Router Freedom Survey Report

The end-user perspective on freedom of terminal equipment in Europe

fsfe

Published by the Free Software Foundation Europe (FSFE)
Berlin, May 2023
EU Transparency register ID: 33882407107-76
www.fsfe.org

Responsible according to European press law:
Matthias Kirschner / FSFE e.V.
Schönhauser Allee 6/7
10119 Berlin
Germany

Contributors:
Lucas Lasota
Brielen Madureira
Ewelyn Kwarteng
Max Mehl

The contributors thank Richard Schmeidler for the proofreading and comments on the report.

Version: 1.0 – 05.2023

How to cite this report:
FSFE (2023). Router Freedom Survey Report – The end-user perspective on freedom of terminal equipment in Europe. Berlin: Free Software Foundation Europe.

Table of Contents

EXECUTIVE SUMMARY

Router Freedom is the right that customers of any internet service provider (ISP) have to be able to choose and use a private modem and router instead of equipment provided by the ISP. The Router Freedom Survey aimed primarily to collect data on the relationship between end-users and ISPs and on the end-users' experiences. The survey gathered responses from 1652 participants. The survey tackled issues such as freedom of choice, technical issues against Router Freedom and ISPs' commercial and technical practices. The survey also inquired how end-users perceive Router Freedom principles, including the FSFE's policy demands. Additional comments were also an important component. The survey's main findings include:

- Limitations to freedom of choice. Some ISPs restrict end-users from connecting their routers, modems and FTTH terminal equipment to the public network. This is observed more intensively in countries where the position of the Network Termination Point is not regulated in a configuration favourable to end-users.

- ISP's lock-in. Besides limiting freedom of choice, some ISPs impose other restrictions that increase switching costs by end-users, charge for the provided equipment and impose fines when end-users use their own equipment. Lock-in is significantly more notable on FTTH contracts and in countries where Router Freedom is not regulated.

- Provision of proprietary devices. The routers, modems and ONT devices provided by ISPs are generally proprietary. End-users cannot inspect their firmware or install an alternative operating system. This is especially problematic with FTTH connections, since in the majority of contracts end-users cannot change the ONT imposed by ISPs.

- Security issues. The lack of Router Freedom generates negative consequences for network security. Some ISPs do not provide security updates for their devices. When end-users cannot manage their own routers, they become more exposed to security flaws.

- Unlawful commercial and technical practices. Even where Router Freedom has been established by legislation, ISPs can still hamper end-users' ability to choose and use their own routers and modems. Some ISPs make it cumbersome to replace the ISP's equipment, take a long time to provide login data or other access credentials, fail to offer technical support for the network or threaten end-users who use personal routers with contract termination or fines.

- Router Freedom as a policy demand. The vast majority of participants agreed that Router Freedom is key for Net Neutrality and Open Internet, security and data protection, fair competition and digital sustainability.

INTRODUCTION

IS THERE ROUTER FREEDOM IN EUROPE?

Is there Router Freedom in Europe? This question was the starting point for this survey. The interests of end-users reflect the necessity to enable freedom of terminal equipment in Europe. Router Freedom is the right that customers of any ISP have to be able to choose and use a private modem and router instead of equipment provided by the ISP. Since 2013, the Free Software Foundation Europe has been working to make this right a reality in Europe. Router Freedom is understood in a broader context as an important element of Device Neutrality, which requires that network operators should allow end-users to run Free Software on their devices. The Router Freedom Survey was part of an initiative for civil society engagement during the national implementation processes of the EU reform of telecommunications law.

The survey had the objective to gather information on the end-user experience with their ISPs, as well as how they perceive Router Freedom. More specifically, the survey aimed to:

1. Collect data on usage of terminal equipment and related problems with ISPs.
2. Gather information on whether end-users are using their own routers/modems and what are the hurdles to doing so.
3. Gather information on possible security issues regarding various types of networks.
4. Identify possible infringements on Router Freedom, including ISPs' contentious practices (commercial and technical) in relation to terminal equipment.
5. Inquire about public opinion on principles of free choice of terminal equipment, in particular security, privacy, fair competition and digital sustainability.

The survey was conducted from October 2020 until March 2023. Respondents were asked about their country of residence, so issues could be identified geographically. By March 22, 2023, the survey had gathered 1652 responses from end-users all over Europe. Not all participants have answered all questions. Therefore, the report charts inform the amount of responses received. More information on the methodology employed can be found at the end of this document.

The survey shed light on how end-users feel towards Router Freedom, their understanding of the importance of this right in the context of Net Neutrality principles, privacy, fair competition and digital sustainability. The survey also collected information about the issues and problems faced by end-users when trying to use their private routers for internet connection.

The Open Internet Regulation (EU) 2015/2120, which introduced Router Freedom in Art. 3(1), had also tasked national regulatory agencies (NRAs) with monitoring of infringing practices by operators against this freedom. Therefore, this survey serves not only civil society and consumer organizations with primary data on end-user experience, but also regulators and policy makers in their regulatory efforts. In particular, the outcome of this survey can:

1. Provide primary information regarding end-user experience related to Router Freedom for development of policies towards terminal equipment in Europe.
2. Orientate national regulators which are still in the process of implementing rules on terminal equipment. More specifically, those regulating fiber (FTTH) networks can profit from the conclusions achieved. For instance, in countries where the position of the Network Termination Point (NTP) is not defined, the lack of Router Freedom urges regulatory intervention. Where the NTP is defined and Router Freedom established, it demands stricter monitoring.
3. Support regulators' monitoring activities. Critically important are the reported practices that could be considered infringements against Router Freedom, so regulators can benefit and be more informed about the issues from the end-user perspective.

The survey questions were grouped around four topics: categorisation of participants, experience with ISPs, policy demands and feedback on FSFE's Router Freedom activity. This report covers only the first three groups.

