Communication on the information security of services implemented abroad

FICORA's recommendations

205/2014 S

Viestintävirasto
Kommunikationsverket
Finnish Communications Regulatory Authority

Itämerenkatu 3 A
PL 313
00181 Helsinki
Puhelin 0295 69 661
www.viestintävirasto.fi

Östersjögatan 3A
PB 313, FI-00181
Helsingfors, Finland
Telefon +358 295 390 100
www.kommunikationsverket.fi

Itämerenkatu 3A
P.O. Box 313, FI-00181
Helsinki, Finland
Telephone +358 295 390 100
www.ficora.fi

DESCRIPTION

Publisher
Finnish Communications Regulatory Authority (FICORA)

Date of publication
25 June 2014

Authors
Finnish Communications Regulatory Authority
Working group for the information security of international services

Type of publication
Recommendation

Commissioned by
-

Name of publication
Communication on the information security of services implemented abroad

Abstract
After the summer of 2013, there have been discussions concerning the effects of international mass intelligence of foreign authorities on the protection of confidential communications. Finnish telecommunications operators have not observed that the intelligence activities have affected the information security of public communications services.

Because part of the communications services are partly or completely implemented outside Finland or by using services provided by foreign companies, which means that regulation deviating from Finnish legislation may apply to the implementation of these services, it is justified that information on the matter is available to the users of the services. This type of information enables that the users can assess potential threats directed against their communications and identification data.

This recommendation describes the type of information telecommunications operators should provide to the users, as well as in which situations and how the information should be provided. 21 persons from 12 different organisations participated in the drafting of the recommendation in the spring of 2014.
Heidi Kivekäs (Chairperson) (FICORA), Eeva Lantto (Secretary) (FICORA), Gustavo Covarrubias (Line Carrier Oy), Seppo Heikura (Fonecta Oy), Tuomas Helistö (Fonecta Oy), Tarja Helkamäki (Elisa Oyj), Kari Jaksola (Finnet Association), Kim Johansson (Corenet Oy), Päivi Konttila-Lokio (TeliaSonera Finland Oyj), Pasi Korhonen (Elisa Oyj), Marja-Leena Lehmus (Line Carrier Oy), Tommi Linnonmaa (Digita Networks Oy), Jorma Mellin (TDC Oy), Pasi Reinonen (AinaCom Oy), Panu Rissanen (DNA Oy), Jarkko Saarimäki (FICORA), Janne Sormunen (Finnet Association/Mikkelin Puhelin Oyj), Tiina Tirkkonen (DNA Oy), Simo Tossavainen (TDC Oy), Jaakko Turunen (Finnet Association) and Simo Volanen (ComSecure Oy).

Keywords
Intelligence, confidential communications, information security, communication

Name of series
FICORA's recommendations

Pages, total	Language	Confidentiality
12	English	public

Distributor	Publisher
Finnish Communications Regulatory Authority (FICORA)	-

Content

1 Introduction

In the summer of 2013, the international intelligence activities of the authorities of the United States were widely discussed in public. It was publicly stated that foreign intelligence authorities would have access to users' confidential data directly via providers of various electronic services. Intelligence activities differ from the traditional measures of constraint, such as telecommunications interception and supervision, with respect to the scope of communications. Measures of constraint are directed very precisely to a certain target on the basis of suspicion, whereas intelligence activities are proactive monitoring of a large crowd.

On the basis of FICORA's surveys carried out in 2013 (see more details in chapter 2.1), telecommunications operators had not observed that the intelligence activities had affected the information security of public communications networks.

However, Finnish telecommunications operators can implement some of their communications services outside Finland or utilise services provided by foreign companies when implementing their own communications services. In addition, Finns can acquire services directly from foreign service providers. When using communications services that have been partly or completely implemented abroad, the users should note that neither Finnish legislation nor Finnish telecommunications operators can guarantee that the confidentiality of the communications is retained outside the Finnish borders.

This recommendation continues the work that FICORA began in 2013. Its purpose is to provide guidelines for telecommunications operators with regard to the communication on the features of internationally implemented services. These recommendations, which have been drafted in cooperation with sectoral actors and whose purpose is to improve the users' access to information, support both telecommunications operators' operations, as well as FICORA's supervision related to the matter.

2 Previous measures

This chapter describes FICORA's previous surveys and the measures taken on the basis of them, concerning the effects of international intelligence activities on the security of communications services.

