

Report of Various Size

Monthly data collection on the current reform of intelligence legislation

Submission template

Country: Finland

Contractor's name: Åbo Akademi University Institute for Human

Rights

Author(s) name: Tuomas Ojanen and Juha Lavapuro

Period covered: January – May 2017

DISCLAIMER: This document was commissioned under a specific contract as background material for the project on [National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies](#). The information and views contained in the document do not necessarily reflect the views or the official position of the EU Agency for Fundamental Rights. The document is made publicly available for transparency and information purposes only and does not constitute legal advice or legal opinion.

1. Legislative reform(s)

(Please, highlight the key aspect(s) of the reform, summarise any key report published in the context of the reform procedure)

The current Finnish legislation does not provide for intelligence work. However, there have been calls by law enforcement authorities and political elite for more surveillance, including intelligence, in recent years. For instance, the President of the Republic urged the raising of the level of surveillance by the Finnish intelligence “to meet the European standards” after the Paris terror attacks in November 2015.¹ Earlier, a working group of the Ministry of Defence (*puolustusministeriö/försvarsministeriet*) had already proposed in January 2015 that the Government should initiate as soon as possible legislative reforms aiming at establishing the appropriate legal framework for intelligence.²

Later in 2015, the Government decided to set up four working groups for preparing legislation regarding civil and military intelligence, including their legal and parliamentary oversight. While the working group of the Ministry of Justice (*oikeusministeriö/justitieministeriet*) was set up to prepare amendments to the provisions on the secrecy of confidential communications laid down in the Constitution, the other two working groups of the Ministry of the Interior (*sisäasiainministeriö/inrikesministeriet*) and the Ministry of Defence were appointed to prepare a legislative framework concerning civilian and military intelligence. In addition, a distinct working group is pondering oversight of intelligence.³

Later, a parliamentary steering group was also appointed by the Ministry of the Interior for the purpose of monitoring the preparation of constitutional and legislative reforms.⁴

The working group of the Ministry of Justice preparing the amendment of the Constitution published its report on 11 October 2016,⁵ but the possible constitutional reform was suspended for the completion of the works of the other working groups considering legislation regarding civilian and military intelligence and their oversight.

¹ For an overview of the background of current legislative reforms, see e.g. Yle News (2015), ‘Finland mulls constitution changes, web surveillance powers for intelligence police’, 15 November 2015, available at: http://yle.fi/uutiset/osasto/news/finland_mulls_constitution_changes_web_surveillance_powers_for_intelligence_police/8456920 (13 February 2017).

² Finland, Ministry of Defence, Guidelines for developing Finnish intelligence legislation. Working group report. March 2015, available at: http://www.defmin.fi/files/3144/GUIDELINES_FOR_DEVELOPING_FINNISH_INTELLIGENCE_LEGISLATION.pdf (13 February 2017).

³ Finland, Ministry of Justice, The decision to appoint a working group available at: <http://oikeusministerio.fi/fi/index/valmisteilla/lakihankkeet/valtiosaanto/turvallisuusviranomaistentiedustelutoiminnanvalvonta.html> (27 November 2016).

⁴ Finland, Finnish Government (*valtioneuvosto/statsrådet*), Press release 11 December 2015, available at: http://valtioneuvosto.fi/artikkeli/-/asset_publisher/parlamentaarinen-seurantaryhman-tiedustelulainsaadannon-uudistamiseen-liittyville-hankkeille (13 February 2017).

⁵ Finland, Ministry of Justice, Luottamuksellisen viestin salaisuus. Perustuslakisäätelyn tarkistaminen, Mietintöjä ja lausuntoja 41/2016, available at: <http://oikeusministerio.fi/fi/index/julkaisut/julkaisuarkisto/1476095590535.html> (13 February 2017).

The task of the working group of the Ministry of Justice was to assess and prepare such amendments to the Constitution that would make it possible to lay down provisions by an act on the necessary limitations to the protection of the secrecy of confidential communications, under certain preconditions deemed necessary, for the purpose of protecting the national security.

