JUHANA RIEKKINEN
University Lecturer in Legal Informatics, LL.D. trained on the bench
University of Lapland, Faculty of Law
E-mail: juhana.riekkinen@ulapland.fi | Publications: https://research.ulapland.fi/en/persons/juhana-riekkinen

VPN Services Between a Rock and a Hard Place: The Freedome Case

Internationales Rechtsinformatik Symposion IRIS 2021

LAPIN YLIOPISTO
UNIVERSITY OF LAPLAND
For the North – For the World

Session 'Sicherheit & Recht II'
26 February 2020, 14:45–16:15
Zoom Konferenzraum B

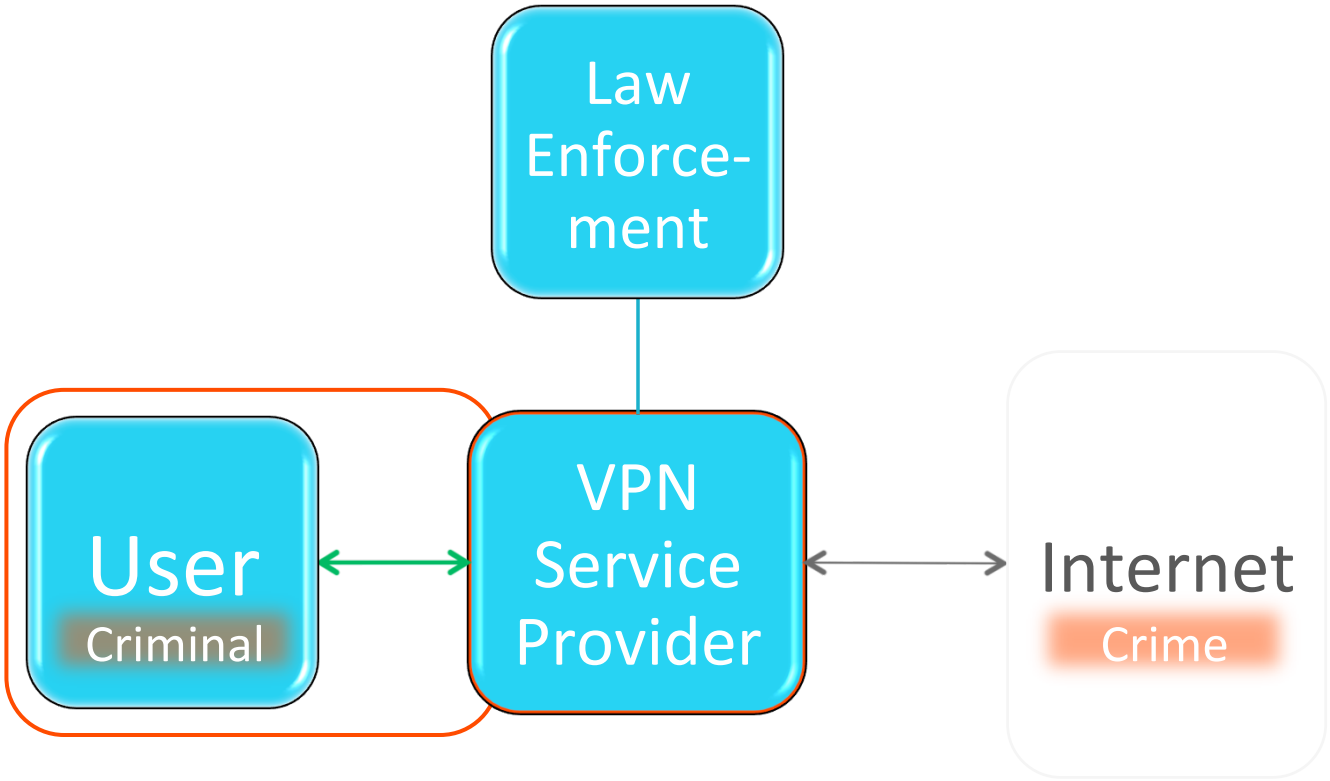
What's a VPN?

