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

FINLAND

13 October 2014

Finnish league for Human Rights
Anni Sams and Anna-Maija Sorjanen

Summary

1. Description of the surveillance legal framework in Finland

   a. types of security services and bodies involved

[1]. The Police (*Poliisi/Polisen*) is headed by the National Police Board (*Poliisihallitus/Polisstyrelsen*). The head of the National Police Board is the head of the Finnish police force. The legality control unit of the National Police Board exercises legality control over the police force and coordinates the internal legality control of the local police units. The Police Department (*Poliisiosasto/Polisavdelningen*) of the Ministry of the Interior (*Sisäasiainministeriö/Inrikesministeriet*) is responsible for the strategic guidance and supervision of the police and the performance guidance for the National Police Board.

[2]. The Finnish Security Intelligence Service (*Suojelupoliisi/Skyddspolisen*) is an operational security authority whose core functions are counterterrorism, counterespionage and security work; preventive security work and internal State security, monitoring the internal State security, especially the development of domestic extremist phenomena and illegal activity relating to them. The Act on Police Administration (*Laki poliisin hallinnosta / Polisförvaltningslag,* 110/1992) provides for tasks of the Security Intelligence Service.

[3]. The most important security bodies concerning surveillance among the Finnish Defence Forces (*puolustusvoimat/försvarsmakten*) are the Investigation Division (*Tiedusteluosasto/Underrättelseavdelning*) of the Defence Command (*Pääesikunta/Huvudstaben*) and the Finnish Defence Intelligence Agency (*Tiedustelulaitos/underrättelsetjänst*). The Finnish Defence Intelligence Agency (FDIA) is a unit subordinate to the Defence Command. The FDIA is in charge of the monitoring, analysis and reporting of the military strategic situation and the military situation of the neighbouring area. The tasks of the FDIA also include responsibility for the geospatial information service of the defence administration

[4]. The Ministry of Defence (*puolustusministeriö/försvarsministeriet*) is in charge of the national defence policy and national security as well as international cooperation in defence policy matters. The Security Committee of the Ministry of Defence (*Puolustusministeriön turvallisuuskomitea/Försvarsministeriets säkerhetskommittén),* also translated as the Security and Defence Committee, is an organ providing aid to the Ministry of Defence and the Cabinet Committee on Foreign and Security Policy in matters related to total defence. The Security Committee, the Defence Command Finland and the Finnish Defence Forces are accountable to the Ministry of Defence.

[5]. The Government Decree on the Ministry for Foreign Affairs (*Valtioneuvoston asetus ulkoasiainministeriöstä /Statsrådets förordning om utrikesministeriet*, 1171/2005)[1] stipulates that the Ministry for Foreign Affairs carries out the international information security obligations as the national security authority

[1] Available in Finnish at: www.finlex.fi/fi/laki/alkup/2005/20051171.

(NSA) in accordance with the Act on International Information Security Obligations (*Laki kansainvälisistä tietoturvallisuusvelvoitteista /Lag om internationella förpliktelser som gäller informationssäkerhet*, 588/2004[2]). The NSA is responsible inter alia for supervising and monitoring that international classified information shall be protected and handled accordingly and coordinating the activities of the Designated Security Authorities (DSAs) and the National Communications Security Authority (NCSA). The Ministry of Transport and Communications' (*Liikenne- ja viestintäministeriö / Kommunikationsministeriet*) key responsibilities include the communications sector, information security and confidentiality of communications and information society policy.

b. the extent of their powers

[6]. Mass surveillance is not explicitly enabled in the national legislation. Surveillance measures are limited to cases with concrete and individualised suspicions of crime and only authorised by courts when necessary to expose the crime and when the seriousness of the crime is considered proportionate to the infringement of privacy. Only those in communication with the suspect are implicated.

[7]. Sections 14a, 14b and 14c of the Act on the Protection of Privacy in Electronic Communications (*Sähköisen viestinnän tietosuojalaki / Lag om dataskydd vid elektronisk kommunikation*) (516/2004) stipulate on the obligation to store data for the purposes of the authorities with references to the Data Retention Directive declared invalid by the Court of Justice of the European Union on 8 April 2014. The Act obliges tele operators to retain data on their clients' e-mail and tele communications for a period of 12 months. Authorities can have data transmitted to them if deemed necessary to fulfil their duties. This practice can be interpreted as a form of mass surveillance. At the moment the obligation to store is being dealt in relation to the on-going legislation process of Information Society Code and serious concerns have been raised (see below e. conditions under which intelligence services can conduct surveillance).The Constitutional Law Committee of the Finnish Parliament gave its statement[3] on 17 June 2014 to the Transport and Communications Committee on the Government Bill on Information Society Code. The Constitutional Law Committee stated that the judgement given by the Court of Justice of the European Union (8 April 2014) can no longer serve as legal basis for the future national legislation on the obligation to store data. However, it concluded that the judgement doesn't prevent national legislation being drafted on the obligation to store data. The proposal for legislation is currently waiting to be confirmed by the President of the Republic of Finland.

[8]. Section 2 of chapter 5 of the Police Act (*Poliisilaki/Polislag*) (872/2011) and section 2 of chapter 10 of the Coercive Measures Act (*Pakkokeinolaki/ Tvångsmedelslag*) (806/2011) stipulate that the use of secret intelligence measures, including telecommunications interception, telecommunications monitoring and technical surveillance is only allowed when there is reason to suspect that their use will provide information of much importance in preventing and investigating a crime. Furthermore, section 89 of the Act on Soldier Discipline and Crime Prevention in the Finnish Defence Forces (*Laki sotilaskurinpidosta ja*

[2] Available in Finnish at: www.finlex.fi/fi/laki/alkup/2004/20040588.

[3] Available in Finnish at: www.eduskunta.fi/faktatmp/utatmp/akxtmp/pevl_18_2014_p.shtml.

rikostorjunnasta puolustusvoimissa/ Lag om militär disciplin och brottsbekämpning inom försvarsmakten) (28.3.2014/255) stipulates that the secret surveillance methods can only be used in revealing the following crimes among the Finnish Defence Forces: Endangering the Finnish autonomy; enticement to war; treason and aggravated treason; espionage and aggravated espionage; revealing of a national security secret; and unlicensed intelligence activity.

[9]. Two important on-going legislative amendment processes can have an impact on surveillance legislation. Firstly, the Government has presented its proposal for Information Society Code to Parliament (*Tietoyhteiskuntakaari/ Informationssamhällsbalken*), and it entered into force on 1 January 2015. The Act incorporates key provisions concerning electronic communications, and the most relevant sections in terms of mass surveillance concern the obligation to store data for the purposes of the authorities. The Information Society Code regulates the providers of publicly available communications services to store only data that is available and lawfully generated or processed in connection with services provided. Furthermore, the Security Committee of the Ministry of Defence (*Puolustusministeriön turvallisuuskomitea/Försvarsministeriets säkerhetskommittén)* has presented their implementation programme of the national cyber security strategy (*Kansallisen kyberturvallisuusstrategian toimeenpano-ohjelma*), which includes 74 measures to improve national cyber security. The measures are not clearly defined and the impact of this programme on national legislation and security policy cannot be foreseen at this stage. The Security Committee expects Ministries to draft implementation programmes in their fields of administration by the end of 2014.

[10]. There are strong proponents of more surveillance in the state security sector. According to their annual report, the Finnish Security Intelligence Service (*Suojelupoliisi/Skyddspolisen*) has emphasized cyber threats to governmental and social systems during the preparation of the national cyber security strategy. In their view, as regards preventing cyber threats to national security, the situation in Finland is not satisfactory in terms of the authorities' competences and capacities.[4] The Ministry of Defence writes in a similar vein in their appointment letter of the Working group on developing the national legislation to increase the security authorities' ability to acquire information about the threats presented by the cyber environment; the purpose of this group is "to better tackle threats to national security occurring in the internet".[5] These developments imply that the reaction to the post-Snowden revelations together with the violations of data security targeted

[4] Finland, the Finnish Security Intelligence Service (*Suojelupoliisi/Skyddspolisen*), Annual Report 2013, available at (accessed 24 July 2014): www.poliisi.fi/poliisi/supo60/home.nsf/files/9F07FC6EA2B39425C2257C90003052CF/$file/2013_Supo-Annual_Report_web.pdf.

[5] Finland, the Ministry of Defence (*Puolustusministeriö/Försvarsministeriet*) (2013), *Asettamispäätös: Kansallisen lainsäädännön kehittäminen kyberturvallisuusviranomaisten tiedonhankintakyvyn parantamiseksi kybertoimintaympäristön uhkista; lainsäädäntöhanke*, document available at (accessed 25 July 2014): www.defmin.fi/files/2669/Kyberlainsaadantotyoryhman_asettamispaatos.pdf.

at the Finnish Foreign Service[6] have led to the demand of more surveillance by the national security authorities instead of strengthening the right to privacy.[7]

[11]. From the beginning of 2014, the new legislation on coercive measures took effect. The use of telecommunications monitoring and telecommunications interception was broadened somewhat, however, the aim of clarifying the legislation on secret data interception measures was not comprehensively met according to the Parliamentary Ombudsman.[8] Currently the Ombudsman´s report is being dealt by the Constitutional Law Committee.

c. control/oversight mechanisms

[12]. The Police Board reports yearly to the Ministry of the Interior on the use of coercive measures and secret intelligence functions in the police.[9] This report is also delivered to the The Parliamentary Ombudsman (*Eduskunnan oikeusasiamies/ riksdagens justitieombudsman*). Section 1 of the Act on Police Administration (*Laki poliisin hallinnosta/Polisförvaltningslag*) (14.2.1992/110)[10] stipulates that the Ministry of the Interior is responsible over the steering and supervision of the functions of the police. The Ministry of the Interior steers the National Police Board.

[13]. The data processing system SALPA managed by the National Bureau of Investigation is used to process information on secret coercive measures. The SALPA system is used by the police, customs, national bureau of investigation and border guard. All the requests for the use of secret coercive measures and data acquisition are delivered via SALPA. Moreover, the SALPA-system is can be used for real time legality control: the National Bureau of Investigation inspects daily the requests made via SALPA before they are sent further, for example to the

---

[6] Finland, Ministry for Foreign Affairs of Finland (ulkoasiainministeriö/ utrikesministeriet): http://formin.finland.fi/public/default.aspx?contentid=291725&nodeid=23&contentlan=2&culture=en-US

[7] The Privacy Surgeon (2014): A Crisis of Accountability, A global analysis of the impact of Snowden revelations, available at: www.privacysurgeon.org/blog/wp-content/uploads/2014/06/Snowden-final-report-for-publication.pdf, p. 36

[8] Finland, the Parliamentary Ombudsman (*Eduskunnan oikeusasiamies/Riksdagens justitieombudsman*) (2014), the Annual Report of the Parliamentary Ombudsman 2013 (Eduskunnan oikeusasiamiehen kertomus vuodelta 2013), page 157, available at (accessed 6 August 2014): www.oikeusasiamies.fi/dman/Document.phx?documentId=hh16114123723149&cmd=download.

[9] Finland, the National Police Board (*Poliisihallitus/Polisstyrelsen*) (2014), *Poliisihallituksen selvitys Sisäasiainministeriölle poliisin tiedonhankinnasta ja sen valvonnasta 2013*, POL-2014-30. Available at (all hyperlinks accessed 14 July 2014): http://poliisi.fi/poliisi/home.nsf/files/8E2337E98D525CF2C2257CA00029F00B/$file/Allekirjoitettu%20toimintakertomus%202013.pdf.

[10] Finland, the Act on Police Administration (*Laki poliisin hallinnosta/Polisförvaltningslag*), (14.2.1992/110), available at (accessed 14 July 2014): www.finlex.fi/fi/laki/ajantasa/1992/19920110.

teleoperators. The information gathered in SALPA-system is used to draw reports[11] on the use of secret coersive measures.[12]

[14]. The Follow-up Group on Secret Data Acquisition (*Salaisen tiedonhankinnan seurantaryhmä*) appointed by the National Police Board (*Poliisihallitus/Polisstyrelsen*) prepares a comprehensive annual report to the Parliamentary Ombudsman based on the reports on the use of coercive measures and surveillance in the Police, the Finnish Border Guard, the Customs and the Finnish Defence Force.[13]

[15]. The Data Protection Ombudsman (*Tietosuojavaltuutettu/Dataombudsmannen*) provides direction and guidance on the processing of personal data, supervises the processing in order to achieve the objectives of the Personal Data Act (523/1999), as well as makes decisions concerning right of access and rectification.[14] When the data subject does not have a right of access to data collected on them, the Data Protection Ombudsman has access to the data in order to inspect the legality of the person register. In accordance with the Personal Data Act: Chapter 9, section 39 (Data protection authorities' right of access and inspection): "Regardless of confidentiality provisions, the Data Protection Ombudsman has the right of access to personal data which are being processed, as well as all information necessary for the supervision of the legality of the processing of personal data.[...]The Data Protection Ombudsman has the right to inspect personal data files and to assign experts to carry out the inspection. For purposes of the inspection, the Data Protection Ombudsman and an expert have the right to enter the premises of the controller and a person operating on the behalf of the controller, where personal data are processed or personal data files are kept in such premises, and to access the information and equipment required for carrying out the inspection. In premises covered by the provisions on the sanctity of the home, an inspection may be carried out only if in the matter at hand there is a specific reason to believe that the provisions on the processing of personal data have been violated or are going to be violated. The inspection shall be carried out so that it does not cause undue inconvenience or cost to the controller."