According to the working group, the current Constitution does not allow to enact by ordinary legislation such limitations to the secrecy of confidential communications that would authorize to obtain civil and military intelligence on serious threats necessary for the national security, especially in order to predict and prepare for such threats and to support the decision-making of the state leaders. Hence, the working group proposed the following new constitutional provision on permissible grounds for limitation of the secrecy of confidential communications: “Provisions concerning limitations of the secrecy of communications which are necessary in the prevention of crimes that jeopardise the security of the individual or society or the sanctity of the home, at trials and security checks, during the deprivation of liberty, and for the purpose of obtaining intelligence on military operations or other such operations that pose a serious threat to the national security may be laid down by an act.”⁶

According to the working group’s report, operations “that pose a serious threat to the national security” would refer to operations threatening the integrity of the state or the basic functions of society, such as terrorism-related activities, violent radicalisation or activities of foreign intelligence services. The operations referred to in the provision could also be such operations that would constitute an offence if they became concrete, but a concrete and individualised suspicion of an offence cannot yet be directed at them. In addition, the working group report states that operations referred to in the provision could be operations that do not constitute an offence under the Finnish law, such as disorders in a foreign state relevant to Finland’s security or steering of mass influx of immigrants to Finland.

Moreover, the report also stated that the requirement of necessity mentioned in the provision means that the powers to interfere with the secrecy of confidential communications must be as precisely defined and limited as possible.

In particular, according to the working groups view, the proposed amendment would not make it possible to enact provisions on general, all-encompassing telecommunications monitoring. In the ordinary legislation to be enacted, the powers to gather intelligence must be specified and the preconditions for limiting fundamental rights, the human rights obligations, and the EU law must be complied with. However, the report does not clarify what kind of concrete limits to intelligence activities this limitation would provide.

⁶ Finland, Ministry of Justice, Luottamuksellisen viestin salaisuus. Perustuslakisääntelyn tarkistaminen, Mietintöjä ja lausuntoja 41/2016, available at: <http://oikeusministerio.fi/fi/index/julkaisut/julkaisuarkisto/1476095590535.html> (13 February 2017).

The working groups of the Ministry of the Interior, the Ministry of Justice and the Ministry of Defence published their reports and proposals for legislation regarding civil and military intelligence, including their legal and parliamentary oversight on 19 April 2017.⁷

All reports are currently subject to formal consultation with multiple authorities, NGOs and other stakeholders. This consultation is a standard tool of Finnish law-making process for the purpose of gathering information to facilitate the drafting and elaboration of legislative proposals by the Government. The deadline for the statements is 16 June 2017. After the closure of the consultation round, the ministries are expected to revise their original proposals in light of the submitted statements before the final Government bills on civil and military intelligence, including their oversight, will be submitted to Parliament in the autumn of 2017.

It must be added that these observations on the forthcoming legislative process are subject to the precondition that there will exist enough strong political support to further these legislative proposals after the closure of the statement round. Currently, however, there seems to exist quite a strong support across the political field to adopt intelligence legislation although there is a great deal of controversy over the appropriate procedure. The desire of the Government, including the President of the Republic, is to adopt the proposed intelligence legislation, including the proposed constitutional amendment, as soon as possible. Hence, it has been proposed that the constitutional amendment should be enacted by taking advantage of the urgency procedure for constitutional enactment under Section 73(2) of the Constitution (*Suomen perustuslaki/Finlands grundlag*, Act No. 731/1999).⁸ This constitutional provision provides as follows: “The proposal may be declared urgent by a decision that has been supported by at least five sixths of the votes cast. In this event, the proposal is not left in abeyance and it can be adopted by a decision supported by at least two thirds of the votes cast”. However, a lot of criticism has been levelled by the opposition parties against adopting the proposed constitutional amendment in accordance with the urgency procedure for constitutional enactment under Section 73(2) of the Constitution. Hence, it is uncertain whether the required parliamentary majority of five sixths of MPs will be found to declare the proposed constitutional amendment “urgent” within the meaning of Section 73(2) of the Constitution.⁹

