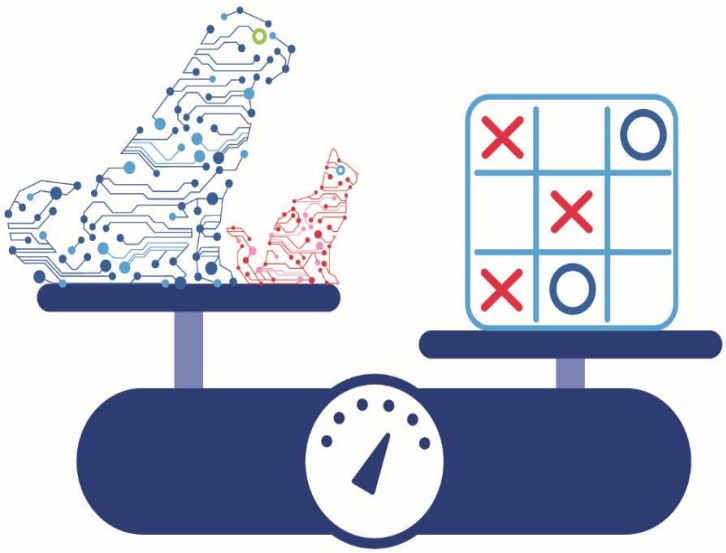

PETs controls matrix

A systematic approach for assessing online and mobile privacy tools

FINAL REPORT

PUBLIC

DECEMBER 2016

www.enisa.europa.eu European Union Agency For Network And Information Security

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact
For contacting the authors please use isdp@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

Acknowledgements
We would like to thank Claude Castelluccia (INRIA) for his support and advice throughout this project. We would also like to thank Rolf Wendolsky (JonDos) and Meiko Jensen (FH Kiel) for their comments and suggestions.

ISBN 978-92-9204-198-4, DOI 10.2824/475340

Table of Contents

Executive Summary

Following previous work in the field of privacy engineering, in 2016 ENISA defined the 'PETs control matrix', an assessment framework and tool for the systematic presentation and evaluation of online and mobile privacy tools for end users. The term 'PET' is used in the context of this work with a narrow focus, addressing standalone privacy tools or services (and not the broader concept of privacy enhancing technologies).

The defined framework relies on a set of assessment criteria, which can be broken down into specific parameters and assessment points, acting as indicators of certain properties and features of the tools. A distinction is made between generic and specific criteria.

The generic criteria aim at assessing general characteristics of PETs that are applicable to all types of tools and relate to privacy and security. These characteristics are not always technical (in contrast with the specific criteria) and aim at providing a general understanding of how privacy and security are taken into consideration in the context of specific applications. Three generic criteria are considered under the proposed framework, namely: maturity and stability, privacy policy implementation and usability.

The specific criteria aim at assessing particular characteristics of distinct categories/types of PETs, exploring in a detailed manner their technical features and their privacy enhancing functionality. As such, they are mainly of technical nature, although in some cases broader data protection aspects may also be considered. For the purpose of this work, the following categories of PETs are analysed: secure messaging, virtual private networks (VPNs), anonymizing networks, and anti-tracking tools (for online browsing). The choice of these PETs categories was based on the popularity of the particular tools, as well as the increasing availability and use of relevant apps in mobile devices. Still, there are many other categories of privacy tools that can be considered, as for example tools in the areas of privacy-enhanced location-based services and access rights control management for mobile applications.

The 'PETs control matrix' is the implementation of the proposed assessment methodology into a practical tool that can be used for performing the assessment of a PET and presenting the relevant results. As such, it comprises different sets of detailed assessment questions (and relevant closed sets of answers) corresponding to the predefined assessment criteria. Due to the inherent difficulty of attributing specific weights and values to distinct controls related to privacy and data protection, no specific scaling or grading is used. Therefore, the 'PETs control matrix' should mainly be seen as a means that can facilitate a standardized and clear presentation of different privacy tools, rather than a tool that can directly offer comparative assessments. The practical use of the 'PETs control matrix' is demonstrated in the document through a number of findings in the area of secure messaging applications.

Based on the aforementioned work, as well as the testing of different privacy tools, the document draws a number of general conclusions and subsequent recommendations to be considered by all involved stakeholders in the area of PETs.

Recommendations - What you see is not always what you get

Although there are several very useful and trustworthy privacy tools available in the market today, users do not always get precise information about their actual operation and features.

The PET developers/providers should offer clear information about the actual functionality and attributes of their tools, as well as opt for privacy by default settings, taking into account the privacy and data protection expectations of their users.

The research community and security/privacy centred EU and national organisations should support PETs assessment frameworks aiming at addressing the technical details of different tools and offering clear information to end users.

Recommendations - Open and closed source software

While open source cannot be considered per se as an indicator of a tool's trustworthiness, information on the tool's development (e.g. use of third party libraries) can be central in increasing transparency.

The PET developers/providers should make available as much as possible information about the basic PET libraries used for the provision of privacy-enhancing features of their tools.

The European Commission, EU standardization bodies and security/privacy centred EU organisations should explore certification schemes for PETs based on commonly accepted assessment frameworks. Such schemes can build more certainty on the functionality of different tools, independently from the licensing type used.

Recommendations - Usability and privacy

Some problems often associated with PETs are low performance and other possible side effects, leading to the perception that users have to trade off usability for privacy protection online.

PET developers/providers and the research community should invest more in 'usable privacy' and 'usable security', involving also end users in the assessment of tools. The European Commission should promote research in this field, as a key enabler of the adoption of privacy technologies in online and mobile environments.

PET developers/providers should provide clear information on known limitations/side effects of their tools to the general public.

Recommendations - Providing information to the general public

Users prefer easy and fast information from trusted sources, rather than detailed technical information. It is, thus important to define how PETs assessment frameworks can really contribute to enhancing user information and awareness.

As a means to enhance transparency, PET providers/developers should make use of assessment frameworks/mechanisms (such as the 'PETs control matrix') and support relevant platforms/schemes to provide comparable presentations of the different features of their tools.

The research community and civil society organisations should engage in publishing technical reviews of PETs based on commonly accepted assessment frameworks.

The European Commission, security/privacy centred national and EU organisations, as well as national and EU privacy regulators/supervisors (e.g. Data Protection Authorities) should support platforms that can enable assessment of PETs (e.g. by independent privacy experts).

National and EU privacy regulators/supervisors (e.g. Data Protection Authorities) should provide more precise guidance on the use of PETs, as well as practical examples of the concepts of 'data protection by design and by default'.

Recommendations - Beyond PETs: a privacy assessment framework for online and mobile applications and services

The work presented in this study was focused on the assessment of PETs, i.e. tools that are already designed to protect users' privacy and personal data. A future step for the developed framework would be its extension to conduct privacy assessments of different types of online and mobile tools that are widely used today by the general public in the context of their everyday activities (e.g. different categories of mobile apps).

The research community, security/privacy centred national and EU organisations, as well as national and EU privacy regulators/supervisors (e.g. Data Protection Authorities) should co-operate and define a generic framework for privacy and data protection assessments of different types of online and mobile tools. Such a framework could on one hand enhance users' information and awareness regarding the privacy policies of different tools, while on the other hand it could contribute to the practical implementation of GDPR by application and service developers/providers.

1. Introduction

1.1 Background

In today's online and mobile world one of the most serious concerns is the preservation of privacy and personal data while conducting everyday activities, such as e-shopping, e-banking or e-communication with colleagues, friends and family. This concern has given rise to an increasing appearance of online tools, with components often open-source and/or freeware, affirming that they can offer certain privacy-preventive functionality for the end user, such as for example secure communication, protection against tracking, data encryption, and anonymous browsing[1]. As it has been shown, the interest of the general public in such tools can become quite strong especially following large scale data breaches and leaks[2]. However, in some cases the functionality of these tools may not be as expected, for example due to limitations in the tool's actual operation or maintenance mechanisms. Privacy enhancing technologies (PETs)[3] that fail to offer what they promise can be risky, as the false sense of protection can result in compromised personal data and negatively affect or even put in harm's way the users' personal life.

Against this background, in 2015 ENISA carried out a study on online privacy tools, aiming at enhancing trust and assurance in their use by the general public [1]. One of the main findings that was highlighted in the study was the need for a widely accepted methodology for the assessment of PETs (privacy tools), which could enable a uniform presentation of their different aspects, thus supporting end users in making informed choices. Such a methodology could be used both by privacy experts providing reviews and/or comparisons of tools, and/or by the tools' developers (in the course of a self-assessment practice). More advanced users could also apply the methodology to assess certain elements of their preferred tools. ENISA, in the same study, proposed a number of criteria that could be applied in the context of PETs assessment, focusing on reliability/trustworthiness and usability of the tools. A number of open issues were also identified, for example relating to the assessment of privacy by design, the analysis of side effects (due to the use of PETs), the usability & accessibility assessment, performance and costs of PETs, and relevant legal, ethical and societal aspects. The practical application of the methodology was outlined as an important element, taking into account maintenance and visualization issues. Moreover, in 2015 ENISA also performed a study on the readiness analysis and evolution of PETs (going beyond standalone privacy tools), aiming at creating measurable indicators and scales for assessing the maturity of privacy enhancing technologies [2].

Following the aforementioned work, ENISA decided, under its 2016 work programme[4], to continue towards the development and practical implementation of a systematic approach for the assessment and presentation of online and mobile privacy tools.

[1] Lists of and advice on privacy tools can be found in several portals available online today, e.g. Electronic Frontier Foundation (www.eff.gr), PRISM break (https://prism-break.org), Me and my shadow (https://myshadow.org), EPIC (https://www.epic.org/privacy/tools.html), etc.

[2] For example, according to studies, in the wake of Edward Snowden's revelation about NSA surveillance, the daily adoption rate of open PGP encryption tripled, http://www.dailydot.com/news/pgp-encryption-snowden-prism-nsa/

[3] Note that the term 'PETs' is used in this document with a narrow scope to refer to standalone privacy tools or services maintained by specific groups or companies.

[4] ENISA Work programme 2016, https://www.enisa.europa.eu/publications/corporate/enisa-work-programme-2016

1.2 Scope and objectives

The scope of this year's project was to develop and present a 'PETs control matrix', i.e. a practical form/tool with clear assessment questions that could be used in order to evaluate different PETs, based on their generic (e.g. maintenance, usability) and specific (functional) characteristics. In this way, the matrix could also offer the possibility of comparative presentations of tools of the same type, aiding end users in defining what is actually useful for them. To this end, the specific objectives of the work performed were as follows:

- To define a thorough assessment framework for PETs, relying on a set of *assessment criteria*, which can be broken down into specific *parameters* and *assessment points*, acting as indicators of certain properties or features of the tools. A distinction is made between *generic criteria*, applicable to all PETs, and *specific criteria*, assessing particular functionalities of different types of tools. For the purpose of this work, the following categories/types of PETs were explicitly considered: *secure messaging applications, Virtual Private Networks (VPNs), anonymizing networks,* and *anti-tracking tools for online browsing*.

- To provide a set of focused questions under each particular assessment criterion, together with its possible answers. These questions are then put together to provide a thorough PETs assessment 'package', i.e. the 'PETs control matrix'.

- To present the 'PETs control matrix' in a practical form (Excel-based tool) to be used both by the parties performing the assessment, as well as by the end users.

It should be noted that to fulfil the scope of this project only tools targeting directly the protection of users' privacy have been considered. To this end, although most general security tools (e.g. antivirus or firewalls) would also contribute to the protection of privacy, they have not been taken into account in the design of the 'PETs control matrix'. Moreover, emphasis is explicitly put on *mobile PETs*, i.e. privacy enhancing tools designed to work during an internet connection and protect the privacy of mobile (e.g. smartphone) users.

It also important to clarify that the term 'PET' is used in this document with a narrow focus, addressing *only* standalone privacy tools or services, which are developed and/or maintained by specific groups or companies. Still, 'PETs' is generally applied to cover any type of privacy enhancing technology that can be part of certain products or services (such as for example anonymization or searchable encryption mechanisms)[5].

1.3 Methodology

The methodology for defining the proposed PETs assessment framework and designing the 'PETs control matrix' was based on:

- An initial desktop research.
- Analysis and testing of different types of PETs (with special focus on PETs for mobile devices).