[16]. The Chancellor of Justice (*Oikeuskansleri/ Justitiekanslern*) and the Parliamentary Ombudsman (*Eduskunnan oikeusasiamies/ riksdagens justitieombudsman*) exercise the highest form of legality control in Finland. The Parliamentary Ombudsman

---

[11] See for example: Finland, the National Police Board (Poliisihallitus/Polisstyrelsen) (2014), Poliisihallituksen selvitys Sisäasiainministeriölle poliisin tiedonhankinnasta ja sen valvonnasta 2013, POL-2014-30. Available at http://poliisi.fi/poliisi/home.nsf/files/8E2337E98D525CF2C2257CA00029F00B/$file/Allekirjoitettu%20toimintakertomus%202013.pdf

[12] Niemi, Johanna & de Godzinsky, Virve-Maria (2009): Telecommunications Surveillance and Legal Protection in Finland. National Research Institute of Legal Policy. Available at: www.optula.om.fi/material/attachments/optula/julkaisut/tutkimuksia-sarja/j719eif2N/243_telepakkokeinojen_oikeussuojaj.pdf

[13] Finland, the Government Decree on pretrial investigations, coercive measures and secret data acquisition (*Valtioneuvoston asetus esitutkinnasta, pakkokeinoista ja salaisesta tiedonhankinnasta/ Statsrådets förordning om förundersökning, tvångsmedel och hemligt inhämtande av information*), 122/2014, available at (accessed 7 July 2014): www.finlex.fi/fi/laki/alkup/2014/20140122.

[14] Information retrieved from the website of Finland, Ministry of Justice (*Oikeusministeriö/Justitieministeriet*), available at (all hyperlinks accessed 9.7.2014): http://oikeusministerio.fi/en/index/theministry/neuvottelu-jalautakunnat/thefinnishdataprotectionboard.html.

exercises oversight to ensure that public authorities and officials observe the law and fulfil their duties in the discharge of their functions. The Ombudsman oversees legality principally by examining complaints received. He can also intervene in perceived shortcomings on his own initiative. In addition, the Ombudsman carries out inspections at offices and institutions. The Chancellor of Justice supervises the authorities by handling any written complaints arising from their actions. The Chancellor of Justice is entitled to perform inspections of those authorities, institutions, offices and other units that fall within the scope of his supervisory authority, such as courts, prosecutor's offices, police departments and other public authorities.[15] The Chancellor of Justice does not handle complaints concerning the Defence Forces or deprivation of liberty as these belong under the mandate of the Parliamentary Ombudsman.

d. geographical scope of surveillance

[17]. Section 89 of the Act on Soldier Discipline and Crime Prevention in the Finnish Defence Forces (*Laki sotilaskurinpidosta ja rikostorjunnasta puolustusvoimissa/ Lag om militär disciplin och brottsbekämpning inom försvarsmakten*) (28.3.2014/255) stipulates that coercive measures can be used in the geographical area in use of armed forces or in other areas in case the use of coercive measures cannot be postponed or executive assistance from the police is not available shortly.

[18]. The implementation programme of the national cyber security strategy (*Kansallisen kyberturvallisuusstrategian toimeenpano-ohjelma*) by the Security Committee of the Ministry of Defence (*Puolustusministeriön turvallisuuskomitea/Försvarsministeriets säkerhetskommittén)*[16] includes brief descriptions of measures foreseen. The goal of the measure titled "National cyber surveillance and cyber intelligence" is defined to "identify and prevent web traffic detrimental to national security already at the borders, in a manner similar to air and sea surveillance." No further details on this measure are available.

[19]. Section 4 of the Personal Data Act (*Henkilötietolaki/ Personuppgiftslag*) (523/1999) stipulates that the Act applies to processing of personal data where the controller is established in the territory of Finland or otherwise subject to Finnish law. The Act applies also if the controller is not established in the territory of a Member State of the European Union, but it uses equipment located in Finland in the processing of personal data, except where the equipment is used solely for the transfer of data through the territory. In this case the controller shall designate a representative established in Finland.

e. conditions under which intelligence services can conduct surveillance

---

[15] Information retrieved from the website of Finland, The Chancellor of Justice (*Oikeuskansleri/ Justitiekanslern*), available at: www.oikeuskansleri.fi/en/.

[16] Finland, the Security Committee of the Ministry of Defence (*Puolustusministeriön turvallisuuskomitea/Försvarsministeriets säkerhetskommittén*), The implementation programme of the national cyber security strategy (*Kansallisen kyberturvallisuusstrategian toimeenpano-ohjelma*), 11.3.2014, 194/8.1.99/2013, available at (accessed 17 July 2014):
www.turvallisuuskomitea.fi/index.php/fi/20-ajankohtaista/45-kyberturvallisuusstrategian-toimeenpano-ohjelma-on-valmis.

[20]. In general, surveillance is currently only enabled when investigating a crime, and it must be targeted at individual suspects or their communications. Furthermore, the crimes allowing for surveillance must be of a serious nature, such as treason, offences committed with terrorist intent or offences for which the most severe punishment is imprisonment for at least four years. The specific titles of offence are listed in each act regulating surveillance. Two on-going legislative and policy developments, the National Cyber Security Strategy (*Kansallinen kyberturvallisuusstrategia*) and the Information Society Code (*Tietoyhteiskuntakaari/ Informationssamhällsbalken*), are considered by NGO and researcher sources[17] in their current draft form to enable surveillance on a wider scale and for less specific purposes, possibly leading to mass surveillance type practices in the future. The data retention provisions of the Information Society Code were however changed by the Transport and Communications Committee and some restrictions were made to retention period and the types of services to which the provisions apply.

f. different stages of surveillance procedure

[21]. Section 1 of the Government Decree on Pre-trial Investigations, Coercive Measures and Secret Data Acquisition (*Valtioneuvoston asetus esitutkinnasta, pakkokeinoista ja salaisesta tiedonhankinnasta/ Statsrådets förordning om förundersökning, tvångsmedel och hemligt inhämtande av information*)[18] stipulates that official records must be drafted after the use of a coercive measure has been ended, without delay, at the latest in 30 days. Section 22 of the Decree stipulates that the pre-trial investigation officials must draft a report on the use of secret coercive measures as defined in Chapter 10 of the Coercive Measures Act and secret data acquisition as defined in Chapter 5 of the Police Act. The reports must be delivered once a year to the Ministry of the Interior, the Ministry of Finance and the Ministry of Defence. These Ministries must present their reports to the Parliamentary Ombudsman each year, by the end of February.

[22]. Section 89 of the Act on Soldier Discipline and Crime Prevention in the Finnish Defence Forces includes a requirement to inform the Finnish Security Intelligence Service (*Suojelupoliisi/Skyddspolisen*) about the use of secret data acquisition methods without delay.

2. Safeguards put in place by the legal framework to ensure respect for privacy and data protection during surveillance measures

[23]. The main legal act regulating data protection is the Personal Data Act (*Henkilötietolaki/ Personuppgiftslag*) (523/1999)[19]. Chapter 6 stipulates the data

---

[17] EFFI, Electronic Frontier Finland ry (NGO), *Effin lausunto turvallisuuskomitean toimittamasta kyberturvallisuuden toimeenpano--ohjelman luonnoksesta*, available at (accessed 14 July 2014): www.effi.org/lausunnot/lausunto-kyberturvallisuus-20140131 and communication by e-mail with Niklas Vainio, researcher, Faculty of Law, University of Turku, 18 July 2014.

[18] Finland, the Government Decree on Pretrial Investigations, Coercive Measures and Secret Data Acquisition (*Valtioneuvoston asetus esitutkinnasta, pakkokeinoista ja salaisesta tiedonhankinnasta/ Statsrådets förordning om förundersökning, tvångsmedel och hemligt inhämtande av information*), 122/2014, available at (accessed 7 July 2014): www.finlex.fi/fi/laki/alkup/2014/20140122.

[19] Finland, Personal Data Act (*Henkilötietolaki/ Personuppgiftslag*), 523/1999, available at (accessed 5 August 2014): www.finlex.fi/en/laki/kaannokset/1999/en19990523.pdf.

subject´s rights: when collecting personal data, the controller shall see to that the data subject can have information on the controller and, where necessary, the representative of the controller, on the purpose of the processing of the personal data, on the regular destinations of disclosed data, as well as on how to proceed in order to make use of the rights of the data subject in respect to the processing operation in question. Section 29 stipulates on rectification of data: "The controller shall, on its own initiative or at the request of the data subject, without undue delay rectify, erase or supplement personal data contained in its personal data file and erroneous, unnecessary, incomplete or obsolete as regards the purpose of the processing. The controller shall also prevent the dissemination of such data, if this could compromise the protection of the privacy of the data subject or his/her rights." […] "If the controller refuses the request of a data subject of the rectification of an error, a written certificate to this effect shall be issued. The certificate shall also mention the reasons for the refusal. In this event, the data subject may bring the matter to the attention of the Data Protection Ombudsman." […] "The controller shall notify the rectification to the recipients to whom the data have been disclosed and to the source of the erroneous personal data. However, there is no duty of notification if this is impossible or unreasonably difficult."

[24]. The Coercive Measures Act stipulates that a court decides on telecommunications interception on request and that the warrant may be given for at most one month at a time. A warrant for traffic data monitoring must also be decided upon by a court on the request of an official with the power of arrest. The Coercive Measures Act further stipulates that a written notice shall be given without delay to the suspect concerning telecommunications interception, the obtaining of data other than through telecommunications interception, traffic data monitoring, extended surveillance, covert collection of intelligence, technical surveillance and controlled delivery directed at him or her, at the latest within one year of the termination of the use of a coercive measure.

3. Judicial or non-judicial remedies available to an individual subject to surveillance

[25]. Section 39 of the Personal Data Act (*Henkilötietolaki/Personuppgiftslag*) (523/1999)[20] stipulates on the role of the Data Protection Ombudsman. The Ombudsman has the right of access to personal data which are being processed, as well as all information necessary for the supervision of the legality of the processing of personal data. Where necessary, the Data Protection Ombudsman shall refer the matter to be dealt with by the Data Protection Board, or report it for prosecution The Data Protection Board has the same right in matters which it is dealing with.

[26]. As stipulated by section 44 of the Personal Data Act, at the request of the Data Protection Ombudsman, the Data Protection Board may: prohibit processing of personal data which is contrary to the provisions of this Act or the rules and regulations issued on the basis of this Act; in matters (other than those referred to in section 40), compel the person concerned to remedy an instance of unlawful conduct or neglect; order that the operations pertaining to the file be ceased, if the unlawful conduct or neglect seriously compromise the protection of the privacy of

[20] Finland, Personal Data Act (*Henkilötietolaki/ Personuppgiftslag*), 523/1999, available at (accessed 5 August 2014): www.finlex.fi/en/laki/kaannokset/1999/en19990523.pdf.

the data subject or his/her interests or rights, provided that the file is not set up under a statutory scheme; revoke a permission (referred to in section 43), where the prerequisites for the same are no longer fulfilled or the controller acts against the permission or the rules attached to it.

[27]. Chapter 3 of the Act on the Openness of Government Activities (*Laki viranomaisten toiminnan julkisuudesta / Lag om offentlighet i myndigheternas verksamhet*) (621/1999)[21] stipulates that everyone shall have the right of access to an official document in the public domain. No access to a secret document or its contents shall be granted. There are some exceptions to the exercise of this right.[22]

[28]. An individual subject to coercive measures as stipulated by the Coercive Measures Act can file an administrative complaint to the National Police Board. The authority can then, if the actions are deemed blameworthy, give a notice to the authority. If the Police Board deems that an offence in office has been committed, the case is transferred to be considered by the Prosecution Office. The head of investigation to police matters is always the prosecutor.[23]

---

[21] Finland, the Act on the Openness of Government Activities (*Laki viranomaisten toiminnan julkisuudesta / Lag om offentlighet i myndigheternas verksamhet*) (621/1999), available at (accessed 5 August 2014): www.finlex.fi/en/laki/kaannokset/1999/en19990621.pdf.

[22] Section 11: Parties' right of access: "A petitioner, an appellant and any other person whose right, interest or obligation in a matter is concerned a party shall also have the right of access, to be granted by the authority which is considering or has considered the matter, to the contents of a document which is not in the public domain, if they may influence or may have influenced the consideration of his/her matter.
A party, his/her representative or counsel shall not have the right of access referred above **for example**: to a document, access to which would be contrary to a very important public interest, the interest of a minor or some other very important private interest; a document produced or prepared in the course of a criminal investigation or police inquiry before the completion of the investigation or inquiry, if access would impede the clearing up of the case; a presentation memorandum, a draft decision or a comparable document prepared by an authority for the preparation of a matter, before the consideration of the matter by that authority has been concluded; a document prepared or procured by an authority acting as a litigant in a trial, if access would be contrary to the interests of the public corporation or the corporation, foundation, institution or person (referred to in section 4(2)) in the trial, etc.

[23] Information retrieved from the website of Finland, the Police, available at (accessed 23 July 2014): www.poliisi.fi/poliisi/home.nsf/pages/6AD3C71197005F3DC2256BC1003FFD3B?opendocument.

