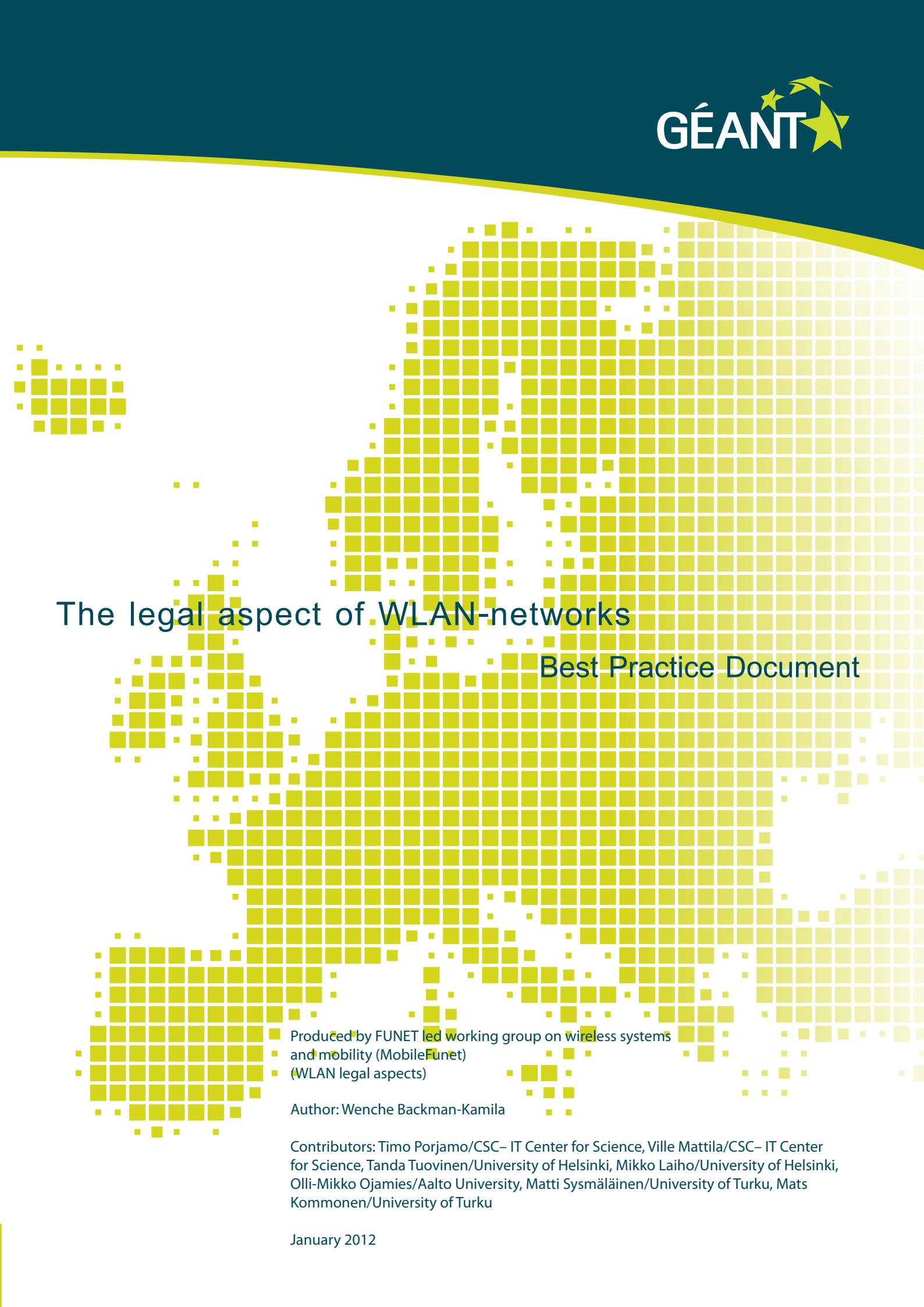

The legal aspect of WLAN-networks

Best Practice Document

Produced by FUNET led working group on wireless systems and mobility (MobileFunet)
(WLAN legal aspects)

Author: Wenche Backman-Kamila

Contributors: Timo Porjamo/CSC– IT Center for Science, Ville Mattila/CSC– IT Center for Science, Tanda Tuovinen/University of Helsinki, Mikko Laiho/University of Helsinki, Olli-Mikko Ojamies/Aalto University, Matti Sysmäläinen/University of Turku, Mats Kommonen/University of Turku

January 2012

Document No: GN3-NA3-T4-wlan-legal-aspects
Version / date: 27.1.2012
Original language: Finnish
Original title: “WLAN-verkot ja lainsäädäntö”
Original version / date: 1.0 of 27.1.2012
Contact: wenche.backman-kamila@csc.fi

Funet bears responsibility for the content of this document. The work has been carried out by a Funet led working group on wireless systems and mobility as part of a joint-venture project within the HE sector in Finland.

