VPN SERVICES BETWEEN A ROCK AND A HARD PLACE: THE FREEDOME CASE

Juhana Riekkinen

University Lecturer in Legal Informatics, University of Lapland, Faculty of Law
Yliopistonkatu 8, PO BOX 122, 96101 Rovaniemi, FI
juhana.riekkinen@ulapland.fi; http://bit.ly/2qvkbYk

Keywords: ***Virtual Private Network, Criminal Investigation, Evidence, Seizure, Log, Traffic Data***

Abstract: *Providers of commercial Virtual Private Network services are expected to protect the privacy of their customers, but also to co-operate with law enforcement in legitimate criminal investigations in accordance with the law. In a case concerning a commercial VPN service, the seizure of VPN user logs was challenged in court by the service provider, a Finnish cybersecurity company. Drawing on this case and the reasoning adopted by the national courts, this paper explores the dual role of VPN service providers and the fine line between subscriber data and traffic data in Finnish law and on the European level. Ultimately, it is argued that uncontrolled and unlimited law enforcement access to VPN user logs would jeopardize privacy rights and the business interests of legitimate VPN providers, and that it might additionally lead to undesirable consequences for law enforcement interests.*

1. Introduction

A virtual private network (VPN) is, simply put, a private network running over a shared public infrastructure like the Internet.[1] VPNs are commonly used in businesses and other organizations for remote working, as VPNs allow workers to connect securely to the corporate network from their homes or any other location. VPNs can also be used by individuals who wish to protect themselves from surveillance and tracing, or to access content that is subject to IP-based geo-restrictions or censorship. Although generally understood to be—and advertised as—tools for safeguarding privacy, anonymity, and confidentiality of communications in the online environment, VPN services do not provide absolute protection, in particular in relation to the service provider itself. Among other things, VPN service providers have access to the original IP address of the user, and typically hold information such as names and addresses of their customers. The privacy benefits of VPN services are, indeed, contingent on the reliability and trustworthiness of the service provider, and their ability to protect sensitive information relating to their users.

On the other hand, in cybercrime investigations and other criminal investigations in the online environment, identifying perpetrators of criminal acts remains a major challenge. Identifying individual users (natural persons) based on IP addresses and other online identifiers is uncertain in the best of circumstances, and the use of VPN services, along with other privacy-protecting technologies such as simple proxy servers and the Tor network[2] further complicate criminal investigations.[3] Due to their role as middlemen in private online com-

[1] Strayer, Privacy issues in virtual private networks, Computer Communications, Vol. 27, Issue 6, April 2004, p. 517. As Strayer recognizes, the concept has been given numerous different definitions in different contexts. It should be noted that VPNs are not a single technology; they can be constructed using various protocols and technologies.

[2] Tor Project. https://www.torproject.org (accessed on 13 November 2020).

[3] See, e.g., Sieber, Straftaten und Strafverfolgung im Internet, Verlag C.H. Beck, München 2012, pp. 36–37, Sieber/Neubert, Transnational Criminal Investigations in Cyberspace: Challenges to National Sovereignty. In: Lachenmann/Röder/Wolfrum (eds.), Max Planck Yearbook of United Nations Law, Vol. 20 (2016), Brill | Nijhoff, Leiden 2017, pp. 242–243, Oerlemans, Investigating Cybercrime, SIKS dissertation series no. 2017-01, Meijers Research Institute and Graduate School of the Leiden Law School of Leiden University 2017, pp. 37–44, and Sund, Global and European Responses to Cybercrime. In: Calcara/Sund/Tolvanen (Eds.),

munications, VPN service providers are in a position to compromise and violate their users' privacy, and, from the law enforcement perspective, also in a position to aid with legitimate criminal investigations.[4] As a result, VPN service providers face conflicting expectations from the law enforcement and from their customers who trust them to protect their privacy and anonymity—in the case of commercial VPN providers, often paying a significant fee for exactly this service.

In the next chapter, I present and analyze a noteworthy Finnish court case on law enforcement access to user logs collected by a VPN service provider. This is followed by a more general discussion and conclusions concerning the need for safeguards in law enforcement access to data held by VPN providers.