2.1 The 2013 survey

In order to evaluate the effects of the intelligence activities, FICORA sent a request for clarification (reg.no. 890/601/2013) to Finnish telecommunications operators on 11 June 2013. On 5 July 2013, the request was sent to the key cooperation partners that the operators had reported. The telecommunications operators were requested, for example, to submit further information on the communications services that are implemented in cooperation with foreign partners and to specify the companies that involve in the implementation of the services. Meanwhile, the cooperation partners were requested to submit information on, for example, the role in which the company provides its services, the party with whom the user enters into an agreement on a service, and the regulation applied to the service.

FICORA received clarifications from 55 telecommunications operators and 7 partners. These clarifications gave a comprehensive picture of the situation. The telecommunications operators reported that the security of services was not compromised by the intelligence activities. FICORA published a summary of the survey results on 16 October 2013[1].

In the summary, FICORA stated, among others, that it will initiate negotiations with the telecommunications operators on ensuring the information security of a service implemented abroad, as well as on a detailed method for implementing the communication on the matter. On 25 November 2013, FICORA held a discussion event related to the matter for the telecommunications operators. On 13 January 2014, it set up a working group to draft a recommendation on the communication on the matter.

2.2 Guidelines for users

In addition to the cooperation with the telecommunications operators, FICORA has previously published on its website guidelines for users to protect their communications[2]. On the website, the users are reminded that "the confidentiality of messages delivered in Finnish telecommunications networks is protected by Finnish legislation. However, Finnish legislation can-

[1] https://www.viestintavirasto.fi/attachments/tiedusteluselvitys16102013_ENG.pdf

[2] https://www.viestintavirasto.fi/en/steeringandsupervision/guidelinesinterpretationsrecommendationsandreports/documentsforguidelinesinterpretationsrecommendationsandreportst/guidelinesforprotectingcommunications.html

not guarantee that confidentiality is retained in foreign communications services or outside the Finnish borders". Because the use of content services on the internet always means that the user's communication and identification data will probably end up outside Finland, the website describes how to protect against threats related to the most commonly used services.

The working group that drafted this recommendation noticed that there are several factors that are common to telecommunications operators with regard to the implementation of such communications services that pertain the recommendation's scope of application (see chapter 3.1) and that have an international linkage. In order for the telecommunications operators to e.g. implement charging[3], the processing of the charging data collection, i.e. the records concerning the charged transaction, may be acquired from abroad, although the billing, i.e. the actions taken to collect fees from the customers for the use of communications services, is implemented in Finland.

Therefore, the working group agreed on that, during 2014, FICORA will supplement the existing general user guidance on its website, so that the information describes e.g. what the handling of identification data (vs. the actual part of the communications network) abroad means in practice. In the same context, FICORA will inform that the telecommunications operators' websites contain information on the areas where the services are implemented as described in this recommendation.

2.3 FRA law in Sweden

After several years of preparation, the so-called FRA law was passed in Sweden in June 2008. The law gave the Swedish National Defence Radio Establishment (Försvarets radioanstalt, FRA) the right, in the intelligence activities related to the defence of the country, to direct signals intelligence at such communication that is transmitted in wireless and fixed networks and that crosses the Swedish borders.

FICORA was informed of the bill on the signals intelligence in Sweden in January 2007. On 23 February 2007, FICORA sent a request for clarification (reg.no. 890/601/2013) to the largest telecommunications operators transmitting foreign traffic to a significant degree. FICORA requested the telecommunications operators to assess the impacts of the bill on the information security of communications services.

[3] In FICORA Regulation 31, charging means technical and administrative functions related to charging data collection, billing and accounting in telecommunications.

Based on the received replies and the discussions with the telecommunications operators in March 2007, FICORA sent, on 30 March 2007, all telecommunications operators an opinion on telecommunications operators' obligation, based on the Act on the Protection of Privacy in Electronic Communications, to ensure the information security of communications services and to notify their customers of information security threats to services implemented abroad, but provided to Finnish customers.

In August 2008, the Minister of Communications, Suvi Lindén, ordered the Ubiquitous Information Society Advisory Board, appointed by Lindén earlier, to assess additional measures required to guarantee Finnish users' confidential communications.

FICORA was given the task of preparing a comprehensive communication project concerning the encryption of communications. The matter was prepared at FICORA in cooperation with the largest telecommunications operators. The project resulted in a website related to the protection of communications. The website was launched on 5 February 2009 (the latest version is available at ficora.fi[3]).