In the first batch of questions, the survey solicited background information about the participants. This included country of residence and level of knowledge in areas such as internet technologies and network, IT security, consumer routers and modems, as well as policy and legal issues regarding Net Neutrality. The majority of participants saw themselves as having intermediate to advanced levels of knowledge in such topics.

The questions related to end-user experience with ISPs are the core of the survey. The survey gathered insights from users using their own routers and those who did not, and why they made that choice. The survey also investigated challenges and issues against Router Freedom, the behaviour of ISPs' technical teams and customer service toward users using personal routers and questionable commercial practices imposed by ISPs on end-users.

The third group of questions prompted participants to say to what extent they agree with Router Freedom policy demands. The vast majority of respondents agreed that Router Freedom is important for Net Neutrality and Open Internet; enhances freedom of choice, security and data protection and promotes fair competition and digital sustainability.

A fundamental contribution from participants was their additional comments, which shed light on real life examples of the issues related to Router Freedom. For almost all questions, respondents could also provide additional information and clarifications. The majority of survey information came from these contributions.

The main findings of the survey include:

- **Limitations to freedom of choice.** Some ISPs restrict end-users from connecting their routers, modems and fiber terminal equipment to the public network. This is observed more intensively in countries where the position of the Network Termination Point is not regulated in a configuration favourable to end-users.

- ISP’s lock-in. Besides limiting freedom of choice, some ISPs impose other restrictions that increase switching costs by end-users, charge for the provided equipment and impose fines when end-users use their own equipment. Lock-in is significantly more notable on FTTH contracts and in countries where Router Freedom is not regulated.

- Provision of proprietary devices. The routers, modems and ONT devices provided by ISPs are generally proprietary. End-users cannot inspect their firmware or install an alternative operating system. This is especially problematic with FTTH connections, since in the majority of contracts end-users cannot change the ONT imposed by ISPs.

- Security issues. The lack of Router Freedom generates negative consequences for network security. Some ISPs do not provide security updates for their devices. When end-users cannot manage their own routers, they become more exposed to security flaws.

- Unlawful commercial and technical practices. Even where Router Freedom has been established by legislation, ISPs can still hamper end-users’ ability to choose and use their own routers and modems. Some ISPs make it cumbersome to replace the ISP's equipment, take a long time to provide login data or other access credentials, fail to offer technical support for the network or threaten end-users who use personal routers with contract termination or fines.

Respondents’ profile

The first group of questions, on country of residence, level of experience and background knowledge, together with topics related to Router Freedom, investigated the overall participation characteristics.

Country of residence

In total, 1427 respondents provided information on their country of residence. In the table below are listed all countries identified and the percentage of the total for the survey.

Country	Number of respondents	Total %
Andorra	1	0.07
Austria	188	13.17
Belarus	1	0.07
Belgium	268	18.78
Bosnia and Herzegovina	2	0.14
Bulgaria	3	0.21
Croatia	2	0.14
Cyprus	14	0.98
Czech Republic	5	0.35
Denmark	5	0.35
Finland	1	0.07
France	33	2.31
Germany	507	35.52
Greece	24	1.68
Hungary	7	0.49
Iceland	1	0.07
Ireland	4	0.28
Italy	29	2.03
Latvia	1	0.07
Luxembourg	3	0.21
Netherlands	73	5.11
Macedonia	1	0.07
Norway	10	0.70
Poland	16	1.12
Portugal	148	10.37
Romania	6	0.42
Serbia	4	0.28
Slovakia	3	0.21
Slovenia	3	0.21
Spain	28	1.96
Sweden	5	0.35
Switzerland	12	0.84
Turkey	2	0.14
United Kingdom	16	1.12
Vatican City	1	0.07
Total	1427	100

With more than 35%, Germany was far in the lead. Belgium (18%), Austria (13%), Portugal (10%) and the Netherlands (5%) also had elevated quantities of responses.

Background knowledge

The survey welcomed inputs from people of different levels. Participants were asked to self-assess and state their own level of experience and background knowledge – from beginner to expert – with topics related to Router Freedom in the following fields:

- IT Security
- Consumer router/modem devices
- Internet technologies and networks
- Net Neutrality legal and/or policy issues

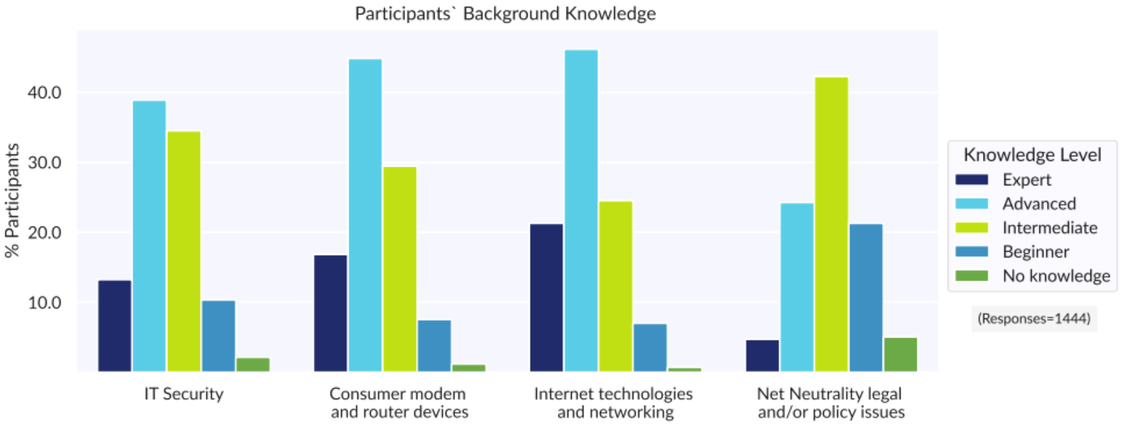

Figure 1. Participants' Background Knowledge.