2. The Freedome Case

2.1. Basic Facts

FREEDOME VPN (hereinafter Freedome) is a commercial VPN service offered by the Finnish cybersecurity company F-Secure Oyj (F-Secure), marketed as an "online privacy app" that, among other things, "blocks online tracking" and "hides your IP address for an extra layer of privacy".[5]

On 14 January 2019, acting in response to a request of assistance from the German Federal Criminal Police Office (*Bundeskriminalamt*), the Finnish National Bureau of Investigation (*keskusrikospoliisi*, NBI) issued a data retention order concerning Freedome user logs to F-Secure.[6] On the following day, the NBI seized[7] Freedome logs relating to an IP address received from the German authorities. The logs were believed to contain information that could be used to identify a suspect in a German investigation relating to a serious criminal offense.[8]

F-Secure contested the seizure in the Helsinki District Court and requested that the seized logs be destroyed. According to F-Secure, the user logs fell under an exception in the national Coercive Measures Act (806/2011, CMA), chapter 7, section 4 prohibiting the confiscation and copying of certain categories of data in the possession of a *telecommunications operator* or a *corporate or association subscriber*. On 10 May 2019, the District Court rescinded the seizure and ordered the destruction of the seized data. The NBI appealed against the decision, which was upheld by the Helsinki Court of Appeal on 21 October 2020. As of the time of writing, the Court of Appeal's decision is not final.[9]

Cybercrime, Law and Technology in Finland and Beyond, Reports of the Police University College in Finland 133/2019, Police University College, Tampere 2019, p. 73.

4 The role of VPN providers in cybercrime response has been highlighted in, e.g., Europol, Internet Organised Crime Threat Assessment (IOCTA) 2020. https://www.europol.europa.eu/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf (accessed on 13 November 2020), p. 61. Due to the risks associated with underground services used by criminals in the past, legitimate commercial services (such as Freedome) are reportedly being used increasingly also to hide criminal activity (p. 17). According to Europol, Internet Organised Crime Threat Assessment (IOCTA) 2019. https://www.europol.europa.eu/sites/default/files/documents/iocta_2019.pdf (accessed on 13 November 2020), p. 48, legitimate services are also being abused by terrorist groups.

5 F-Secure FREEDOME VPN – Protect your privacy. https://www.f-secure.com/en/home/products/freedome (accessed on 13 November 2020).

6 Data retention (or preservation) orders, which are not further discussed in this paper, are regulated in Coercive Measures Act, chapter 8, sections 24–26.

7 In this paper, the terms *seizure* and *seize* are used to refer collectively to both confiscation (of physical objects) and copying (of documents and data) according to the Finnish law.

8 The exact nature of the suspected offense is not clarified in the court decisions, and the court documents concerning the offense are classified at the time of writing.

9 An application for leave to appeal to the Supreme Court has been submitted by the NBI.

2.2. Legal Questions

The main legal questions in the case concerned the different classifications of data in national legislation and the extent of the constitutional protection of confidentiality of communications. F-Secure argued that the logs contained *traffic data* or *identifying data* that were protected under the fundamental right of protection of confidential communications. In contrast, the NBI argued that the data were to be considered *subscriber data* (or *client data*), which are not afforded constitutional protection and can be seized under CMA, chapter 7, or alternatively obtained under Police Act (872/2011), chapter 4, section 3 without restrictions.

Another key question related to the role of a VPN service provider as a party or intermediator of communication. The seized logs were generated when a user logged in to Freedome and opened a VPN connection (which are two different events). F-Secure argued that the logged data nevertheless concerned confidential communication between a user and a third party, and that F-Secure was not a party of communication but an intermediator. The NBI, instead, argued that such logs related to communication between F-Secure and the user.

A further legal question considered by the Court of Appeal was whether a VPN service provider should be considered a *telecommunications operator*, or a *corporate or association subscriber*, and if not, whether this would prevent the application of the exception in CMA, chapter 7, section 4. In the District Court, this legal point had not been a subject of disagreement between the parties, and the section had been considered to apply to any traffic data collected while relaying communications.

2.3. Relevant Law

In Finland, investigatory powers in the context of criminal investigations are defined in the Coercive Measures Act, with related provisions also in the Criminal Investigation Act (806/2011) and the Police Act, which all entered into effect on 1 January 2014.[10]

According to CMA, chapter 7, section 1(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. In the following subsection, it is stated that all the provisions in chapter 7 regarding documents also apply to (computer) data, which entails that data can be seized either by copying the data to a suitable storage medium, or by physically confiscating the storage medium or computer device. There are no further specific material prerequisites for seizure, although the general principles of proportionality and minimum intervention need to be considered. No *ex ante* judicial warrant is required, but a seizure may later be challenged in court under CMA, chapter 7, section 15 (as F-Secure did in the present case).

CMA, chapter 7, section 4(1) states that a document or data in the possession of a *telecommunications operator*[11] or a *corporate or association subscriber*[12] 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).