According to information received from Ficom ry, all its member companies had delivered a customer notice concerning the subject to their customers after February 2009.

As the legislation in Sweden entered into force, FICORA published, on 7 May 2009, its following opinion on the same subject. In the opinion, FICORA stated, among others, that the customers must be informed of potential information security threats that cannot be prevented.

3 Recommendations for telecommunications operators

3.1 Scope of application

This recommendation concerns communication networks and services[4], as well as the communications provided via them in the following situations:

[4] According to section 2(1)(2) of the Act on the Protection of Privacy in Electronic Communications (516/2004), communications network means a system comprising cables and equipment joined to each other for the purpose of transmitting or distributing messages by wire, radio waves, optically or by other electromagnetic means. According to section 2(1)(6) of the Act, communications service means the transmission, distribution or provision of messages by a telecommunications operator in a communications network to a set of users that is not subject to any prior restriction. FICORA has published on its website interpretation guidelines for defining communications services and networks (i.e. telecommunications):

1. both parties participating in the communications are located in Finland
2. the customer has entered into an agreement on communications services with a service provider doing business in Finland, and
3. the communications and related identification data[5] are processed or they can be processed abroad.

The recommendation concerns all communications services except for internet access services[6] for the actual data transfer between a subscription and the public internet. This definition has been made because the data transfer connection in itself should enable an access to the internet and the services available on the internet. Meanwhile, the content services (from the viewpoint of the service provider and the technical implementation) are located around the world. They are independent of the telecommunications operator that provide internet access services. Therefore, when drafting this recommendation, the working group deemed appropriate to restrict the recommendation's scope of application to concern internet access services.

The recommendation does not apply to the production or maintenance of network devices, customer or management systems or related software either. Neither does it apply to the software used for monitoring and maintaining functionality of communications services or networks. For example, when a disruption in a communications service is caused by a problem in a network device, the device manufacturer may have to involve in the repair of the problem. Because network device and software manufacturers are multinational companies, it is not possible in all situations to investigate faults entirely in Finland. When investigating a fault, a restricted amount of mainly identification data related to communications may end up in the possession of device manufacturers.

Examples of the implementations the recommendation applies to:

---

https://www.viestintavirasto.fi/en/steeringandsupervision/regulatoryobjectives/interpretationguidelinesontelecommunicationsandtelecomsoperators.html

[5] According to section 2(1)(8) of the Act on the Protection of Privacy in Electronic Communications, identification data means data which can be associated with a subscriber or user and which is processed in communications networks for the purposes of transmitting, distributing or providing messages.

[6] In FICORA's regulations, internet access service refers to a communications service through which a connection can be established to the internet, and the services available on the internet can be accessed. The definition covers data transfer from a subscription to the public internet, DNS resolvers and DHCP service, which are obligatory for accessing the internet. However, services used while being connected are excluded from the definition.

- The e-mail server of a telecommunications operator is located abroad or the service is acquired through subcontracting from a foreign subcontractor.
- In order to implement charging, the telecommunications operator acquires service for the processing of the charging data collection, i.e. the records that contain identification data and that concern the charged transaction, from a foreign subcontractor.
- The telecommunications operator's DHCP, DNS or authentication service (RADIUS) is located abroad.

Examples of the situations the recommendation does not apply to:

- The users communicate themselves abroad or to abroad, i.e. they use their telephone abroad or they make calls to foreign telephone numbers.

3.2 Assessment of information-secure implementation

According to section 10(2) of the Constitution of Finland, the secrecy of correspondence, telephony and other confidential communications is inviolable. The protection can be broken only with consent of the party to the communication or on the basis of grounds found in the Finnish legislation. According to the Penal Code, communications secrecy violation is a punishable act.

According to the Act on the Protection of Privacy in Electronic Communications, telecommunications operators are obliged to ensure that their services are information-secure. According to section 2(1)(13) of the Act on the Protection of Privacy in Electronic Communications, information security means, among others, the administrative and technical measures taken to ensure that data is only accessible by those who are entitled to use it.

Communications services that are partly or completely implemented outside Finland are also subject to imperative legislation in other countries. The legislation in the countries where services are implemented can oblige the person who handles data to disclose it to a foreign authority or intelligence organisation. Telecommunications operators cannot restrict the operational preconditions of foreign authorities for instance with reservations in contracts.