- Virtual Private Network = a private network running over shared public infrastructure; can be constructed with different technologies and protocols for different purposes

- Provides enhanced (but not absolute) privacy, anonymity and confidentiality online
  - Secure remote working (client-to-site VPNs for working from home)
  - Protection from surveillance & tracing
  - Bypassing geo-restrictions & censorship

- Risks
  - Does not protect users from abuses by the VPN service provider → a VPN service is only as reliable as the VPN service provider
  - Use of VPN services (along with other PETs) may hinder criminal investigations

The Role of the VPN Provider?



The Freedome Case

FREEDOME VPN is a commercial VPN service offered by **F-Secure**, marketed as an "**online privacy app**" that "**blocks online tracking**" and "**hides your IP address for an extra layer of privacy**"

On 14 Jan 2019, after a request of assistance from the German *Bundeskriminalamt*, the Finnish National Bureau of Investigation issued a data retention order concerning Freedome VPN user logs to F-Secure

On the following day, the NBI seized Freedome logs relating to an IP address received from the German authorities

Subsequently, F-Secure challenged the seizure in Court

In May 2019, the **District Court** rescinded the seizure and ordered the logs to be destroyed

In October 2020, following an appeal by the NBI, the **Court of Appeal** upheld the DC's decision

By the deadline in January 2021, an application for leave to appeal to the **Supreme Court** had been submitted by the NBI

What Was in the Logs?

- When a user **logged into** Freedome, their device was identified and their right to use the service was checked; in the process of identifying the user, their IP address was logged and stored for three days

- When a **VPN connection was established**, additional data were logged and stored for 90 days; in addition to the user IP address, this data included
  - device identifiers
  - session identifiers
  - timestamps (beginning and end of the session)
  - volume of transferred data

Legal Questions

- Should the VPN logs be considered *traffic data/identifying data* or *subscriber information?*
  - *Traffic data/identifying data* are protected under the fundamental right of protection of confidential communications and can not be seized under the conventional power of seizure (**Coercive Measures Act**, chapter 7, section 4)
  - *Subscriber information* can be seized under CMA, ch 7 (or alternatively, under Police Act, ch 4, section 3) without restrictions

- Should a VPN service provider be considered 1) a *telecommunications operator*, 2) a *corporate or association subscriber*, or 3) neither under Finnish law?
  - If neither, would this prevent the application of CMA, ch 7, section 4?

Relevant Law

- CMA, chapter 7, section 1: an object, property or document may be seized, inter alia, if there are grounds to suspect that it may be used as evidence in a criminal case (what concerns documents applies also to computer data)

- CMA, chapter 7, section 4(1): a document or data in the possession of **a telecommunications operator** or a **corporate or association subscriber** may not be confiscated or copied, if it contains data related to a message referred to in CMA, chapter 10, section 3(1), or **identifying data referred to in chapter 10, section 6(1)**, or base station data referred to in chapter 10, section 10(1)

- Seizure is practically always available in a criminal investigation (no *ex ante* warrant, no minimum level of punishment for the suspected offence), whereas *traffic data monitoring* (CMA ch 10, sec 6) is limited to investigations involving relatively serious offenses and generally requires an *ex ante* court decision

Definitions in Finnish Law

- Identifying data (*tunnistamistieto*) in CMA, ch 10, sec 6(1)
  - Before amendment 587/2019: reference to the Act on the Protection of Privacy in Electronic Communications (repealed)
  - After amendment 587/2019: data *concerning a message* that
    - can be associated with a *user* or a *subscriber* (defined in **ECSA**); and
    - is processed in telecommunications networks in order to transmit or distribute messages or keep messages available

- Traffic data (*välitystieto,* lit. "relaying data")
  - **Act on Electronic Communication Services**, sec 3, para 4**0**: "information (that can be) associated with a legal or natural person used to transmit a message --"

- According to the law drafting materials, both terms are supposed to refer to the same data – both the District Court and the Court of Appeal accepted this

Definitions in EU & International Law

- Traffic data
  - **Directive 2002/58/EC**, art. 2(b): “any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof”
  - **Convention on Cybercrime**, art. 1(d): “any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication’s origin, destination, route, time, date, size, duration, or type of underlying service”

  - To add to the terminological confusion, in Finnish translations of the above instruments, the equivalent term is “*liikennetieto*” (lit. “traffic data”), which is further used in national legislation in a section concerning data retention orders (with a definition matching the Convention definition)