As a first step, the desktop research was focused on existing PETs assessment methodologies and/or projects, such as for example the Electronic Frontier Foundation Secure Messaging Scorecard [3] and

[5] For a more detailed analysis on the concept of PETs, see: https://www.enisa.europa.eu/topics/data-protection/privacy-enhancing-technologies

Surveillance Self-Defence [4] projects, as well as other initiatives in the field[6]. In this context we also reviewed documents and reports from independent organisations and public authorities on mobile privacy and security [5] [6] [7] [8], as well as policy and technical reports from developers of mobile OS and applications (apps).

As a second step, the analysis and testing of tools was carried out in order to understand the functionalities currently offered, with special attention to the level of privacy-enhancing features that are provided by different tools (which is the focus of PETs). A deeper understanding of the tools was central in defining the assessment criteria, as well as the specific parameters and points that are related to their functionalities. To this end, tools of all four categories addressed in the 'PETs control matrix' (secure messaging applications, VPNs, anonymizing networks, anti-tracking tools) were analysed, with special attention to relevant mobile apps.

The analysis was mainly performed by installing and using the tools in different OS platforms, in many cases with the support of publicly available information (e.g. technical documentation from app developers). In some cases a more detailed technical analysis was performed (traffic analysis, app analysis for open source tools and using publicly available software), which could in some cases reveal more information on certain technical aspects of the tools.

It should be noted that the assessment of specific tools was not the purpose of this work and any analysis performed was only to guide the research and support the provision of a sound PETs assessment framework. Therefore, no evaluation or comparison of specific tools is provided as part of the present report.

1.4 Structure

In order to provide a thorough insight on the overall PET's assessment framework, this document is structured as follows:

- Chapter 2 provides an overview of the PETs assessment criteria, explaining the approach followed in their definition, as well as related considerations.
- Chapters 3 and 4 present in depth each assessment criterion (generic and specific), providing a detailed analysis of the parameters/indicators that they are comprised of, as well as the possible methods that can be applied for their assessment.
- Based on the aforementioned analysis, Chapter 5 explains the concept of the 'PETs control matrix' and includes some conclusions from its pilot application in the area of secure messaging tools (example). The matrix itself is available in two forms: a) a set of questionnaires for each particular criterion in Annex 1 to this document; b) an EXCEL tool (with integrated questionnaires) as Annex 2 to this document.
- Finally, Chapter 6 draws some conclusions and recommendations regarding the adoption of the 'PETs control matrix' and the general role of PETs assessment for providing guidance to the general public.

The target audience for this document includes all interested stakeholders in the area of privacy tools (PET developers, Data Protection Authorities, industry, academia), as well as the general public, i.e. internet or mobile users who would like to use specific tools for the preservation of their privacy and personal data.

[6] See list of relevant initiatives in [1]

2. PETs assessment criteria: an overview

2.1 Introduction

On a conceptual basis, the first (and most critical) part of the conducted work was the definition of the assessment criteria, which set the basis for the further design and implementation of the 'PETs control matrix'. These criteria, which build on both generic and specific characteristics of different types of tools, are in fact comprised of a number of more detailed parameters and assessment points, which can finally be 'translated' into particular questions, filling the 'PETs control matrix' (Figure 1).

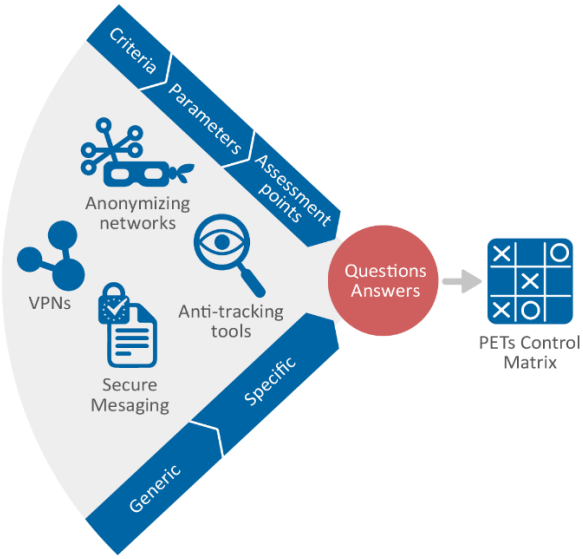

Figure 1: Schematic representation of the PETs assessment framework

Therefore, the selection of the 'right' criteria, which can thoroughly address all aspects of the PETs under consideration is of upmost importance for the whole project. In this Chapter we aim at explaining the rationale and main considerations in this regard, together with a snapshot of all defined criteria (which are further detailed in later Chapters).

2.2 Generic and specific criteria

As already mentioned, the 'PETs control matrix' distinguishes between two categories of criteria: generic and specific. One could argue that the reason for this approach is quite obvious; while each type of tools has dedicated functional characteristics, there are still certain elements that are crucial to all types of tools (in terms of privacy and security) and could be grouped in a more abstract way. For example, while end-to-end encryption is an important functionality for secure messaging applications, it is probably not an element to assess in the area of anti-tracking browser extensions, where blocking of trackers is the most critical function. However, in both cases, maintenance of the tools is critical, as poorly updated tools often fall short in providing an adequate level of protection.

Nevertheless, it is important to note that it is not always easy to distinguish between generic and specific features (or otherwise to define the desired level of abstraction). Indeed, while certain features can be found (or are expected to be found) in all types of PETs, in many cases it is the particular implementation of these

features in the context of specific tools that really matters. As an example, while the implementation of privacy by default is an important feature for both secure messaging applications and anti-tracking browser exceptions, it is most interesting to assess how this feature is explicitly addressed in each type of tools (e.g. via their particular default settings).

This consideration was significantly taken into account in the 'PETs control matrix', trying to find the right balance between general and specific characteristics and accordingly present them under relevant criteria.

2.3 Putting privacy into practice

Another important consideration in the definition of the criteria was the practical implementation of privacy and data protection requirements/concepts in the context of particular types of tools. These requirements stem primarily from the General Data Protection Regulation 2016/679/EC (GDPR) [9], which will be applicable from May 2018 as the main and commonly applied legal framework for the protection of personal data in the European Union, replacing the current Data Protection Directive 95/46/EC [10]. GDPR sets a number of principles for the processing of personal data, in particular the principles of lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality. It also provides for the possible legal basis for the processing of personal data, putting special emphasis on the notion of consent and relevant information provided to the data subjects. Security of personal data is central to GDPR, as well as the newly introduced obligations of data controllers for data protection by design and by default and the reinforced data subjects' rights for data erasure and portability. On top of GDPR provisions, privacy requirements in the context of our work also stem from the Directive on privacy and electronic communications 2002/58/EC (ePrivacy Directive) [11], especially with regard to confidentiality of communications (art. 5), where it is stated that no data can be accessed or stored in the user's terminal equipment without user's consent[7].

Following the aforementioned legal framework, an issue that became crucial in the definition of the PETs assessment criteria was how to practically address questions posed by the data protection principles, obligations and/or rights (while analysing specific tools). This is particularly important, taking into account that practical implementation of data protection requirements may vary, translating to a number of distinct (but still correlated) technical and organisational controls. In order to avoid abstract descriptions, the approach we took was to assess implementation of the different controls (e.g. for requesting consent, providing information to data subjects, data retention and erasure, etc.), sometimes under different criteria, which at the end can provide a consolidated understanding of how privacy and data protection are overall considered in a given tool. To this end, we also used previous ENISA work in the field of privacy [12].

An example of this approach can be demonstrated in the assessment of privacy and data protection by design. Indeed, in this case, instead of asking general questions on if and how privacy and data protection by design has been applied for a specific mobile app, we directly assess what types of data the app accesses or stores on the user's device (data minimization), for what purpose this is performed (purpose limitation), if the data are stored in an encrypted form (security), etc.[8] Therefore, although a specific assessment criterion on privacy by design is not provided as such, the assessment of privacy by design is a core focus of many different parts of the 'PETs control matrix' (both under the generic and the specific criteria). The same approach has been applied to other cases, such as for example the practical implementation of the right of access, data erasure, data protection by default, etc. In order to show the links to the applicable legal

[7] It should be noted that the ePrivacy Directive is currently undergoing a review by the EC in order to get streamlined with the GDPR provisions, see latest information in https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-evaluation-and-review-eprivacy-directive

[8] Following the privacy by design strategies mentioned in [12]

framework, references to GDPR and ePrivacy Directive are made while describing the assessment criteria whenever relevant.

Having said that, it is also important to note that not all aspects addressed under the 'PETs control matrix' are directly related to the data protection legal framework. Indeed, many criteria and assessment parameters are of purely technical nature, relating to particular security features of different tools, while others are of a broader scope, assessing for example business models or maintenance plans of the tools (to the extent that these are related to the privacy and security features of the tool – see section 2.4).

2.4 Defining privacy-related characteristics

An additional point of attention in the course of this exercise was to define which criteria/parameters/assessment points are indicators of (good or poor) privacy and security practices. Although some criteria are pretty obvious (e.g. requesting user consent for accessing/storing data on user's device, setting default settings to highest level of privacy protection, generating and storing encryption keys only on user's device, etc.), others are more indirect and require further analysis.

An example of the latter case is the whole area of usability. Indeed, despite the fact that usability is not directly related to privacy, it can still be a very important privacy enhancing factor, since it can enable the broader adoption of a PET. On the contrary, difficult to use PETs have very low adoption levels by the general public, even if they offer very strong privacy guarantees.

This dimension has been broadly considered in our proposed framework, including all types of factors that could directly or indirectly affect the use of a PET by the general public.

2.5 Specificities of mobile apps

Although the assessment of PETs is in principle unrelated to the user's device/equipment, for the purpose of this work we paid particular attention to the field of mobile PETs (apps). This is due to the fact that users are increasingly relying on mobile devices for their everyday online activities, while at the same time the level of privacy and security of mobile apps is in many cases relatively low. Moreover, apps marketplaces do not always apply adequate vetting procedures in order to disallow rogue apps from infiltrating[9].

To this end, attention was paid to aspects that are critical in this area, such as for example access to/transfer of data stored on the user's device, connection to remote servers, etc. Although most of these aspects would also be applicable for desktop applications, they may take specific forms of implementation in mobile devices (which were analysed through the testing of different apps).

[9] See a relevant example in New York Times article: http://www.nytimes.com/2016/11/07/technology/more-iphone-fake-retail-apps-before-holidays.html?hpw&rref=technology&action=click&pgtype=Homepage&module=well-region&region=bottom-well&WT.nav=bottom-well&_r=0

2.6 The list of assessment criteria: a snapshot

Taking into account the aforementioned considerations and following the methodology presented in Section 1.3, we concluded to the lists of generic/specific criteria presented in Tables 1 and 2 below.

PETS ASSESSMENT FRAMEWORK – GENERIC CRITERIA	
CRITERION	**DESCRIPTION**
MATURITY AND STABILITY	The way that a tool responds to existing and/or new security and privacy challenges; the way that a tool evolves over time in order to address the security and privacy needs of its user group.
PRIVACY POLICY IMPLEMENTATION	The definition of a thorough personal data processing policy by the PETs developer/provider; the practical implementation of this policy through the use of relevant controls.
USABILITY	The extent to which a tool can be used by its users to achieve its privacy protection functionality with effectiveness, efficiency and satisfaction.

Table 1: PETs assessment framework: generic criteria

PETS ASSESSMENT FRAMEWORK – SPECIFIC CRITERIA		
CATEGORY	**CRITERION**	**DESCRIPTION**
SECURE MESSAGING TOOLS	End-to-end encryption	A system of communication where the only people who can read the messages are the people communicating.
	Client-server encryption	Encrypting the communication channel established between a client and a server.
	Security of stored data	Level of security of stored data (locally and remotely).
	Authentication	Verification of communicating parties' identities; authenticity of communication data.
	Anonymous communication	A communication where no third party can identify the communicating parties.
VIRTUAL PRIVATE NETWORKS (VPN)	Identity protection	Hiding user's real IP address or other identifiers from third parties.
	VPN encryption	Securing the communication channel between user and VPN provider.
	Side effects	Adverse effects on user's online experience caused by the VPN.
ANONYMIZING NETWORKS	Anonymity protection	Ensuring that the user cannot be identified by any party within the network or by any other third party.
	Encryption	Securing communication end-to-end or in certain parts of the network.
	Side effects	Adverse effects on user's online experience caused by the network.
ANTI TRACKING TOOLS (ADD-ONS)	Blocking	Ability to block different types of online trackers.
	Data collection	Collection of data related to the users' blocking/browsing habits.
	Side effects	Adverse effects on user's online experience caused by the tool.