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*

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)?
Act on the Protection of Privacy in Electronic Communications (*Sähköisen viestinnän tietosuojalaki/ Lag om dataskydd vid elektronisk kommunikation*) (516/2004), unofficial translation available at (accessed 17 July 2014): http://finlex.fi/en/laki/kaannokset/2004/en20	*The act does not enable mass surveillance, however, it contains sections that might contribute to enabling such procedures.* All clients of tele-operators in Finland, more specifically: persons under suspicion of a crime or persons who are in communication	Sections 14a to 14c of the Act on the Protection of Privacy in Electronic Communications stipulate on the Obligation to store data for the purposes of the authorities. These sections refer to the Data Retention Directive declared invalid by the Court of Justice of the European Union on 8 April 2014.	Authorities can have data transmitted to them if deemed necessary to fulfil their duties. Section 36 of the Act stipulates that authorities are entitled to data in prevention, investigation and revealing of crimes. The authorities may obtain data only for the purposes stipulated in the Section 6, Chapter 10 of the	As stipulated by Section 17 of the Chapter 5 of the Act on the Exercise of Freedom of Expression in Mass Media (*Laki sananvapauden käyttämisestä joukkoviestinnässä/ Lag om yttrandefrihet i masskommunikation*) [25], the request by an authority to obtain information required for the identification of the sender of a network message must be decided upon by a court. The Act	Section 14 b of the Act on the Protection of Privacy in Electronic Communications stipulates the following: "A service operator under the retention obligation shall discuss the implementation and application of data retention with the Ministry of the Interior in order to ensure that all data considered necessary by the authorities will be retained. If no consensus is reached on the	Section 3 of the Act on the Protection of Privacy in Electronic Communications stipulates: "This Act does not apply to the actions of public authorities in public authority networks as defined in the Communications Market Act or in any other communications network built for the needs of public order and security, national	*Does not allow mass surveillance in any country.*

[25] Finland, the Act on the Exercise of Freedom of Expression in Mass Media (*Laki sananvapauden käyttämisestä joukkoviestinnässä/ Lag om yttrandefrihet i masskommunikation*) (13.6.2003/460), unofficial translation available at (accessed 21 July 2014): http://finlex.fi/en/laki/kaannokset/2003/en20030460.pdf

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)?
040516.pdf From 1 January 2015 Information Society Code, Tietoyhteiskuntakaari, Informationssamhällsbalk. Sections 157-159 http://www.eduskunta.fi/faktatmp/utatmp/akxtmp/ev_106_2014_p.shtml	with persons under suspicion of a crime.	The Act obliges tele operators to retain data on their clients' e-mail and tele communications for a period of 6 to 12 months.	Coercive Measures Act, which stipulates the following: "telecommunications interception may be directed only at a message that originates from or is intended for a suspect in an offence." […] "Criminal investigation authority may receive permission for telecommunications interception directed at a network address or terminal end	stipulates: "On the request of an official with the power of arrest, as referred to in chapter 1, section 6(1), of the Coercive Measures Act (450/1987), a public prosecutor, or an injured party, a court may order the keeper of a transmitter, server or other similar device to release the information required for the identification of the sender of a network message to the requester, provided that there are probable reasons to believe that the contents of the	implementation of data retention, the service operator decides on the technical implementation of the retention. […] Data should be retained in such a way as to avoid the same data being retained by several service operators. It must be ensured that the data retained can be transmitted to the authorities entitled to it without undue delay. […] A service operator under the retention obligation shall ensure that information about data retention and its purposes is available	defence, rescue operations, civil defence or the safety of land, sea, rail or air transport." Section 14 a of the Act on the Protection of Privacy in Electronic Communications stipulates the following: "A requirement for the retention obligation is that the data is available and generated or processed in connection with publicly available communications services provided	

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)?
			device in the possession of or otherwise presumably used by a suspect in an offence, when there are grounds to suspect him or her of certain crimes.[24]	message are such that providing it to the public is a criminal offence. […] A court order on the release of identifying information shall be open to appeal as a separate matter. The order	to the subscriber."	on the basis of this Chapter or the provisions of the Personal Data Act."	

[24] These offences are, as stipulated by Chapter 10, Section 3 of Finland, the Coercive Measures Act (*Pakkokeinolaki/ Tvångsmedelslag*), 806/2011: 1) genocide, preparation of genocide, a crime against humanity, an aggravated crime against humanity, a war crime, an aggravated war crime, torture, violation of a prohibition against chemical weapons, violation of a prohibition against biological weapons, violation against a prohibition against anti-infantry mines; (1468/2011) (2) endangerment of the sovereignty of Finland, incitement to war, treason, aggravated treason, espionage, aggravated espionage, disclosure of a national secret, unlawful gathering of intelligence; (3) high treason, aggravated high treason, preparation of high treason; (4) aggravated distribution of a sexually offensive picture depicting a child; (5) sexual abuse of a child, aggravated sexual abuse of a child; (6) manslaughter, murder, homicide, preparation of an aggravated offence directed against life or health as referred to in Chapter 21, section 6a of the Criminal Code and in accordance with sections 1, 2 and 3 of said Chapter; (438/2013) (7) arrangement of aggravated illegal entry into the country, aggravated deprivation of liberty, trafficking in persons, aggravated trafficking in persons, kidnapping, preparation of kidnapping; (438/2013) (8) aggravated robbery, preparation of aggravated robbery, aggravated extortion; (438/2013) (9) aggravated concealment of illegally obtained goods, professional concealment of illegally obtained goods, aggravated money laundering; (10) criminal mischief, criminal traffic mischief, aggravated sabotage, aggravated endangerment of health, a nuclear device offence, hijacking; (11) an offence committed with terrorist intent, preparation of an offence committed with terrorist intent, directing of a terrorist group, promotion of the activity of a terrorist group, provision of training for the commission of a terrorist offence, recruitment for the commission of a terrorist offence,

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)?
			According to Section 158 of the Chapter 19 of the Government proposal (page 298), the Ministry of the Interior can obtain a server in which the tele operators can transfer data under the obligation to store data. This would be financially feasible for the operators, thus probably widely used albeit voluntary. This would form a	shall not be enforced until it has become final, unless the appellate court otherwise orders."			

financing of terrorism, as referred to in Chapter 34(a), section 1, subsection 1, paragraphs 2-7 or subsection 2 of the Criminal Code; (12) aggravated damage to property; (13) aggravated fraud, aggravated usury; (14) aggravated counterfeiting; (15) aggravated impairment of the environment; or (16) an aggravated narcotics offence.

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)?
			massive database of data concerning citizens' communications.				

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)?
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)?**
Finland, the Security Committee of the Ministry of Defence (*Puolustusministeriön turvallisuuskomitea/Försvarsministeriets säkerhetskommitté n)*, The implementation	The implementation of the cyber strategy could possibly enable mass surveillance of internet traffic without a specific target or a suspicion of a crime.	According to EFFI (NGO)'s comments[26], the proposed programme text suggests that the state powers strive to mass surveillance of internet communications in the common infrastructure, comparable to	Section 2.4 of the proposed programme suggests that internet surveillance will be more prominent in the future: "National cyber surveillance provides authorities with the kind of situational	Currently, the decision to enable authorities to access data is made by courts (see Section 17 of the Chapter 5 of the Act on the Exercise of Freedom of Expression in Mass Media (*Laki sananvapauden käyttämisestä joukkoviestinnässä/*	No key steps mentioned; the implementation measures are concisely and vaguely defined in the programme.	In the measure titled "national cyber surveillance and cyber intelligence" has as its goal to "identify and prevent web traffic detrimental to national security already at the borders, in a	

[26] EFFI, Electronic Frontier Finland ry (NGO), *Effin lausunto turvallisuuskomitean toimittamasta kyberturvallisuuden toimeenpano--ohjelman luonnoksesta*, available at (accessed 14 July 2014): www.effi.org/lausunnot/lausunto-kyberturvallisuus-20140131.

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)?
programme of the national cyber security strategy (*Kansallisen kyberturvallisuusstrategian toimeenpano-ohjelma*), 11.3.2014, 194/8.1.99/2013, available at (accessed 17 July 2014): www.turvallisuuskomitea.fi/index.php/fi/20-ajankohtaista/45-kyberturvallisuusstrategian-toimeenpano-ohjelma-on-valmis		some foreign intelligence services surveillance practices.	information not available in any other sources […] Cyber surveillance and intelligence also includes the development of a cross-sectional model among the authorities."	*Lag om yttrandefrihet i masskommunikation*)[27] as explained above). However, the development of a cross-sectional model among the authorities as suggested in the programme might lead to non-judicial approval procedures.		manner similar to air and sea surveillance." No further details on this measure are available.	

[27] Finland, the Act on the Exercise of Freedom of Expression in Mass Media (*Laki sananvapauden käyttämisestä joukkoviestinnässä/ Lag om yttrandefrihet i masskommunikation*) (13.6.2003/460), unofficial translation available at (accessed 21 July 2014): http://finlex.fi/en/laki/kaannokset/2003/en20030460.pdf.

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)?
Working group on developing the national legislation to increase the security authorities' ability to acquire information about the threats presented by the cyber environment (*Kansallisen lainsäädännön kehittämistä turvallisuusviranomaisten tiedonhankintakyvyn parantamiseksi kybertoimintaympäristön uhkista valmisteleva työryhmä*), PLM004:00/2013, information about	The working group has been appointed by the Ministry of Defence in order to evaluate national legislation in terms of the risks presented by information networks. This working group was appointed as part of the implementation of the national cyber security strategy, see above. The working group is expected to finish their work by the end of 2014. There are no publications or	The working group is expected to finish their work by the end of 2014.	The working group is expected to finish their work by the end of 2014.	The working group is expected to finish their work by the end of 2014.	The working group is expected to finish their work by the end of 2014.	The working group is expected to finish their work by the end of 2014.	The working group is expected to finish their work by the end of 2014.

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 working group in the project register of the Government available at (accessed 17 July 2014): www.hare.vn.fi/mHankePerusSelaus.asp?h_iID=19825&tVNo=1&sTyp=Selaus	statements published by the working group yet, thus no specifics on the outcome of their work are available.						

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)?
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 Police Act (*Poliisilaki/Polislag*), 872/2011, available at (accessed 24 July 2014): www.finlex.fi/fi/laki/alkup/2011/20110872#Pidp2207488	*The act does not enable mass surveillance, however, it contains sections that might contribute to enabling such procedures.* Persons suspected of a crime, or persons in communication of such persons.	Chapter 5 of the Police Act stipulates on the use of secret intelligence measures, including telecommunications interception, telecommunications monitoring and technical surveillance. The use of these measures, as stipulated by section 2 of chapter 5, is only	Section 1 of Chapter 5 stipulates that the use of secret intelligence measures is only allowed when they are expected to provide information needed to prevent or investigate a crime or prevent danger. According to section 5, the crimes allowing for	Section 7 and 10 of the Chapter 5 of the Police Act Stipulate that the court decides on telecommunications monitoring and interception on the request of an official with the power of arrest and that the warrant may be given for at most one month at a time.	The Act does not specify steps to be followed in the course of surveillance. For details on steps to be followed, see below: Finland, the Government Decree on pre-trial investigations, coercive measures and secret data acquisition (*Valtioneuvoston asetus esitutkinnasta, pakkokeinoista ja salaisesta*		

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)?
		allowed when there is reason to suspect that their use will provide information of much importance in preventing and investigating a crime.	telecommunications monitoring are: endangerment of the sovereignty of Finland, incitement to war, treason, aggravated treason, espionage, aggravated espionage, disclosure of a national secret, unlawful gathering of intelligence, high treason, aggravated high treason, preparation of high treason; an offence committed with terrorist intent,		*tiedonhankinnasta/ Statsrådets förordning om förundersökning, tvångsmedel och hemligt inhämtande av information*), 122/2014		

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)?
			preparation of an offence committed with terrorist intent, directing of a terrorist group, promotion of the activity of a terrorist group, provision of training for the commission of a terrorist offence, recruitment for the commission of a terrorist offence, and financing of terrorism. According to section 8, the crimes allowing for telecommunications interception are: an offence				

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)?
			for which the most severe punishment is imprisonment for at least four years; an offence committed with the use of the network address or terminal end device, for which the most severe punishment provided is imprisonment for at least two years; exploitation of a person subjected to the sex trade, solicitation of a child for sexual purposes or pandering; a narcotics offence; preparation of an offence				

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)?
			committed with terrorist intent; and an aggravated customs offence.				
Finland, the Coercive Measures Act (*Pakkokeinolaki/ Tvångsmedelslag*), 806/2011, unofficial translation available at (accessed 7 July 2014): http://finlex.fi/en/laki/kaannokset/2011/en20110806.pdf	The act does not enable mass surveillance, however, it contains sections that might contribute to enabling such procedures. persons under suspicion of committing an offense; persons in communication with persons under suspicion of committing an	Section 2 of the Chapter 10 of the Coercive Measures Act stipulates that "a general prerequisite for the use of covert coercive measures is that their use may be assumed to produce information needed to clarify an offence, and they may be used only if they can be assumed to be of significance in	Section 2 of the Chapter 10: "to produce information needed to clarify an offence" and "only if they can be assumed to be of particularly important significance in the clarification of an offence".	Section 5 of the Chapter 10 of the Coercive Measures Act Stipulates that "the court decides on telecommunications interception [….] on the request of an official with the power of arrest." and that the warrant "may be given for at most one month at a time". Section 9, Chapter 10 of the Coercive Measures Act stipulates that: The	The Act does not specify steps to be followed in the course of surveillance. For details on steps to be followed, see below: Finland, the Government Decree on pre-trial investigations, coercive measures and secret data acquisition (*Valtioneuvoston asetus esitutkinnasta, pakkokeinoista ja salaisesta tiedonhankinnasta/ Statsrådets*	Section 2 (par. 3) of the Chapter 10: "The use of covert coercive measures shall be terminated before the end of the period designated in the decision, if the purpose of their use has been achieved or their prerequisites no longer exist."	No, does not allow mass surveillance in any country.

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)?
	offense	the clarification of an offence." Section 3 of the Chapter 10 of the Coercive measures Act stipulates on telecommunications interception: "Telecommunications interception may be directed only at a message that originates from or is intended for a suspect in an offence." [..] "Criminal investigation authority may receive permission for		court decides on traffic data monitoring […] and on the obtaining of location data 8 […] on the request of an official with the power of arrest. If the matter does not brook delay, an official with the power of arrest may decide on traffic data monitoring and on the obtaining of location data until such time as the court has decided on the request for the issuing of the warrant. The matter shall be submitted for the decision of the court as soon as	*förordning om förundersökning, tvångsmedel och hemligt inhämtande av information*), 122/2014		

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)?
		telecommunications interception directed at a network address or terminal end device in the possession of or otherwise presumably used by a suspect in an offence, when there are grounds to suspect him or her of certain		possible, but at the latest within 24 hours of the initiation of the use of the coercive measure. The warrant may be issued and the decision may be made for at most one month at a time and the warrant or decision may be issued to extend also to the period prior to the issuing of the warrant or			

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)?
		crimes."[28] […] "A warrant for telecommunications interception may be issued also when there are grounds to suspect a person" of certain crimes		the making of the decision, which may be longer than one month."			