It is also important to note in this context that the Constitutional Law Committee (*perustuslakivaliokunta/grundlagsutskottet*) of Parliament, the primary authority of constitutional interpretation in Finland, has emphasized that, as a rule, constitutional amendments should be made in accordance with the procedure for constitutional enactment

⁷ Finland, Ministry of the Interior, Siviilitiedustelulainsäädäntö. Työryhmän mietintö, Sisäministeriön julkaisu 8/2017, available at: <http://urn.fi/URN:ISBN:978-952-324-129-9>. Ministry of Defence, Ehdotus sotilastiedustelua koskevaksi lainsäädännöksi. Förslag till lagstiftning om militär underrättelseverksamhet, available at: <http://urn.fi/URN:ISBN:978-951-25-2899-8>. Ministry of Justice, Tiedustelutoiminnan valvonta. Työryhmän mietintö, Oikeusministeriön julkaisu 18/2017, available at: <http://urn.fi/URN:ISBN:978-952-259-576-8> (25 May 2017).

⁸ All acts referred to in this report are available in Finnish and Swedish at www.finlex.fi.

⁹ YLE news (2017), ‘Thursday’s papers: New intelligence powers under scrutiny, also, warm summer ahead. Nope, 20 April 2017, English summary is available at: http://yle.fi/uutiset/osasto/news/thursdays_papers_new_intelligence_powers_under_scrutiny_also_warm_summer_ahead_nope/9572719 (28 May 2017).

under Section 73(1) of the Constitution. This provision stipulates that constitutional amendment “shall in the second reading be left in abeyance, by a majority of the votes cast, until the first parliamentary session following parliamentary elections”. The proposal shall then, once the Constitutional Law Committee has “issued its report, be adopted without material alterations in one reading in a plenary session by a decision supported by at least two thirds of the votes cast.” The Constitutional Law Committee has noted that the urgency procedure under Section 73(2) of the Constitution is an exception to the rule and that there must be particularly compelling needs for the enactment of a constitutional amendment in accordance with the procedure under Section 73(2).¹⁰

The Ministry of the Interior’s report proposes that the Finnish Security Intelligence Service (*suojelupoliisi/skyddspolisen*) be given intelligence powers both in Finland and abroad. According to the report, the Police Act (*poliisilaki/polislagen*, Act No. 872/2011) would be amended with provisions concerning location tracking, replication and stopping of shipment for copying. In particular, Finnish Security Intelligence Service would be given the power to conduct network surveillance for obtaining information about activities that seriously threaten national security. The working group proposes that these powers would be based on a new Act on Network Surveillance in Civilian Intelligence (*laki tietoliikennetiedustelusta siviilitiedustelussa/lag om civil underrättelseinhämtning avseende datatrafik*).

According to the proposal by the Ministry of the Interior, the use of network traffic intelligence would be decided by the District Court (*käräjäoikeus/tingsrätt*) of Helsinki. The proposed network surveillance would be targeted at a restricted part of the communications network and the information could only be gathered by using specific search criteria approved by the Court. The gathering of network traffic intelligence could only be used for activities that pose a serious threat to national security. When gathering network traffic intelligence, the intelligence authorities would also obtain such information that is not significant in terms of national security. In such cases, this information would be deleted immediately.

According to the report, provisions on international intelligence cooperation and the methods of surveillance used in that connection will be enacted separately.¹¹

Key provisions of the proposed Act are as follows¹² (unofficial translation by the authors of this report):

Section 3 – The objectives of electronic surveillance of network communications

Electronic surveillance of network communications can be used to obtain information about following activities that threaten the national security:

- 1) terrorism;

¹⁰ Finland, Constitutional Law Committee of Parliament, Report No. 5/2005 available at:

https://www.eduskunta.fi/FI/vaski/mietinto/Documents/pevm_5+2005.pdf (28 May 2017).