---

[10] Generally about the Finnish legal framework for investigative powers relating to computer data and cybercrime investigations, see Riekkinen, Evidence of cybercrime and coercive measures in Finland, Digital Evidence and Electronic Signature Law Review, Vol. 13, 2016, pp. 49–66.

[11] The CMA provision contains an outdated reference to the Telecommunications Services Act (393/2003) to define this term. This act was repealed and replaced by the Act on Electronic Communication Services (917/2014, ECSA; original title "Information Society Code") on 1 January 2015. According to ECSA, section 3, paragraph 27 telecommunications operator means "a network operator or a communications service operator offering services to a set of users that is not subject to any prior restriction, i.e. provides public telecommunications services".

[12] Here, another outdated reference is made to the Act on the Protection of Privacy in Electronic Communications (516/2004), which has also been replaced by ECSA. ECSA, section 3, paragraph 41 states that corporate or associate subscriber means "an undertaking or organisation which subscribes to a communications service or an added value service and which processes users' messages, traffic data or location data in its communications network."

For the concept of *identifying data* (Finnish: *tunnistamistieto*), the CMA originally referred to the Act on the Protection of Privacy in Electronic Communications (516/2004), which was repealed on 1 January 2015 when the Act on Electronic Communications Services (917/2014, ECSA) entered into effect. After the District Court decision, the CMA section containing the definition has been updated. According to chapter 10, section 6(1) (587/2019), in order to qualify as identifying data, data must 1) concern a message, which is associated with a user or a subscriber[13], and 2) be processed in telecommunications networks in order to transmit or distribute messages or keep messages available. Further, in ECSA, section 3, paragraph 41 *traffic data* (Finnish: *välitystieto*) are defined as "information associated with a legal or natural person used to transmit a message".[14] According to law drafting materials, the two terms were intended to have the same meaning, and the choice of a new term for ECSA was mostly motivated by the fact that the Finnish word "tunnistamistieto" had been associated with identification services in common parlance.[15] Indeed, in the present case, both courts understood *identifying data* in CMA (and the repealed Act on the Protection of Privacy in Electronic Communications) and *traffic data* in ECSA to refer to the same data.

It should be noted that the prohibition of seizure in CMA, chapter 7, section 4 does not, as such, mean that the police have no legal way of accessing such documents or data under any circumstances. This may be possible under the powers defined in CMA, chapter 10 (on covert coercive measures), including *telecommunications interception* and *traffic data monitoring*[16], which are both limited to investigations involving relatively serious offenses and generally require an *ex ante* court decision. The function of the exception is, in fact, to prevent the circumvention of the rules on these more invasive measures by replacing them with seizure (confiscation or copying) regulated in chapter 7, for which the prerequisites defined in law are considerably less stringent (e.g., no prerequisites regarding the severity of the suspected offense or *ex ante* judicial oversight).[17]

The relevant legal questions in the Freedome case have not been answered directly in previous national or European case law. However, the NBI referred to the European Court of Justice (ECJ) case *Ministerio Fiscal* (C-207/16, Grand Chamber Judgment of 2 October 2018) in support of their arguments in the Court of Appeal. This case concerned a Spanish investigating magistrate's decision refusing to grant the police access to personal data retained by providers of electronic communications services, more specifically information on phone numbers that had been activated with the International Mobile Equipment Identity (IMEI) code of a stolen mobile phone, as well as names and addresses of the owners or users of the SIM cards corresponding to these numbers. 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, enshrined in articles 7 and 8 of the Charter of Fundamental Rights of the European Union. However,

---

13 For the concepts of user and subscriber, a reference is made to ECSA, section 3, paragraphs 7 and 30, respectively.

14 In Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), article 2, traffic data is defined as "any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof". In the Finnish version of the directive, the (very literal) translation for this term is *liikennetieto*. The term adopted in ECSA (*välitystieto*) could more literally be translated as "relaying data". – Cf. Convention on Cybercrime, article 1, paragraph d, which defines traffic data (again, in Finnish *liikennetieto*) as "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." The term *liikennetieto* (and a definition resembling the Convention definition) is used in a CMA provision concerning data retention orders (chapter 8, section 24), but not elsewhere in Finnish legislation. This multitude of closely related but differing terms and definitions appearing in European and national legislative texts can hardly be considered ideal in terms of clarity, transparency and foreseeability of the law.

15 See Government Proposal HE 221/2013 vp, p. 95.

16 This is the translation adopted in an unofficial English translation of CMA in the legal database Finlex (https://www.finlex.fi/, accessed on 13 November 2020). It should be clarified that this power specifically concerns the obtaining of *tunnistamistiedot* ("identifying data") defined in CMA, chapter 10, section 6. A more literal translation for the Finnish term (*televalvonta*) would be "tele[communications] monitoring".