[28] These offences are, as stipulated by Chapter 10, Section 3 of Finland, the Coercive Measures Act (*Pakkokeinolaki/ Tvångsmedelslag*), 806/2011: 1) genocide, preparation of genocide, a crime against humanity, an aggravated crime against humanity, a war crime, an aggravated war crime, torture, violation of a prohibition against chemical weapons, violation of a prohibition against biological weapons, violation against a prohibition against anti-infantry mines; (1468/2011) (2) endangerment of the sovereignty of Finland, incitement to war, treason, aggravated treason, espionage, aggravated espionage, disclosure of a national secret, unlawful gathering of intelligence; (3) high treason, aggravated high treason, preparation of high treason; (4) aggravated distribution of a sexually offensive picture depicting a child; (5) sexual abuse of a child, aggravated sexual abuse of a child; (6) manslaughter, murder, homicide, preparation of an aggravated offence directed against life or health as referred to in Chapter 21, section 6a of the Criminal Code and in accordance with sections 1, 2 and 3 of said Chapter; (438/2013) (7) arrangement of aggravated illegal entry into the country, aggravated deprivation of liberty, trafficking in persons, aggravated trafficking in persons, idnapping, preparation of kidnapping; (438/2013) (8) aggravated robbery, preparation of aggravated robbery, aggravated extortion; (438/2013) (9) aggravated concealment of illegally obtained goods, professional concealment of illegally obtained goods, aggravated money laundering; (10) criminal mischief, criminal traffic mischief, aggravated sabotage, aggravated endangerment of health, a nuclear device offence, hijacking; (11) an offence committed with terrorist intent, preparation of an offence committed with terrorist intent, directing of a terrorist group, promotion of the activity of a terrorist group, provision of training for the commission of a terrorist offence, recruitment for the commission of a terrorist offence, financing of terrorism, as referred to in Chapter 34(a), section 1, subsection 1, paragraphs 2-7 or subsection 2 of the Criminal Code; (12) aggravated damage to property; (13) aggravated fraud, aggravated usury; (14) aggravated counterfeiting; (15) aggravated impairment of the environment; or (16) an aggravated narcotics offence.

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)?
		in connection with commercial or professional activity.[29] […] ”An additional prerequisite to the issuing of the warrant referred to above in subsection 3 is that the offence was committed in order to obtain especially large benefit and the offence has been					

[29] These offences are, as stipulated by Chapter 10, Section 3 of Finland, the Coercive Measures Act (*Pakkokeinolaki/ Tvångsmedelslag*), 806/2011: (1) aggravated giving of a bribe; (2) aggravated embezzlement; (3) aggravated tax fraud, aggravated assistance fraud; (4) aggravated forgery; (5) aggravated dishonesty by a debtor, aggravated dishonesty by a debtor; (6) aggravated taking of a bribe, aggravated abuse of public office; (7) aggravated regulation offence; (8) aggravated abuse of insider information, aggravated market price distortion; or (9) an aggravated customs offence.

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)?
		committed in an especially methodical manner. A warrant for telecommunications interception may also be issued if there are grounds to suspect someone of aggravated pandering in which especially large benefit is sought and the offence has been committed in an especially methodical manner or the offence is one					

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)?
		referred to in Chapter 20, section 9a, subsection 1, paragraph 3 or 4 of the Criminal Code." Section 6 of the Chapter 10 of the Coercive Measures Act further stipulates: "a criminal investigation authority may be issued a warrant for traffic data monitoring of a network address or terminal end device in the possession of or otherwise presumably used					

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)?
		by a suspect in an offence, when there are grounds to suspect said person of" certain offences.[30]					
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)?**
Finland, the Government Decree on pretrial investigations,	*See above, Finland, the Coercive Measures Act*	*See above, Finland, the Coercive Measures Act*	*See above, Finland, the Coercive Measures Act*	*See above, Finland, the Coercive Measures Act (Pakkokeinolaki/*	Section 1 of the Government Decree stipulates that	*Not applicable*	*Not applicable*

[30] These offences are, as stipulated by Chapter 10, Section 6 of Finland, the Coercive Measures Act (*Pakkokeinolaki/ Tvångsmedelslag*), 806/2011: "(1) an offence for which the most severe punishment is imprisonment for at least four years; (2) an offence committed with the use of the network address or terminal end device, for which the most severe punishment provided is imprisonment for at least two years; (3) unauthorized use, damage to property, message interception or computer break-in directed at an automatic data processing system and committed with the use of a network address or terminal end device; (4) exploitation of a person subjected to the sex trade, solicitation of a child for sexual purposes or pandering; (5) a narcotics offence; (6) preparation of an offence committed with terrorist intent; (7) an aggravated customs offence; (8) aggravated concealment of illegally obtained goods; (9) preparation of the taking of a hostage; or (10) preparation of aggravated robbery."

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)?
coercive measures and secret data acquisition (*Valtioneuvoston asetus esitutkinnasta, pakkokeinoista ja salaisesta tiedonhankinnasta / Statsrådets förordning om förundersökning, tvångsmedel och hemligt inhämtande av information*), 122/2014, available at (accessed 7 July 2014): www.finlex.fi/fi/laki/alkup/2014/20140122	*(Pakkokeinolaki/ Tvångsmedelslag), 806/2011*	*(Pakkokeinolaki/ Tvångsmedelslag), 806/2011*	*(Pakkokeinolaki/ Tvångsmedelslag), 806/2011*	*Tvångsmedelslag), 806/2011*	official records must be drafted after the use of a coercive measure has been ended, without delay, at the latest in 30 days. Section 22 of the Decree stipulates that the pre-trial investigation officials must draft a report on the use of secret coercive measures as defined in Chapter 10 of the Coercive Measures Act and secret data acquisition as defined in Chapter 5 of the Police Act. The reports must be delivered once a year to the Ministry of the Interior, the Ministry		

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)?
					of Finance and the Ministry of Defence. These Ministries must present their reports to the Parliamentary Ombudsman each year, by the end of February.		
Finland, the Act on Soldier Discipline and Crime Prevention in the Finnish Defence Forces (*Laki sotilaskurinpidosta ja rikostorjunnasta puolustusvoimissa / Lag om militär*	The act does not enable mass surveillance, however, it contains sections that might contribute to enabling such procedures. Category of	Section 89 of the Act stipulates that the secret surveillance methods can only be used in revealing the following crimes: Endangering the Finnish autonomy; enticement to	Investigating crimes committed among the Finnish Defence Forces, national security.	As stipulated by Section 17 of the Chapter 5 of the Act on the Exercise of Freedom of Expression in Mass Media (*Laki sananvapauden käyttämisestä joukkoviestinnässä/ Lag om yttrandefrihet i*	No steps mentioned other than the requirement to inform the Finnish Security Intelligence Service (*Suojelupoliisi/Skydd spolisen*) about the use of secret data acquisition methods without delay, stipulated by section	Section 89 of the Act stipulates that coercive measures can be used in the geographical area in use of armed forces or in other areas in case the use of coercive measures cannot be postponed or	No, does not allow mass surveillance in any country.

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)?
disciplin och brottsbekämpning inom försvarsmakten), 28.3.2014/255, available at (accessed 7 July 2014): www.finlex.fi/fi/laki/alkup/2014/20140255	persons whose surveillance is enabled under the act are soldiers as defined by the Criminal Code of Finland (*Rikoslaki/Brottslag*), (19.12.1889/39), Chapter 45, Section 27: ”soldier is defined as follows: (1) the regular personnel of the armed forces and the temporary personnel of the	war; treason and aggravated treason; espionage and aggravated espionage; revealing of a national security secret; and unlicensed intelligence activity.		*masskommunikation*) [31], the request by an authority to obtain information required for the identification of the sender of a network message must be decided upon by a court. The Act stipulates: “On the request of an official with the power of arrest, as referred to in chapter 1, section 6(1), of the Coercive Measures Act (450/1987), a public prosecutor, or an injured party, a court may order	89 of the Act on Soldier Discipline and Crime Prevention in the Finnish Defence Forces .	executive assistance from the police is not available shortly.	

[31] Finland, the Act on the Exercise of Freedom of Expression in Mass Media (*Laki sananvapauden käyttämisestä joukkoviestinnässä/ Lag om yttrandefrihet i masskommunikation*) (13.6.2003/460), unofficial translation available at (accessed 21 July 2014): http://finlex.fi/en/laki/kaannokset/2003/en20030460.pdf.

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)?
	armed forces, the latter when appointed to military duties, (2) conscripts performing armed or unarmed national service or those performing the service referred to in section 79 of the National Service Act (1483/2007), and those performing the service referred to in the Act on the Voluntary National Service for Women (194/1995), and (1441/2007)			the keeper of a transmitter, server or other similar device to release the information required for the identification of the sender of a network message to the requester, provided that there are probable reasons to believe that the contents of the message are such that providing it to the public is a criminal offence. […] A court order on the release of identifying information shall be open to appeal as a separate matter. The order			

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)?
	(2)(a) a person serving in voluntary exercises of the armed forces referred to in section 18 of the Voluntary National Defence Act (556/2007) and trainers and a person in command of artillery exercises referred to in section 21 of said act, and (563/2007) (3) cadets being trained for regular service in the armed forces. (2) In addition, the provisions on			shall not be enforced until it has become final, unless the appellate court otherwise orders.”			

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)?
	soldiers apply, as separately provided by law, also to the military personnel of the frontier guard service and to the personnel undergoing crisis management training, engaged in crisis management exercises or performing crisis management service referred to in the Military Crisis Management Act (211/2006). (3) In addition, the provisions of this chapter						

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)?
	apply, as separately provided in the Act on Voluntary National Defence, to volunteers participating in armed forces executive assistance duties, as referred to in section 23 of said Act. (563/2007)						

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*
Act on the Protection of Privacy in Working Life *(Laki yksityisyyden suojasta työelämässä/ Lag om integritetsskydd i arbetslivet, 759/2004)* *www.finlex.fi/en/laki/kaannokset/2004/en20040759.pdf*	Mainly this Act regulates what kind of data employers can collect on their employees and how this data can be used. The Act doesn't list specifically any safeguards against unlawful surveillance. However, it stipulates inter alia in Section 4 on general requirements for collecting personal data about employees and the employer's duty to provide information: "The employer shall collect personal data about the employee primarily from the employee him/herself. In order to collect personal data from elsewhere, **the employer must obtain the consent of the employee**. However, this consent is not required when an authority discloses information to the employer to enable the latter to fulfil a statutory duty or	To all (nationals, EU citizens and third country nationals)	Only inside the country

	when the employer acquires personal credit data or information from the criminal record in order to establish the employee's reliability." **"The employer shall notify the employee in advance that data on the latter is to be collected** in order to establish his/her reliability. If information concerning the employee has been collected from a source other than the employee him/herself, **the employer must notify the employee of this information before it is used in making decisions concerning the employee.** The employer's duty to provide information and the employee's right to check the personal data concerning him/herself are also subject to other relevant provisions of the law. " "The collection of personal data during recruitment and during an employment relationship is governed by the cooperative procedure referred to in the Act on Cooperation within Undertakings (725/1978) and the Act on Cooperation in Government Departments and Agencies (651/1988)." In accordance with the Act Section 21 on cooperation in organizing technical monitoring and data network use: "The purpose and introduction of and methods used in camera surveillance, access control and other technical monitoring of employees, and		

	the use of electronic mail and other data networks, are governed by the cooperative procedure referred to in the Act on Cooperation within Undertakings and the Act on Cooperation in Government Departments and Agencies. In undertakings and in organizations subject to public law that are not governed by the legislation on cooperation, the **employer must, before making decisions on these matters, reserve the employees or their representatives an opportunity to be consulted**." "After the cooperative or consultative procedures, the employer shall determine the purpose of the technical monitoring of employees and the methods used**, and inform employees about the purpose and introduction of and methods used in the monitoring system, and about the use of electronic mail and the data network**."		
Act on the Protection of Privacy in Electronic Communications (*Sähköisen viestinnän tietosuojalaki / Lag om dataskydd vid elektronisk*	In accordance with the Act (chapter 5, section 21a): "If a specific violation or threat is posed to the information security of a service (referred to in section 19), **the telecommunications operator and value added service provider shall immediately notify the subscriber and the user and inform them of the measures available to them for combating the threat, of the probable costs of such measures, and inform**	To all (nationals, EU citizens and third country nationals)	Inside the country

kommunikation, 516/2004) www.finlex.fi/fi/laki/kaannokset/2004/en20040516.pdf From 1 January 2015 Information Society Code, Tietoyhteiskuntakaari, Informationssamhällsbalk. Sections 272, 146-156, 158, 161 http://www.eduskunta.fi/faktatmp/utatmp/akxtmp/ev_106_2014_p.shtml	**the sources of further information available to them**." Moreover, the Act stipulates (Section 13 g – 13 i) that a corporate or association subscriber shall draw up a report of manual processing of identification data. A corporate or association subscriber shall annually inform the Data Protection Ombudsman of manual processing of identification data after the processing has taken place. The report shall reveal the grounds for and the number of times of identification data processing during the year. According to section 14 b a service operator under the retention obligation shall ensure that information about data retention and its purposes is available to the subscriber. Section 17 stipulates that "the telecommunications operator shall ensure that the subscriber can easily and at no separate charge **prohibit processing of location data, unless otherwise provided by law**. The telecommunications operator shall ensure that the subscriber has easy and continuous access to information on the precision of the location data processed, the purpose of the processing and whether location data can be disclosed to a third party for the purpose of providing value added services." General guidance and development for the		

	purpose of implementing this Act is the responsibility of the Ministry of Transport and Communications. The Finnish Communications Regulatory Authority and the Data Protection Ombudsman also supervise the Act.		
Finland, the Act on the Processing of Personal Data by the Police (*Laki henkilötietojen käsittelystä poliisitoimessa/ Lag om behandling av personuppgifter i polisens verksamhet*), 761/2003, unofficial translation available at (accessed 7 July 2014): http://finlex.fi/en/laki/kaannokset/2003/en20030761.pdf	In accordance with the Act, Section 43: "When collecting personal data for the purpose of performing duties (as referred to in section 1(3)) of the Police Act, the police shall be mindful of their obligation to provide information under section 24(1) of the Personal Data Act. This obligation does not apply when the police are collecting, recording or supplying personal data necessary for the performance of duties as referred to in section 1(1) of the Police Act. Section 44 & 45: The provisions of sections 26 and 28 of the Personal Data Act apply to the application of the right of access. The data to be accessed is provided by the file keeper. Restricting the right of access The right of access does not apply in any way to: 1) data in the Suspect Data System; 2) data in the Europol Data System; 3) data in the Operational Data System of the Security Police;	To all (nationals, EU citizens and third country nationals)	Inside the country