¹¹ Finland, Ministry of the Interior, Siviilitiedustelulainsäädäntö. Työryhmän mietintö, Sisäministeriön julkaisu 8/2017, available at: <http://urn.fi/URN:ISBN:978-952-324-129-9>, p. 122 (29 May 2017).

¹² Finland, Ministry of the Interior, Siviilitiedustelulainsäädäntö. Työryhmän mietintö, Sisäministeriön julkaisu 8/2017, pp. 301-303, available at: <http://urn.fi/URN:ISBN:978-952-324-129-9> (29 May 2017).

- 2) foreign intelligence;
- 3) activities threatening the state and social order;
- 4) weapons of mass destruction;
- 5) a serious threat to the national security of dual-use items;
- 6) the life or health of a large number of people or the vital functions of society;
- 7) a foreign country's plan or activity that may cause damage to foreign or international relations, economic or other important interests;
- 8) a global peace and security crisis;
- 9) activities threatening an international crisis management operation;
- 10) international organized crime, which is seriously threatening national security.

Section 4 – Targeting of electronic surveillance of network communications

According to paragraph 1 of Section 4, targeting of electronic surveillance of network communications is accomplished through automated analysis of communications data. Automated separation is based on the use of the search criteria approved under the procedure in Section 7 or Section 9.

The explanatory text of the proposal states that the use of content based search criteria is prohibited except in two cases as provided in paragraph 2 of Section 4. Accordingly, the search criteria describing the content of the message can be used only if 1) The search criteria are used solely for the purpose of accessing communication of foreign countries or a comparable entities, or 2) The search criteria describes the contents of a malicious computer program or command.

As a result, the proposal does not allow for automated processing of the content of the confidential communications of individuals. However, the proposal does not exclude the automatic processing of content data either since that is allowed in two distinct situations. Therefore, the proposal allows for a bulk access to both the content and metadata.

The search criteria may not use unique information for a telecommunications terminal or a telecommunications terminal owned by a person in Finland or supposedly otherwise used by a person in Finland.

Section 5 – Further processing of information gathered through automated analysis

The communication from the telecommunications system that has been collected automatically under Section 4 above, can be processed automatically and manually. Processing can be used to access the contents of the message and other confidential information. According to the report of the Ministry of the Interior, this provision authorizes the intelligence service to gather the content of the message. Moreover, this processing may also combine information gathered from both the contents of the messages and the metadata, including location data.¹³

¹³ Finland, Ministry of the Interior, Siviilitiedustelulainsäädäntö. Työryhmän mietintö, Sisäministeriön julkaisu 8/2017, available at: <http://urn.fi/URN:ISBN:978-952-324-129-9>, pp. 235-236.

Section 6 – Conditions for electronic surveillance of network communications

Electronic surveillance of network communications can be used if it is presumable that it may provide information on the serious threat of national security as referred to in Section 3.

Section 7 – Court Permission

The court decides on an electronic surveillance of network communications on the written request of the Chief of the Finnish Security Intelligence Service.

The request and the court decision must state:

- 1) The serious threat to the national security referred to in Section 3, to which the surveillance measures are to be based on,
- 2) The facts of the operation referred to in paragraph 1,
- 3) The facts on which the conditions for using the surveillance measures are based,
- 4) The search terms used for the electronic surveillance of network communications or the categories of search criteria and their justifications,
- 5) The part of the cross-border communication network where surveillance measures are used as well as the reasons for choosing a part of the communication network,
- 6) The period of validity of a surveillance permit with the accuracy of the time of day,
- 7) The police officer managing and supervising the surveillance measures. The officer must be one of the officers of the Finnish Security Intelligence Service and be familiar with the use of surveillance measures,
- 8) Any restrictions and conditions for surveillance measures.

Permission to adopt surveillance measures can be granted for a maximum of six months at a time. The surveillance must be terminated before the expiry of the deadline specified in the authorization if the purpose of the surveillance has been achieved or no longer exists.