17 See Riekkinen, Evidence of cybercrime and coercive measures in Finland, Digital Evidence and Electronic Signature Law Review, Vol. 13, 2016, pp. 58–59, 61–62.

the ECJ ruled this interference not to be sufficiently serious to entail this access being limited to the objective of fighting serious crime.[18]

F-Secure, instead, relied on another European court, the European Court of Human Rights (ECtHR). The case of *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 Internet service provider to disclose data regarding the user to whom a certain dynamic IP address had been assigned at a designated time. The IP address had been received from Swiss law enforcement authorities, who had been conducting a monitoring exercise of users in a peer-to-peer file-sharing network, in which child abuse material was distributed. The request was based on 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. Therefore, the interference on the applicant's right to privacy was not "in accordance with the law" as required by article 8(2) of the European Convention on Human Rights (ECHR), and there had been a violation of said article.[19]

2.4. Decision of the District Court

As the main legal question concerned the classification of the seized data, it was of importance to determine how the Freedome logs functioned. According to a witness (an F-Secure employee), when a user logged into Freedome, their device was identified and their right to use the service was checked, because the service was not free of charge. The validity of the user's license was checked every time they opened a VPN connection. In the process of identifying the user, their IP address was logged and stored for three days. Additional data were generated when a VPN connection was made, and stored for 90 days. This information included the session identifier, timestamps (beginning and end of the session) and the volume of transferred data. No information about sources or destinations of online traffic were logged by F-Secure during a VPN session.

A representative of the Finnish telecommunications authority Traficom testified (as an expert witness) that Traficom considered the data logged by Freedome to be traffic data. In particular, IP addresses were traffic data that were necessary for providing communications services. According to the expert witness, device identifiers, session identifiers and IP addresses could also be considered subscriber data, but when processed for the purposes of relaying communications, they were traffic data.

In accordance with the Traficom position, the District Court found that some of the seized data could be considered subscriber data. In particular, the District Court stated that information used to identify a user, such as an IP address, could be subscriber data (under some circumstances), whereas session timestamps or data on traffic volumes could not be considered subscriber data. Considering the nature of the Freedome service and the purposes for which the logged data were stored, even the other data in the seized logs could not be considered merely subscriber data in this context.

The District Court recognized that the 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 third parties. The Freedome service was to be understood only as a tool for making anonymous communications possible, and therefore logging in to the service and opening a VPN connection were not to be understood as communication between the user and F-Secure.

[18] ECJ, Ministerio Fiscal, C-207/16, Grand Chamber Judgment of 2 October 2018, paragraphs 20 and 63.
[19] ECtHR, Benedik v. Slovenia, Judgment of 24 April 2018, paragraphs 132–134.

The District Court concluded that the seized data were traffic data that F-Secure had possessed as an intermediator (or communications provider as defined in ECSA). The NBI, therefore, did not have the right seize the logs under CMA, chapter 7. Thus, the District Court rescinded the seizure and ordered the data to be destroyed.

2.5. Decision of the Court of Appeal

In its decision dismissing the NBI's appeal, the Court of Appeal accepted the District Court's reasoning with some additions concerning arguments presented in the appeal stage.

First, the Court of Appeal concluded that the question of F-Secure's potential legal status as a telecommunications operator or a corporate or associate subscriber did not have a decisive role in the application of CMA, chapter 7, section 4. The Court of Appeal noted that the references in the section are outdated and that current law (ECSA) contains a wider concept of "communications provider" which covers, in addition to telecommunications operators and corporate or associate subscribers, "other parties that convey electronic communications for other than personal or comparable customary private purposes".[20] Drawing also on law drafting materials and the stated function of the provision (to prevent any circumvention of rules on telecommunications interception and traffic data monitoring),[21] the Court of Appeal ruled that despite its wording, CMA, chapter 7, section 4 should be interpreted as applying to all communications providers as defined in ECSA. F-Secure, as a VPN service provider, was to be considered an "other party that conveys electronic communications", and therefore a communications provider.

As mentioned before, both parties had brought forward arguments supported by European case law. In relation to *Ministerio Fiscal*, the Court of Appeal distinguished the present case from it in two ways. First, *Ministerio Fiscal* concerned access based on a court warrant (an investigating magistrate's decision, to be precise), while the present case concerned *ex post* evaluation of legality of seizure. Second, as the ECJ case concerned different types of communication and data than the present case, the Court of Appeal did not see it as providing any guidance on whether the seized logs should be considered traffic data or subscriber data. Therefore, the Court of Appeal did not give weight to the *Ministerio Fiscal* case.