Table 2: PETs assessment framework: specific criteria

Chapters 3 and 4 present in detail each of the criteria, the logic behind their (consolidated) definition and their related parameters and assessment points.

2.7 Assessment methods

Broadly speaking, we could say that the assessment of the criteria for PETs can be based on three different levels of analysis:

- Level 1- Use of publicly available information: Such information includes web sites of PETs, public forums and blogs, existing reviews and audits, technical reports from PET developers or other parties, etc.
- Level 2- Hands on testing of the tools: This concerns the exploration of the different features of the PET by simple installation and use. In some cases it might include some minimum testing with the use of external tools, e.g. to test the installation of certificates or check specific side effects.
- Level 3- Technical analysis: This concerns the more in-depth technical testing and it can include different methods, e.g. traffic analysis or code review. It requires the use of supporting software/equipment (e.g. setting of a 'lab', the use of packet sniffing tools, specific tools for automated app analysis, etc.).

Obviously, as the level of analysis increases, the difficulty also increases, with the technical analysis being the most demanding one. At the same time, the 'deeper' one digs into the technical implementation of the tool, the more detailed and accurate information he/she can obtain, as the declared features of a tool can be evaluated in practice. This shows in fact the limitations of the assessment framework, due to the inherent limitations of the technical analysis per se. Indeed, this type of analysis is not always possible, due to the technical complexity that is often involved, as well as the specific technical limitations (e.g. unavailability of the source code) or legal restrictions (e.g. relating to code review) that may be present.

To this end, it is interesting to note that the assessment methods (and the depth of the assessment) may significantly vary depending on the party that performs the assessment. This variation does not relate only to the required level of privacy/technical expertise or skills of the evaluator, but also on the actual technical possibilities that a party has to perform an assessment. In that sense, the PET developers can of course have the deepest level of knowledge regarding their tools' functionalities, which cannot in practice be possible for any other party. Yet, the developers are not a neutral third party and, thus, a self-assessment process presents certain limitations with regard to the trustworthiness of the final results.

3. Generic assessment criteria

In the context of the 'PETs control matrix', the generic criteria aim at assessing general characteristics of PETs that are applicable to all types of tools and relate to privacy and security. More specifically, under this category of criteria, we tried putting together different 'angles' of PETs development, operation and use, that are not directly relevant to their specific functionalities, but still play an important role with regard to their privacy preserving features. These characteristics are, thus, not always technical (in contrast with the specific criteria) and aim at providing a general understanding of how privacy and security are taken into consideration in the context of specific apps. In particular, following the methodology and approach described in Chapters 1 and 2, the following three broad criteria have been defined:

- Maturity and stability.
- Privacy policy implementation.
- Usability.

The next sections explain in more detail the logic of the criteria, breaking them down into particular parameters and assessment points.

3.1 Maturity and stability

As discussed in previous ENISA's work [1], maturity and stability are integral parameters for building trust and assurance in software. Time can be a useful element to consider, in the sense that tools dating back a few years might have had the opportunity to get tested (and probably be improved). Still, time cannot alone define the level of maturity and stability of a certain piece of software: it is the overall evolution of the software and the way that is has grown with time that finally determines its maturity and stability [13].

In PETs the criterion of maturity and stability is mainly set to address how a tool deals with privacy and security challenges over time in a fast changing online environment, by particularly analysing:

- The way that a tool responds to existing and/or new security and privacy issues (e.g. new security threats and vulnerabilities).
- The way that the tool evolves in order to address the security and privacy needs of its user group (e.g. by developing/upgrading certain features to enhance privacy protection).

To this end, maturity and stability is clearly associated with two principal parameters: on one hand the *maintenance* of a tool and on the other its functional updates (over time) with regard to *privacy protection*. Two additional parameters in this respect are the level of *community support* that the tool receives, as well as relevant *audits and reviews* (regarding the tool's overall functionality). These parameters are analysed in more detail in the next paragraphs, together with their subsequent assessment points/indicators.

3.1.1 Maintenance

In software engineering maintenance is defined as 'the modification of a software product after delivery to correct faults, to improve performance or other attributes' [14]. For the scope of this study, maintenance is mainly considered with regard to security and privacy, taking into account a number of specific parameters, as shown below.

Updates
The existence of regular updates is the best way to assess whether a tool is 'alive' and can be a strong indicator of the tool's overall maintenance plan [15]. To this end, it is important to assess the last update/frequency of updates, as well as the information provided to the users (e.g. whether automatic updates notification is provided). However, one should always have in mind that updates are also very much dependant on the tool's functionality and, therefore, there is not a 'one fit for all' solution (e.g. regarding time or number of updates).

Reactivity to publicly known security vulnerabilities
The public disclosure of security vulnerabilities can greatly hinder the operation of PETs[10]. It is, thus, essential to assess whether such security vulnerabilities have indeed been discovered, if and how they have been addressed by the PET's developer, and the type of information that is provided to the users, especially in cases where the vulnerability has not been addressed (e.g. providing advice to the users on recommended alternate configurations).

Version history
A complete and documented version history (especially regarding the security and privacy preserving functionalities of the tool) provides the users valuable information about the evolution of the PET over time. It is, thus, interesting to assess the availability of such feature, as well as the way that it is presented to users.

3.1.2 Privacy protection

This parameter is related to functional updates, enhancements or restrictions with regard to a tool's privacy preserving functionalities. It can serve as indicator of whether and how the developer seeks to constantly address new privacy and security risks (and therefore new user needs). Its assessment can be based on two main points/indicators, as shown in the following.

New privacy enhancing features
Including new features to face new privacy and security challenges is key for a PET to remain state-of-the-art (e.g. introducing the option of anonymous communication in a secure messaging application). The provision on such enhancements over time and the subsequent information to users are therefore interesting elements to assess. Still, this parameter needs to be assessed very carefully and in combination with the parameters on maintenance, as the dynamic addition of new features, if not properly implemented, may introduce new vulnerabilities, thus reducing the overall trustworthiness of the software.

Limitations
A PET may present certain limitations with regard to its privacy enhancing functionalities (e.g. known weakness of the tool and/or specific types of attacks that could compromise the protection offered). Therefore, it is interesting to assess whether indeed such limitations exist and if the developers provide relevant information and/or advice to the users (e.g. informing them about best configuration options in certain environments or advising on the combined use of other PETs).

3.1.3 Community support

This parameter refers to the existence of communities and/or forums which can help the overall upgrade and evolution of the tool (and, thus, maturity and stability), e.g. by reporting defects or functionality issues, as well as by driving enhancements for privacy protection[11]. Different communities (e.g. of users or

[10] For more information, see ENISA's Good Practice Guide on Vulnerabilities Disclosure [53].
[11] See for example the Tor project user community, https://blog.torproject.org/category/tags/community

developers) might be available and it is, thus, interesting to assess their level of involvement and engagement.

It is important to note that in many cases community support is closely related to the software distribution and licensing scheme (open or closed software), which in turn is also an important aspect to consider. Indeed, although the maturity and stability of a PET does not per se depend on its distribution model, the possibility of source code revision in open source allows users to contribute to code development, building in this way community support. Still, relying explicitly on community support might be a discouraging factor for companies to adopt an open source distribution model, as the level of support is not contractually agreed and, thus, cannot be adequately trusted. In the case of open-source PETs, it is useful to assess the particular licensing schemes (e.g. GNU General Public License, GPL or GNU Lesser General Public License, LGPL) with regard to possible intellectual property rights/copyrights.

3.1.4 Audits and reviews

Another important parameter to consider is the existence of technical audits and reviews, as well as formal verifications or evaluations by independent experts or by a certification body (based on, for example, Common Criteria [16]). Such material can bring very useful insight with regard to the maturity and stability of a tool and is closely linked to the parameter of community support.

3.1.5 Summary and assessment methods

Following the aforementioned analysis, Table 3 presents an overview of all assessment parameters/points for maturity and stability.

PETS ASSESSMENT FRAMEWORK – GENERIC CRITERIA: MATURITY AND STABILITY	
PARAMETER	**ASSESSMENT POINTS**
MAINTENANCE	Updates Reactivity to publicly known security vulnerabilities Version history
PRIVACY PROTECTION	New privacy enhancing features Limitations
COMMUNITY SUPPORT	User/developer communities Software distribution and licensing
AUDITS AND REVIEWS	Formal reviews/audit reports Accreditations and certifications

Table 3: Analysis of maturity and stability criterion

The main assessment method that can be applied in the case of maturity and stability is the use of publicly available information, e.g. through the tool's web site or other official stores, user forums, blogs, websites publishing public reviews, scientific journals (for example regarding vulnerabilities or formal verifications), etc. Some information could also be obtained by hands on use of the tool (e.g. scheduling for updates). More in-depth technical analysis would most probably not be easily applicable in the case of this particular criterion.

3.2 Privacy policy implementation

The criterion of privacy policy implementation is related to the way that a PET (or rather the PET's developer/provider) processes personal data stored on the user's device. Processing of personal data should follow the principles and legal obligations set by the EU General Data Protection Regulation (GDPR) [9] and the Directive on privacy and electronic communications (ePrivacy Directive) [11] (see also section 2.3 of the report).

It is important to note that the focus of this criterion is not on personal data generated or processed as part of the functionality of the tool (e.g. communication data in the context of a secure messaging app), but rather on data stored on the user's device *independently of the tool's functionality* (e.g. an application gaining access upon installation to contacts or photos previously stored on the user's device). The reason for this is that personal data processed as part of the tool's functionality are explicitly covered under the specific criteria on secure messaging, VPNs, anonymizing networks and anti-tracking tools. The scope of this generic criterion, thus, is to assess in a broader way:

- How a tool, once installed in the device, 'treats' users' personal data (e.g. whether it accesses certain types of data, such as location, contacts, device identifiers, etc., transfers data to third parties, provides for information and user's consent, etc.)
- The overall availability, presentation and practical implementation of a thorough privacy policy.

Therefore, it is an essential criterion for understanding the 'behaviour' of a tool with regard to privacy and data protection. Although one would expect that a PET developer would primarily be focused on addressing this particular dimension, this might not always be the case, e.g. due to lack of attention or design faults.

Following the aforementioned description, privacy policy implementation can be primarily assessed based on four main parameters, namely the *access that a tool gains to data stored in the user's device*, the *data transferred by the tool from the user's device*, any potential *profiling* that takes place in the course of the tool's operation, as well as the overall availability of a *documented privacy policy* for the tool. These parameters are further analysed in the next paragraphs.

3.2.1 Access to personal data stored on user's device

This parameter is the starting point for understanding and assessing the overall processing of personal data by a particular tool, especially in the case of mobile apps, following the principles of the GDPR and ePrivacy Directive[12]. To this end, it can be detailed to a number of assessment points, as described below.

Types of personal data being accessed
This can include any type of data possibly stored on the user's device, such as user profile information, user accounts, device identifiers, contacts, calendar, text and multimedia messages, call logs, photos, video and audio files, documents, browsing history, network information, location data, etc.

Frequency of access
It relates to the number of times each particular type of personal data is being accessed by the tool (e.g. several times per day, per week or per month).

[12] Specific guidance on the processing of personal data by apps on smart devices has been provided by the Article 29 Data Protection Working Party in Opinion 02/2013, see in [54].

Purpose of access
This point is of upmost importance to assess the reason why access to data is required (or not) in correlation with the types of data and frequency of access described above. All together they can serve the assessment of the fairness and necessity of the processing, purpose limitation, and data minimization (art. 5 GDPR). Possible purposes can include the tool's basic functionality (e.g. establishing contacts for a messaging app), provision of value added services (e.g. offering a location based service to registered users), or analytics.

User information
According to GDPR (art. 13), users should be clearly informed before any processing of their personal data takes place. It is, therefore, essential to assess whether indeed such information is provided by the tool and the way that this is done (e.g. if specific information is provided via pop-up windows/banners or whether the tool only relies on the general information provided in the privacy policy).