Section 9 – Urgent procedures

If an intelligence does not tolerate delay, the Chief of the Finnish Security Intelligence Service will decide on an electronic surveillance of network communications until the Court has ruled on the request for authorization. The decision must be made in writing. The matter must be referred to the Court as soon as possible, but not later than 24 hours after the commencement of the telecoms inquiry.

If the Court finds that there are no conditions for an electronic surveillance of network communications under Section 6, the use of the electronic surveillance of network communications must be terminated immediately, and the data obtained therein and the notes on the data obtained must be immediately disposed of. If the Court considers that the decision referred to in subsection 1 has otherwise been erroneous, the use of telecommunications information must be terminated immediately in so far as it is required by the Court's decision and the data obtained through the electronic surveillance of network communications and the notes on the information received must be immediately disposed of. However, the data can be stored in the register referred to in the Act on the Processing of Personal Data in Police Activities under the conditions laid down in Chapter 5, Section 44, Subsection 2 of the Police Act.¹⁴

As to the legal safeguards, Section 20 includes a provision about the duty of the authorities to notify the target of the network traffic intelligence. If the contents of a confidential message or recording of a person in Finland have been manually processed as provided by Section 5, the person must be notified as provided by Section 46 of Chapter 5a of the Police Act, as amended. However, the notification obligation does not apply in cases where the intelligence data has been destroyed pursuant to Section 9(2) or Section 15 of the proposed Act on Network Surveillance in Civilian Intelligence.

According to Section 46 of Chapter 5a of the Police Act, as amended, the targeted person must be notified after the purpose of the use of the surveillance has been achieved. At the same time, the court which granted the permit, must also be notified. However, according to paragraph 2 of Section 46, the court may, upon the request of a police officer of the Finnish Security Intelligence Service decide that the notification referred to in subsection 1 may be postponed for a maximum of two years at a time if justified to safeguard the use of intelligence, to protect national security or to protect the life or health of individuals. The notification procedure can be completely disregarded, if it is necessary to protect national security or to protect the life and health. Moreover, if the identity of the target of the surveillance is unknown at the end of the period or suspension referred to in subsection 1 or 2, the use of the surveillance measures must be reported to him in writing without undue delay after the target has been identified.

The proposed Act on Network Surveillance in Civilian Intelligence does not include further provisions about the remedial procedure applicable to individual.

The working group of the Ministry of Defence proposes that the military intelligence authorities are granted powers to gather human intelligence, signals intelligence and foreign information systems intelligence as well as telecommunications intelligence in traffic crossing the Finnish borders. The key provisions on the preconditions of gathering telecommunications intelligence by the military intelligence authorities are essentially similar to those governing civil intelligence (see above). The military authorities would have these powers both in Finland and abroad. The proposed Act would also contain provisions on military intelligence authorities'

¹⁴ Finland, Act on the Processing of Personal Data in Police Activities (*Jaki henkilötietojen käsittelystä poliisitoimessa/lag om behandling av personuppgifter i polisens verksamhet*, Act No. 761/2003) and the Police Act (*poliisilaki/polislagen*, Act No. 872/2011).

cooperation with other authorities, international cooperation and prohibitions on intelligence gathering and data processing.

The proposal also includes provisions on the purpose and targets of military intelligence, the principles complied with in intelligence activities as well as the steering and oversight of intelligence activities in the defence administration.

According to Section 3 of the proposed Act, the purpose of the military intelligence is to acquire and process information on external threats to support the decision making of the Government and to perform the tasks of the Defence Forces referred to in Section 2 of the Finnish Defence Forces Act (*laki puolustusvoimista/lag om försvarsmakten*, Act No. 551/2007).¹⁵

A working group of the Ministry of Justice proposes that a new authority, the Intelligence Ombudsman, be established to oversee the legality of civilian and military intelligence gathering.¹⁶ The oversight system needs to be reformed, because the new intelligence legislation proposed by the working groups of the Ministry of the Interior and the Ministry of Defence would provide the civilian and military intelligence authorities with new and significant intelligence gathering duties and powers.