	4) data in the National Schengen In formation System in cases as referred to in Article 109(2) of the Schengen Convention; 5) classification, surveillance or modus operandi data concerning persons or acts included in ot her police personal data files." However, at the request of the data subject, the Data Protection Ombudsman may examine the lawfulness of this data that is held on the data subject. The Act stipulates in Section 47: "Everyone has the right to ask the supervisory authority referred to in Article 115 of the Schengen Convention to verify that the collection, recording, processing and utilization of personal data on themselves in the data file maintained by the technical support function of the Schengen Information System occur in a lawful and correct manner. **A request to this effect shall be presented to the Data Protection Ombudsman or the District Police**. The police shall forward any verification request presented to the District Police to the Data Protection Ombudsman without delay.		
Population information Act (*Laki väestötietojärjestelm*	In accordance with the Act (section 75): A written rectification can be sought from the Population Register Centre or the Local Register Offices in a matter related to a	To all (nationals, EU citizens and third country nationals)	Inside the country

ästä ja Väestörekisterikeskuksen varmennepalveluista / Lag om befolkningsdatasystemet och Befolkningsregistercentralens certifikattjänster, 661/2009) www.finlex.fi/fi/laki/ajantasa/2009/20090661	register entry or a disclosure of data.		
Personal Data Act (*Henkilötietolaki/ Personuppgiftslag*, 523/1999) www.finlex.fi/en/laki/kaannokset/1999/en19990523.pdf	Chapter 6 stipulates the data subject´s rights, such as information on the processing of data: "when collecting personal data, **the controller shall see to that the data subject can have information on the controller and, where necessary, the representative of the controller, on the purpose of the processing of the personal data,** on the regular destinations of disclosed data, as well as on how to proceed in order to make use of the rights of the data subject in respect to the processing operation in question." "**Regardless of secrecy provisions, everyone shall have the right of access, after having supplied sufficient search criteria, to the data on him/her in a personal data file**, or to	To all (nationals, EU citizens and third country nationals)	The Act applies to processing of personal data where the controller is established in the territory of Finland or otherwise subject to Finnish law. The Act applies also if the controller is not established in the territory of a Member State of the European Union, but it uses equipment located in Finland in the processing of personal data, except where the equipment is used solely for the transfer of data through the territory. In this case the controller shall designate a representative established in Finland. (Section 4)

	a notice that the file contains no such data. The controller shall at the same time provide the data subject with information of the regular sources of data in the file, on the uses for the data in the file and the regular destinations of disclosed data." There are certain restrictions to right of access. Section 29 stipulates rectification: "The controller shall, on its own initiative **or at the request of the data subject, without undue delay rectify, erase or supplement personal data contained in its personal data file and erroneous, unnecessary, incomplete or obsolete as regards the purpose of the processing. The controller shall also prevent the dissemination of such data, if this could compromise the protection of the privacy of the data subject or his/her rights**." "If the controller refuses the request of a data subject of the rectification of an error, a written certificate to this effect shall be issued. The certificate shall also mention the reasons for the refusal. **In this event, the data subject may bring the matter to the attention of the Data Protection Ombudsman**." "**The controller shall notify the rectification to the recipients to whom the data have been disclosed and to the source of the erroneous personal data**. However, there is		

	no duty of notification if this is impossible or unreasonably difficult." Section 39 stipulates the role of the Data Protection Ombudsman: "**Regardless of confidentiality provisions, the Data Protection Ombudsman has the right of access to personal data which are being processed, as well as all information necessary for the supervision of the legality of the processing of personal data. The Data Protection Board has the same right in matters which it is dealing with.** The Data Protection Ombudsman has the right to inspect personal data files and to assign experts to carry out the inspection." Section 40 stipulates: "**The Data Protection Ombudsman shall promote good processing practice and issue directions and guidelines so as to achieve a situation where unlawful conduct is not continued or repeated.** Where necessary, the Data Protection Ombudsman shall refer the matter to be dealt with by the Data Protection Board, or report it for prosecution. The Data Protection Ombudsman shall decide matters brought to his/her attention by data subjects on the basis of sections 28 and 29. **The Ombudsman may order a controller to realise the right of access of the data subject or to rectify an error**."		

	Section 44 stipulates the role of the Data Protection Board: "At the request of the Data Protection Ombudsman, the Data Protection Board may: prohibit processing of personal data which is contrary to the provisions of this Act or the rules and regulations issued on the basis of this Act; in matters (other than those referred to in section 40), **compel the person concerned to remedy an instance of unlawful conduct or neglect**; order that the operations pertaining to the file be ceased, **if the unlawful conduct or neglect seriously compromise the protection of the privacy of the data subject or his/her interests or rights, provided that the file is not set up under a statutory scheme**; a revoke a permission referred to in section 43, where the prerequisites for the same are no longer fulfilled or the controller acts against the permission or the rules attached to it."		
Act on the Openness of Government Activities ,621/1999 (*Laki viranomaisten toiminnan julkisuudesta / Lag om offentlighet i myndigheternas verksamhet*) www.finlex.fi/en/laki/kaannokset/1999/en19990	Chapter 3 stipulates the right of access to a document. Everyone shall have the right of access to an official document in the public domain. No access to a secret document or its contents shall be granted. However, there are some exceptions. A petitioner, an appellant and any other person whose right, interest or obligation in a matter is concerned (a party) shall also have the right of	To all (nationals, EU citizens and third country nationals)	Inside the country

621.pdf	access, to be granted by the authority which is considering or has considered the matter, to the contents of a document which is not in the public domain, if they may influence or may have influenced the consideration of his/her matter. There are certain restrictions to applying this section. Unless otherwise provided in an Act, every individual shall have the right of access to information contained in an official document and pertaining to themselves, subject to the restrictions provided in this Act.		

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 ongoing/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.*
Data Protection ombudsman (*Tietosuojavaltuutettu/Dataombudsmannen*)	The Office of the Data Protection Ombudsman is an independent authority operating in connection with the Ministry of Justice.	The Government Decree on the Data Protection Board and the Data Protection Ombudsman (*Asetus tietosuojalautakunnasta ja tietosuojavaltuutetusta/ Förordning om datasekretessnämnden och dataombudsman*	The Data Protection Ombudsman provides direction and guidance on the processing of personal data, supervises the processing in order to achieve the objectives of the Personal Data Act (523/1999), as well as makes decisions concerning right of access and rectification.[34]	The office is run by the Data Protection Ombudsman, appointed by the Council of State for a term of five years. Reijo Aarnio has been the Data Protection Ombudsman since November 1, 1997. The deputy and assistant to the Ombudsman is Head of Department. The total number of staff is 20.[35]	The Data Protection Ombudsman guides and controls the processing of personal data and provides related consultation and exerts power in issues related to the implementation of the right of verification and the correction of personal data. The Ombudsman also follows the general development in the processing of personal data, launching initiatives if necessary.

		nen) (3.6.1994/432)[32] and the Act on the Data Protection Board and the Data Protection Ombudsman (*Laki tietosuojalautakunnasta ja tietosuojavaltuutetusta/ Lag om datasekretessnämnden och dataombudsmannen*) (27.5.1994/389) [33]			In addition to general guidance, the Data Protection Ombudsman provides controllers and data subjects with guidance and advice on request, and makes decisions pertaining to the compliance with legislation and implementation of the rights of data subjects. In matters concerning the implementation of the right of verification and the correction of personal data, the decisions of the Ombudsman are binding and subject to appeal. The Data Protection Ombudsman provides statements and participates

[34] Information retrieved from the website of Finland, Ministry of Justice (*Oikeusministeriö/Justitieministeriet*), available at (all hyperlinks accessed 9.7.2014): http://oikeusministerio.fi/en/index/theministry/neuvottelu-jalautakunnat/thefinnishdataprotectionboard.html.

[35] Information retrieved from the website of Finland, Data Protection Data Protection ombudsman (*Tietosuojavaltuutettu/Dataombudsmannen*) available at (all hyperlinks accessed 9.7.2014): www.tietosuoja.fi/en/index.html.

[32] Finland, The Goverment Decree on the Data Protection Board and the Data Protection Ombudsman (*Asetus tietosuojalautakunnasta ja tietosuojavaltuutetusta/ Förordning om datasekretessnämnden och dataombudsmannen*) (3.6.1994/432), available at (all hyperlinks accessed 9 July 2014): www.finlex.fi/sv/laki/ajantasa/1994/19940432.

[33] Finland, The Act on the Data Protection Board and the Data Protection Ombudsman (*Laki tietosuojalautakunnasta ja tietosuojavaltuutetusta/ Lag om datasekretessnämnden och dataombudsmannen*) (27.5.1994/389), available at (all hyperlinks accessed 9 July 2014): www.finlex.fi/fi/laki/ajantasa/1994/19940389.

					in working groups set up for the preparation and review of legislation and administrative reforms concerning the protection of personal rights and freedoms in the processing of personal data.[36]

[36] Information retrieved from the website of Finland, Data Protection Data Protection ombudsman (*Tietosuojavaltuutettu/Dataombudsmannen*) available at (all hyperlinks accessed 9.7.2014): www.tietosuoja.fi/en/index/tietosuojavaltuutetuntoimisto/duties.html.

Data Protection Board (*Tietosuojalautakunta/Datasekretessnämnden*)	independent authority affiliated to the Ministry of Justice	The Government Decree on the Data Protection Board and the Data Protection Ombudsman (*Asetus tietosuojalautakunnasta ja tietosuojavaltuutetusta/ Förordning om datasekretessnämnden och dataombudsmannen*) (3.6.1994/432)[37] and the Act on the Data Protection Board and the Data Protection Ombudsman (*Laki tietosuojalautak*	**ex ante, ex post, regular** The Data Protection Board deals with questions of principle relating to the processing of personal data, where these are significant to the application of the Personal Data Act. The Board also has the power to grant permissions and issue orders.[39]	The Data Protection Board is appointed by the Council of State for three years at a time. The current board consists of 5 members, vice president, president and a secretary.[40]	At the request of the Data Protection Ombudsman, The Data Protection Board may: prohibit processing of personal data which is contrary to the provisions of the Personal Data Act or the rules and regulations issued on the basis of the Act; in matters other than those concerning right of access or rectification, compel the person concerned to remedy an instance of unlawful conduct or neglect; order that the operations pertaining to the file be ceased, if the unlawful conduct or neglect seriously compromise the protection of the privacy of the data subject or his/her interest or rights, provided that the file is not set up under a statutory scheme; and

[37] Finland, The Goverment Decree on the Data Protection Board and the Data Protection Ombudsman (*Asetus tietosuojalautakunnasta ja tietosuojavaltuutetusta/ Förordning om datasekretessnämnden och dataombudsmannen*) (3.6.1994/432), available at: www.finlex.fi/sv/laki/ajantasa/1994/19940432.

[39] Information retrieved from the website of Finland, Ministry of Justice (*Oikeusministeriö/Justitieministeriet)*.

[40] Information retrieved from the website of Finland, Ministry of Justice (*Oikeusministeriö/Justitieministeriet*), available at (all hyperlinks accessed 9.7.2014): http://oikeusministerio.fi/fi/index/ministerio/neuvottelu-jalautakunnat/tietosuojalautakunta/kokoonpano.html

		unnasta ja tietosuojavaltuutetusta/ Lag om datasekretessnämnden och dataombudsmannen) (27.5.1994/389) [38]			revoke a permission granted by the Board, where the prerequisites for the same are not longer fulfilled or the controller acts against the permission or the rules attached to it.[41]
The Parliamentary Ombudsman (*Eduskunnan oikeusasiamies/ riksdagens justitieombudsman*)	independent, appointed by the Parliament	The Parliamentary Ombudsman Act (*Laki eduskunnan oikeusasiamiehestä/ Lag om riksdagens justitieombudsman*) (14.3.2002/197) [42] and The act on the division of the obligations between the Chancellor of	**ex post, regular** The Parliamentary Ombudsman exercises oversight to ensure that public authorities and officials observe the law and fulfil their duties in the discharge of their functions. The Ombudsman oversees legality	The parliamentary ombudsman, the Deputy-Ombudsman and the second Deputy-Ombudsman are elected for four-year terms, which may be renewed, by the Eduskunta, the parliament of Finland. Total number of staff is 59. The ombudsman and the deputy-ombudsmen manage three sub-sections of the office, and the administrative manager manages the administration sub-section.	The Ombudsman provides the Parliament (*Eduskunta/Riksdagen*) with an annual report on activities and observations in the preceding year. The Ministry of Defence (*puolustusministeriö/försvarsministeriet*) has reporting obligation to the Parliamentary Ombudsman over the use of secret data acquisition and tele surveillance in the armed forces, the Ministry of the

[38] Finland, The Act on the Data Protection Board and the Data Protection Ombudsman (*Laki tietosuojalautakunnasta ja tietosuojavaltuutetusta/ Lag om datasekretessnämnden och dataombudsmannen*) (27.5.1994/389), available at: www.finlex.fi/fi/laki/ajantasa/1994/19940389

[41] Information retrieved from the website of Finland, Ministry of Justice (*Oikeusministeriö/Justitieministeriet)*.