European Case Law: Ministerio Fiscal

- ECJ, Ministerio Fiscal, C-207/16, GC Judgment of 2 October 2018
  - Concerned a Spanish *investigating magistrate's decision* refusing to grant the police access to personal data retained by providers of electronic communications services (phone numbers that had been activated with the IMEI code of a stolen mobile phone & names and addresses of the SIM card owners/users)
  - The ECJ stated that the access of public authorities to the data for the purpose of identifying the owners of SIM cards activated with a stolen mobile telephone entails interference with their fundamental rights (CFR art. 7 and 8)
  - However, this interference was not sufficiently serious to entail this access being limited to the objective of fighting *serious* crime

European Case Law: Benedik v. Slovenia

- ECtHR, Benedik v. Slovenia, Judgment of 24 April 2018
  - Concerned law enforcement access to subscriber information relating to a dynamic IP address *without* a court warrant
  - The Slovenian police had requested an ISP to disclose data regarding the user to whom a certain dynamic IP address (linked to CAM file-sharing) had been assigned at a designated time
  - Basis: a section of the Slovenian Criminal Procedure Act which required the operators of electronic communication networks to disclose to the police information on the owners or users of certain means of electronic communication whose details were not available in the relevant directory
  - The ECtHR stated that this national law and the way it was interpreted by the domestic courts lacked clarity and offered insufficient safeguards against arbitrary interference with privacy rights → the interference was not “in accordance with the law” as required by ECHR art. 8(2)

The District Court Decision

- The Court stated that some of the seized log data (including IP addresses) could, under some circumstances, be considered subscriber information; however, session timestamps and traffic volumes could only be considered traffic data

- Considering the nature of the Freedome service and the purposes for which the logged data were stored, the Court found that no data in the seized logs could be considered merely subscriber information in this context

- The Court also acknowledged that purpose of the Freedome service was to anonymize the user's online communications by masking their IP address, and that the objective of the users was not to communicate with F-Secure but with 3rd parties → logging in to the service and opening a VPN connection were not to be understood as communication between the user and F-Secure → logs could not be seized from F-Secure based on them being a party to the communication, not an intermediator

The Court of Appeal Decision

- The Court of Appeal upheld the District Court decision with some additional reasoning
  - It did not matter that a VPN service was neither a *telecommunications operator* nor a *corporate or association subscriber* – despite the wording, CMA, ch 7, art 4 applies to all *communications providers*, which include VPN service providers
  - The NBI's argumentation relying on *Ministerio Fiscal* was disregarded because unlike the present case, that case concerned 1) access based on a court warrant and 2) different types of communication and data than the present case
  - Instead, the assertions in *Benedik v. Slovenia* regarding online privacy were considered to support the conclusion that the logged data seized in the Freedome case should be considered traffic data covered by the protection of confidential communications

Evaluation

- The approach can be characterized as contextual, focusing on the nature of Freedome **as a privacy-enhancing service designed to protect the anonymity and confidentiality of the user's online communications**

- This can be contrasted with an alternative approach based on **strictly textual interpretation** of the relevant sections and definitions and/or **rigid categorization** based on the type of individual data points

- While the argumentation in the decisions can certainly be criticized for lack of precision, both the result and these general viewpoints are surely welcomed by VPN users and legitimate commercial VPN service providers