The Court of Appeal noted that in *Benedik v. Slovenia*, the ECtHR had stated that the purpose of obtaining subscriber information associated with a dynamic IP address in this case had clearly been to connect the computer usage to a location and, potentially, to a person. The subscriber information, which contained also the address, had allowed the police to identify the home from which the Internet connections in question had been made.[22] The Court of Appeal further noted that in the ECtHR's view, the applicant's expectation of privacy with respect to his online activity could not be said to be unwarranted or unreasonable.[23]

Based on the evidence, the Court of Appeal noted that F-Secure did not collect any data on sources or destinations of online traffic routed via Freedome. The authorities already possessed this kind of information, and the identity of the person associated with the relevant online traffic could be discovered by combining this information with the information contained in the Freedome logs. Taking into account the nature of Freedome as a privacy-enhancing additional service designed to protect the customer's communications, the Court of Appeal ruled that the seized logs could not be considered only subscriber information that could be seized without restrictions. Further, the Court of Appeal stated that the assertions in *Benedik v. Slovenia* regarding online privacy supported the conclusion that the logged data seized in the Freedome case should be considered traffic data covered by the protection of confidential communications. While the Court of Appeal seems to

[20] ECSA, section 3, paragraph 36. As noted in earlier footnotes, ECSA also contains definitions for the two terms specifically mentioned in CMA, chapter 7, section 4 (ECSA, section 3, paragraphs 27 and 41).

[21] See Government Proposal 222/2010 vp, p. 94.

[22] ECHR, Benedik v. Slovenia, Judgment of 24 April 2018, paragraph 113.

[23] ECHR, Benedik v. Slovenia, Judgment of 24 April 2018, paragraph 118.

have considered the facts of *Benedik v. Slovenia* to be similar or at least comparable to the present case, the decision does not explicate how the Court of Appeal arrived at this conclusion or specify which assertions in the ECtHR judgment are meant by this reference.[24]

3. Evaluation and Conclusions

In the Freedome case, both courts gave weight to the original purposes for which the seized data had been stored, and the nature of Freedome as a privacy-enhancing service designed to protect the anonymity and confidentiality of the user's online communications. This could be described as a contextual approach to classifying logged data, as opposed to strictly textual interpretation of the legal definitions provided in the current law, or rigid categorization based on the types of individual data points. While the courts' argumentation can certainly be criticized for lack of precision and clarity, both the result and these general viewpoints are surely welcomed by VPN users and legitimate commercial VPN service providers with an interest in protecting their customers' privacy rights, as well as the reputation of their services and their own business interests.[25]

In this paper, it is not reasonable to attempt to conclusively define the concept of (online) privacy, nor to map all the possible harms of uncontrolled and unlimited law enforcement access to VPN user logs. Suffice it to say that access to data that allows online users to be identified is commonly—and correctly—considered to form an interference in the privacy rights of the affected individual(s). An example of a concrete harm which can follow from any—even justified and proportionate—law enforcement access to any data related to IP addresses or similar online identifiers is that further investigative measures and even deprivation of liberty may be targeted at an innocent individual. The common use of dynamic IP addresses and carrier-grade NAT, in part, make it more likely that the investigation may involve data of individuals who are not connected to the crime at all.[26]

While EU law does not, as such, require limiting law enforcement access to such data to criminal investigations involving serious crime (as ruled in *Ministerio Fiscal*), there is undeniably a better justification for such interference and the possibility of harms affecting innocent individuals in cases involving particularly serious criminal offenses. As ECtHR case law makes clear, such interference must not only pursue a legitimate interest (such as investigating crime) but also be *necessary in a democratic society* and, furthermore, *in accordance with the law*. The latter entails the requirements of accessibility, foreseeability and quality of the law.[27] If Finnish law was to be interpreted in a way allowing uncontrolled and unlimited access to VPN user logs, particularly the requirements of quality and foreseeability might not be fulfilled due to the lack of appropriate safeguards and substandard legislative technique including outdated references and conflicting terms and definitions.

---

[24] Notably, the Court of Appeal did not consider or cite any ECJ or ECtHR privacy cases other than the two mentioned above, and even the two cases were described and discussed rather briefly in the decision.

[25] Indeed, in taking legal action in the present case, F-Secure specifically claimed to be acting for the purpose of safeguarding the rights of other Freedome users, and also in public interest by defending the confidentiality of communications. This was presented as an argument in favor of full compensation for the relatively high legal expenses incurred by F-Secure during the trial.