User consent and rights
According to GDPR (art. 6 & 7), users should provide their consent before any processing of their personal data takes place, unless another legal basis is applicable. Moreover, according to the ePrivacy Directive (art. 5(3)), access to data stored on a user's device can be performed only if the user has provided his/her consent. Consent should be freely given, specific and informed [17]. Thus, it is important to address whether users are indeed asked for consent before each specific access to personal data (permission), as well as whether the tool provides the same functionality in case that consent is not granted. Moreover, it should be checked whether users can withdraw their consent and if they can have their data blocked or deleted through the app (and how this can be done).

3.2.2 Transfer of personal data from user's device

This parameter is very much related to the previous one (access to personal data) and seeks to assess whether any transfers of personal data take place from the user's device and if they are appropriately justified (i.e. with regard to the user's privacy expectations for a certain type of PET). It is again essential to understand the processing of personal data conducted by the tool's developer/provider or other third parties, following the GDPR and ePrivacy Directive principles.

To this end, the first critical assessment point to consider who are the recipients of the data, i.e. the parties where the data are being transferred to (e.g. the tool's provider, OS developer, device manufacturer, third party service provider, etc.), the location of these parties (e.g. within EU or not), as well as their overall role in the processing of personal data. Attention should be given to the fact that in case of transfers to third countries or international organisations special conditions need to be met (charter V GDPR).

In addition to this, as in the case of access to personal data, it is essential to consider for each particular recipient of the data the following points: the types of data being transferred, the frequency of the transfer, the purpose of the transfer, as well as relevant user information, prior consent and user rights (see section 3.2.1).

3.2.3 Profiling

Profiling is defined in GDPR (art. 4(4)) as '*any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements*.' Especially in the case of mobile devices and apps, profiling can take place in a subtle way (e.g. though 'silent' access to and transfer of personal data to remote servers) and for different purposes (e.g. advertising or analytics), without the

users being able to protect themselves from it. It can be generally assessed through two main points, as shown below[13].

Storage of data on the user's device
Storing of data on the user device (e.g. cookies) is a usual way of relating the device to a unique identifier that can be later used for tracking and profiling. Therefore, it is important to assess if this indeed occurs, whether the user is informed about possible profiling and, most importantly, if the user is asked for prior consent (as stipulated in ePrivacy Directive art. 5(3)).

Third party libraries
In some cases the use of third party software is associated with hidden profiling practices (e.g. for advertising). It is, thus, interesting to consider whether such software has been used in the development of the tool and assess pertinent details.

3.2.4 Documented privacy policy

The purpose of this parameter is to assess the overall availability and presentation of a documented privacy policy that can provide adequate information to the users about any processing of personal data involved in the operation of the PET. It is an important aspect, relating also the principle of accountability that is enshrined in GDPR (art. 5). It can be detailed to two main assessment points as described in the following.

Availability and completeness
The privacy policy should be made easily available to users and it should cover all data processing operations performed by the tool. Taking into account the relevant GDPR provision (art. 13), for each processing operation, the following information can be provided: types of personal data and purpose of the processing, recipients of data, retention periods, security measures in place, accountability and quality controls measures in place, procedures for exercising the right of access and modification.

Change policy
Another interesting element to consider is whether users are informed in case of a change of the privacy policy (or in general the terms and conditions)[14], as well as if it is clearly indicated how the users' personal data are treated in case the tool/service is no longer provided. This information can be part of the privacy policy or other formal document provided by the developer/provider of the tool.

3.2.5 Summary and assessment methods

Following the analysis of the previous paragraphs, Table 4 presents an overview of the privacy policy implementation assessment criterion.

[13] Note that specific assessment points to address technical means of profiling (e.g. fingerprinting) are also further detailed in the specific criteria for different types of tools, e.g. anti-tracking tools.
[14] See for example recently announced change of Google policy, linking advertising data to users' accounts, https://www.engadget.com/2016/10/21/googles-redefined-privacy-policy-lets-ads-follow-you-everywhere/

PETS ASSESSMENT FRAMEWORK – GENERIC CRITERIA: PRIVACY POLICY IMPLEMENTATION	
PARAMETER	**ASSESSMENT POINTS**
ACCESS TO PERSONAL DATA STORED ON USER'S DEVICE	Types of personal data being accessed Frequency of access Purpose of access User information User consent and rights
TRANSFER OF PERSONAL DATA FROM USER'S DEVICE	Recipients of data Types of personal data being transferred Purpose of transfer User information User consent and rights
PROFILING	Storage of data on user's device Third party libraries
DOCUMENTED PRIVACY POLICY	Availability and completeness (of privacy policy) Change policy

Table 4: Analysis of privacy policy implementation criterion

The assessment methods applicable for the criterion of privacy policy implementation vary depending on the assessment parameter/point. Available documentation can be used (e.g. tool's privacy policy), as well as relevant inputs or opinions from user forums. However, this would not be enough to assess the access to and transfer of personal data stored on the user's device. In this case, hands-on use of the tool is definitely necessary in order to understand certain features (e.g. information and consent), whereas in many cases traffic and code analysis would also be required (e.g. verifying access to data and permissions or transfer of data to remote servers).

3.3 Usability

Usability has been defined as '*the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use*' [18]. This definition can be expanded to cover also flexibility, error tolerance/recovery, ease of learning, user support, as well as user feedback [19] [20] [21] [22] [23]. For the scope of this study, usability is considered as a key factor that can facilitate the use of a PET (e.g. through an easy installation process or comfortable user interface), thus boosting its overall adoption by the general public.

In order to address usability in a broad way, we can consider this criterion under three different levels (parameters) relating to the overall use of a tool: a) *installation process*, b) *uninstallation process*, c) *use and configuration* of the tool. The following sections describe each of the parameters in more detail.

3.3.1 Installation process

Installation of a software tool can be defined as the process of making the tool ready to run for execution. Usability during installation process is an important factor with regard to the final use of the tool. It can be assessed using a number of specific points/indicators, as described below.

Available documentation
Documented guidance can offer help to users upon installation. Therefore, it is interesting to assess if such guidance is provided and in what form (e.g. technical manual, user tutorial, frequently asked questions, etc.). Moreover, the trustworthiness of this documentation is also important to consider (as this may vary between different sources and types of available information, e.g. from PET developers/providers, independent users, user communities, etc.).

Level of difficulty
Although one can argue that this point is rather subjective, there are still a number of indicators that can be used to assess the difficulty of the installation process, as for example whether an installer automatically completes the whole process (e.g. by simply clicking a button), if certain actions/tasks are required by the user or if the user needs to consult the tool's documentation to complete the process.

Minimum requirements
Another important aspect to consider in this respect is whether the tool's installation requires any minimum technical requirements (e.g. certain environment, OS, settings, etc.) and/or whether the installation of additional software is needed for the tool to offer its functionality. It is also interesting to assess whether this information is clearly indicated to the user before the beginning of the installation process.

Personal data upon installation
In some cases it might be required during the installation process of a tool that the user provides certain personal data (e.g. password, email address/account, phone number), for example for registration purposes. In those cases it is interesting to assess the purpose that these data are needed for, as well as whether the tool offers the same functionality if the user refuses to provide the data. Sometimes relevant information can be found in liability agreements and privacy statements (e.g. on a tool's website) which are, though, usually very lengthy and complicated for users to read.

Changes upon installation
Some tools might automatically perform certain changes to the user's device or installed applications upon installation (e.g. changes in selected search engine or homepage for browser add-ons). It is, thus, useful to consider whether the user is informed about these changes, whether he/she is asked to consent, as well as whether the changes can be undone by the user.

3.3.2 Uninstallation process

Uninstallation of a software tool can be defined as the process of removing the tool (or part of it) from the user's device. It is, thus, the opposite of installation and it can be accordingly detailed to assessment points similar to those mentioned in section 3.3.1, in particular with regard to available documentation and level of difficulty.

Moreover, another aspect to consider under this parameter is that certain application data might be maintained in the user's device even after the uninstallation process has been completed. It is, thus, important to assess if the user is informed about these types of data and whether he/she can locate them in the device and permanently delete them. Similarly, it is important to consider relevant server-side deletion of data once the user has requested the termination of a certain tool or service[15].

[15] Deletion of personal data (both local and remote) is explicitly considered under the specific criteria for secure messaging applications, VPNs, anonymizing networks and anti-tracking tools.

3.3.3 Use and configuration

This parameter is directly related to the use of the tool and its possible configuration options. It is the most critical dimension with regard to creating a balance between usability and privacy protection. Its assessment can be addressed through a number of specific points/indicators, as follows.

Available documentation
As in the case of installation/uninstallation, documentation can offer support to the users, especially if provided in a clear and understandable way. Options such as live demos and frequently asked questions can be very helpful in this respect.

Level of difficulty
This point is obviously a subjective matter and is very much related to the user's familiarity and expertise with certain types of tools. For its assessment it is, thus, preferable to refer to the required level of user expertise, rather than to the easiness/difficulty of the tool per se. The assessment should cover both the user interface of the tool, as well as the configuration and customisation options.

Privacy by default settings
This point mainly seeks to assess whether the tool (after installation) is set to the highest level of privacy protection (with regard to its particular functionality). Although, in the context of this study, privacy by default is addressed in more detail under the specific criteria for different types of tools, under this generic criterion we aim to obtain an overall understanding of the PET's provider approach towards this matter. Besides being an obligation under GDPR (art. 25), it is an important point also from a usability point of view, as privacy by default settings automatically protect the user and save him/her from the need to take additional actions (e.g. opting out from certain features, changing settings, etc.).

User support
This point refers to the availability of a support service, which can offer additional advice, guidance or feedback to the user with regard to the tool's functionality. Such service can be provided in the form of forum, email list or other means.

3.3.4 Summary and assessment methods

Following the previous paragraphs, Table 5 presents an overview of the usability criterion.

PETS ASSESSMENT FRAMEWORK – GENERIC CRITERIA: USABILITY	
PARAMETER	**ASSESSMENT POINTS**
INSTALLATION PROCESS	Available documentation Level of difficulty Minimum requirements Personal data upon installation Changes upon installation
UNINSTALLATION PROCESS	Available documentation Level of difficulty Data after uninstallation
USE AND CONFIGURATION	Available documentation Level of difficulty Privacy by default settings User support

Table 5: Analysis of usability criterion

The assessment of this criterion can be mainly based on the available public information from the tool's web site (e.g. manuals, user guides, FAQs, or Wikis) or other sources (e.g. user forums or reviews of the tool). Moreover, hands-on use of the tool can provide input, especially with regard to the possible configuration and customization options, as well as the overall user experience. Technical analysis (e.g. in terms of source code review) is not especially applicable for this criterion. However, usability test labs can be very useful in the area of PETs, providing interesting (comparative) results.

4. Specific assessment criteria

In the context of the 'PETs control matrix' the specific criteria aim at assessing particular characteristics of distinct categories/types of PETs, exploring in a detailed manner their technical features and their privacy enhancing functionality. As such, they are mainly of technical nature, although in some cases aspects related to GDPR/ePrivacy requirements are also addressed in a more analytic way, e.g. with regard to data protection by design and default or secure data erasure (see also section 2.2). In particular, the following categories of PETs are considered:

- Secure messaging.
- VPNs.
- Anonymizing networks.
- Anti-tracking tools (for online browsing).

The selection of the aforementioned PETs categories was based on the popularity of the particular tools, as well as the increasing availability and use of relevant apps in mobile devices. Still, it is important to note that there are many other categories of privacy tools that can be considered, as for example in the areas of privacy-enhanced location-based services and access rights control management in mobile applications. Starting from the current analysis, the PETs assessment framework could be expanded in the future to cover also these types of applications and relevant solutions.

The next sections present in detail the assessment criteria for each PET category, breaking them down into specific parameters and assessment points.

4.1 Secure messaging

Secure instant messaging applications (secure messaging apps) focus on providing secure transmission of instant messages —i.e. messages transmitted in real time over the internet— among two or more communicating parties. They are usually designed to enhance communications' privacy in a way that no unauthorized third party can access the content of communications (such as text, voice, images, files, video, etc.).

Secure messaging apps fall under the area of PETs as they go beyond the mere provision of communication by making privacy and security a core aspect of their functionality. Moreover, taking into account their large and growing user base, it is a most interesting area for privacy enhancing characteristics to assess. Indeed, although in the past it was mainly sensitive user groups that would engage in the use of secure messaging (e.g. activists, journalists, and whistleblowers), today more and more users and organizations are moving to secure messaging for their everyday communications[16].