From the 1444 responses gathered, most participants considered themselves as having an advanced (38%) or intermediate (34%) level of knowledge regarding IT Security. Those at the expert level (13%) and beginners (10%) came after.

An elevated number of participants (44%) considered themselves as having an advanced level of knowledge regarding consumer router and modem devices. Intermediate (29%) and expert (15%) followed. Beginners were only 7% of the survey.

Even more participants (46%) considered themselves as having an advanced level of knowledge regarding internet and network technologies. The number of experts also grew (21%), almost reaching the reduced number of Intermediate participants (24%). Beginners (6%) also were present.

On the other hand, 42% of the participants considered themselves as having an intermediate level of knowledge regarding policy and legal issues related to Net Neutrality. 24% saw themselves as having advanced knowledge but only 4% saw themselves as experts. Within this topic, 21% see themselves as beginners.

End-user experience with ISPs

In this section the survey questioned the participants about their experience with IISPs. The information gathered from these questions is the core of the survey. It sheds light on the behaviour and practices of ISPs, both the problematic ones and the ones serving as good business examples.

Identified ISPs

In total, 1510 respondents (91%) identified their ISPs, which are listed in the table below.

Identified ISPs				
1&1	Epic	KOMRO	Primetel	Telia
Altibox	Eurosignal	KPN	Proximus	Tetaneutral.net
Aruba	Euskaltel	Liwest Mobil	PŸUR	Teutel
BECONET	Fastweb	Magenta	Rootsecurity bvba	TIM
BeotelNet	Fonira	Maverick	Salt	Tiscali
Bouygues	franciliens.net	MEO	SCARLET	Tkrz Stadtwerke
BT	Free	Merula	Scarlet	Turkcell Superonline
Cablelink	Freedom.nl	Movistar	SFR	Tweak
Caiway	FunkFeuer.at	NetAachen	Simyo	UPC
Citynet Hall	Goetel	NetCologne	SKYTELECOM	UPC Polska
Congstar	GoMo	Netllar	Studentenwerk Potsdam	Velocity 1
Cosmote	Greenlan	NOS	Sunrise	Vereinigte-Stadtwerke
Cyta	HostProfis	Nova	Supernova	Virgin Media
Delta	Htp	Nowo	Swisscom	Vodafone
Digi	Hutchison Drei	Nynex	Swisscom	Wien Energie
DNS:NET	Inalan	O2	T-mobile	Wind
Dokom21	Init7	Oja.at	Telenet	Wind3
Easybell	Jazztel	Orange	Telenet Belgium	XS4ALL
EDPnet	Juno	Osnatel	Telenor	Youfone
Elisa	Kabelplus	Otenet	Teletronic	Ziggo
Energie AG	Kapper	Pepephone	Telfort/KPN	

Internet connection type usage

Based on the 1165 responses gathered, DSL is still the most used internet connection among the respondents (44%). Coaxial garnered 29%, and 20% of the respondents identified fiber (FTTH) as their main internet connection type. A minority of users (2%) identified mobile as their type of connection.

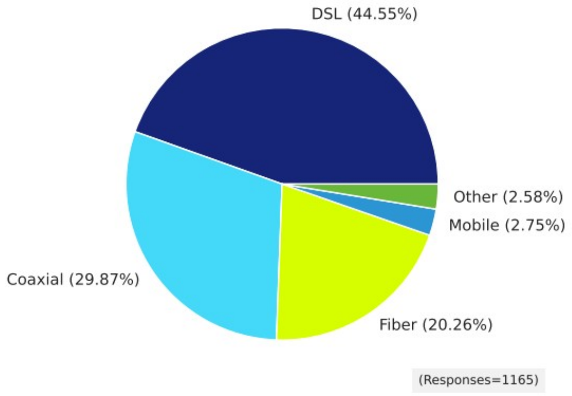

Figure 2. Internet connection type usage.

Usage of personal router/modem

From 1130 responses received, less than half of respondents were using their own router/modem for internet connection. The majority of end-users with their own routers are DSL subscribers. 11% of participants use their own routers with coaxial connections and less than 5% on FTTH networks are using their own equipment. Many fiber subscribers (8%) are using exclusively the ISP's optical equipment, while most of the rest (7%) are using their own router on bridge mode in conjunction with the ISP ONT. Coaxial and fiber subscribers are still the majority who depend on ISP's routers and modems.

In total, 55% of the participants reported using the ISP's provided equipment in one way or another.

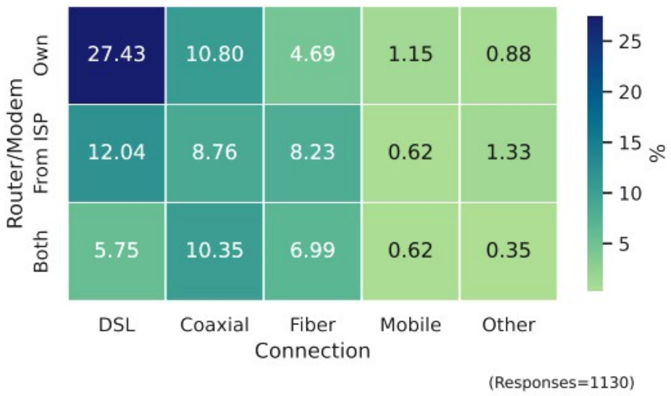

Figure 3. Types of connection and router usage.

Participants' comments

Some of those using personal routers in bridge mode commented that, due to ISPs' lack of support for connectivity standards like DOCSIS 3.1, using a modem for direct connection with the network is not possible. For others, ISPs' modems or ONTs have limitations. So using both a modem and a router limits the functionality available for end-users. For instance, one participant mentioned that using the ISP's modem restricts features of a personal router when using it in bridge mode. Others also added that they need to use the ISP's modem in order to access features such as static IP addresses (IPv4).