[42] Finland, the Parliamentary Ombudsman Act (*Laki eduskunnan oikeusasiamiehestä/ Lag om riksdagens justitieombudsman*) (14.3.2002/197), unofficial translation available at (accessed 9 July 2014): www.finlex.fi/en/laki/kaannokset/2002/en20020197.pdf.

		Justice of the Government and the Parliamentary Ombudsman (*Laki valtioneuvoston oikeuskanslerin ja eduskunnan oikeusasiamiehen tehtävien jaosta/Lag om fördelningen av åligganden mellan justitiekanslern i statsrådet och riksdagens justitieombudsman*) (21.12.1990/1224)[43]	principally by examining complaints received. He can also intervene in perceived shortcomings on his own initiative. In addition, the Ombudsman carries out inspections at offices and institutions, especially prisons, military garrisons and other closed institutions in order to oversee the treatment of prisoners, persons confined to institutions, conscripts doing their national service and peacekeeping personnel.[44]	In addition to the permanent staff, during 2013, 8 persons worked under part-time or terminable contracts.[45]	Interior (*sisäasiainministeriö/inrikesministeriet*) in the police, and the Ministry of Finance (*valtiovarainministeriö/finansministeriet*) in customs.

[43] Finland, The Act on the Division of the Obligations between the Chancellor of Justice of the Government and the Parliamentary Ombudsman (*Laki valtioneuvoston oikeuskanslerin ja eduskunnan oikeusasiamiehen tehtävien jaosta/Lag om fördelningen av åligganden mellan justitiekanslern i statsrådet och riksdagens justitieombudsman*) (21.12.1990/1224) available at (accessed 9 July 2014): www.finlex.fi/fi/laki/ajantasa/1990/19901224.

[44] Information retrieved from the website of Finland, the Parliamentary Ombudsman (*Eduskunnan oikeusasiamies/ riksdagens justitieombudsman*), available at (accessed 10 July 2014): www.oikeusasiamies.fi/Resource.phx/eoa/english/ombudsman/tasks/index.htx.

The Chancellor of Justice (*Oikeuskansleri/ Justitiekanslern*)	independent, in connection with the government	the Act on the Chancellor of Justice of the Government (*Laki valtioneuvoston oikeuskanslerista/Lag om justitiekanslern i statsrådet*) (25.2.2000/193)[46] and The act on the division of the obligations between the Chancellor of Justice of the Government and	Handling of complaints as well as observations made through inspections and otherwise. The duty to oversee the realisation of fundamental and human rights is also embedded in the Chancellor of Justice's activities pertaining to the supervision of the Government's decision-making processes.[48]	The President of the Republic appoints the Chancellor of Justice and Deputy Chancellor of Justice, and names the substitute for the Deputy Chancellor of Justice. An assignment to serve as substitute to the Deputy Chancellor of Justice is temporary, with a maximum term of five years.[49] The office of the Chancellor of Justice has 37 permanent positions, of which 3 are the directors (the Chancellor of Justice, the Deputy, and the head of secretariat) and 2 in other managing positions.[50]	The Chancellor of Justice supervises the authorities by handling any written complaints arising from their actions. A complaint may be filed with the Chancellor of Justice if the complainant believes that an authority, civil servant or public official or other person or body assigned to perform public tasks has acted in an unlawful manner, otherwise wrongfully or failed to fulfil their responsibilities. The Chancellor of Justice can also open an investigation on an issue on

[45] Finland, the Parliamentary Ombudsman (*Eduskunnan oikeusasiamies/ riksdagens justitieombudsman*) (2014), *Eduskunnan oikeusasiamiehen kertomus vuodelta 2013*, Vammalan kirjapaino: Sastamala, page 56, available at (accessed 10 July 2014): www.oikeusasiamies.fi/dman/Document.phx?documentId=hh16114123723149&cmd=download.

[46] Finland, the Act on the Chancellor of Justice of the Government (*Laki valtioneuvoston oikeuskanslerista/Lag om justitiekanslern i statsrådet*) (25.2.2000/193), available at (all hyperlinks accessed 9 July 2014): www.finlex.fi/fi/laki/ajantasa/2000/20000193.

[48] Information retrieved from the website of Finland, The Chancellor of Justice (*Oikeuskansleri/ Justitiekanslern*), available at (all hyperlinks accessed 10 July 2014): www.oikeuskansleri.fi/en/.

[49] Information retrieved from the website of Finland, The Chancellor of Justice (*Oikeuskansleri/ Justitiekanslern*), available at: www.oikeuskansleri.fi/en/.

[50] Finland, the Chancellor of Justice (*Oikeuskansleri/ Justitiekanslern*) (2013), *Oikeuskanslerinviraston toiminta- ja taloussuunnitelma vuosille 2015-2018 sekä tulossuunnitelma vuodelle 2014*, page 18. Available at (accessed 24 July 2014): www.oikeuskansleri.fi/media/uploads/talousasiakirjat/toiminta-_ja_taloussuunnitelma_vuosille_2015_2018.pdf.

		the Parliamentary Ombudsman (*Laki valtioneuvoston oikeuskanslerin ja eduskunnan oikeusasiamiehen tehtävien jaosta/Lag om fördelningen av åligganden mellan justitiekanslern i statsrådet och riksdagens justitieombudsman*) (21.12.1990/1224) [47]			his own initiative, such as matters brought forth in the media. The Chancellor of Justice is entitled to perform inspections of those authorities, institutions, offices and other units that fall within the scope of his supervisory authority.[51] The Chancellor of Justice does not usually handle complaints concerning the Defence Forces or deprivation of liberty, as these belong under the mandate of the Parliamentary Ombudsman.
Name of the body/mechanism	**Type of the body/mechanism**	**Legal basis**	**Type of oversight**	**Staff**	**Powers**

[47] Finland, The Act on the Division of the Obligations between the Chancellor of Justice of the Government and the Parliamentary Ombudsman (*Laki valtioneuvoston oikeuskanslerin ja eduskunnan oikeusasiamiehen tehtävien jaosta/Lag om fördelningen av åligganden mellan justitiekanslern i statsrådet och riksdagens justitieombudsman*) (21.12.1990/1224).

[51] Information retrieved from the website of Finland, The Chancellor of Justice (*Oikeuskansleri/ Justitiekanslern*), available at: www.oikeuskansleri.fi/en/.

The National Police Board (*Poliisihallitus/Polisstyrelsen*)	government	The Act on Police Administration (*Laki poliisin hallinnosta/Polisförvaltningslag*), (14.2.1992/110) [52]	Police units report yearly to the Police Board on their use of coercive measures and secret intelligence functions.	Total number of staff 235, 29 in managing positions. The legality control unit has total staff 8, 1 of which in a managing position.[53]	Reporting obligation to the Ministry of the Interior (*Sisäasiainministeriö/Inrikesministeriet*). The head of the National Police Board is the head of the Finnish police force.
The Follow-up Group on Secret Data Acquisition (*Salaisen tiedonhankinnan seurantaryhmä*)	appointed by the National Police Board (*Poliisihallitus/Polisstyrelsen*)	Finland, the Government Decree on pretrial investigations, coercive measures and secret data acquisition (*Valtioneuvoston asetus esitutkinnasta, pakkokeinoista ja salaisesta tiedonhankinnasta/ Statsrådets förordning om förundersökning*	Section 21 of Chapter 3 of the Government Decree on pretrial investigations, coercive measures and secret data acquisition stipulates that the tasks of the group are: Follow-up of functions, education and cooperation, reporting issues concerning legality control to the National Police Board, presenting	In 2013, the group consisted of a representative of the police, representative of the judicial system appointed by the Ministry of Justice (*Oikeusministeriö/Justitieministeriet*), representative of the Prosecution Service (*Syyttäjänvirasto/Åklagarämbetet*) appointed by the National Prosecution Service (*Valtakunnansyyttäjäcvirasto/ Riksåklagarämbetet*), representative of the Customs (*Tulli/Tull*) appointed by the National Board of Customs	Recommendations, reporting obligation to the Parliamentary Ombudsman

[52] The Act on Police Administration (*Laki poliisin hallinnosta/Polisförvaltningslag*), (14.2.1992/110), available at (accessed 14 July 2014): www.finlex.fi/fi/laki/ajantasa/1992/19920110.

[53] Copmmunications with Finland, the National Police Board 21 July 2014, by correspondence, letter titled "The staff of the National Police Board (*Poliisihallituksen henkilöstömäärät, POL-2014-9130*)", signed by the head of staff of the National Police Board, Tiina Eränkö.

		, tvångsmedel och hemligt inhämtande av information), 122/2014[54], Section 21.	development suggestions, and preparing a comprehensive report on surveillance statements to the Parliamentary Ombudsman.	(*Tullihallitus/Tullstyrelsen*) and a representative of the Finnish Border Guard (*Rajavartiolaitos/Gränsbevakningsväsendet*) appointed by their headquarters.[55]	
Ministry of the Interior (*Sisäasiainministeriö/Inrikesministeriet*)	government	The Act on Police Administration (*Laki poliisin hallinnosta/Polisförvaltningslag*), (14.2.1992/110) [56] and Finland, the Government Decree on	The Police Board reports yearly to the Ministry of the Interior on the use of coercive measures and secret intelligence functions in the police.[58] This report is also delivered to the Parliamentary	The police unit of the Ministry of the Interior, total number of staff in 2013 was 178, and 23 additional in projects. [59]	Section 1 of the Act on Police Administration stipulates that the Ministry of the Interior is responsible over the steering and supervision of the functions of the police. The Ministry of the Interior steers the National Police Board.

[54] Finland, the Government Decree on pretrial investigations, coercive measures and secret data acquisition (*Valtioneuvoston asetus esitutkinnasta, pakkokeinoista ja salaisesta tiedonhankinnasta/ Statsrådets förordning om förundersökning, tvångsmedel och hemligt inhämtande av information*), 122/2014, available at (accessed 7 July 2014): www.finlex.fi/fi/laki/alkup/2014/20140122.

[55] Finland, the National Police Board (*Poliisihallitus/Polisstyrelsen*) (2014), The Annual Accounts of the National Police Board 2013 (*Poliisihallituksen tilinpäätös vuodelta 2013)*, POL-2014-513, page 27.

[56] Finland, the Act on Police Administration (*Laki poliisin hallinnosta/Polisförvaltningslag*), (14.2.1992/110), available at (accessed 14 July 2014): www.finlex.fi/fi/laki/ajantasa/1992/19920110.

[58] Finland, the National Police Board (*Poliisihallitus/Polisstyrelsen*) (2014), *Poliisihallituksen selvitys Sisäasiainministeriölle poliisin tiedonhankinnasta ja sen valvonnasta 2013*, POL-2014-30. Available at (all hyperlinks accessed 14 July 2014): http://poliisi.fi/poliisi/home.nsf/files/8E2337E98D525CF2C2257CA00029F00B/$file/Allekirjoitettu%20toimintakertomus%202013.pdf.

[59] Finland, the National Police Board (*Poliisihallitus/Polisstyrelsen*) (2014), The Annual Accounts of the National Police Board 2013 (*Poliisihallituksen tilinpäätös vuodelta 2013)*, POL-2014-513.

		pretrial investigations, coercive measures and secret data acquisition (*Valtioneuvoston asetus esitutkinnasta, pakkokeinoista ja salaisesta tiedonhankinnasta/ Statsrådets förordning om förundersökning, tvångsmedel och hemligt inhämtande av information*), 122/2014[57]	Ombudsman (*Eduskunnan oikeusasiamies/ riksdagens justitieombudsman*).		

[57] Finland, the Government Decree on pretrial investigations, coercive measures and secret data acquisition (*Valtioneuvoston asetus esitutkinnasta, pakkokeinoista ja salaisesta tiedonhankinnasta/ Statsrådets förordning om förundersökning, tvångsmedel och hemligt inhämtande av information*), 122/2014, available at (accessed 7 July 2014): www.finlex.fi/fi/laki/alkup/2014/20140122.

Annex 3 – Remedies[60]

Act on the Protection of Privacy in Electronic Communications (*Sähköisen viestinnän tietosuojalaki/ Lag om dataskydd vid elektronisk kommunikation*) (516/2004) and Information Society Code, Tietoyhteiskuntakaari, Informationssamhällsbalk. Sections 157, 158				
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.*

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

Collection*	Yes with exceptions[61] (information must be made available to the client of a teleoperator about the storing and use of the information (Section 14b).	Yes (section 26 of the Personal data act (*Henkilötietolaki/Personuppgiftslag*))	Remedies described in the Personal data act (*Henkilötietolaki/Personuppgiftslag*), 22.4.1999/523, see below. The authority supervising the compliance with this Act is for the most part the Finnish Communications Regulatory Authority (*Viestintävirasto/Kommunikationsverket*) as stipulated by section 31 of the Act on the Protection of Privacy in Electronic Communications. Location data and right to be informed are supervised by the Data Protection Ombudsman (*Tietosuojavaltuutettu/Dataombudsmannen*) as stipulated by section 32 of the Act on the Protection of	the Personal data act (*Henkilötietolaki/Personuppgiftslag*), 22.4.1999/523 Section 41 of the Act on the Protection of Privacy in Electronic Communications stipulates that when some party does not comply with this law, the Finnish Communications Regulatory Authority and the Data Protection Ombudsman can oblige the party to correct their mistakes. They can order penalty payments or penalties in the form of discontinuation of the operations of the transgressor. The supervising bodies can also proceed to take the case further to pre-trial

* 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

[61] Finland, Personal data act (*Henkilötietolaki/Personuppgiftslag*), 22.4.1999/523, section 24: "The duty of providing information […]may be derogated from: (1) if the data subject already has the relevant information; (2) if this is necessary for the protection of national security, defence or public order or security, for the prevention or investigation of crime or for carrying out the monitoring function pertaining to taxation or the public finances; or (3) where the data are collected from elsewhere than the data subject, if the provision of the information to the data subject is impossible or unreasonably difficult, or if it significantly damages or inconveniences the data subject or the purpose of the processing of the data and the data are not used when making decisions relating to the data subject, or if there are specific provisions in an Act on the collection, recording or disclosure of the data."