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 238875, relating to the project 'Multi-Gigabit European Research and Education Network and Associated Services (GN3)'.

Table of Contents

Executive Summary

This document presents an overview of the Finnish legislation pertaining to WLANs (Wireless Local Area Networks) with the aim of providing Funet members with an overall understanding of what is required of their WLANs. Legislation makes a distinction between network provision to a restricted set of users and to a set of users that is not subject to any restriction. Should the WLAN be used to provide Internet access to an unrestricted user base, the activity would constitute public telecommunications.

In all WLAN networks Information security must be secured through sufficient technical means. If user identification and location data are collected, the information security of such data must be ensured. All communications networks and services are also subject to technical quality requirements.

Funet members are not obligated to collect or store identification data. If identification data are collected, their processing is allowed by law for a few specified purposes.

A description of file is required for log files associated with the services of Funet organisations. By law, the description of file is only required to indicate the data that is actually collected, i.e. not the services for which data is collected. Similar data are collected for several services; in such cases one description of file is sufficient.

1 Introduction

This document presents an overview of the Finnish legislation pertaining to WLANs (Wireless Local Area Networks) with the aim of providing Funet members with an overall understanding of what is required of their WLANs. The document begins with an overview of legislation specifically applicable to WLANs, followed by topics closely related to WLANs – such as description of file and log files – which are also applicable to services other than WLANs. Since the subject matter deals with legislation, the statements contained in this document can be considered orders. However, since the document was drawn up within the Funet community and is based on the consensus of the community, it cannot be considered an authoritative order. If in doubt, please consult a lawyer. The section at the end of the document deals with guidelines pertaining to WLANs and does NOT examine legislation.

It should be stated here that if the legislation is open to interpretation, the size of the Funet community gives it a relatively large amount of influence as regards any interpretation. Therefore the consensus of Funet members with regard to issues that are open for interpretation is also presented here. The Funet community was also consulted during the drafting of legislation, as a result of which the IT departments of universities and educational institutions are clearly distinguished from telecommunications operators in the legislation.

2 Legislation specifically applicable to WLANs

The key legislation relating to WLANs comprises the Communications Market Act (23.5.2003/393) [1] and the Act on the Protection of Privacy in Electronic Communications (16.6.2004/516) [2]. The view of the Finnish Communications Regulatory Authority as regards the application of the legislation can be found in its memorandum: Application of the communications market legislation to the provision of wireless broadband connections 21 August 2007 [3].

The Act on the Protection of Privacy in Electronic Communications makes a clear distinction between corporate and association subscribers and telecommunications operators. For purposes of the Act, corporate or association subscriber means “a company or organisation which subscribes to a communications service or a value added service and which processes users’ confidential messages, identification data or location data in its communications network”. From a legal perspective, Funet members are therefore considered corporate subscribers since they provide free-of-charge communications services to their students and staff.

The Communications Market Act contains detailed provisions on the rights of the user, with particular emphasis on a scenario in which a user purchases a subscription from a telecommunications operator. Since the WLANs of Funet members are provided to users free of charge, these regulations can be disregarded. However, both the Communications Market Act and the Act on the Protection of Privacy in Electronic Communications place requirements on the technical functionality, reliability, safety and information security of WLANs. These requirements also apply to WLANs provided to users free of charge, and are described under “Legislation applicable to all WLANs”. First, a brief introduction to the differences between open WLANs and those requiring authentication:

2.1 Differences between open WLANs and those requiring authentication

Legislation makes a distinction between network provision to a restricted set of users and to a set of users that is not subject to any restriction. The user base of a campus network requiring authentication is subject to advance restrictions. Similarly, the open WLANs of small campuses are considered restricted due to their limited coverage area; according to the memorandum of the Finnish Communications Regulatory Authority the WLAN offered by, for example, a café is offered to a restricted set of users. The WLANs provided by Funet members are limited to campus areas. The Funet community therefore considers the user base of an open campus network to be restricted due to the limited coverage area of the network. Should the WLAN be used to provide Internet access to an unrestricted user base, the activity would constitute public telecommunications.