The proposed new Intelligence Ombudsman would function in connection with the Office of the Data Protection Ombudsman (*tietosuojavaltuutetun toimisto/dataombudsmannens byrå*) and would be an independent and autonomous authority. The Intelligence Ombudsman would be responsible for overseeing the legality of the use of intelligence gathering methods and the observance of fundamental and human rights in intelligence gathering activities. The Intelligence Ombudsman would have an extensive right of access to information and the right to receive reports on intelligence gathering from the competent authorities and other parties performing public administrative tasks. The Intelligence Ombudsman would also be able to conduct inspections in the premises of the authorities and other parties performing public administrative tasks.

The Intelligence Ombudsman would also have the competence to order that the use of a certain intelligence gathering method should be suspended or terminated, if the Ombudsman considers that the competent intelligence authority has acted unlawfully in the course of its intelligence gathering.

In respect of the use of such intelligence gathering methods which require court authorization, the working group of the Ministry of Justice proposes a special procedure where the Intelligence Ombudsman could first issue an interim order on suspension or termination. After this, the matter should, without delay, be referred for consideration to the court that had issued the authorization. The court should decide on the matter urgently.

¹⁵ Finland, Ministry of the Defence, Ehdotus sotilastiedustelua koskevaksi lainsäädännöksi. Förslag till lagstiftning om militär underrättelseverksamhet, p. 314, available at: <http://urn.fi/URN:ISBN:978-951-25-2899-8> (29 May 2017).

¹⁶ Finland, Ministry of Justice, Tiedustelutoiminnan valvonta. Työryhmän mietintö, Oikeusministeriön julkaisu 18/2017, pp. 77-80, available at: <http://urn.fi/URN:ISBN:978-952-259-576-8> (29 May 2017).

Furthermore, the Intelligence Ombudsman would be able to order that unlawfully gathered intelligence data must be destroyed without delay. If the Intelligence Ombudsman notices that a party subject to oversight has acted unlawfully, the Ombudsman would report the case to the competent criminal investigation authority (e.g. the police or military authorities).

On 29 May 2017, a working group appointed by the Secretary General of Parliament to consider parliamentary oversight of civil and military intelligence published its report. In essence, the working group proposes the adoption of a new parliamentary committee, the Oversight Committee of Intelligence (*tiedusteluvalvontavaliokunta*). The Committee would consist of 11 MPs, and it would oversee the appropriateness of civilian and military intelligence gathering, as well as its compatibility with fundamental rights and human rights obligations binding upon Finland. The proposed parliamentary oversight system would be complementary to the legal oversight system proposed by the working group of the Ministry of Justice (see above).¹⁷

2. Reports and inquiries by oversight bodies

The Parliamentary Ombudsman (*eduskunnan oikeusasiamies/riksdagens justitieombudsman*) provided his statement about the report of the Ministry of Justice working group, preparing amendments to the constitutional provisions on the secrecy of confidential information, in December 2016.¹⁸ The Ombudsman emphasized that the investigatory powers must be clearly defined in the legislation so that those powers are limited to what is necessary. Moreover, the legislation must include provisions about efficient oversight and guarantees of legal protection. Finally, the Parliamentary Ombudsman emphasized that the conformity of intelligence legislation with the fundamental and human rights can be evaluated only after the concrete proposals for civil and military intelligence legislation are made public.