In order to protect user's communications, secure messaging apps most commonly rely on the use of strong cryptographic protocols and algorithms to support *end-to-end encryption*. End-to-end encryption ensures that only the communicating users can have access to the content of communication. On top of this, *client-server encryption* can secure transport of data between the users' device and any remote servers (e.g. the

[16] It is interesting to note that the interest of the general public in secure messaging apps has considerably grown after the 2013 revelations of Edward Snowden regarding the NSA surveillance program, see also: http://www.scmp.com/lifestyle/article/1980679/growth-demand-encrypted-apps-no-cause-alarm-say-tech-experts

messaging service provider's server) that may be involved in the communication. Secure (encrypted) *storage of communication data* is another usual feature of these tools. *Authentication* protocols are also utilized to support authenticity of communicating users and communication data. The feature of *anonymous communication*, i.e. the possibility that no party involved in the communication can be identified, may also be offered, although in practice this area still needs to be explored[17]. Figure 4 illustrates a common use case scenario for secure messaging applications, where the different risks and relevant security controls are indicated.

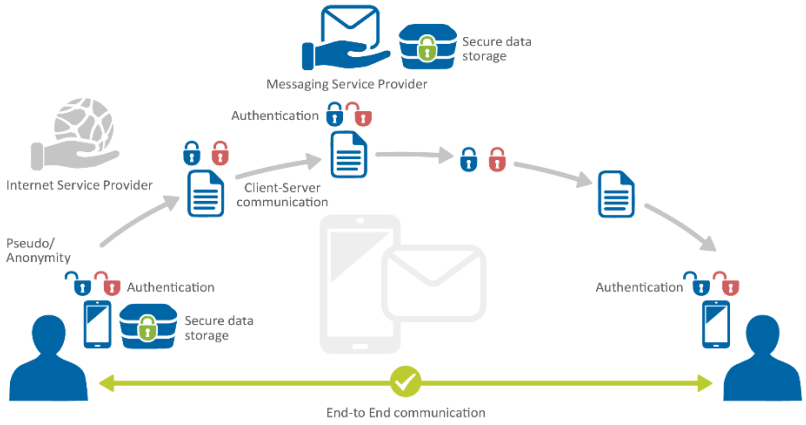

Figure 2: Use case scenario for secure messaging apps

There is a wide variety of secure messaging apps available in the market today for different operating systems and platforms, especially in the mobile sector. Some examples of popular mobile apps include Whatsapp[18], Telegram[19], Signal[20], Chatsecure[21], Threema[22] and Wickr[23]. All of them aim at providing the same core functionality, i.e. secure (encrypted) communication, although the implementation may vary.

Due to the popularity of messaging apps, evaluation metrics have been already developed at different levels and detail, with the EFF Secure Messaging Scorecard [3] being one of the most known ones. In the context of the 'PETs control matrix', the assessment of secure messaging apps is based on five broad criteria, each relating to a specific technical feature of these tools, namely:

- End-to-end encryption.
- Client-server encryption.
- Security of stored data.
- Authentication.
- Anonymous communication.

In the next paragraphs we explain in detail each criterion and its related parameters and assessment points.

[17] Aspects related to Off-The-Record (OTR) messaging and deniability of communication can also be considered to this respect, see also: https://otr.cypherpunks.ca/. For a more detailed description of the functionalities offered by secure messaging apps, see [55].
[18] https://www.microsoft.com/en-gb/store/apps/whatsapp/9wzdncrdfwbs
[19] https://itunes.apple.com/app/telegram-messenger/id686449807
[20] https://play.google.com/store/apps/details?id=org.thoughtcrime.securesms&hl=en
[21] https://itunes.apple.com/us/app/chatsecure/id464200063
[22] https://play.google.com/store/apps/details?id=ch.threema.app&hl=en
[23] https://play.google.com/store/apps/details?id=com.mywickr.wickr2&hl=en

4.1.1 End-to-end encryption

End-to-end encryption can be simply defined as 'a system of communication where the only people who can read the messages are the people communicating'[24]. This means that no eavesdropper or any other party, including the messaging service provider, can access the cryptographic keys needed to decrypt the communication and, thus, gain access to its content. The implementation of end-to-end encryption is clearly a fundamental feature for secure messaging apps, as it is at the core of private communications. It can be practically analysed through a set of specific parameters and assessment points, as shown below.

Cryptographic algorithms and key lengths
The correct implementation of cryptographic algorithms and the use of sufficient key length are critical parameters to ensure strong encryption. To this end, it is essential that standard and up-to-date cryptographic protocols are used (and not custom solutions), following relevant recommendations of national (e.g. BSI in Germany, ANSI in France, NIST in USA) or international organizations (e.g. IETF, ISO) in the field[25]. On top of this, it is interesting to examine whether the tool gives the user the flexibility of choosing between different encryption algorithms and key lengths (although such a feature would probably be useful only for advanced users).

Default configuration
This parameter aims to address the default settings (i.e. after installation) of a secure messaging app with regard to end-to-end encryption. The following points should be essentially considered:

- End-to-end encryption by default: Having end-to-end encryption enabled by default is an important feature for a secure messaging app, especially for non-expert users who may not know how to activate it. It follows the concept of data protection by default, supporting both privacy protection and usability.

- User notification: If end-to-end encryption is not activated by default, it is useful that users are notified and given appropriate advice on how to activate it. This follows the principle of data protection by default enshrined in the GDPR (art. 25). Notification to users is also important in case that end-to-end encryption has not been established or has failed (e.g. some applications might inform the user when end-to-end encryption mode is activated but do not do so when it is not).

Perfect forward secrecy
Forward secrecy is a property of secure communications where the compromise of a key does not consecutively lead to the compromise of past encrypted communication sessions [24]. It is an important feature supporting privacy in end-to-end encrypted communications..

Key generation and storage
This critical parameter assesses where and how the encryption keys are generated and stored and which parties can access them. To ensure the communication privacy during end-to-end encryption, keys should be generated and stored only at users' devices. Having said that, it is important to note the limitations of key generation in smart devices due to the lack of computational power, which often makes randomness hard to achieve. This can result to weak implementations that, if not appropriately considered, can compromise the security of the whole encryption scheme. Alternatively, if keys are stored at the provider's servers, they should be encrypted with a private key that only the user is in possession of, or with

[24] https://www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption/
[25] See also ENISA's relevant report on algorithms, key sizes and algorithms in [39].

information that only the user knows (e.g. derived from a user's password) using standard encryption algorithms[26].

Encrypted data types

Secure messaging applications generally support many types of communication content, such as text, voice, images, audio, etc. between two or more communicating parties. It is, thus, important to assess which data types are protected by end-to-end encryption. Moreover, it is interesting to assess whether certain types of metadata (e.g. telephone number or device identifiers) are also end-to-end encrypted. In any case, users should be clearly informed about the types of data that are *not* encrypted.

Encrypted group chats

Group chat is a form of communication which extends beyond the commonly known one-to-one communication, involving multiple users' grouping and exchanging messages. In cases where group chats are supported, it is important to assess whether the communication is also end-to-end encrypted (for different types of data) and if the level of protection is the same as in one-to-one communication.

4.1.2 Client-server encryption

Client-server encryption refers to the encrypted communication channel established between a client and a server. In the context of secure messaging the client-server model is applicable in any case where communication between the user's device (client) and the communication service provider (server) takes place. The user's device might also need to connect to other types of remote servers (e.g. for back-up), depending on the underlying use case scenario. In client-server encryption the service provider at the server side can potentially access and read the users' communication data (in contrast with end-to-end encryption).

In order to assess the implementation of client-server encryption in different tools, a number of specific parameters and assessment points need to be considered, as shown below.

Connection to remote servers

As already mentioned, depending on the use case scenario, the user's device might need to connect to one or more remote servers. The following points should be considered in more detail:

- Server owners/providers: This might refer to servers of the messaging service provider or other third party service providers (e.g. cloud service providers).
- Location: The location of the servers where personal data processing takes place is important with regard to the underlying data protection legal framework. A distinction between servers in EU and third countries can primarily be made, taking into account the special conditions set in GDPR in the latter case (GDPR charter V).
- Purpose: The purpose of the connection may vary, including for example the need to perform basic operations related to the tool's core functionality or to support back-up options. In any case, following GDPR principles (art. 5), the purpose needs to be clear and justified in the context of the overall scope of the messaging app/service[27].

[26] For example iOS uses AES-256 encryption for protecting users' keys with 'keychain', and Android keeps them within encrypted storage in the internal 'app data directory'.

[27] It is interesting to note the recent example of known smartphone brand that has been questioned for sending their users' personal data to remote servers for no justified reason http://timesofindia.indiatimes.com/tech/tech-news/Xiaomi-phones-send-user-data-to-remote-servers-F-Secure/articleshow/39950622.cms

Encrypted communication
For each remote server connection, client-server communication needs to be encrypted. In this respect it is essential to consider, as in the case of end-to-end encryption, if standard and up-to-data cryptographic protocols are used (e.g. Transport Layer Security -TLS [25] protocol), together with sufficient key length. In addition it is important to consider whether the user is notified in cases where client-server encryption has not be established or has failed.

4.1.3 Security of stored data

The secure storage of communication data is another important feature of secure messaging apps. Stored data may include both the content of communications (e.g. text messages, voice or video calls, file attachments, etc.), as well as the communications metadata (e.g. telephone number, location, device identifier, etc.). Data can be stored either on the user's device (local storage) or on remote servers. Obviously in the first case the user can have more control over his/her personal data. In both cases specific controls need to be in place to ensure security of the data, as well as the relevant data protection requirements set by GDPR.

In order to address the implementation of this feature in different tools, in the 'PETs control matrix' a primary distinction has been made between *storage on user's device* and *remote storage*. The specific assessment points for each case are described in the following sections.

4.1.3.1 Data storage on user's device

When communication data are stored on the user's device, the user can be the one in control of these data. This, however, depends a lot on the implementation of this feature and particularly on the parties that are authorized to access data on the device and the security measures in place. Some essential aspects to consider in this respect are shown below.

Types of communication data stored
This parameter refers to communications' content or metadata or both. Particular attention should be paid on backups (of content or metadata) that may be performed on the user's device, especially by explicitly informing the user on the type and location of the backups.

User choice
Following the definition of the types of data, it is also interesting to assess whether the user is provided with the possibility not to have his/her data stored and/or backed up on the device, as well as whether he/she can access all stored data and how.

Retention period
In this respect, it is also important for the user to know the exact retention period of the data on the device, as well as whether he/she can have the data permanently erased (and how).

Encryption of stored data
In some cases encryption is offered as a feature to secure stored communication data on the user's device. This is obviously a valuable feature, as long as standard and state-of-art encryption algorithms and sufficient key lengths are used and only the user has access to the encryption keys. An interesting point to assess in such case is whether the communication data can be retrieved if the encryption key is lost.

4.1.3.2 Data storage on remote servers

When data are stored on remote servers, the user has less control over the processing of these data. It is, thus, essential to address how the processing of data is performed in such cases, as well as the users' options on managing their data. The following points can be addressed in more detail.

Servers, location and purpose of processing
The first aspect to consider is which servers are used for the storage of data. These can typically include the server of the messaging service provider or that of a third party service provider (e.g. cloud service provider). The physical location of the servers is also important to consider (e.g. whether it is within EU or in a third country), taking into account the relevant GDPR provisions (charter V). For each case of storage on remote server, it is essential to assess the purpose of the processing, e.g. whether storage is necessary for the provision of the core service or it is performed for back-up or other purposes (such as analytics). This point can be correlated with the one on connection to remote servers under the criterion of client-server encryption (see 4.1.2.2).

Types of communication data stored
As in the case of data stored on user's device, it is important to assess the types of personal data stored in each remote server (content, metadata), paying particular attention to back-ups which in some cases might be stored without the users being aware of them.

User information and choice
Information and choice is of particular importance in the case of remote storage, when the users has less control over his/her data. In this respect, it is interesting to assess whether the user is informed about the remote storage (in all cases) and whether he/she has choice not to have his/her data stored on any remote server. Moreover, it is important to consider whether the user can access all of his/her data stored on all remote servers and which procedure he/she should follow in each particular case.

Retention period
In this respect, it is also important for the user to know the exact retention period of the data on each remote server, as well as whether he/she can have the data permanently erased from all servers and what procedure he/she should follow for this. An important point is also to check when the data are actually deleted from the servers following a user's request (e.g. if this is done immediately or after a certain period of time).