Operators must submit a written notification to the Finnish Communications Regulatory Authority before launching public telecommunications operations (guidelines on submitting a telecommunications notification can be found on the website of the Finnish Communications Regulatory Authority: [4]).

A notification is also required of any changes in activity and of its termination. The notification duty is subject to payment liability; since the fee is determined on the basis of turnover, no fee is likely to be involved with free, open networks. If it were found that an open WLAN covering a large campus could be deemed to constitute public telecommunications activity, campuses would be required to comply with the requirements set for public telecommunications networks, which are not covered in this document.

Log data is often collected both in open WLANs and in those requiring authentication. Log files may contain identification and location data, which must be protected in accordance with the provisions of the Act on the Protection of Privacy in Electronic Communications; see under “Log files” below.

As a result of the legislative amendment of 15 March 2011 the use of an unencrypted WLAN for Internet access is no longer punishable: further information is available in [5]: the press release of the Ministry of Justice of 3 March 2011 (in Finnish).

This clarifies the situation considerably: a user may not be able to tell in advance whether an unencrypted network is intended for public use or whether the lack of encryption is unintentional.

2.2 Legislation applicable to all WLANs

The Communications Market Act and the Act on the Protection of Privacy in Electronic Communications contain requirements regarding the technical functionality, reliability, safety and information security of WLANs.

2.2.1 Information security

Information security must be secured through sufficient technical means. The rights and obligations relating to information security are governed by Sections 19 and 20 of the Act on the Protection of Privacy in Electronic Communications, while more detailed specifications can be found in the Finnish Communications Regulatory Authority memorandum “Application of the communications market legislation to the provision of wireless broadband connections”. The following measures are required:

- Telecommunications must be protected against unlawful interception. If traffic is not encrypted at the air interface, users must be informed of the risks of unlawful interception and rerouting, as well as of the means available for protection against these threats. Neither open nor web-authenticated networks use traffic encryption at the air interface. To meet the above requirements, users may be directed to a landing page providing instructions after successful authentication or connection to the network. Users can be instructed to use a VPN (Virtual Private Network) connection whenever possible to protect them from unlawful interception and rerouting. If the operator does not wish to use a landing page providing instructions, these may be posted at entrances to buildings, for example. The minimum requirement is that information regarding the unencrypted WLAN is available on the website of the organisation. However, it is unclear whether this is sufficient.

- The WLAN provider must have the ability to disconnect a user from the network in the event that the user is guilty of, for example, Denial of Service attacks or other disturbance to the network. Users may be disconnected by closing the user account or by using a revocation list based on the MAC addresses (Media Access Control) of terminals. The obligation to disconnect users causing disturbance is also applicable to WLANs utilising Network Address Translation (NAT).

- The Finnish Communications Regulatory Authority must be notified of significant faults and disruptions. The notification duty may apply, for example, to cases in which the WLAN was used for spreading malware or for significant data breach attempts.

It should also be stated that the decryption of WLAN encryption, regardless of the technical level of encryption, is a criminal offence. Even the decryption of WEP (Wired Equivalent Privacy) encryption, which is relatively simple due to the weak level of encryption, is therefore a crime. Motivations and basic instructions on the use of WLAN encryption techniques (including technical terminology) can be found in the instructions “Koti-WLANin suojaaminen 27.7.2010“ (“Protecting your home WLAN”), [6], available in the Information Security Guide published by the Finnish Communications Regulatory Authority.

If user identification and location data are collected, the information security of such data must be ensured. The Finnish Communications Regulatory Authority memorandum states that the measures taken towards ensuring the information security of the service and related data processing should be commensurate with the seriousness, technical sophistication and cost of the threat. There is no obligation to eliminate all information security threats, for example, in cases in which this would result in unreasonable costs or would be technically impossible.

2.2.2 Quality and other technical requirements

All communications networks and services are subject to technical quality requirements specified in Section 128 of the Communications Market Act:

- The technical quality of telecommunications must be of a high standard, and the networks must be able to withstand normal, foreseeable climatic, mechanical and electromagnetic interference. Moreover, the networks and services must not cause electromagnetic or other interference.