Trying to use personal routers

The survey asked those who used only the equipment provided by the ISP whether they had already tried to use their own personal router or modem or to explain why not. Participants were asked if they were allowed by the ISPs to use their own router/modem. They were also requested to indicate how they got this information – if they were informed by the ISP's website, customer service or if it was even a contractual clause.

From 417 responses gathered, 17% of respondents tried to use their own routers but were expressly not allowed by ISPs. 14% of them tried and were allowed. In comparison, although allowed in some fashion by ISPs, 21% of the respondents had not tried to use their own routers. Almost 26% were unsure if Router Freedom was allowed and therefore had not tried. 10% were not sure if using personal routers was allowed but tried anyway.

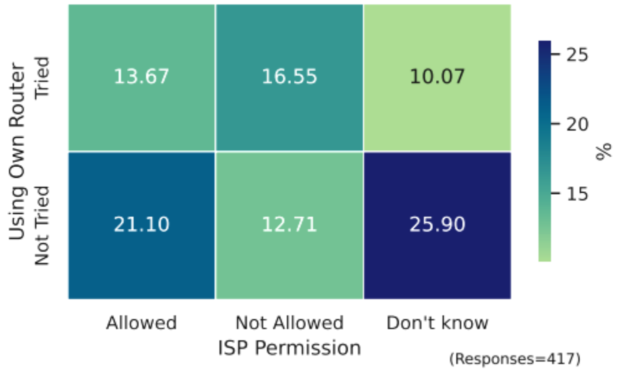

Figure 4. End-users trying to use their own router and ISPs' permission.

Participants' comments on trying to use personal routers

Participants who tried using their own routers/modems either had success or failed at it. The ones who tried but did not succeed had several reasons: in some cases, ISPs could not provide or accept a router running Free Software. Other ISPs imposed technical or operational restrictions that made the use harder, such as ISPs affirming that they only support their own equipment, not allowing users to use fiber routers or not providing installation support. Some users mentioned ISPs blocking access to ports by constant monitoring, even though there were no technical issues. Others related more extreme cases, when ISPs allowed neither the use of a private modem, nor for a modem to be put in bridge mode.

On the other hand, respondents who had not tried using their own router listed several reasons, such as the cost of buying a private router, or the fear of losing some services provided by the ISP's modem/router, or because they used bundled connections and services. Some could not find the necessary information to install their private router/modem. Particularly for those respondents, although there are tutorials online, relying on such third party information can be risky, and it does not necessarily cover individual needs.

Participants' comments on ISPs' restrictions on routers

Several of those reporting that they were allowed to use personal routers/modems pointed out the corresponding information on ISPs' websites. Others mentioned they were informed during the contracting phase by customer service.

Some users checked their contracts and found dubious or vague language. One respondent reported a clause which warns that "if the user blocks the subscription's terminal device to be 'callable', then the contract will be cancelled", although no clear definition of what "callable" means was given. Others reported that ISPs list technical specifications to which a personal router/modem should comply.

Some users heard about the possibility of using their own routers on the news due to the change of law in their countries. Others were frustrated because the use of a router was allowed, but not advertised or well disclosed in the contracting phase.

Participants who said they were not allowed listed several issues. Some responses relate to the fact that some ISPs do not provide support for installation and configuration, neither on their website, by phone nor by email. In some cases, although permission is explicitly provided on the ISP's website or in the contract, no help-desk support is provided for any router other than the one provided by the ISP. Other limitations highlighted by users included: restrictions on some features of their personal router due to ISPs' modem settings, no provision for network passwords, users could not get a fixed IP address and usage of only a few certified routers with certified firmware.

Regarding fiber connections, GPON users related that the ISP provided and allowed PPPoE pass-through but did not let them use their own fiber routers to access the FTTH network. Others related that the ONT was accessible only through bridge mode. Some related that when the ISP sent them the ONT, it included a leaflet with explanation how to use the router, but not a modem. On the other hand, one respondent related that the ISP was quick in helping to configure the ONT into bridge mode. It allowed configuring a firewall behind the terminal equipment.

In some extreme cases, there were reports of ISPs charging a monthly fee if users used their private router/modem. In one particular case, a respondent related that the ISP handed out modems with router functionality as standard, devices that cannot be configured by the end-user. The respondent was allowed to use another one only after many complaints and paying a fee.

Getting general information and login data

End-users should be informed if they can use personal equipment for internet connection. We wanted to know how difficult is it to find information on ISPs' websites. For the metrics for comparing how easily this kind of information is available, we have established:

- No information readily available: if the respondent tried to find it for more than 5 minutes;
- Very difficult: when it took 3 to 5 minutes to find;
- Difficult: if it took 2 to 3 minutes;
- Easy: if it took 1 to 2 minutes; or
- Very easy: if it was available in under 1 minute.

Besides, one of the alleged hurdles end-users suffer when trying to use their own equipment is receiving login data to the ISPs' networks. The survey asked those who already used a personal router/modem how difficult it was to receive the login data to the public network from the ISP, and to describe their experience.

From 879 responses gathered, 18% could not readily find information about Router Freedom on ISPs' websites. They are also the ones not using their own routers (N/A). More than 1% found it very difficult to find this type of information and also reported it very difficult to get login data for their routers. In total, 36% could not find readily available information on the website and 20% found difficult or very difficult to find such information.

On the other hand, although more than 9% could not find information about Router Freedom on the ISPs' websites, they reported it to be very easy to receive the login data from their ISPs. 37% said they were able to easily or very easily find such information and to get login data to the network.

