) 625 6342 info@mkm.ee	www.mkm.ee
Siseministeerium (Ministry of the Interior)	government	Pikk 61, 15065 Tallinn (+372) 612 5008 info@siseministeerium.ee	www.siseministeerium.ee
Eesti Infotehnoloogia ja Telekommunikatsioo ni Liit (Association of Information Technology and Telecommunications)	other	Lõõtsa 6, 11415 Tallinn (+372) 617 7145 info@itl.ee	www.itl.ee
Eesti Inimõiguste Keskus (Estonian Human Rights Centre)	Civil society organisation	Narva mnt 9j, 10117 Tallinn (+372) 644 5148 info@humanrights.ee	www.humanrights.ee
Andmekaitse Inspektsioon (Estonian Data Protection Inspectorate)	Public authority	Väike-Ameerika 19, 10129 Tallinn (+372) 627 4135 info@aki.ee	www.aki.ee
Kaitsepolitseiamet (Estonian Internal Security Service)	Security authority	Toompuiestee 3, 10142 Tallinn (+372) 612 1455 kapo@kapo.ee	www.kapo.ee
Teabeamet (Information Board)	Security authority	Rahumäe tee 4b, 11316 Tallinn (+372) 693 5000 info@teabeamet.ee	www.teabeamet.ee

Tehnilise Järelevalve Amet (Technical Regulatory Authority)	Public authority	Sõle 23 A, Tallinn 10614 (+372) 667 2000 info@tja.ee	www.tja.ee
Eesti Interneti Kogukond (Estonian Internet Society)	Civil society organisation	+372 5661 6933 juhatus@kogukond.org,	www.kogukond.org

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

    a. ERR uudised (2014), 'Anvelt: sideandmete kasutamine ei tohi tulla isikute põhiõiguste arvelt' (Anvelt: use of communication data cannot lessen fundamental rights protection'), 7 June 2014, available at: http://uudised.err.ee/v/eesti/ff1a9de1-2865-4b0d-8163-0c9d8f1a2e35

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

    a. Estonia, Õiguskantsler (Chancellor of Justice), '*Teabe nõudmine, Elektoonilise side seaduse § 111[1]*' (Request for information, Electronic Communications Act Article 111[1]), 15 July 2014, Available at http://adr.rik.ee/okk/dokument/3764037

3. Non-governmental organisations (NGOs)

    a. *Eesti Interneti Kogukond* (Estonian Internet Society), '*Eksklusiivne usutlus "KAPO-komisjoni" endise aseesimehega: komisjonil puudub ülevaade luure ja vastuluure tegevusest*' ('Exclusive interview with the former vice-chairman of KAPO-committee: committee has no overview of intelligence and counter-intelligence actitivities'), 25 June 2013, Available at: http://kogukond.org/2013/06/eksklusiivne-usutlus-kapo-komisjoni-endise-aseesimehega-komisjonil-puudub-ulevaade-luure-ja-vastuluure-tegevusest/

    b. Kukk, U. and Väljataga, A. (2014), 'Right to respect for family and private life', *Human Rights in Estonia 2013*, available at: http://humanrights.ee/en/annual-human-rights-report/human-rights-in-estonia-2013/right-to-respect-for-family-and-private-life/

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

    a. None.