Encryption of stored data
Encryption of remotely stored data (e.g. at the messaging service provider's side) does not offer full control to the user regarding access to these data (as the provider usually holds the encryption key) but still is an important measure to protect against unauthorized external access. Again, it is essential that standard and up-to-date cryptographic protocols and sufficient key lengths are used, and that the user is adequately informed on what is encrypted (and what is not), as well as whether his/her data can be retrieved in case that the encryption key is lost. An additional point to assess is data integrity controls upon retrieval from the remote servers.

4.1.4 Authentication

Authentication can be generally defined as '*verification of the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system*'[28]. Without proper authentication mechanisms, it is possible that the user's identity is impersonated, allowing an attacker to pretend that he/she is the rightful user. For the operation of a secure messaging app, there are different levels of authentication required, i.e. authentication in the context of end-to-end and client-server communication. An additional aspect is message authentication, which relates to the authenticity of the communication data. To this end, the particular parameters and assessment points for authentication as shown below.

User authentication

Most secure messaging apps would support some type of user authentication mechanism performed via the encrypted end-to-end communication channel. It is interesting in this respect to assess:

- Cryptographic protocol used: As mentioned earlier for encryption, authentication should follow standard and state-of-the-art protocols, following recommendations of national or international organizations in the field.

- In-band and out-band authentication: In-band authentication takes place automatically during the initialization of a communication session. In case that such option is not offered, out-band authentication could be available, i.e. authentication that takes place in a non-automated way, e.g. by 'manually' exchanging information via a separate communication channel. It is in general interesting to consider whether the tool offers a 'manual' identity verification technique, such as encryption key fingerprints[29] or QR code scanning[30].

Client-server authentication

Client-server authentication is commonly performed through the encrypted communication channel with the use of public key cryptography (e.g. RSA, DH-RSA, ECDH-RSA, etc.). As in the case of user authentication, the protocols used should be standard and up-to-date, following relevant recommendations of national/international security organizations. Moreover the next parameters should also be more explicitly considered:

- Public key pinning: Public key pinning (also known as certificate pinning) is a security mechanism that allows a server to resist impersonation by attackers using fraudulent certificates [26]. It is, thus, an essential aspect to assess under client-server authentication, as a means to prevent such types of attacks (e.g. man-in-the-middle attacks).Still, it should be mentioned that in practice there are many weak or wrong implementations of public key pinning which can even lead to bypassing the trust chain between the user and the Certificate Authority (e.g. if certificate revocation lists are not validated)[31].

- Self-signed certificates: A self-signed certificate is an identity certificate signed by the same entity whose identity it certifies. Self-signed certificates obviously do not provide the same level of trust as certificates

[28] See definition in http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=913810.
[29] https://help.gnome.org/users/seahorse/stable/misc-key-fingerprint.html.en
[30] http://www.webopedia.com/TERM/Q/QR_Code.html
[31] For more information, see OWASP guide on certificate and public key pinning, https://www.owasp.org/index.php/Certificate_and_Public_Key_Pinning#Examples_of_Pinning

signed by a Certification Authority (CA)[32] and vulnerabilities related to self-signed certificates have over the last years given rise to a number of Trojan attacks[33].

Message authentication

Message authentication is important to ensure authenticity of messages both in end-to-end and client-server communication. Authenticated Data Encryption (AE) can be provided by combining an encryption scheme and a Message Authentication Code (MAC) [27] [28]. It is interesting to assess if such possibility is indeed offered in a secure messaging app and what authentication protocol is used.

4.1.5 Anonymous communication

Anonymous end-to-end communication can be defined as a communication where no third party, including the messaging service provider, can identify the communicating parties. In that sense, anonymity implies also unlinkability and unobservability[34]. It is clearly a powerful feature for privacy protection, which, however, is not currently an integral part of most secure messaging apps. The main parameters and assessment points to consider under this criterion are described below.

Anonymity protection

The first (and most important) aspect of assessment in this area is whether communication is truly anonymous, following the aforementioned definition. Therefore, it is important to consider the particular measures that are in place to ensure anonymous communication, e.g. protection against traffic analysis or fingerprinting. Moreover, as metadata can reveal a lot of information about a user's identity and service providers do not always consider them as personal data, it is essential to check if any remote server involved in the communication does process metadata and which specific types of metadata are being processed.

Other measures

In case that the communication is not anonymous, it is also useful to consider whether there are other measures in place to protect the identity of the users, such as for example the use of pseudonyms that can disguise the user's real identity. Moreover, it is interesting to address whether the protection offered by the tool can be enhanced with the combined use of other tools/PETs.

4.1.6 Summary and assessment methods

Following the previous analysis, Table 6 summarizes the assessment criteria, parameters and assessment points for secure messaging apps.

[32] See for example in https://www.globalsign.com/en/ssl-information-center/dangers-self-signed-certificates/
[33] See e.g. http://www.scmagazine.com/trojan-uses-fake-adobe-certificate-to-evade-detection/article/299085/ and https://threatpost.com/small-number-of-malicious-tor-exit-relays-snooping-on-traffic/103771/
[34] http://freehaven.net/anonbib/cache/terminology.pdf

PETS ASSESSMENT FRAMEWORK – SECURE MESSAGING APPS: SPECIFIC CRITERIA		
CRITERION	**PARAMETERS**	**ASSESSMENT POINTS**
End-to-end encryption	Cryptographic algorithms and key lengths	Use of standard/up-to-date crypto protocols User choice
	Default configuration	End-to-end encryption by default User notification
	Forward/backward secrecy	Properties of forward and backward secrecy
	Key generation and storage	Key location Parties accessing the keys Encryption of keys
	Encrypted data types	Types of data encrypted User information
	Encrypted group chats	Group messages encryption User information
Client-server encryption	Connection to remote servers	Server owners/providers Location (of servers) Purpose (of connection)
	Encrypted communication	Use of standard/up-to-date crypto protocols User notification
Security of stored data	Data storage on the user's device	Types of communication data stored User choice Retention period Encryption of stored data
	Data storage on remote servers	Servers, location and purpose of processing Types of communication data stored User information and choice Retention period Encryption of stored data
Authentication	User authentication	Cryptographic protocol used In-band and out-band authentication
	Client server authentication	Cryptographic protocol used Public key pinning Self-signed certificates
	Message authentication	Cryptographic protocol used User information
Anonymous communication	Anonymity protection	Specific measures in place (to protect anonymity) Protection of metadata
	Other measures	Use of pseudonyms Combined use of other PETs

Table 6: Analysis of assessment criteria for secure messaging applications

For both user-to-user and client-server modes of encryption, as well as for authentication, the use of available public documentation can be very helpful in assessing relevant features (e.g. type of cryptographic protocols and key lengths, key distribution, etc.). Examples of such documentation are available whitepapers from tools' developers [29] [30] [31] [32] [33], as well as relevant technical papers [34]. Hands-on use of the tools can also be useful in some cases, for example to assess default settings and types of communication data encrypted or the use of self-signed certificates (e.g. by creating self-signed certificates and testing if the application accepts them or not). However, for establishing a clear understanding of the implementation aspects of encryption and authentication (e.g. aspects like forward and backward secrecy, key storage or public key pinning), an elaborated assessment needs to be performed, e.g. through source code and traffic analysis. Still, even technical analysis might not be possible in practice for certain cases (e.g. assessing the server side in client-server communication).

Regarding the storage of communication data, locally stored data (on the device) can be assessed through hands-on use and analysis, whereas storage on remote servers is more difficult to address. Indeed, although source code and traffic analysis could provide insight, in many cases more information from the remote server's side would be needed to complete the assessment.

With respect to anonymous communication, traffic analysis can be applied to a certain extent, e.g. to verify if any metadata are being processed by remote servers. Assessing the possible use of pseudonyms is relatively easy by hands-on use of the tool. Publicly available documentation can support the assessment of this parameter, e.g. with regard to measures applied for anonymity protection or the possible combined use with other tools.

4.2 Virtual Private Networks

A Virtual Private Network (VPN) can be defined as a network technology that creates a secure (encrypted) network connection over a public network (e.g. internet) or a private network of a service provider[35]. VPNs are widely used by many companies and organisations to enable remote users (e.g. employees) to connect to their private network.

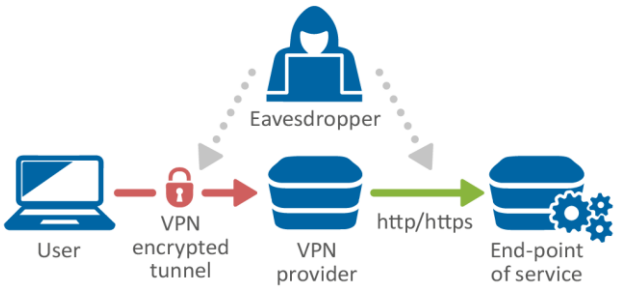

Figure 3: VPN service use case scenario

For the purpose of this study we have concentrated on the consumer (personal) VPN networks/services, which enable a user to direct all communication traffic via the secure (encrypted) tunnel with the VPN service provider before exiting to the internet (so in fact offering an encrypted proxy). By doing so, the VPN can hide the user's real IP address, as the observers standing outside the tunnel can only see the IP address of the VPN service provider. In this way, the user's online activity (e.g. websites visited) is protected from disclosure

[35] See relevant definition in http://whatismyipaddress.com/vpn

to third parties. It should be stressed though that the VPN provider can still be in position of identifying both the user and his/her online activity.

VPNs are a very broadly used technology currently[36] and can clearly be deemed as a privacy enhancing one. There are distinct services offered by a great number of VPN providers to support different user needs[37]. In all cases trust in the VPN provider is core for the protection offered by a VPN and in that sense the VPN's business model is also central (e.g. subscription-based versus free services). To this end, there are different evaluation metrics[38] and comparisons of VPN services[39] available online.

In the context of the 'PETs control matrix' we build the assessment of VPNs around their two principal functional characteristics, i.e. identity (IP address) protection, and encryption. On top of this, one additional dimension is considered: VPNs do have limitations and in some cases side effects, which might affect the users' online experience[40]. Users should, thus, be appropriately informed before selecting a particular VPN service. To this end, the criteria for VPNs assessment in the 'PETs control matrix' are as follows:

- Identity protection.
- Encryption.
- Side effects.

In the next paragraphs each criterion and its relevant parameters and assessment points are explained in detail.

4.2.1 Identity protection

As already mentioned, identity protection is one of the core privacy enhancing features of VPNs, in the sense that they can hide the user's real IP, thus also hiding his/her online activity from third parties. This can be very important for users that wish to avoid IP based tracking, as well as those who want to bypass IP based internet censorship. Still, it is important that users get the right information about the service offered, as well as that they are clearly aware that the use of a VPN service does not provide anonymity (since the VPN service provider is usually in the position of identifying the users of its service). For the analysis of the protection offered by a VPN service, a number of parameters and assessment points can be considered, as shown below.

General information
This includes the basic information provided to the user by the VPN service provider, which should clarify as a minimum the following important points:

- Service offered: The VPN service might be applied to different use cases and needs, e.g. ensuring confidentiality of communications when using untrusted networks, bypassing IP-based censoring or protection against internet surveillance. Adequate information should, thus, be provided to the user, not only for the supported use case scenarios, but also for the advantages and attributes that a particular VPN service offers.

[36] For more information, see: https://www.cactusvpn.com/vpn/vpn-services-popularity/
[37] For example, see http://bestvpn.com for a list of different VPNs providers.
[38] See for example: https://torrentfreak.com/anonymous-vpn-service-provider-review-2015-150228/
[39] For example, see http://bestvpn.com for a list and comparison of different VPNs providers.
[40] http://security.stackexchange.com/questions/11382/what-are-the-pros-and-cons-of-a-vpn-for-privacy

- Provider/infrastructure jurisdiction: Depending on the jurisdiction of the VPN provider, as well as the location of the VPNs servers, different data protection legal frameworks might be applicable (e.g. EU law or third country law). This might be an important issue, e.g. with regard to warrants issued to the VPN provider or specific laws on data retention in a particular country. To this end, another important element is whether the VPN servers are hosted by the VPN service provider or a third party provider. Also, whether the user can select the country where the VPN server used for the tunneling of communication is located.