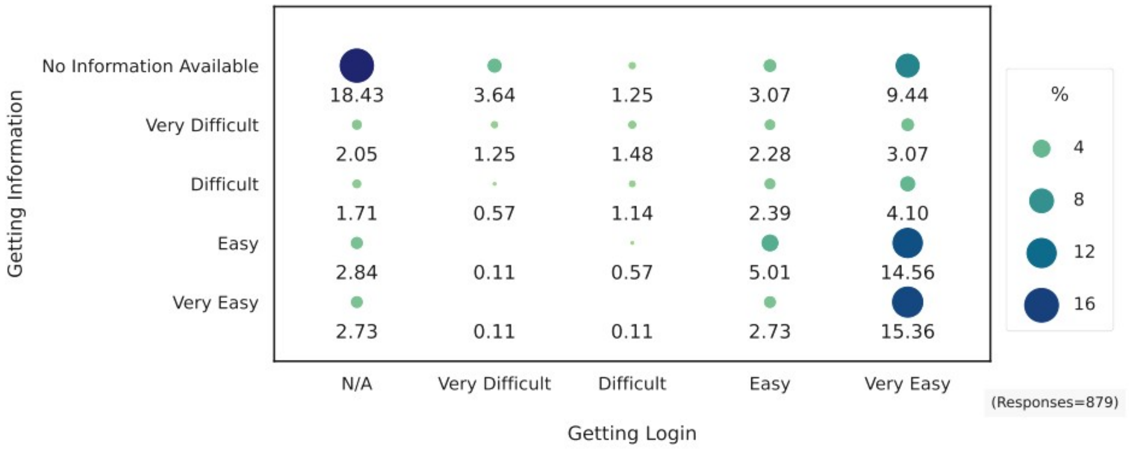

Figure 5. Information about Router Freedom on ISPs' website and getting login data to the network.

Participants’ comments on ISPs’ websites

Some participants who reported that no information was available on the ISPs’ websites said it took significant time and effort to get this information after requesting it by telephone or email. Other participants related that they received an answer to their request days or weeks later by snail mail.

Respondents who could get this information more easily reported that it might take up to 4 minutes even if they knew specifically where to look on the website – Q&A pages or on support-related areas.

Participants also related that they could only find such information on public forums and third-party websites. No official confirmation was given. Others added that the ISPs’ website directed them to the router manufacturer help desk.

Participants’ comments on getting login data

Respondents relating how getting login data was difficult said that the router had to be previously approved via mac address, and the login data was sent some days after. Several others related receiving these credentials by snail mail after days or even weeks. Some had to spend long or several phone calls with customer support. Others added that the ISP did not give them the login details, so they extracted them from the ISP's modem. Some used other means, such as using a virtual machine and a PPPoE server to capture the information. Several participants pointed out that, although the login details are publicly available, sometimes they are scattered across websites, support tweets and web forums.

Users who reported that it was easy to obtain the credentials reported that ISPs sent the credentials automatically, especially with recommended modems. Others also received the PPPoE credentials without requesting them. However, others who received the PPPoE credentials with a changeable password as part of their contract added that the ONT credentials to the OLT and GPON/VoIP credentials were not available.

Those using coax connections did not need login data, as ethernet connection is without the need for a PPPoE setup. The same is true for those using tv boxes or bundled equipment.

Proprietary plugs and connections

The survey intended to clarify whether ISPs use non-standard or proprietary plugs or connections on the network, which could hamper personal routers being used. From 1058 responses received, the overwhelming majority of responses (95%) replied that their ISPs use standard plugs for internet connection.

However, one respondent affirmed that the ISP would charge a financial penalty in case the user don't use the ISP’s proprietary VDSL filter. Others pointed out that imposing a proprietary ONT on fiber connections could be considered a violation of Open Standards.

ISPs' technical support

A controversial topic is whether ISPs should provide technical support for end-users employing personal routers for internet connection. The survey inquired if end-users have had technical service denied, or if the ISP provided support only for general connection requests but not for the router itself.

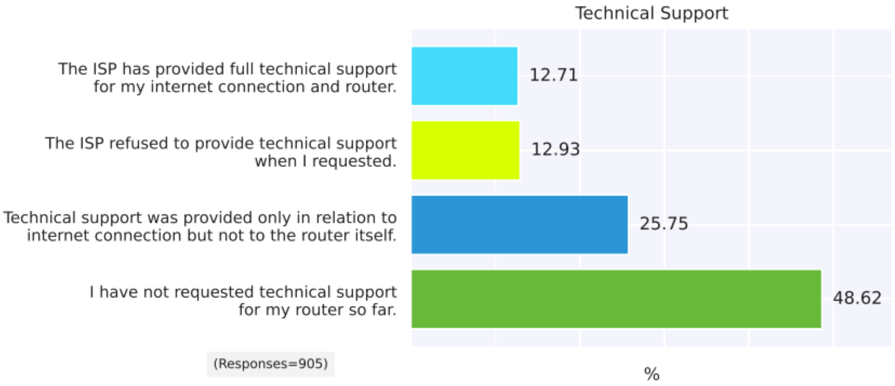

Figure 6. End-users' experience with ISPs' technical support.

From 905 responses received, although many of the respondents (48%) had not requested technical support for their router so far, a significant part (25%) reported ISPs offering support only for the internet connection and not for personal routers. In extreme cases, 12% reported ISPs refusing to provide technical support at all. On the other hand, 12% described the ISP being ready to provide support for both the connection and the personal router.

Participants' comments

Several participants reported that, although some ISPs do not provide technical support for personal routers, there are Q&As and other tutorials online with basic troubleshooting information. Others reported that ISPs' technicians informally helped them setting up routers during a visit to check connectivity problems.

More serious issues involve ISPs persistently blaming end-users' routers for connection problems, although the users have enough technical skills and knowledge to determine that the issues were not related to routers. Several respondents mentioned how hard is to convince support to the contrary. Some prefer to avoid mentioning that are using personal routers in order to get proper attention to their problems. Others mentioned that that if they had a technical problem with their own router/modem, they would call the manufacturer rather than the ISP.