[26] About these characteristics of IP addresses, see, e.g., Dupont/Cilli/Omersa/Borrett/Moulac/Vogiatzoglou/Nikova, Study on the retention of electronic communications non-content data for law enforcement purposes, Final report, Publications Office of the European Union, Luxembourg 2020, pp. 50–51. See also Council of Europe, Conditions for obtaining subscriber information in relation to dynamic versus static IP addresses: overview of relevant court decisions and developments, T-CY (2018)26, Cybercrime Convention Committee, Strasbourg, 25 October 2018, p. 23.

[27] See, e.g., Kokott/Sobotta, The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR. In: Hijmans/Kranenborg (eds.), Data Protection Anno 2014: How to Restore Trust? Contributions in honour of Peter Hustinx, European Data Protection Supervisor (2004–2014), Intersentia, Cambridge 2014, pp. 87–89, Oerlemans, Investigating Cybercrime, SIKS dissertation series no. 2017-01, Meijers Research Institute and Graduate School of the Leiden Law School of Leiden University 2017, pp. 73–77 and, from the perspective of secret surveillance legislation, van der Sloot, The Quality of Law: How the European Court of Human Rights gradually became a European Constitutional Court for privacy cases, JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law, Vol. 11, Issue 2, 2020, pp. 163–169.

As a matter of current law, the legal classification of data logged by VPN providers is the key question also within a wider European context. A broadly similar division of data categories exists in many national laws, and the conditions of law enforcement access are often dependent on whether certain data are determined to belong to the more protected or to the less protected category.[28] The basis for this division is the perceived level of interference that a person is subjected to as a consequence of processing or access to different types of data, and what kinds of inferences about private life can be drawn based on the data.[29]

While the national definitions of these basic legal categories of non-content data—which can be referred to as *subscriber data* and *traffic data*[30]—have their roots in international instruments such as the Convention on Cybercrime (ETS No. 185, Budapest, 23 November 2001),[31] classification of certain types of data has proven to be difficult, and national interpretations have not been uniform. This has been observed in a recent study, which examined the retention of non-content data for law enforcement purposes, as well as law enforcement access to such data, in select EU countries.[32] On the European level, data belonging clearly to the category of subscriber data include, i.e., names, physical addresses, telephone numbers, billing and payment information and e-mail addresses, whereas data uniformly recognized as traffic data include data points such as date and time of communication, duration of communication, start and end of communication and data volume. The data points on which there is no European consensus include IP addresses, device identification numbers, SIM numbers and port numbers for dynamic IP addresses (in the aforementioned study, these are referred to as *identifying data*).[33] As noted earlier, in the Freedome case the District Court recognized that IP addresses can be both subscriber data and traffic data depending on the context in which they are processed, thus placing IP addresses on the border area of the two categories also within Finnish law.

In relation to VPN user logs, however, the data points clearly belonging to the category of traffic data are not necessarily the ones that may lead to the most detailed inferences concerning the private life or online communications of a given person. If one considers the extent of privacy interference in the particular scenario where law enforcement authorities are requesting access to data associated with a given IP address belonging to the VPN service provider, one should note that the authorities usually already possess detailed information pertaining to the online traffic originating from this IP address, or even content data. In fact, knowledge of an identified VPN user's data volumes or the start and end times of a VPN connection are not very useful for making inferences. Instead, the data linking a certain IP address to an identifiable person, or to another IP address that can be further linked to an identifiable person through data held by an Internet access provider,

---

28 See, e.g., Dupont/Cilli/Omersa/Borrett/Moulac/Vogiatzoglou/Nikova, Study on the retention of electronic communications non-content data for law enforcement purposes, Final report, Publications Office of the European Union, Luxembourg 2020, pp. 48, 71–81.

29 The same idea serves as the basis for differences in the legal treatment of content data and non-content data (an umbrella term for subscriber data, traffic data and location data relating to online communications). Cf. the concurring opinion of Judge Yudkivska in ECHR, Benedik v. Slovenia, Judgment of 24 April 2018, which challenges this idea.

30 Some national legislators have created additional categories (i.e., *Zugangsdaten* or "access data" in Austrian law). The Cybercrime Convention Committee (T-CY) has discouraged introducing such categories, stating that it "may lead to further misunderstandings regarding applicable rules on the retention of or access to such data and may be difficult to apply by practitioners" (Council of Europe, Conditions for obtaining subscriber information in relation to dynamic versus static IP addresses: overview of relevant court decisions and developments, T-CY (2018)26, Cybercrime Convention Committee, Strasbourg, 25 October 2018, p. 23).