- Financial model and anonymous payments: Another critical element, which is often related to the VPN's business model, is the way the VPN service is financed (e.g. subscription fees, advertisements or donations) and whether in particular its financing is based on the processing of users' personal data (e.g. selling of profiling data for advertising purposes). Moreover, it is interesting to assess whether anonymous payment systems are supported and in what form (e.g. cryptocurrency[41] or store gift cards[42]).

IP address management

Management of allocated IP addresses is a core aspect of the VPN service with regard to identity protection. In particular, the first (and most crucial) aspect is IP address sharing, as the more users share the same IP, the more difficult it becomes to associate a user with a particular IP. Therefore, it is essential to assess the amount of users that share the same IP address (e.g. within an hourly timeslot on daily basis), whether there are minimum/maximum thresholds for IP address sharing, as well as whether all the devices of one user (single account) share the same IP address. Moreover, it is important to consider if the allocated IP addresses change automatically, whether the user can request a change of IP address on demand or prevent the change of his/her IP address, as well as whether IP changes result to new allocated IP address in the same country (e.g. based on pre-defined user preferences).

Protection against abuse of service

In order for this parameter to be efficient, it is first necessary to define what actions could be considered as 'abuse' of a VPN service (e.g. incoming/outgoing cyberattacks, illegal context, torrent/file sharing, etc.). Based on this, the VPN service provider should be able to explain the measures that are taken to prevent possible abuse, considering in particular the following key controls:

- VPN firewall: The firewall is a fundamental network security measure that monitors and controls incoming and outgoing network traffic based on predetermined security rules (filters) [35]. Firewalls are basic security controls for VPNs and, depending on the network topology, can be placed in front or behind the VPN server[43].

[41] A type of a digital currency that uses cryptography to secure the transactions and to control the creation of additional units of the currency without linking the user to the currency. Bitcoin is the most commonly used cryptocurrency today, see https://bitcoin.org/en/

[42] A user can purchase gift cards at a store with cash and then digitally transfer the balance of the gift card to a designated service provider (e.g., VPN provider). In exchange the user will be provided the requested service at a fixed exchange rate (e.g., gift card value to VPN service value).

[43] https://technet.microsoft.com/en-us/library/cc958037.aspx

- Built-in DNS leakage protection: This feature, which can be available at the VPN client, can protect against disclosure of the user's real IP address due to a DNS leak. A DNS leak may occur if an IP request is not sent through the VPN tunnel but through another server (e.g. the Internet Service Provider).[44].

- VPN kill switch: This is a mechanism to monitor the internet connection, shut it down when a VPN failure is detected and, in such case, automatically attempt to reconnect to the VPN[45]. Again it prevents from possible leakage of the user's IP address in case of a VPN dropout.

- Protection against fingerprinting: A fingerprint is a set of information elements that identifies a device or application [36] and can be used for user identification in a completely subtle way [37] [38]. It is important to assess if the VPN service offers any protection against this technique[46], as well as whether any advice is provided to the users.

- Traffic analysis: Traffic analysis can be defined as the process of intercepting and analyzing messages in order to infer information from patterns in the communication[47]. It can be performed even when the communication is encrypted and can be a very powerful technique for identifying the communicating parties and/or the content of the communication. It is, thus, interesting to consider the measures that the VPN provider has in place to prevent traffic analysis, as well as relevant advice provided to the users.

Log files

The maintenance of log files by the VPN provider can allow matching an IP address or other identifier to a user of the service. It is, thus, important to assess what type of information is included in the logs and which parties have access to them. Another important issue is the retention period of logs, which can vary from a few days to more than a year (and can be very critical, e.g. in case of a court order where the VPN provider is asked to provide all logs for a certain period of time). It should be noted in this respect that in different countries specific legislation for retention of logs might exist (which is why the jurisdiction of the VPN provider and location of VPN servers also play an important role – see relevant point under the criterion on General information above). Moreover, it is also interesting to consider whether the user has the option not to have the logs maintained, as well as whether he/she can request the permanent deletion of the logs from all servers and locations (before the end of the 'normal' retention period).

Limitations

The VPN service might have certain limitations that affect the users' privacy and are already known to the VPN provider. These include any type of known attack or vulnerability that could result in limiting the functionality of the service. In such cases, it is important to assess the available documentation and the information provided to users. Moreover, it is interesting to consider whether the VPN provider proposes any ways for overcoming these limitations, e.g. through the combined use of other services or tools[48].

[44] Such a leak may occur for example due to predefined default settings (in IPv4) or in cases of IPv6 requests. See also in [56] and [57] for more information.
[45] http://www.torrentvpn.org/en/what-is-a-vpn-killswitch/
[46] See for example in [58].
[47] For more information, see: http://www.sans.edu/research/security-laboratory/article/traffic-analysis
[48] For example, it is possible to combine the use of a VPN service with an anonymizing network, such as Tor, see: https://www.bestvpn.com/blog/42672/using-vpn-tor-together/

4.2.2 Encryption

Encryption is a fundamental feature of a VPN service and the reason why many users rely on VPNs. It should be noted that VPNs can only encrypt the communication between the user's device (client) and the VPN server. The security of communication between the VPN server and the destination (e.g. the website a user is trying to reach) is very much dependent on the possibility of the destination's server to support encrypted communication (e.g. HTTPS). In order to assess this criterion, a number of parameters and assessment points can be considered, as shown below.

Cryptographic algorithms and key lengths

Different VPN protocols can be applied, following different authentication and encryption techniques (e.g. OpenVPN, L2TP/IPsec, PPTP, etc.[49]). As mentioned earlier, it is essential to use standard and up-to-date protocols, following relevant recommendations of national or international organizations in the field [39]. On top of this, an interesting point is to examine whether the VPN service gives the user the flexibility of choosing between different VPN protocols (although this feature would probably be useful only for advanced users). Moreover, it is important to consider whether the user is informed in case that the VPN protocol has failed and, thus, encryption has not been properly established.

Keys generation and storage

The generation and further storage of the encryption keys is critical with regard to the security of the communication channel established between the user and the VPN provider. In particular, it is important to assess the location of the keys (e.g. VPN client, VPN service provider, other service provider), as well as which parties may have access to them.

4.2.3 Side effects

VPNs can have certain side effects with regard to the user's online experience, which should be clearly explained to the users. This is of course greatly related to the VPN service provider and the quality of the service offered[50]. Two main parameters should be considered in this respect, as follows.

Known side effects on users' online activity

There are different cases where users' online activity might be affected by the use of VPNs. For example, restrictive network firewall policies might block the use of certain VPNs or the used VPN protocol/technology might limit connection to certain services or protocols. It is, thus, important to assess if the VPN provider offers relevant information to the users, as well as whether any blocking circumvention mechanisms are provided.

Known performance issues

Low network traffic and performance are often associated with the use of VPNs[51]. It is, thus, again interesting to consider whether the VPN provider is aware of these problems and if relevant information is provided to the users.

[49] See for example a comparison of different VPN protocols in https://www.bestvpn.com/blog/4147/pptp-vs-l2tp-vs-openvpn-vs-sstp-vs-ikev2/

[50] See for example: http://www.idownloadblog.com/2016/01/29/avoid-free-vpn/

[51] For more information, see: https://hide.me/en/blog/2016/02/how-to-improve-vpn-speed-and-performance/

4.2.4 Summary and assessment methods

Based on the aforementioned analysis, Table 7 shows the assessment criteria, parameters and assessment points for VPNs.

PETS ASSESSMENT FRAMEWORK – VIRTUAL PRIVATE NETWORK (VPN) APPS: SPECIFIC CRITERIA		
CRITERION	**PARAMETERS**	**ASSESSMENT POINTS**
Identity Protection	General information	Service offered
		Provider/infrastructure jurisdiction
		Financial model and anonymous payments
	IP address management	IP address sharing
		IP address change
	Protection against abuse of service	Service abuse semantics
		Protection/mitigation methods
		VPN firewall
		DNS leakage protection
		VPN kill switch
		Protection against fingerprinting
		Protection against traffic analysis
	Log files	Type of logs
		Location and access
		User choice
	Limitations	Known limitations affecting users' privacy
Encryption	Cryptographic algorithms and key lengths	Protocols used
		User information and choice
	Keys generation and storage	Location and access to keys
Side Effects	Known side effects on uses' online activity	List of issues and user information
	Known performance issues	List of issues and user information

Table 7: Assessment framework criteria for Virtual Private Networks (VPNs)

The main assessment method in the case of VPNs includes publicly available documentation, such as websites of the VPN providers, published reviews and comparison of tools, user forums/blogs, etc. Hands-on use and experience with a VPN client/service can also be useful to assess certain aspects, such as user choices (e.g. to verify encrypted communication), default settings[52] or certain features that are in place to prevent abuse (e.g. VPN leakage protection or kill switch[53]). More in-depth technical analysis (e.g. code

[52] In some cases there is an option to show a log of the session where different protocol parameters are provided, see e.g. in https://blog.g3rt.nl/openvpn-security-tips.html for some tips on OpenVPN security.
[53] For example by running relevant tests, see https://ipleak.net , http://test-ipv6.com , or https://www.doileak.com

review) would probably be most difficult to apply in the case of VPNs, although in some cases traffic analysis could be used to a limited extend (e.g. to verify the use of encryption).

4.3 Anonymizing networks

Anonymizing networks are designed to anonymize internet communications in a way that it is hard to link communication parties (e.g. a user and the web page he/she is visiting)[54]. In order to offer this functionality, anonymizing networks often rely on a distributed overlay network[55] and on onion routing [40] for anonymizing TCP-based applications, such as web browsing or P2P networks [41]. The most widely known anonymizing network today is Tor[56], which sends communication traffic through a number of different randomly-selected nodes (at least three), re-encrypting the communication packages at each node. Each node 'knows' where the package comes from and to which node it is going to, but ignores the whole route; in this way the identity of the original source remains hidden to anyone observing the communication. Other examples of popular anonymizing networks are the Java Anon Proxy (JAP, also known as JonDonym)[57] and the Invisible Internet Project (I2P)[58]. Today there is an increasing number of mobile applications, which allow use of anonymizing networks in mobile devices, such as for example the Tor-based tools Orbot[59], Orfox[60], Fire.onion[61] and Orxy[62].

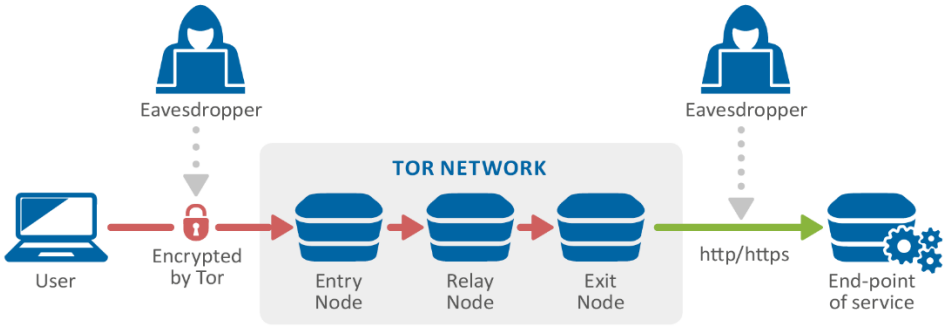

Figure 4: A use case scenario for anonymizing networks (based on Tor)

Clearly the main focus of anonymizing networks is to provide for user's anonymity. This is also the most important differentiating factor between anonymizing networks and VPNs (and the reason why they are presented under two different sections in the present document). Anonymity can be defined as 'the property of being not identifiable within a set of subjects, known as anonymity set'[63]. In that sense, it is very closely

[54] https://team.inria.fr/privatics/anonymizing-networks/
[55] For more information on overlay networks, see: http://www.networkcomputing.com/networking/network-overlays-introduction/1093920874
[56] The TOR project, https://www.torproject.org/
[57] https://anonymous-proxy-servers.net/index.html
[58] https://geti2p.net/en/
[59] Orbot, Tor for Android, https://www.torproject.org/docs/android.html.en
[60] Orfox, Tor browser for Android, https://play.google.com/store/apps/details?id=info.guardianproject.orfox&hl=en
[61] Fire.onion, https://play.google.com/store/apps/details?id=onion.fire&hl=en
[62] Orxy, Tor Proxy, https://play.google.com/store/apps/details?id=com.inetric.orxy&hl=en
[63] See in : http://freehaven.net/anonbib/cache/terminology.pdf

related to the notions of unlinkability[64] and unobservability[65]. Under the data protection legislation (GDPR), a set of data is considered as anonymous when it does not relate to an identified or identifiable natural person. The GDPR provisions do not apply to anonymous data[66].