The Office of the Finnish Data Protection Ombudsman provided its statement about the Ministry of Justice working group report on 13 January 2017. The Ombudsman emphasized, among others, that the recent decisions of the Court of Justice of the European Union (especially in case *Digital Rights Ireland*) require more context specific weighing of the significance of meta data in relation to personal data and right to private life. The Ombudsman was also concerned how surveillance operations could be targeted in a manner that would respect the principle of proportionality, when the operations subject to intelligence gathering are not necessarily punishable under Finnish law or have not proceeded to the point where a concrete and individualised suspicion of a crime could be directed at them. According to the

¹⁷ Finland, The Office of the Parliament, Tiedustelun parlamentaarinen valvonta -työryhmän mietintö, Eduskunnan kanslia 2017, available at:

www.eduskunta.fi/FI/tiedotteet/Documents/tiedustelun%20parlamentaarinen%20valvonta.pdf (30 May 2017).

¹⁸ Finland, Parliamentary Ombudsman (*eduskunnan oikeusasiamies/riksdagens justitieombudsman*), Statement 22 December 2016, available at:

www.hare.vn.fi/Uploads/21370/262728/LAUSUNTO_20161223031502_262728.pdf (13 February 2017).

Data Protection Ombudsman, these constitutional proposals can be appropriately assessed only after the concrete proposals for Finnish intelligence legislation are published.¹⁹

3. Work of specific ad hoc parliamentary or non-parliamentary Commissions

Nothing to report in addition to Section 1 above.

4. Work of non-governmental organisations and academia

The report of the Ministry of Justice working group, on constitutional amendments, raised criticism immediately after its publication. In an interview of National Broadcasting Company YLE²⁰ as well as in a separate blog post in “*Perustuslakiblogi*”,²¹ professor Martin Scheinin criticized the report for creating an overbroad and vague authorization for such surveillance legislation that may well be in conflict with the international human rights conventions and the Charter of Fundamental Rights of the European Union. He suggested that the Constitution should also be amended with specific provision prohibiting mass surveillance. However, this proposition was explicitly rejected as “systematically unfit” by the representative of the Ministry of Justice in the expert hearing arranged by the Parliamentary Steering Group for the reform of Finnish Intelligence Legislation.

A number of Finnish newspapers cited *Svenska Presstjänst*'s interview of Swedish surveillance law expert Mark Klamberg who argued that one of the reasons for the Finnish government's interest for urgent reform of surveillance legislation is based on the upcoming Sea Lion communications cable. The cable that is currently being built will connect Finland directly to Germany. As such, communications from and to Russia could bypass the current signals intelligence activities of the National Defence Radio Establishment of Sweden (*Försvarets radioanstalt, FRA*).²² No additional discussion took place.

Amnesty International released its Annual Report for 2016 to 2017 on 21 February 2017. With regard to the intelligence legislation reform in Finland, the report mentions the draft

¹⁹ Finland, Data Protection Ombudsman (*tietosuojavaltuutettu/dataombudsman*), Statement 13 January 2017, available at: www.hare.vn.fi/Uploads/21370/405249/LAUSUNTO_20170117234515_405249.pdf (13 February 2017).

²⁰ YLE News report (2016), 'Professori Scheinin aiotusta tiedustelulainsäädännöstä: Tässä on pantu lumiaura menemään edeltä umpihankeen', 11 October 2016, available at <http://yle.fi/uutiset/3-9223300> (13 February 2017).

²¹ Martin Scheinin (2016), 'Lumiaura lähestyy yksityisyyden hankea' 1 November 2016, available at: <https://perustuslakiblogi.wordpress.com/2016/11/01/martin-scheinin-lumiaura-lahestyy-yksityisyyden-hankea/> (13 February 2017).

²² Turun Sanomat (2016), 'Tutkijan mukaan Sea Lion -kaapeli voi kiirehtiä Suomen uutta tiedustelulakia', 20 October 2016, available at: www.ts.fi/uutiset/kotimaa/2966197/Tutkijan+mukaan+Sea+Lion+kaapeli+voi+kiirehtia+Suomen+uutta+tiedustelulakia (13 February 2017).

constitutional amendment which aims to enable the acquisition of information on threats to national security.²³

As noted above, the proposals by the working groups are currently in the consultation phase in which some NGOs and academic stakeholders have been requested to present their views on the proposals. The expiry date of their statements is on 16 July 2017.