			Privacy in Electronic Communications. [62]	investigation.

[62] Finland, information retrieved from the website of the Data Protection Ombudsman, available at (accessed 22 July 2014): /www.tietosuoja.fi/fi/index/lait/sahkoisenviestinnantietosuojalaki.html.

Analysis*	Yes with exceptions[63] (information must be made available to the client of a teleoperator about the storing and use of the information (Section 14b).			
Storing*	Yes with exceptions[64] (information must be made available to the client of a teleoperator about the			

[63] Finland, Personal data act (*Henkilötietolaki/Personuppgiftslag*), 22.4.1999/523, section 24: "The duty of providing information […]may be derogated from: (1) if the data subject already has the relevant information; (2) if this is necessary for the protection of national security, defence or public order or security, for the prevention or investigation of crime or for carrying out the monitoring function pertaining to taxation or the public finances; or (3) where the data are collected from elsewhere than the data subject, if the provision of the information to the data subject is impossible or unreasonably difficult, or if it significantly damages or inconveniences the data subject or the purpose of the processing of the data and the data are not used when making decisions relating to the data subject, or if there are specific provisions in an Act on the collection, recording or disclosure of the data."

[64] Finland, Personal data act (*Henkilötietolaki/Personuppgiftslag*), 22.4.1999/523, section 24: "The duty of providing information […]may be derogated from: (1) if the data subject already has the relevant information; (2) if this is necessary for the protection of national security, defence or public order or security, for the prevention or investigation of crime or for carrying out the monitoring function pertaining to taxation or the public finances; or (3) where the data are collected from elsewhere than the data subject, if the provision of the information to the data subject is impossible or unreasonably difficult, or if it significantly damages or inconveniences the data subject or the purpose of the processing of the data and the data are not used when making decisions relating to the data subject, or if there are specific provisions in an Act on the collection, recording or disclosure of the data."

	storing and use of the information (Section 14b).			
Destruction *	The Act doesn't specifically stipulate on the informing on the destruction of information but the general processing provisions apply After processing, identification data must be destroyed or rendered such that they cannot be associated with the subscriber or user involved, unless otherwise provided by law (section 8).			

After the whole surveillance process has ended			The authority supervising the compliance with this Act is for the most part Finnish Communications Regulatory Authority (*Viestintävirasto/Kommunikationsverket*) as stipulated by section 31 of the Act on the Protection of Privacy in Electronic Communications. Location data and right to be informed are supervised by the Data Protection Ombudsman (*Tietosuojavaltuutettu/Dataombudsmannen*) as stipulated by section 32 of the Act on the Protection of Privacy in Electronic Communications. [65]	

[65] Finland, information retrieved from the website of the Data Protection Ombudsman, available at (accessed 22 July 2014): /www.tietosuoja.fi/fi/index/lait/sahkoisenviestinnantietosuojalaki.html.

Finland, the Coercive Measures Act (*Pakkokeinolaki/ Tvångsmedelslag*), 806/2011				
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, as stipulated by section 60 of the Coercive Measures Act.*[66]	*Yes, as stipulated by section 62 of the Coercive Measures Act.*[67]	*Remedies available as described in the Personal Data Act, see below.* The individual concerned can file an administrative complaint to the National Police Board. The	According to section 65 of the Coercive Measures Act, supervision of the application of covert coercive measures is divided between the following

* 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

[66] Finland, the Coercive Measures Act (Pakkokeinolaki/ Tvångsmedelslag), 806/2011, Section 60: "Written notice shall be given without delay to the suspect concerning telecommunications interception, the obtaining of data other than through telecommunications interception, traffic data monitoring, extended surveillance, covert collection of intelligence, technical surveillance and controlled delivery directed at him or her, after the matter has been submitted to the consideration of the prosecutor or the criminal investigation has otherwise been terminated or interrupted. However, the suspect shall be informed at the latest within one year of the termination of the use of a coercive measure."

[67] Finland, the Coercive Measures Act (*Pakkokeinolaki/ Tvångsmedelslag*), 806/2011, Section 62: "When the notice referred to in section 60 has been made, the person referred to in subsection 1 has the right to obtain information on a document or recording connected with the use of a covert coercive measure, unless it is necessary to not release this in order to ensure the security of the state or to protect life, health or privacy, or tactical and technical procedures that are to

			authority can then, if the actions are deemed blameworthy, give a notice to the authority. If the Police Board deems that an offence in office has been committed, the case is transferred to be considered by the Prosecution Office. The head of investigation to police matters is always the prosecutor.[68]	bodies: (1) The National Police Board and the chiefs of units using covert coercive measures supervise the use of covert coercive measures on the part of the police. (2) The Ministry of the Interior shall submit an annual report to the Parliamentary Ombudsman on the use and supervision of covert coercive measures and their protection. The Pre-trial Investigations Act (*Esitutkintalaki/Förunderskning slag*), 805/2011 and the Administration Act (*Hallintolaki/Förvaltningslag*), 6.6.2003/434 stipulate on the administrative complaints and criminal investigations on the conduct of the police.

be kept secret. When deciding on non-release of a document, recording or information, consideration shall be given to the right of the person referred to in subsection 1 to a proper defence or otherwise to appropriately secure his or her rights in court proceedings."

[68] Information retrieved from the website of Finland, the Police, available at (accessed 23 July 2014): www.poliisi.fi/poliisi/home.nsf/pages/6AD3C71197005F3DC2256BC1003FFD3B?opendocument.

Analysis*	The Act doesn't specifically stipulate on the informing on the analysis, storing nor destruction of the information.			
Storing*				
Destruction *				
After the whole surveillance process has ended				

Finland, the Act on Soldier Discipline and Crime Prevention in the Finnish Defence Forces (*Laki sotilaskurinpidosta ja rikostorjunnasta puolustusvoimissa/ Lag om militär disciplin och brottsbekämpning inom försvarsmakten*), 28.3.2014/255

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, as stipulated by section 60 of the Coercive Measures Act.[69]	No. Section 123 of the Act on Soldier Discipline and Crime Prevention in the Finnish Defence Forces stipulates that the individual does not have access to data in the security information register or	Section 2 of the Act on Soldier Discipline and Crime Prevention in the Finnish Defence Forces stipulates that crime prevention among the armed forces is regulated by the Police Act (872/2011), the Pre-trial Investigations Act (805/2011) and the Coercive Measures Act (806/2011) unless otherwise	Section 128 of chapter 12 titled Supervision stipulates that the records on the use of coercive measures, drafted as per the obligation laid down in the Act, must be delivered to the Ministry of Defence. Ministry of Defence must be notified about all matters concerning crime prevention among the armed

* 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

[69] Finland, the Coercive Measures Act (Pakkokeinolaki/ Tvångsmedelslag), 806/2011, Section 60: "Written notice shall be given without delay to the suspect concerning telecommunications interception, the obtaining of data other than through telecommunications interception, traffic data monitoring, extended surveillance, covert collection of intelligence, technical surveillance and controlled delivery directed at him or her, after the matter has been submitted to the consideration of the prosecutor or the criminal investigation has otherwise been terminated or interrupted. However, the suspect shall be informed at the latest within one year of the termination of the use of a coercive measure."

		temporary person register. However, the Data Protection Ombudsman can access this data by request from the registered person in order to inspect its legality.	specified.	forces that are societally or economically significant or otherwise of importance. Furthermore, section 129 stipulates that the Ministry of Defence must deliver yearly a report on the use and supervision of coercive measures. This report shall be delivered to the Finnish Security Intelligence Service (*Suojelupoliisi/Skyddspolisen*) as well.

Analysis*	The Act doesn't specifically stipulate on the informing on the analysis, storing nor destruction of the information.			
Storing*				
Destruction *				
After the whole surveillance process has ended				

Personal Data 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 (some exceptions* Personal Data Act, Section 24: "The duty of providing information[70], may be derogated from: (1) if the data subject already has the relevant information; (2) if this is necessary for the protection of national security, defence or public order or security, for the prevention or investigation of crime or for carrying out the monitoring function pertaining to taxation or the public finances; or	*Yes (some exceptions)* Personal Data Act, Section 27: There is no right of access, as referred to in section 26[71]: (1) if providing access to the data could compromise national security, defence or public	The Data Protection Ombudsman has the right of access to personal data which are being processed, as well as all information necessary for the supervision of the legality of the processing of personal data. Where necessary, the Data Protection Ombudsman shall refer the matter to be dealt with by the Data Protection Board, or report it for prosecution The Data Protection Board has the same right in matters which it is dealing with. At the request of the Data Protection Ombudsman, the Data Protection Board may: prohibit processing of personal data which is contrary to the provisions of this Act or the rules and regulations issued on the basis of this Act; in matters (other than those referred to in section 40), compel the person concerned to remedy an instance of unlawful conduct or neglect; order that the operations pertaining to the file be ceased, if the unlawful	(Violation of data protection) The Data Protection Ombudsman provides direction and guidance on the processing of personal data, supervises the processing in order to achieve the objectives of this Act, as well as makes decisions, as provided in this Act. The Data Protection Board deals with questions of principle relating to the processing of personal data, where these are

* 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

[70] Data Protection Act, Section 24:
"When collecting personal data, the controller shall see to that the data subject can have information on the controller and, where necessary, the representative of the controller, on the purpose of the processing of the personal data, on the regular destinations of disclosed data, as well as on how to proceed in order to make use of the rights of the data subject in respect to the processing operation in question. This information shall be provided at the time of collection and recording of the data or, if the data are obtained from elsewhere than the data subject and intended for disclosure, at the latest at the time of first disclosure of the data."

[71] Personal Data Act, Section 26:
"Regardless of secrecy provisions, everyone shall have the right of access, after having supplied sufficient search criteria, to the data on him/her in a personal data file, or to a notice that the file contains no such data. The controller shall at the same time provide the data subject with information of the regular sources of data in the file, on the uses for the data in the file and the regular destinations of disclosed data. Where an automated decision referred to in section 31 is involved, the data subject shall also have the right of access to information on the operating principles of the pertinent automatic processing of data.

	(3) here the data are collected from elsewhere than the data subject, if the provision of the information to the data subject is impossible or unreasonably difficult, or if it significantly damages or inconveniences the data subject or the purpose of the processing of the data and the data are not used when making decisions relating to the data subject, or if there are specific provisions in an Act on the collection, recording or disclosure of the data.”	order or security, or hinder the prevention or investigation of crime; (2) if providing access to the data would cause serious danger to the health or treatment of the data subject or to the rights of someone else; (3) if the data in the file are used solely for historical or scientific research or statistical purposes; or (4) if the personal data in the file are used in the carrying out of monitoring	conduct or neglect seriously compromise the protection of the privacy of the data subject or his/her interests or rights, provided that the file is not set up under a statutory scheme; a revoke a permission (referred to in section 43), where the prerequisites for the same are no longer fulfilled or the controller acts against the permission or the rules attached to it.	significant to the application of this Act, as well as makes decisions in matters of data protection, as provided in this Act. The penalty for a personal data offence is provided in The Finnish Criminal Code.

		or inspection functions and not providing access to the information is indispensable in order to safeguard an important economic interest or financing position of Finland or the European Union. If only a part of the data on a data subject is such that it falls within the restriction on the right of access provided in paragraph (1), the data subject shall have the right of access to the remainder of the data.		

Analysis*	*Yes (some exceptions)* See above Personal Data Act, Sections 24, 26 and 27.In accordance with the Personal Data Act the processing of personal data means the collection, recording, organisation, use, transfer, disclosure, storage, manipulation, combination, protection, deletion and erasure of personal data, as well as other measures directed at personal data.			
Storing*	Yes (some exceptions) See above: Analysis			
Destruction*	Yes (some exceptions) See above: Analysis			
After the whole surveillance process has ended	Yes (some exceptions) See above: Analysis			

Act on the Processing of Personal Data by the Police				
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, in accordance with the Personal Data Act (chapter 6)*	*Yes (some exceptions)* The right of access does not apply in any way to: 1) data in the Suspect Data System; 2) data in the Europol Data System; 3) data in the Operational Data System of the Security Police; 4) data in the National Schengen In formation System in cases as referred to in Article 109(2) of the Schengen Convention; 5) classification, surveillance or modus operandi data concerning persons or acts included in other police personal data files."	*The Data Protection Ombudsman can examine the lawfulness of the data that is held on the data subject*	

[*] 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

		However, at the request of the data subject, the Data Protection Ombudsman may examine the lawfulness of this data that is held on the data subject.		
Analysis*	The Act doesn't specifically stipulate on the informing on the analysis, storing nor destruction of the information.			
Storing*				
Destruction*				
After the whole surveillance process has ended				

Annex 4 – Surveillance-related case law at national level

Please provide a maximum 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	Helsingin HO 21.3.2014 Helsinki Court of Appeal 21.3.2014
Decision date	21 March 2014
Reference details (type and title of court/body; in original language and English [official translation, if available])	Helsingin HO 21.3.2014 Helsinki Court of Appeal 21.3.2014 www.finlex.fi/fi/oikeus/ho/2014/helho20140001
Key facts of the case (max. 500 chars)	The District Court of Helsinki granted a permission for telecommunications interception and electronic surveillance of suspect A´s subscriber connection and a company Y´s subscriber connection. The person A made a complaint to the Court of Appeal and argued that there are no legitimate grounds for telecommunications interception and electronic surveillance.
Main reasoning/argumentation (max. 500 chars)	The Helsinki Court of Appeal overruled the decision of the District Court and concluded that the telecommunications interception and electronic surveillance must be targeted at a specific person that is under coercive measures in order to investigate a suspicion of a crime involving this specific person. The Court of Appeal stated that according to the application for a permission of a warrant for telecommunications interception made to the District Court the intention of the coercive measures targeted at person A was to investigate a crime committed by another person. Thus, there were no legitimate grounds for the use of coercive measures targeted at person A.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	The permission for the use of coercive measures, telecommunications interception and electronic surveillance, can be only used to obtain information of a suspicion of a crime involving this specific person who is subject to the coercive measures. If another person is under a suspicion the coercive measures must be targeted directly at him/her.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The Helsinki Court of Appeal overruled the decision of the District Court to grant a permission for telecommunications interception and electronic surveillance. There is no information on the sanctions. Part of the information on the case has been declared classified.