ISPs' customer service

The survey inquired if ISPs' customer service is somehow imposing specific routers on end-users. We asked participants to relate their experience. From 1075 responses, although many (33%) had no experience in this regard, more than 7% reported customer service expressly prohibiting end-users to use personal routers on a contractual basis. 30% affirmed that ISPs' customer service did not try to impose a specific router on them, but an almost identical number reported arguments against using a personal router. 16% said customer service said they could not provide technical support for personal routers. 5% reported ISPs saying the router was not compatible with the network, 3% that the ISP's router is safer to use and 3% that the ISP's router is cheaper to buy, rent or use. 3% used other arguments.

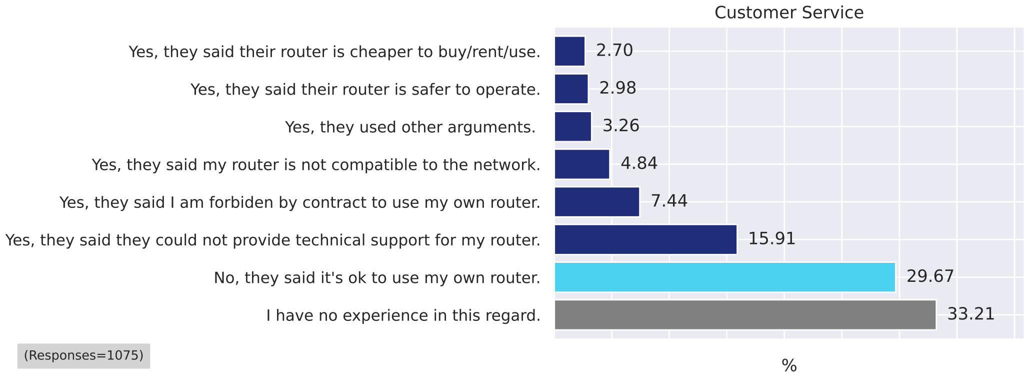

Figure 7. End-users' experience with ISPs' technical support.

Participants' comments

Respondents related ISPs trying to push their own routers at extra cost and with features not interesting for the end-user. Others related customer service advising against personal routers because it would be a threat to the ISP's network. Some argued in favour of better performance and connection speed for the ISP's router, which ended up not being true.

In some more telling cases, ISPs delivered routers without asking or billing, even when the provision of such equipment was not in the contract. One participant related having to keep the router until the contract ended. In another case, customer service affirmed the router would be free of charge and could be owned by the end-user, a situation which was afterwards not true. Other participants said that the ISPs' customer service refused to activate/authorize any other router. One respondent added that the ISP blocked any other router except their own one. Others related the ISP not authorising because "the fiber infrastructure provider (public body) requires the ONT to be part of the public network".

There was one case of an ISP not allowing a personal router admitting the end-user contract was an older one, and saying that the legislation giving freedom of choice was only for newer contracts. Some users who used their own routers did not get enough support from their ISP. Although the ISP did not force them to use its prescribed router/modem, it did not offer any support for anything else.

One respondent related the ISP imposing technical conditions for the users such as: "personal hardware would not 'cooperate' with the network operator." Another participant reported that the ISP forced their device out of IPv4 modem-only-mode with firmware updates, making it impossible for the end-user to use the router. It took several calls and days of waiting to get the ISP to revert it to IPv4 and associated modem-only mode.

On the other hand, even if the ISP's router is part of the internet contract, customer service was sometimes amenable to end-users adopting their own routers. In some cases, an ISP in the Netherlands even encourages users to employ their own equipment. This ISP offers a fixed discount for those who want to supply their own router.

Additional respondents' comments

The survey allowed respondents to list practices against Router Freedom they have encountered with their ISPs.

Proprietary devices and vendor lock-in

Some users pointed out that the provided router/modem or ONT devices are usually proprietary. End-users are not allowed to install custom Free Software operating systems.

In some extreme cases, there were reports of ISPs preventing users from using their own routers behind the ISP's modem. This severely limits end-users' rights and the ability to use any alternative router. For instance one mentioned that "the ISP uses IPv6 Dual Stack-Lite by default. In this setup, their modem doesn't allow bridge mode".

Others raised issues against the lack of important functionality with default routers. For instance, restriction for IPv6 or public IPv4, or little to no customization like changing the DNS. Others pointed out that with some ISPs is hard to get DOCSIS 3.1 routers that work on their network.

Participants have reported that, since they are not allowed to customize the router or install a different OS, energy efficiency is negatively affected.

Respondents also criticized ISPs for not providing the necessary documentation and technical specification of the network, even with contracts that allow Router Freedom. For instance, one participant complained about the use of a proprietary, undocumented authentication scheme for DHCP/DHCPv6. Within this network, Router Freedom is not possible until the protocol can be reverse-engineered and information published online. Besides, others pointed out that ISPs' customer support usually has no competence in dealing with technical issues and it is hard to get even simple issues resolved.

The situation with FTTH is in some cases worse. Participants denounced that ISPs refuse to provide alternative ONTs and force users to rent only a specific model. Users cannot subscribe to a contract without it, and are required to pay monthly fees for undesirable devices.

One user asserted that "the ISP reduces the connection speed if they detect a personal modem, and charge high fees in case I need technical support for issues, even if it is not related to my personal router." One ISP threatened to charge a user 125€ for support and a penalty if the problem was in the router.