An information request on telecommunications operators customer information which a foreign authority submits to a telecommunications operator or its subcontractor is not an acceptable reason referred to in the Act on the Protection of Pri-

vacy in Electronic Communications for handling messages and related identification data. The way how the access to data is arranged does not have any relevance in the matter. Therefore, implementing communications services outside Finland can pose a particular information security threat to the data handled in communication services.

Telecommunications operators should implement their services in such a manner that the users' confidential communications and other information are not revealed to third parties. However, the Act on the Protection of Privacy in Electronic Communications gives telecommunications operators an opportunity to make the measures taken to ensure information security commensurate with the seriousness of threats, technical development level, and expenses. It is not possible for telecommunications operators to assess on the behalf of the users the severity of threats caused by the implementation of a service in a certain legal system.

Telecommunications operators can assess mainly in terms of their own business operation and at a general level how significant the information security threat that the implementation of a communications service partly or completely outside Finland poses to the communications service. Typically, this kind of assessment is part of the internal risk management of telecommunications operators. It affects not only operators' own consideration on how and where it implements its services, but also the question of whether the subscribers and users should be notified of the implementation.

3.3 Obligation to notify subscribers and users

Implementing a communications service partly or completely outside Finland may pose a particular information security threat to subscribers or users[7] because their data is handled in the communications services. Therefore, telecommunications operators must notify their subscribers and users of the threat.

Telecommunications operators are obliged to investigate different possibilities to implement their services when assessing potential information security threats directed against the services. However, telecommunications operators do not have any actual possibility to assess the severity of threat on the behalf

[7] According to section 2(1)(10) of the Act on the Protection of Privacy in Electronic Communications (516/2004), subscriber means a legal person or a natural person who has entered into an agreement concerning the provision of a communications service. According to section 2(1)(12) of the Act, user means a natural person who uses a communications service without necessarily being a subscriber to the service.

of the users because it depends on what kind of data and how sensitive the data handled in the services is. Business secrets and the users' personal communications, among others, can be targets for different types of threats. In order to assess potential threats posed by the areas where the services are implemented, as well as the severity of the threats, the subscribers and users must have access to the information on the areas where the services are implemented.

If a telecommunications operator's communications service is implemented completely or partly abroad, i.e. the data handled in the service may be subject to such regulation that deviates from the legislation in Finland, telecommunications operators must notify their subscribers and users of the matter. The information provided to the subscribers and users must indicate, at least, whether confidential communications and identification data are handled only in Finland, elsewhere in the EU or EEA, or outside these areas.

Recommendation 1: FICORA recommends that telecommunications operators notify their subscribers and users of the areas where their communications services are implemented, at least by providing information on whether the data is handled only in Finland, elsewhere in the EU or EEA, or outside these areas.

When communicating on the handling outside the EU or EEA, it is recommended to also mention in which countries exactly the handling takes place.

Recommendation 2: When communicating on the implementation outside the EU or EEA, FICORA recommends to also mention in which countries exactly the implementation or partial implementation takes place.

In practice, telecommunications operators can publish information on the international implementation of communications services on their websites. Naturally, the corresponding information must also be available via other customer service channels of the operators. It is essential that the subscribers or users are able to assess the significance of the threats when choosing services. If the information described in this recommendation is already available in the telecommunications operator's person register descriptions, privacy policies or other cor-

responding documents, it suffices to fulfil the issued communication recommendations.

The above-mentioned communication measures should be started on 1 January 2015.

Recommendation 3: FICORA recommends that the telecommunications operators start communicating in accordance with this recommendation on 1 January 2015.

3.4 Notifications to FICORA

Section 21 of the Act on the Protection of Privacy in Electronic Communications obliges telecommunications operators to notify the Finnish Communications Regulatory Authority without undue delay of significant violations of information security in network services and communications services and of any information security threats to such services that come to the attention of telecommunications operators. FICORA states that the so-called permanent factors that are discussed in this recommendation and that concern the implementation of services abroad do not require separate notifications to FICORA. FICORA gathers this type of information by separate surveys, if necessary.

Naturally, acute information security incidents and threats are subject to the notification obligations referred to in the Act and the complementary regulation 9 D/2009 M[8]. Commission Regulation (EU) No 611/2013[9] concerns especially the notifications of violations of personal data (such as identification data).

[8] FICORA Regulation 9 D/2009 M on the obligation to notify of violations of information security in public telecommunications (https://www.viestintavirasto.fi/attachments/maaraykset/Viestintavirasto09D2009M.pdf)
[9] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:EN:PDF