Up until now, the NGOs and academia have remained quite silent on the working group's reports with the exception of some individual professors and other academics. For instance, Professor of International Law and Human Rights of the European University Institute, Martin Scheinin, who was interviewed by the newspaper *Helsingin Sanomat* right after the reports by the three working groups were published, said that Finland does not need the proposed legal reform – at least not in the form proposed by the Ministry of the Interior and the Ministry of Defence. “It has not been shown that there are any shortcomings in the powers of the Finnish police, customs and intelligence police”, Scheinin told *Helsingin Sanomat*. Scheinin was especially concerned about the proposal to extend network surveillance powers beyond national borders, saying that it would violate personal privacy. He said that the proposed bill could lead to a situation in which individuals would fear discussing terrorism online, out of concerns that they might end up on a watch list. “No matter how often we are told it is not mass surveillance, that is what it is. Even if we conduct such surveillance with computers and algorithms, we are intruding on [individual] privacy”, Scheinin added according to *Helsingin Sanomat*.²⁴

In a recent blog post published in *Perustuslakiblogi*, professor Scheinin further details his criticism towards the proposal for civilian intelligence legislation.²⁵ According to Scheinin, the report is based on a misunderstanding of what constitutes mass surveillance. In particular, the report ignores one of the main findings of the CJEU's decisions in *Digital Rights Ireland*, *Max Schrems* and *Tele2*, namely that already a legislation permitting the public authorities to have access to the flow of electronic communications constitutes an intrusion on the right to private life. Moreover, professor Scheinin criticizes the proposal as overly vague which reduces the possibilities of the courts to provide adequate legal safeguards. Finally, professor Scheinin suggests that an explicit prohibition of mass surveillance should be included in the proposed legislation.

²³ Amnesty International Report 2016/2017. The State of the World's Human Rights. Amnesty International 2017. 21 February 2017, p. 159.

²⁴ Helsingin Sanomat (2017), 'Tiedustelulain luonnoksessa on asiantuntijoiden mukaan korjattavaa – 'Vaikka kuinka monta kertaa hoetaan, ettei kyse ole massavalvonnasta, niin sitä se on', 19 April 2017, available in Finnish at www.hs.fi/politiikka/art-2000005177146.html (28 May 2017). See also YLE news (2017), 'Thursday's papers: New intelligence powers under scrutiny, also, warm summer ahead.' Nope, 20 April 2017, available at: http://yle.fi/uutiset/osasto/news/thursdays_papers_new_intelligence_powers_under_scrutiny_also_warm_summer_ahead_nope/9572719 (28 May 2017).

²⁵ Perustuslakiblogi (2017), 'Martin Scheinin: Kommentteja mietinnöstä siviilitiedustelua koskevaksi lainsäädännöksi'. 16 June 2017, available in Finnish at: <https://perustuslakiblogi.wordpress.com/2017/06/16/martin-scheinin-kommentteja-mietinnosta-siviilitiedustelua-koskevaksi-lainsaadannoksi/> (18 June 2017).

According a news article by *Helsingin Sanomat*, the Finnish Center of Expertise in ICT (CSC) has provided its opinion on the Ministry of the Interior's proposal for civilian intelligence legislation where it states that the proposal is in effect based on mass surveillance technology.²⁶

²⁶ Helsingin Sanomat (2017), "Tosiasiallista massavalvontatekniikkaa" – Valtion supertietokoneiden haltija kritisoi tiedustelulakeja', 16 June 2017, available in Finnish at: www.hs.fi/kotimaa/art-2000005257960.html (18 June 2017).

ANNEX – Court decisions

Thematic area	Please provide the most relevant high court decision relating to the use of surveillance measure.
Decision date	No court decisions to report.
Reference details	
Key facts of the case (max. 500 chars)	
Main reasoning/argumentation (max. 500 chars)	
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	
Key quotation in original language and translated into English with reference details (max. 500 chars)	