End-user perception on Router Freedom policy demands

More than a mere technical issue, we believe freedom of terminal equipment is also a policy demand. The survey prompted participants to share whether they agree or not with the main principles that guide the FSFE's Router Freedom activity:

- Freedom of choice
- Privacy and data protection
- Interoperability and sustainability
- Fair competition and technological progress
- Security

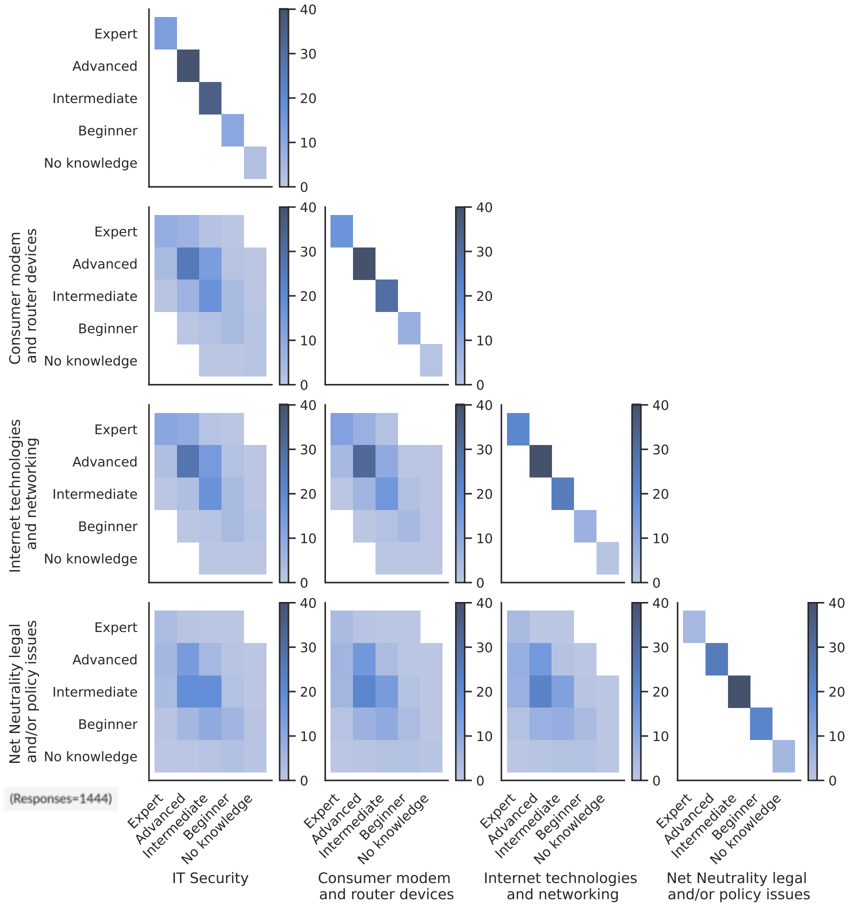

Figure 8. Participants' background knowledge.

The evaluation of the policy demands benefited from participants' self-assessment of their own level of experience and background knowledge – from beginner to expert – with topics related to Router Freedom. From 1444 responses, those who considered themselves with advanced knowledge with consumer routers/modems see themselves also having advanced or at least intermediate level with IT security and internet technologies. The self-assessment regarding political and legal issues related to Net Neutrality resulted in the majority seeing themselves as with an advanced or, at least, intermediate knowledge level.

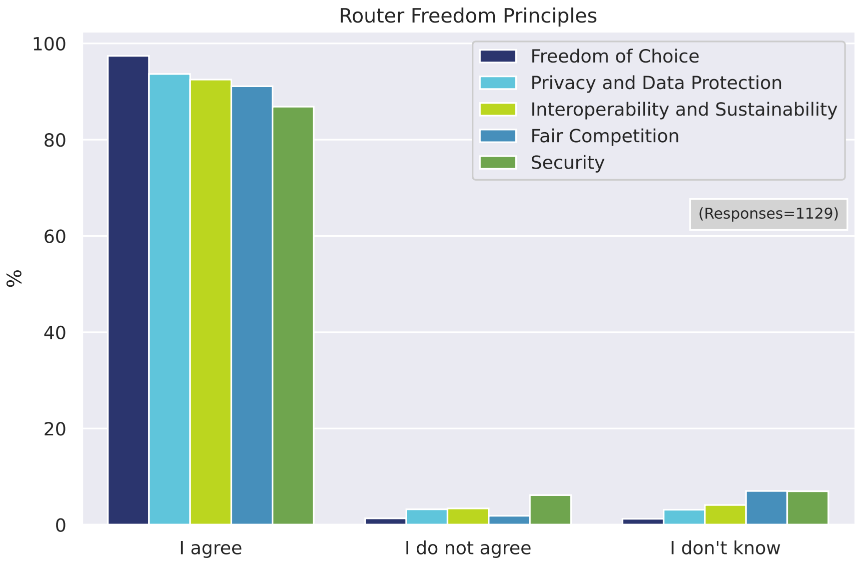

Figure 9. Participants' level of agreement on Router Freedom principles.

The FSFE's Router Freedom initiative's main demand is that end-users should be able to freely choose their routers and modems for internet connection. This is a corollary of broader policy concepts, like Net Neutrality and device neutrality, as network operators should not unduly discriminate which legitimized equipment the end-user can plug into the network.

From 1129 responses, 97% of participants agreed to the statement "Freedom of choice: the right to choose and use routers/modems is fundamental for a technological neutral internet access". 93% agreed with the statement "Router Freedom is fundamental for privacy and data protection". 92% agreed with "Router Freedom promotes the compatibility of devices, avoiding unnecessary costs for end-users and electronic waste". 91% were in favour of "Router Freedom supports competition and promotes technological progress" and 86% of "Router Freedom is important for internet access security".

Participants' comments regarding freedom of choice

Participants who agreed with the statement highlighted that freedom of choice means better functionality available for consumers, including better speed performance, flexibility in setting up different equipment in home networks and better features regarding IP and DNS, as well as installing different Free Software operating systems. Freedom of choice also fosters digital autonomy – as users can better configure their home network and deploy protective and security measures.