- The protection of privacy and information security must not be endangered, and the health and assets of users or other persons must not be put at risk.

- The networks must function together and it must be possible to connect terminal equipment to them that meets the requirements of the Radio Act.

- The debiting of potential fees relating to network use must be reliable and accurate.

- Access to emergency services must be secured as reliably as possible even in the event of network disruptions.

Access to emergency services may also need to be taken into consideration with regard to disruptions, if no alternative access to emergency services is available.

In principle, communications networks are also required to prepare for disruptions during normal conditions and contingencies. However, according to the Finnish Communications Regulatory Authority memorandum these obligations have so far not been applicable to WLANs.

3 Description of file

According to Section 10 of the Personal Data Act (22.4.1999/523), [7] (in Finnish), the controller shall draw up a description of the personal data file, which must be publicly available on the controller's premises or website. Personal data means any information that can be used to identify a natural person and his or her family (or other comparable set of people), his or her personal properties or living conditions. Further information is available in the following guide published by the Data Protection Ombudsman: "Ota oppaaksi henkilötietolaki! 15.9.2010" ("Let the Personal Data Act be your guide") [8]. The description of file form in Finnish and instructions for filling in the form are available on the website of the Data Protection Ombudsman [9].

A description of file is required for log files associated with the services of Funet organisations. By law, the description of file is only required to indicate the data that is actually collected, i.e. not the services for which data is collected. Similar data are collected for several services; in such cases one description of file is sufficient. However, a separate description of file is generally required for e-mail services, for example; data collected from wireless networks can be covered by the description covering other IT services.

Should the Funet member wish to present the data collected on WLAN users on a separate description of file, the description of file for the eduroam service at the University of Helsinki is a useful example: [10].

4 Log files

The Act on the Protection of Privacy in Electronic Communications does not obligate corporate and association subscribers to collect or store identification data. If identification data are collected, their processing is allowed by law for the following purposes:

- provision of network, communications and value added services and measures geared towards ensuring their information security
- billing
- technical development of services and operation
- prevention and investigation of misuse
- determination of technical faults.

The processing of identification data is governed by Chapter 3 of the Act on the Protection of Privacy in Electronic Communications.

If the police or rescue authorities are entitled by law to obtain the information, any stored identification data relating to WLANs must be handed over to them. Even in such cases the authority in question must present legal justifications for the request.

5 Guidelines specifically applicable to WLANs

Guidelines applicable to WLANs are presented here separately from statutory obligations.

5.1 VAHTI instructions

The VAHTI instructions of the Ministry of Finance, [11] (in Finnish), are only binding on public and state administration and therefore do not obligate most Funet members. Although the instructions are not binding, it is advisable to follow them. Chapter 10 of the VAHTI LAN instructions contain instructions relating to wireless LANs, [12] (in Finnish).

References

[1] Communications Market Act (23.5.2003/393), Available at http://www.finlex.fi/en/laki/kaannokset/2003/en20030393.pdf

[2] Act on the Protection of Privacy in Electronic Communications (16.6.2004/516), Available at http://www.finlex.fi/en/laki/kaannokset/2004/en20040516.pdf

[3] Application of the communications market legislation to the provision of wireless broadband connections 21 August 2007, Available at http://www.ficora.fi/attachments/englantiav/5vnsXQSlh/Wlan_memorandum.pdf

[4] http://www.ficora.fi/en/index/luvat/teletoimintailmoitus.html

[5] http://www.om.fi/Etusivu/Ajankohtaista/Uutiset/Uutisarkisto/Uutiset2011/1290610236338

[6] http://www.tietosuoja.fi/uploads/n5us2z25j9.pdf

[7] http://www.finlex.fi/fi/laki/ajantasa/1999/19990523#P10

[8] http://www.tietosuoja.fi/uploads/aue2z4d.pdf

[9] http://www.tietosuoja.fi/2584.htm

[10] http://www.helsinki.fi/atk/osasto/selosteet/eduroam_seloste.html

[11] http://www.vm.fi/vm/fi/16_ict_toiminta/009_Tietoturvallisuus/index.jsp

[12] http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20101203Sisaeve/Sisaeverkko-ohje.pdf

Glossary

Funet	Finnish University and Research Network
HE	Higher Education
IT	Information Technology
MAC	Medium Access Control
MobileFunet	a working group on wireless systems and mobility led by Funet
NAT	Network Address Translation
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network