31 See Convention on Cybercrime, article 1, paragraph d and article 18, paragraph 3.

32 See Dupont/Cilli/Omersa/Borrett/Moulac/Vogiatzoglou/Nikova, Study on the retention of electronic communications non-content data for law enforcement purposes, Final report, Publications Office of the European Union, Luxembourg 2020, pp. 48–49. Finland was not among the countries examined in this study.

33 Dupont/Cilli/Omersa/Borrett/Moulac/Vogiatzoglou/Nikova, Study on the retention of electronic communications non-content data for law enforcement purposes, Final report, Publications Office of the European Union, Luxembourg 2020, pp. 48–49. Cf. Council of Europe, Conditions for obtaining subscriber information in relation to dynamic versus static IP addresses: overview of relevant court decisions and developments, T-CY (2018)26, Cybercrime Convention Committee, Strasbourg, 25 October 2018, p. 23 ("[s]ubscriber information may comprise access numbers, including Internet Protocol addresses, strictly needed to identify a subscriber, such as the first login IP, last login IP or the login IP used at a specific moment in time").

is what allows inferences about a natural person's actions and activities, and thus constitutes the interference with their privacy rights.

As a counterpoint to the previous argument, it can be noted that it is not possible to make these inferences without cross-referencing with more detailed traffic data and/or content data,[34] and that the prerequisites for investigative measures that make the collection of these data possible are typically stricter. Thus, there are safeguards in place that influence the criminal investigation as a whole, even if one step of the investigative process lacks these safeguards. While this argument has some merit, it should be noted that online investigations are typically transnational (as exemplified by both the Freedome case and *Benedik v. Slovenia*), and the prerequisites for different measures vary between different jurisdictions, and consequently the level of protection in these other phases might vary. Further, establishing a chain of safeguards and fail-safe mechanisms at different stages of the investigative process would certainly help to avoid a procedural "single point of failure", and to prevent and de-incentivize arbitrary actions by public authorities.[35] It falls outside the scope of this paper to determine exactly what type and level of safeguards would be necessary (or optimal) for access to VPN user logs, but applying the safeguards that the legislator has deemed suitable for access to traffic data certainly seems more appropriate than applying virtually no safeguards at all.

Another possible angle from which to approach the need for safeguards is the user's expectation of privacy. In any online communications, a user can expect that their privacy is respected to some extent. When using a legitimate commercial service whose main feature is the promise of enhanced privacy, that expectation of privacy can only become stronger and more justified. If this expectation is not honored in legitimate VPN services by at least putting in place strong safeguards for law enforcement access, this may incentivize both criminals and law-abiding, privacy-conscious users to switch to underground services, which will not co-operate with law enforcement in any cases, even when the interests of criminal justice clearly outweigh the privacy rights of the users. This may undermine criminal investigations, legitimate business interests and—potentially, if these services are run by malicious actors—safety and security of law-abiding online users all at once.[36] Another mechanism by which uncontrolled access might damage law enforcement interests is that legitimate service providers might be pressured to respond to their customers' privacy concerns by relocating to a different jurisdiction or by revising their logging practices and minimizing the amount of logged data, thus making useful information unavailable even in serious cases. Notably, in the Freedome case, the requested data had not been logged because of a mandatory data retention obligation but because of business purposes, and therefore it would be legally possible for the company to, e.g., further shorten the storage times of certain data.[37]

In conclusion, there seem to be good arguments against allowing unlimited and uncontrolled law enforcement access to data held by legitimate VPN service providers. The approach adopted by the Finnish courts in the Freedome case, which places value on the context and reasons for processing the data as well as the

---

34 A somewhat similar argument was made by the ECJ in Ministerio Fiscal, C-207/16, Grand Chamber Judgment of 2 October 2018, paragraph 60.

35 Protecting the individual against arbitrary actions by public authorities is a key purpose of ECHR article 8(2), as stated in case law. See, e.g. ECtHR, Niemietz v. Germany, Judgment of 26 December 1992, paragraph 31 and ECtHR, Kroon and Others v. The Netherlands, Judgment of 27 October 1994, paragraph 31.

36 This argument is related to the longstanding discussion concerning weakening cryptography products in order to allow law enforcement access. As long as strong cryptographic applications remain available, criminals are likely to make use of them. Backdoors or restrictions on applications offered by legitimate providers primarily endanger the security of law-abiding users, and are not necessarily effective in advancing law enforcement purposes.