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**
The Finnish Defence forces: Finnish Defence Intelligence Agency (*Puolustusvoimien tiedustelulaitos/ Försvarsmaktens underrättelsetjänst*)	Public authority	Finnish Defence Intelligence Agency/ Puolustusvoimien tiedustelulaitos PL 1, 00161 Helsinki kirjaamo.pvtk@mil.fi +358 (0) 299 800	**www.puolustusvoimat.fi/en**
Ministry of the Interior (*Sisäasiainministeriö/Inrikesministeriet*)	Public authority	Ministry of the Interior PO Box 26, FI-00023 Government, Finland kirjaamo@intermin.fi +358 295 480 171	**www.intermin.fi**

The National Police Board (*Poliisihallitus/Polisstyrelsen*)	Public auhtority	The National Police Board PL 302, 00101 Helsinki +358 (0) 295 480 181 kirjaamo.poliisihallitus@poliisi.fi	**www.poliisihallitus.fi**
National Bureau of Investigation **(*Keskusrikospoliisi/Centralkriminalpolisen*)**	Public authority	National Bureau of Investigation PO Box 285 FI-01301 VANTAA +358 295 480 141 kirjaamo.keskusrikospoliisi@ poliisi.fi	**https://www.poliisi.fi/poliisi/krp/home.nsf/pages/indexfin**
Finnish Security Intelligence Service	Public authority	Finnish Security Intelligence Service	**www.poliisi.fi/supo**

(*Suojelupoliisi/ Skyddspolisen*)		PO BOX 151 00121 HELSINKI suojelupoliisi@poliisi.fi	
Local police departments (*Paikalliset poliisilaitokset/ Polisinrättningar*)	Public authority	Various (There are 11 police departments in Finland.)	**www.poliisi.fi/poliisi/home.nsf/pages/index_eng**
Finnish Customs (*Tulli/Tul*)	Public authority	PO Box 512, 00101 Helsinki +358 (0)295 5200 kirjaamo@tulli.fi	**www.tulli.fi/en/index.jsp**
The Finnish Border Guard (*Rajavartiolaitos/ Gränsbevakningsvä sendet*)	Public authority	PO Box 3, 00131 Helsinki, Finland +358 295 420 000 rajavartiolaitos@raja.fi	**www.raja.fi**
District courts (*Käräjäoikeudet/Tin gsrätterna*)	Courts	Various. (There are 27 district courts in Finland)	**www.oikeus.fi/tuomioistuimet/karajaoikeudet/en/index.html**
The Follow-up Group on Secret Data Acquisition	Public authority		**www.poliisihallitus.fi**

(*Salaisen tiedonhankinnan seurantaryhmä*) appointed by the National Police Board (*Poliisihallitus/Polis styrelsen*)		The National Police Board PL 302, 00101 Helsinki +358 (0) 295 480 181 kirjaamo.poliisihallitus@poliisi.fi	
Finnish Communications Regulatory Authority (*Viestintävirasto / Kommunikationsverket*)	Public authority	PO Box 313, FI-00181 Helsinki +358 295 390 100 kirjaamo@ficora.fi	**www.viestintavirasto.fi/en/index.html**
Eletronic frontier Finland (EFFI)	civil society organisation	puheenjohtaja@effi.org	**www.effi.org**
The Office of the Prosecutor General (*Valtakunnansyyttäjänvirasto/ Riksåklagarämbetet*)	Public authority	PO Box 333, FIN-00181 Helsinki +358 29 562 0800 vksv@oikeus.fi	**www.vksv.oikeus.fi/en/index.html**
Ministry of Transport and Communications	Public authority	PO Box 31, FI–00023 Government, Finland	**www.lvm.fi/web/en/home**

(*Liikenne- ja viestintäministeriö / Kommunikationsministeriet*)		+358 295 16001 kirjaamo@lvm.fi	
The Ministery for Foreign Affairs (*Ulkoasiainministeriö/ Utrikesministeriet*)	Public authority	Merikasarmi, PO Box 176, 00023 Government, Finland +358 295 350 000 kirjaamo.um@formin.fi	**www.formin.fi**
Data Protection ombudsman (*Tietosuojavaltuutettu/Dataombudsmannen*)	Ombudsman	Office of the Data Protection Ombudsman P.O. Box 800, FIN-00521 HELSINKI +358 29 56 66700 tietosuoja@om.fi	**www.tietosuoja.fi/en/index.html**
**Data Protection Board (*Tietosuojalautakunta/Datasekretessnä*	The Data Protection Board is an independent authority affiliated to the	Data Protection Board/Ministry of	**http://oikeusministerio.fi/en/index/theministry/neuvottelu-jalautakunnat/thefinnishdataprotectionboard.html**

***mnden*)**	Ministry of Justice	Justice PO BOX 25, FI-00023 Government tietosuojaltk.om@om.fi	
The Parliamentary Ombudsman (*Eduskunnan oikeusasiamies/ riksdagens justitieombudsman*)	Parliamentary	Arkadiankatu 3 FI-00102 Helsinki +358 (0)9 *4321 ombudsman(at)parliament.fi	**www.oikeusasiamies.fi/Resource.phx/eoa/english/index.htx**
The Chancellor of Justice (*Oikeuskansleri/ Justitiekanslern*)	Public authority	P.O. Box 20, 00023 Government +358 (0)295 16001 kirjaamo@okv.fi	**www.oikeuskansleri.fi/en/chancellor/chancellor-justice/**
VTT Technical Research Centre of Finland (*VTT, valtion teknillinen tutkimuslaitos*)	Public authority	P.O. Box 1000, FI-02044 VTT, Finland Tel. +358 20 722 111 info@vtt.fi	**www.vtt.fi**

Tieke, Information Society Development centre (*Tieke, tietoyhteiskunnan kehittämiskeskus /Tieke, Utvecklingscentralen för Informationssamhälle*)		Salomonkatu 17 A, 10th floor FI-00100 HELSINKI FINLAND tieke(at)tieke.fi	**www.tieke.fi**

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

Finland, the Ministry of Defence (*Puolustusministeriö/Försvarsministeriet*) (2013), *Asettamispäätös: Kansallisen lainsäädännön kehittäminen kyberturvallisuusviranomaisten tiedonhankintakyvyn parantamiseksi kybertoimintaympäristön uhkista; lainsäädäntöhanke*. No official English translation available. This document is an appointment letter of the Working group on developing the national legislation to increase the security authorities' ability to acquire information about the threats presented by the cyber environment. Document available at (accessed 25 July 2014): www.defmin.fi/files/2669/Kyberlainsaadantotyoryhman_asettamispaatos.pdf

Finland, the Ministry of Defence (*Puolustusministeriö/Försvarsministeriet*), The Cyber Security Strategy (*Kyberturvallisuusstrategia*), available at (accessed at 5 August 2014): www.yhteiskunnanturvallisuus.fi/

Finland, the Ministry of the Interior (*Sisäministeriö/Inrikesministeriet*) (2013), The Internal Legality Control in the Police (*Poliisiin kohdistuva sisäinen laillisuusvalvonta)*, Sisäasiainiministeriön julkaisu 19/2013, Helsinki: Sisäministeriön monistamo, available at (accessed 8 August 2014): www.intermin.fi/download/46914_poliisiin_kohdistuva_sisainen_valvonta_julkaisu_192013.pdf?a5d313551c05d188

Finland, the Security Committee of the Ministry of Defence (*Puolustusministeriön turvallisuuskomitea/Försvarsministeriets säkerhetskommittén*), The implementation programme of the national cyber security strategy (*Kansallisen kyberturvallisuusstrategian toimeenpano-ohjelma*), 11.3.2014, 194/8.1.99/2013, available at (accessed 17 July 2014): www.turvallisuuskomitea.fi/index.php/fi/20-ajankohtaista/45-kyberturvallisuusstrategian-toimeenpano-ohjelma-on-valmis

Finland, the Finnish Security Intelligence Service (*Suojelupoliisi/Skyddspolisen*), *Annual Report 2013*, available at (accessed 24 July 2014): www.poliisi.fi/poliisi/supo60/home.nsf/files/9F07FC6EA2B39425C2257C90003052CF/$file/2013_Supo-Annual_Report_web.pdf

Finland, the Chancellor of Justice (*Oikeuskansleri/ Justitiekanslern*) (2013), *Oikeuskanslerinviraston toiminta- ja taloussuunnitelma vuosille 2015-2018 sekä tulossuunnitelma vuodelle 2014*. Available at (accessed 24 July 2014): www.oikeuskansleri.fi/media/uploads/talousasiakirjat/toiminta-_ja_taloussuunnitelma_vuosille_2015_2018.pdf

Finland, the National Police Board (*Poliisihallitus/Polisstyrelsen*) (2014), *Poliisihallituksen selvitys Sisäasiainministeriölle poliisin tiedonhankinnasta ja sen valvonnasta 2013*, POL-2014-30. Available at (accessed 14 July 2014): http://poliisi.fi/poliisi/home.nsf/files/8E2337E98D525CF2C2257CA00029F00B/$file/Allekirjoitettu%20toimintakertomus%202013.pdf

Finland, the National Police Board (*Poliisihallitus/Polisstyrelsen*) (2013), *Poliisihallituksen selvitys Sisäasiainministeriölle poliisin tiedonhankinnasta ja sen valvonnasta 2012*, 2020/2013/74. Available at (accessed 14 July 2014): www.intermin.fi/download/40590_kertomus_poliisin_tiedonhankinnasta_2012.pdf?bb79dd91885ed188

Finland, the National Police Board (*Poliisihallitus/Polisstyrelsen*) (2014), The Annual Accounts of the National Police Board 2013 (*Poliisihallituksen tilinpäätös vuodelta 2013)*, POL-2014-513. Available at (accessed 14 July 2014): http://poliisi.fi/poliisi/home.nsf/files/8E2337E98D525CF2C2257CA00029F00B/$file/Allekirjoitettu%20toimintakertomus%202013.pdf

Finland, Committee for Constitutional Law of the Government (*perustuslakivaliokunta/grundlagsutskott*) (2013), Statement of the Committee for Constitutional Law about the Information Society Code (*Perustuslakivaliokunnan lausunto tietoyhteiskuntakaaresta*), available at (accessed 25 July 2014): www.eduskunta.fi/valtiopaivaasiat/he+221/2013

Finland, Ministry of transport and communications (*Liikenne- ja viestintäministeriö/Kommunikationsministeriet*) (2014), Press release: *Information Society Code to Parliament*, available at (accessed 21 July 2014): valtioneuvosto.fi/ajankohtaista/tiedotteet/tiedote/fi.jsp?oid=407502

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

Finland, Data Protection ombudsman (*Tietosuojavaltuutettu/Dataombudsmannen*) (2014), *Tietosuojavaltuutetun lausunto liikenne- ja viestintäministeriön asettaman työryhmän valmistelemasta kansallisen big data -strategian luonnoksesta*, available at (accessed 18 July 2014): www.tietosuoja.fi/fi/index/ajankohtaista/tiedotteet/2014/06/tietosuojavaltuutetunlausuntoliikenne-javiestintaministerionasettamantyoryhmanvalmistelemastakansallisenbigdata-strategianluonnoksesta.html

Finland, the Parliamentary Ombudsman (*Eduskunnan oikeusasiamies/Riksdagens justitieombudsman*) (2014), the Annual Report of the Parliamentary Ombudsman 2013 (*Eduskunnan oikeusasiamiehen kertomus vuodelta 2013*), available at (accessed 6 August 2014): www.oikeusasiamies.fi/dman/Document.phx?documentId=hh16114123723149&cmd=download

3. Non-governmental organisations (NGOs)

   EFFI, Electronic Frontier Finland ry (NGO), *Effin lausunto turvallisuuskomitean toimittamasta kyberturvallisuuden toimeenpano--ohjelman luonnoksesta*, available at (accessed 14 July 2014): www.effi.org/lausunnot/lausunto-kyberturvallisuus-20140131

   EFFI, Electronic Frontier Finland ry (NGO), *Effin lausunto Tietoyhteiskuntakaaresta Hallintovaliokunnalle 7.3.2014*, available at (accessed 14 July 2014): www.effi.org/uutiset/140309-effin-lausunto-tietoyhteisku.html

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

It is difficult to give a comprehensive list of academic research carried out on this field. ICT and information technology are being researched for example in the University of Eastern Finland (one professor of Information and information technology law: Mr. Tomi Voutilainen), The Aalto University has established a new professorship on cybersecurity (Mr. Jarno Limnéll). The Faculty of Law in the University of Turku has on ongoing research project called: Rights, Information and Security. The Architecture and Anti-Constitutional Implications of the New Security Constitutionalism (http://www.utu.fi/en/units/law/research/research-projects/activeprojects/Pages/Rights,-Information-and-Security.aspx)