International Perspective on Data Categories

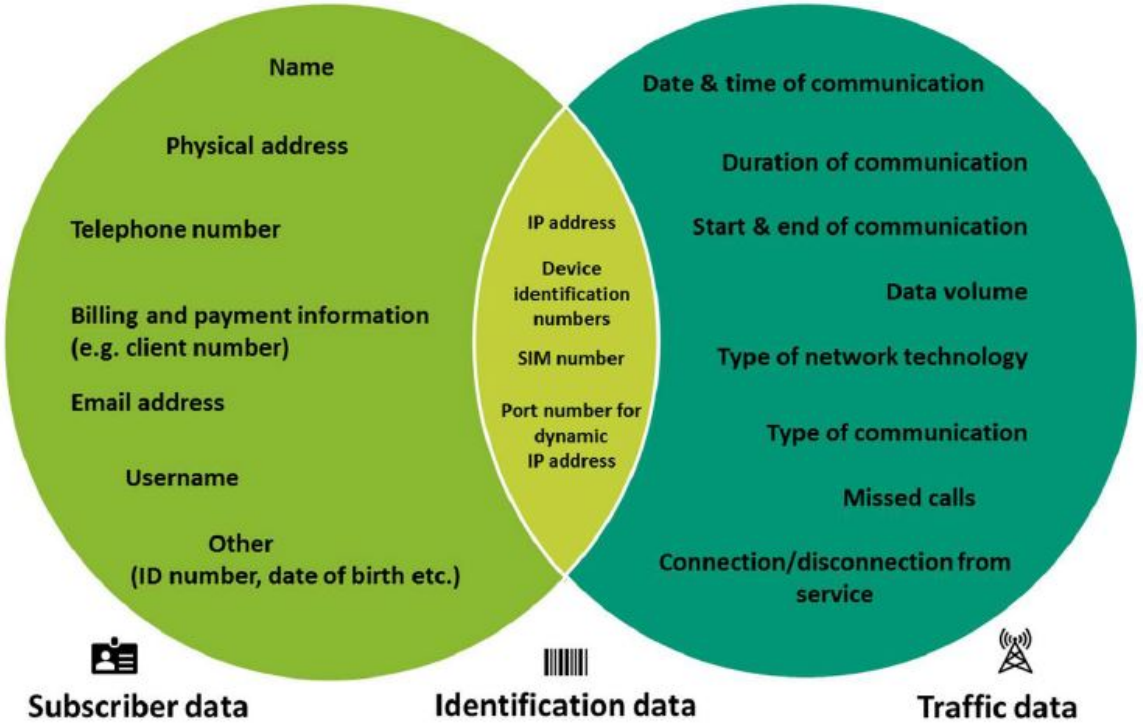
- In law, data is commonly classified to more and less protected categories
  - **Content data** vs **non-content data**
  - Non-content data is typically sub-categorized to **traffic data** and **subscriber data (or subscriber information)**
  - Some national laws add further categories, such as **access data** / **Zugangsdaten**; additional categories have also been suggested in the EU E-Evidence proposal (which differentiates **subscriber data**, **access data**, **transactional data & content data**)

- Definitions vary, and borders between categories are hazy in different legislative instruments & jurisdictions (and even within them!)

- Different treatment of different data can be justified by different levels of privacy interference, but it is questionable whether the prevailing categorization actually captures the reality of the current online environment

International Perspective on Data Categories

Figure 7: Classification differences between subscriber and traffic data



Source: Milieu elaboration

Dupont et al., Study on the retention of electronic communications non-content data for law enforcement purposes, Final report, Publications Office of the European Union, Luxembourg 2020, p. 49.

What Constitutes the Privacy Interference?

- The practical level of interference or intrusion can vary even if the data stays the same; what matters is not the type of the individual data point but how different data are combined

- Easy access to “identifying” data can be justified with safeguards relating to obtaining other data – however, transnational investigations are common and different jurisdictions have
  - Different categories and classifications for data
  - Different prerequisites for data collection methods

- I argue for a **chain of safeguards and fail-safe mechanisms at different stages** of the investigative process
  - No procedural “single point of failure”
  - Helps to prevent and de-incentivize arbitrary actions by public authorities

Other Viewpoints

- Online users have a legitimate expectation of privacy → should using a commercial, legitimate privacy-enhancing service not lead to (at least somewhat) increased expectation?

- If this expectation is not honored by putting in place strong safeguards for law enforcement access, this may incentivize both criminals and law-abiding users to switch to underground services, which
  - do not co-operate with law enforcement in any cases
  - may themselves violate the rights of the users

- Further, in response to their users' privacy concerns, legitimate services may respond by relocating to a different jurisdiction or by revising their logging policies, making data needed to identify perpetrators of serious crime unavailable

Conclusion

- Unlimited access to VPN user logs might simultaneously undermine
  - Criminal investigations
  - Legitimate business interests
  - Safety and security of law-abiding internet users

That does not seem like a good thing.

Paper published in Proceedings (p. 349 ff.) and Jusletter IT (**https://jusletter-it.weblaw.ch/issues/2021/25-Februar-2021/07_datenschutz_und_p_d2ff820682.html**)

Feedback and questions: **juhana.riekkinen@ulapland.fi**
Information on my research & publications:
https://research.ulapland.fi/en/persons/juhana-riekkinen

Thank you very much!
Vielen Dank!
Paljon kiitoksia!

ulapland.fi