Summary of the dissenting opinion to the report by the intelligence rights working group

The Ministry of Transport and Communications takes very seriously the concerns expressed by the defence forces and the police about the threats to national security and the need to gather information about those threats.

The Ministry of Transport and Communications advocates extensive intelligence powers to track and monitor foreign information systems. The defence forces need the powers to conduct foreign intelligence operations focused on information systems that handle information deemed critical to Finland's military defence. Such an intelligence strategy is much more effective, and much less harmful to society, than an online surveillance regime that takes in the whole of Finnish civilian society.

However, the Ministry has on 15 December 2014 submitted to the Ministry of Defence a dissenting opinion to the report of the intelligence rights working group. Our only differences of opinion centre around online surveillance and the lack of an adequate investigation into its effects and implications and into alternative methods of threat prevention that would be less harmful to society.

The working group proceeded on the basis of the Swedish FRA system and set out to provide justifications for its introduction. The report has not established whether heavy-calibre online surveillance is necessary or even an effective means of threat prevention. However, we have made it clear in our dissenting opinion that we are prepared to revise our position if sound reasons are presented.

In preparing its position on online surveillance, the Ministry of Transport and Communications has extensively consulted both domestic and foreign business communities. The Ministry of Employment and the Economy and the National Police Board have issued separate statements on the report. We know that Finnish business and industry also takes a highly critical view of online surveillance, but industry representatives have not been involved in the preparatory process. However, since the publication of the report, the Confederation of Finnish Industries (EK) and the Federation of Finnish Technology Industries have announced in a press release that they cannot accept the introduction of telecommunications intelligence as outlined in the report, and feel that the arguments put forward in this respect are neither adequate nor compelling.

There are several reasons why we take a negative position on online surveillance. These reasons are detailed in our dissenting opinion.

Ministry of Transport and Communications

Office
Eteläesplanadi 16
(Registry)
FI-00100 Helsinki

Postal address
PO Box 31

FI-00023 Government

Tel
+358 295 16001

www.lvm.fi
firstname.lastname@lvm.fi

kirjaamo@lvm.fi

1. Our principal objection is that online surveillance violates fundamental rights, specifically to confidentiality of communications and privacy protection.
   - Online surveillance would necessarily target Finnish communications. In practice, it would be impossible to selectively track and monitor only foreign, cross-border communications. (This is due to the international and therefore cross-border nature of digital services and the servers on which they run. Furthermore, communications are often routed via foreign networks even when both parties to the exchange of information are Finnish.)
   - The introduction of online surveillance would require constitutional amendment: this is the working group's unanimous view. The same might apply to the processing of identification data.
   - One of the provisions included by Parliament in the Information Society Code was that every possible step shall be taken to safeguard the rights of electronic service users in online environments, such as the protection of privacy and confidentiality of messages, and that the development of cyber security shall give special consideration to the protection of these rights.

2. Online surveillance is a rather ineffective means to achieve the desired results. It does not produce the information it might have produced earlier. This is due to the development and increased use of encryption techniques as well as the increasing volume of data communications. It is unlikely that security authorities from other countries would choose to send their messages without any encryption. The deciphering of encrypted communications would, in turn, require substantial resources that the working group has not identified. In other words, it is also necessary to weigh the priorities of cyber security development. Recently there have been media reports stating that authorities in the UK are considering a ban on services that use encrypted communication that is beyond the reach of online surveillance. In other words, even Britain does not have the tools it would need to decrypt communication.

3. Online supervision can have major business implications, especially for data-driven businesses and business location decisions. On this point the Ministry of Employment and the Economy concurs with our dissenting opinion. It is paramount to carefully weigh the implications for business. It might be a competitive advantage for Finland to refrain from online surveillance. We appreciate the difficulty of assessing the implications for business, but the working group's investigations have not been sufficiently thorough. The report refers to two international studies, one of which is actually focused on other issues than online surveillance. The other study was conducted by a consultancy that in another report, commissioned by the Ministry of Transport and Communications, arrived at quite different conclusions. The consultancy's work predates the Snowden revelations.

4. Online surveillance would not improve information security, but on the contrary undermine it. Online surveillance would be designed to bypass or crack the protection mechanisms set up for communication in the channels and networks targeted. It would compromise the information security of everyone sending and receiving messages carried over the communications networks subject to surveillance. There might, of course, be individual cases where online surveillance could improve the information security of a certain company or agency, for instance. However, the development of information security is a far more necessary, more effective and less costly way of achieving the desired results. Besides, this path would not violate anyone's fundamental rights.

5. Intelligence powers, just as any other powers given to authorities, must be justified by reference to the authority's statutory duties.
   - The Ministry of Transport and Communications takes the view that the police have comprehensive access to crime-related information through existing data systems in Finland pursuant to the Police Act and the Coercive Measures Act. If the current powers of the police are deemed inadequate in view of their tasks, the Ministry considers it justified that the regional or material scope or other conditions for the application of these secret coercive means be reassessed.
   - The working group justifies the need for online surveillance on grounds that it will be used to ”prevent cyber threats”. However, intelligence or general threat prevention are not among the statutory tasks of either the defence forces or the police. This would first need to be discussed in open, public debate, and it would require a political decision.

The working group would have benefited from greater openness and diversity in the preparatory process. It should have weighed various alternatives to online surveillance, and it should have given more extensive consideration to its effects and implications.