Other participants noted the policy component, arguing that Router Freedom is important for Open Internet and Net Neutrality, since it represents a safeguard for consumers against undue discrimination from network operators.

Some stressed the unethical element of ISPs forcing users to use proprietary devices where they cannot run Free Software. Users are better served when they have the right to choose Free Software for their routers because this contributes to the overall transparency in the telecom sector.

Respondents confirmed that the lack of Router Freedom enables ISPs to lock customers in. They can force their specific equipment, charge for alternatives and block completely the use of personal routers. This overloads end-users with high switching costs, hampering their ability to switch operators.

Participants' comments on privacy and data protection

The lack of Router Freedom may compromise privacy and the security of our sensitive personal data. Participants who agreed with the statement highlighted that Router Freedom enables them to control what runs on their devices and also the kind of data that goes out. Proprietary devices may have back doors to access local data. ISPs also can have remote control over provided routers, which is taken with suspicion by many users. Instead, users with their own routers can enable security features that protect data, such as firewalls or running state of the art VPNs. Even though some ISPs make available the source code of the firmware from some models upon request, end-users can benefit from having their own hardware. End-users should have a right to configure their own DNS, routing (subnets, DMZ, etc.), VPN, port forwarding and many other essential network options based on their preferences.

However, those not agreeing completely with the statement highlighted that online surveillance and data protection are broader and more complex topics that do not depend exclusively upon routers. ISPs can monitor internet traffic in different ways and it is not possible to change fundamentally how this is done. There are other elements in the internet chain that are susceptible to surveillance. Encryption does not necessarily start with the router. Even if the "mistrusted traffic" begins from the ISP infrastructure, encryption can do better than routers.

Others have also pointed out that a badly configured or updated modem/router can jeopardize not only personal data but also the security and stability of the network.

Participants' comments on interoperability and sustainability

Imposing specific models upon users and forcing them to acquire only compatible hardware can be bad for interoperability and the environment, due to the build-up of electronic waste even though the devices would still work. Respondents who agreed with the statement noted that Router Freedom allows them to determine when and whether to change the hardware. It may save e-waste, since with new updates and Free Software operating systems, the router can be used for longer periods. Others added that they can choose whether or not to stay with the same router manufacturer, which allows them to continue using features they are familiar with. Obsolescence of routers can be mitigated with alternative operating systems and updates. Users also can have better interoperability capabilities available with other devices in their homes, such as network repeaters, wi-fi devices and other smart hardware.

However, participants who disagreed with the assertion pointed out that some ISPs do refurbish their devices and provide them to other customers. They believe that Router Freedom only saves resources if users have routers already; if they have to buy new ones, there will be extra cost. Besides, end-users without the necessary knowledge can benefit from their ISP's support to provide better configuration for their hardware. One participant believes that, since ISPs acquire routers in bulk, the cost of acquisition can sometimes be lower.

Participants' comments on fair competition and technological progress

End-users profit from the free and fair competition in digital markets that guarantees free choice and steady improvement of products. Those supporting the assertion noted that Router Freedom supports competition on both ends (hardware manufacturers but also ISPs) as changing ISPs becomes simpler and less expensive if it is not necessary to purchase a new router. For others, running Free Software firmware clearly denotes technological progress. Some noted that competition in the router market can benefit from better interoperability.

Others warned that the FTTH market is concentrated with few options, since ISPs are imposing their own ONTs. This can lead to dysfunctional competition and vendor lock-in. Participants also manifested concern that monopolization of the FTTH equipment can lead to less innovation and worse security features.

Respondents in disagreement with the statement noted that ISPs incur expenses to integrate different hardware. New devices and functionalities may be good for consumers, but the costs of enabling these in the networks should be considered as well.

Participants' comments on security

The lack of Router Freedom increases the probability that large parts of the router market will be dominated by only one or a few product families or manufacturers. This can be problematic when security updates are not provided quickly or frequently enough for end-users. Security is one of the strongest arguments in favour of Router Freedom. Several participants stated that the main reason for getting their own router was to ensure internet access security. They are able to control network access, and easily and quickly implement new protocols and upgrades of firmware. End-users have more options to address their security needs. Free Software operating systems are kept up-to-date, constantly providing users new security patches, different from some proprietary vendors that are known to stop providing security updates after a while. For instance, one participant reported that "the ISP's router hasn't had security updates for more than 4 years".

Those against this statement argued that an ISP's centralized control and management make it easier for routers to be kept up-to-date and to deal with troubleshooting, finding and correcting security risks. Non-technical people could benefit from ISP security-related support as well. Others are concerned for the integrity of the public network and fear that badly configured routers can create security issues.

METHODOLOGY

The survey had a qualitative aspect and employed exploratory and descriptive approaches. The objective was to capture primary data about end-users and their relations with network operators. No secondary data was surveyed. The survey was made available to respondents online and disseminated by FSFE's communication channels.

Key facts:

- Total number of respondents: 1652. Not all respondents answered all questions. Report charts inform the amount of responses received for each analysed question.
- Geographical coverage: Europe
- Format: Online
- Time frame:
  - Data gathering: 20.10.2020 – 22.03.2023
  - Input analysis: March-April, 2023
  - Validation study and report: April-May, 2023

The Free Software Foundation Europe (FSFE) is a charity that empowers users to control technology. Software is deeply involved in all aspects of our lives; it is important that this technology empowers rather than restricts us. Free Software gives everybody the rights to use, understand, adapt and share software. These rights help support other fundamental freedoms like freedom of speech, press and privacy.

The FSFE was founded in 2001 as a non-profit, non-governmental organisation and network that is itself part of a global network of people with common goals and visions. The FSFE is supported by its members from all over Europe and has regional chapters in eleven countries. The central component of the FSFE’s work is keeping the legal, political, and social base of Free Software strong, secure, and free of particular interests.