37 The legality of national mass data retention frameworks has been unclear since the invalidation of the so-called Data Retention Directive (2006/24/EC) in ECJ, Digital Rights Ireland, C-293/12 and C-594/12, Grand Chamber Judgment of 8 April 2014, as well as ECJ, Tele2 Sverige/Watson, C-203/15 and C-698/15, Grand Chamber Judgment of 21 December 2016. The Finnish data retention framework has not been significantly amended since these judgements, but it does not apply to VPN service providers. Concerning the situation in some other EU countries, see Dupont/Cilli/Omersa/Borrett/Moulac/Vogiatzoglou/Nikova, Study on the retention of electronic communications non-content data for law enforcement purposes, Final report, Publications Office of the European Union, Luxembourg 2020, pp. 39–43.

privacy-enhancing nature of VPN services, seems like a good alternative to trying to rigidly classify certain types of data points to less and more protected categories, or to relying on strictly textual analysis of the legal definitions, which leave considerable room for different interpretations and are found in various similar but not identical iterations in different legislative documents.

4. References

Council of Europe, Conditions for obtaining subscriber information in relation to dynamic versus static IP addresses: overview of relevant court decisions and developments, T-CY (2018)26, Cybercrime Convention Committee, Strasbourg, 25 October 2018.

Dupont, Claire/Cilli, Valentina/Omersa, Ela/Borrett, Camille/Moulac, Maxime/Vogiatzoglou, Plixavra/Nikova, Svetla, Study on the retention of electronic communications non-content data for law enforcement purposes, Final report, Publications Office of the European Union, Luxembourg 2020.

Europol, Internet Organised Crime Threat Assessment (IOCTA) 2019. https://www.europol.europa.eu/sites/default/files/documents/iocta_2019.pdf (accessed on 13 November 2020).

Europol, Internet Organised Crime Threat Assessment (IOCTA) 2020. https://www.europol.europa.eu/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf (accessed on 13 November 2020).

F-Secure FREEDOME VPN – Protect your privacy. https://www.f-secure.com/en/home/products/freedome (accessed on 13 November 2020).

Finlex. https://www.finlex.fi/ (accessed on 13 November 2020).

Government Proposal HE 222/2010 vp [In Finnish: Hallituksen esitys 222/2010 vp eduskunnalle esitutkinta- ja pakkokeinolainsäädännön uudistamiseksi].

Government Proposal HE 221/2013 vp [In Finnish: Hallituksen esitys 221/2013 vp eduskunnalle tietoyhteiskuntakaareksi sekä laeiksi maankäyttö- ja rakennuslain 161 §:n ja rikoslain 38 luvun 8 b §:n muuttamisesta].

Kokott, Juliane/Sobotta, Christoph, The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR. In: Hijmans, Hielke/Kranenborg, Herke (eds.), Data Protection Anno 2014: How to Restore Trust? Contributions in honour of Peter Hustinx, European Data Protection Supervisor (2004–2014), Intersentia, Cambridge 2014, pp. 83–95.

Oerlemans, J.J., Investigating Cybercrime, SIKS dissertation series no. 2017-01, Meijers Research Institute and Graduate School of the Leiden Law School of Leiden University 2017.

Riekkinen, Juhana, Evidence of cybercrime and coercive measures in Finland, Digital Evidence and Electronic Signature Law Review, Vol. 13, 2016, pp. 49–66.

Sieber, Ulrich, Straftaten und Strafverfolgung im Internet, Verlag C.H. Beck, München 2012.

Sieber, Ulrich/Neubert, Carl-Wendelin, Transnational Criminal Investigations in Cyberspace: Challenges to National Sovereignty. In: Lachenmann, Frauke/Röder, Tilmann J./Wolfrum, Rüdiger (eds.), Max Planck Yearbook of United Nations Law, Vol. 20 (2016), Brill | Nijhoff, Leiden 2017, pp. 241–321.

Sund, Peter, Global and European Responses to Cybercrime. In: Calcara, Giulio/Sund, Peter/Tolvanen, Matti (Eds.), Cybercrime, Law and Technology in Finland and Beyond, Reports of the Police University College in Finland 133/2019, Police University College, Tampere 2019, pp. 67–108.

Strayer, W. Timothy, Privacy issues in virtual private networks, Computer Communications, Vol. 27, Issue 6, April 2004, pp. 517–521.

Tor Project. https://www.torproject.org/ (accessed on 13 November 2020).

van der Sloot, Bart, The Quality of Law: How the European Court of Human Rights gradually became a European Constitutional Court for privacy cases, JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law, Vol. 11, Issue 2, 2020, pp. 160–185.