On top of anonymity protection, anonymizing networks can also provide for encryption of communication as it travels through the network (i.e. encryption between the nodes of the network). This is for example the case of the Tor network, where data are re-encrypted at every node (as part of the anonymity protection mechanism offered). Still, however, encrypting traffic within the network does not usually include encryption of communication end-to-end, i.e. between the user's device and the final destination (e.g. the web page accessed).

As in the case of VPNs, anonymizing networks have certain limitations and side effects, which can affect the overall users' online experience (e.g. being blocked from certain sites/content or performance issues). Therefore, users need to be aware of these problems and be appropriately prepared[67].

In the context of the 'PETs control matrix', the assessment criteria for anonymizing networks are built primarily on their two defining technical features, i.e. the protection of anonymity and the possibility of encryption of communications, as well as their possible side effects. In particular, the criteria are as follows:

- Anonymity protection.
- Encryption.
- Side effects.

In the next paragraphs each criterion and its related parameters and assessment points are explained in detail.

4.3.1 Anonymity protection

Anonymity protection is the main scope and functionality of anonymizing networks, in the sense that they can hide the user's real IP address and/or other identifiers (direct or indirect), thus also hiding his/her online activity from third parties. This can be very important for online users that wish to remain anonymous from any party, including the entities running the different network's nodes. This is also a fundamental difference between anonymizing networks and VPNs: indeed, although the latter can hide the user's real IP address, they do not provide anonymity (since the VPN provider is in position of identifying the users of the service). In order to assess the level of anonymity protection in an anonymizing network, a number of parameters and assessment points can be considered, as shown below.

General information

This parameter relates to general information on the service that is provided to the users and includes the following critical points:

[64] Unlinkability of two or more items or actions means that these items are no more and no less related than they were previously (attacker gains no information), see in http://freehaven.net/anonbib/cache/terminology.pdf

[65] Unobservability of an item of interest means that all uninvolved subjects cannot sufficiently distinguish whether or not that item of interest exists, see in http://freehaven.net/anonbib/cache/terminology.pdf

[66] See GDPR, recital (26) in [9]. Also Article 29 Data Protection Working Party Opinion 5/2014 on anonymization techniques in [59].

[67] See for example known problems of using Google through Tor; Also known performance (speed) issues of Tor, https://www.torproject.org/docs/faq

- Functionality and use case scenarios: In order to clarify the scope of the anonymizing network and the way it operates, it is important that information is provided on specific use case scenarios (i.e. when and why a user might be interested in using the network)[68], as well as on the specific attributes and advantages of the network. In addition, it is interesting to address the adversarial model (e.g. passive/active adversary) that the anonymizing network is protecting against, i.e. the specific types of possible attackers and attack scenarios [42] [43].

- Network nodes: As the anonymizing networks is comprised of on a number of nodes, it is interesting to provide more information on the operation of these nodes, e.g. how they are established, who are their typical operators, as well as whether there is any party in the network that can restrict and/or control some or all the nodes.

- User choice: Another important parameter in this respect is to consider if the user has the option to select and/or exclude specific nodes in the network (e.g. a list of exit/entry nodes)[69], as well as whether he/she has the option to request a change of nodes in a particular connection.

Protection against abuse of service

As in the case of VPNs, monitoring possible abuse of the network is key for the provision of a high level of protection. Starting from the definition of 'abuse', different protection and mitigation measures can be considered here (see relevant section under VPNs in 4.2.2.1). In particular, for anonymizing networks it is interesting to assess measures in place to protect anonymity, including specific controls against fingerprinting [44] and traffic analysis [45].

Log files

In contrast with VPNs, anonymizing networks are not expected to maintain central logs, linking the users with specific identifiers. However it is still interesting to assess if any party in the network does maintain logs, as well as whether the combination of logs residing in various network nodes could potentially lead to users' identification. Still, the existence of logs might not be easy to verify in the context of a network with multiple nodes controlled by different parties.

Limitations

As in VPNs, this parameter is concerned with specific limitations that the anonymizing network might have with regard to its primary scope, which in this case is anonymity protection. It is, therefore, essential to consider any relevant known issues, as well as possibilities of enhancing the protection with the combined use of other services (see relevant section on limitations under VPNs in 4.2.2.1). In addition, it is particularly interesting to consider whether there is any guidance provided to users on how they can maximize the protection offered by the service, as well as whether specific tips are provided on actions that should not be performed (as they could lessen the overall protection of anonymity).

[68] See e.g. description of different cases of Tor network users, https://www.torproject.org/about/torusers.html.en

[69] For example in Tor, the StrictNodes option, when set to 1, implies that Tor will treat the nodes excluded as a mandatory requirement, even if doing so breaks the tool's functionality. If StrictNodes is set to 0, Tor will still try to avoid nodes included in the ExcludeNodes list, but it will use them in case it is necessary to perform its function without breaking the connection.

4.3.2 Encryption

As already mentioned, encryption might be an additional feature offered by an anonymizing network. It can be detailed to a number of specific parameters, as follows.

Level of encryption
As in many cases users confuse protection of anonymity with confidentiality (encryption) of communication, it is first of all important to assess if the network offers encryption end-to-end, i.e. between the user's device and the end-point of service (e.g. a webpage that the user wants to access). If this is not the case, it is also interesting to consider whether communication is encrypted in specific parts of the network (e.g. between different nodes). In all cases, it is should be clear to the users what level of encryption is offered and especially which parts of the network are *not* encrypted.

Combined use of other tools
Another parameter that is important to consider in this respect (and especially if the anonymizing network does not provide for encrypted communications end-to-end) is whether there are any other tools which could be used on top of the network to enhance the protection of confidentiality of communications[70].

4.3.3 Side effects

As in the case of VPNs, anonymizing networks may have certain side effects with regard to the user's overall use of internet, both in terms of limitations in accessing particular websites or content, as well as in performance.

Known side effects on users' online activity
There are different cases where users' online activity might be affected by the use of an anonymizing network. For example, certain servers might block traffic from an anonymizing network, e.g. considering it as spyware or due to censoring issues. It is, thus, important to assess if the anonymizing network offers relevant information to the users, as well as whether any blocking circumvention mechanisms are provided[71].

Known performance issues
Performance (e.g. speed) might also be affected and it is again interesting to assess if relevant information is provided to the users, including possible solutions to mitigate the problem.

4.3.4 Summary and assessment methods

Following the previous analysis, Table 8 shows the assessment criteria, parameters and assessment points for anonymizing networks.

[70] For example the use of tools like Https Everywhere (https://www.eff.org/Https-everywhere) to force https connections at destination (end-point of service).
[71] See for example the Tor bridges used to circumvent censorship, https://www.torproject.org/docs/bridges

PETS ASSESSMENT FRAMEWORK – ANONYMIZING NETWORKS: SPECIFIC CRITERIA		
CRITERION	**PARAMETERS**	**ASSESSMENT POINTS**
Anonymity Protection	General information	Functionality and use case scenarios
		Network nodes
		User choice
	Protection against abuse of service	Service abuse semantics
		Protection/Mitigation methods
		Protection against fingerprinting
		Protection against traffic analysis
	Log files	Verification of existence of logs
	Limitations	Known limitations affecting user's privacy
Encryption	Level of encryption	Encryption from source to destination
		Encrypted parts of the network
		Non encrypted parts of the network
	Combined use of other tools	Use of other tools to support encryption
Side Effects	Known side effects on user's online activity	List of issues and user information
	Known performance issues	List of issues and user information

Table 8: Assessment framework criteria for anonymizing networks

The main assessment method in the case of anonymizing networks includes publicly available documentation, such as the websites of the networks, published reviews, user forums/blogs, etc. Hands-on use and experience with the anonymizing network can also be useful to assess certain aspects, especially with regard to the client used for accessing the service (e.g. the Tor browser). For example hands on experience can help understand the overall functionality of the service, relevant user choices (e.g. selection of nodes) or issues related to side effects (blocking or low performance). More in-depth technical analysis (e.g. code review) is generally not possible to apply in the case of anonymizing networks (i.e. to assess their functionality), although in some cases traffic analysis could be used to a limited extend (e.g. to verify the use of encryption). Technical analysis can also be used to assess certain features of the clients used to access the network (e.g. Tor client).

4.4 Anti-tracking tools for online browsing

Online tracking is a very powerful technique for collecting information about an individual over time. Depending on the type and extend of tracking, this information can vary from detecting a user's interests upon visiting a specific web page (e.g. which pages he/she prefers) to a detailed analysis of the user's private life. Such analysis could include for example location data, personal interests and social relations, as well as sensitive data about his/her health, political beliefs or sexual preferences (e.g. through the combination of information derived from the user's visits to multiple web pages and/or online services). Tracking is very closely linked to profiling (see also section 3.2.3 and relevant GDPR definition).

Trackers use various techniques today, varying from the use of cookies[72] to more advanced mechanisms, such as device fingerprinting[73] and wifi/bluetooth tracking[74]. Some of these tracking mechanisms are hard to detect/control and resilient to blocking or removing, as is the case of device fingerprinting [46] [47] [48] (including canvas-based fingerprinting [49]), evercookies (also known as zombie cookies) or cookie syncing.

Anti-tracking tools are designed to block attempts of different types of trackers to monitor users' online activity and personal data. For the purpose of this study we mainly focus on the most common category of anti-tracking tools, i.e. anti-tracking browser extensions or add-ons (for mobile or desktop devices), which typically block elements like scripts, pop-ups, cookies, social buttons, etc. as well as advertisements[75].

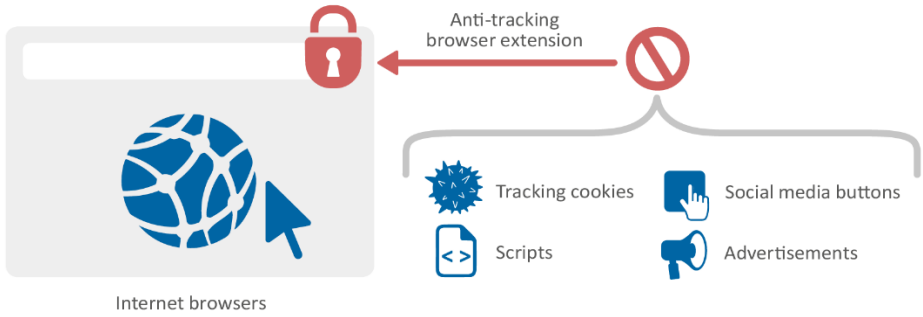

Figure 5: Use case scenario of anti-tracking tool for online browsing

Examples of widely used anti-tracking browser add-ons for desktop computers include Ghostery[76], Disconnect[77], uBlock origin[78], Privacy Badger[79], NoScript[80], AdBlockPlus[81], etc.[82] Examples of mobile apps which provide anti-tracking functionalities are the private browsing mode of Firefox[83], Ghostery Privacy Browser[84], Maxthon Web Browser[85], and Disconnect Privacy Pro[86].

As expected, in the context of the 'PETs control matrix' the assessment for anti-tracking tools is primarily built around their main functionality, i.e. blocking of different types of online trackers. Still, another interesting element of consideration is that, despite their anti-tracking functionality, in some cases anti-tracking tools might engage in their own collection and processing of users' data, e.g. for analytics purposes.

[72] A tracking cookie is a small piece of information stored in the user's web browser by a website so as to allow the user's identification each time he/she visits the same website. See also relevant Opinion 2/2010 of the Data Protection Working Party 29 on online behavioural advertising [62].
[73] A fingerprint is a set of information elements that can be used to identify a device or application [36]. See also in [38].
[74] Wifi/bluetooth tracking is based on the monitoring of probe requests that are being periodically broadcasted by a user's device (e.g. smartphone) to connect to a wifi/bluetooth network.
[75] It should be noted that ad-blockers cannot directly be considered as anti-tracking tools, but are still included in this category due to the fact that blocking of advertising is often affiliated with blocking of other types of tracking. See also in [60].
[76] www.ghostery.com
[77] disconnect.me
[78] https://github.com/gorhill/uBlock
[79] https://www.eff.org/privacybadger
[80] noscript.net
[81] adblockplus.org
[82] See in [1] for a more detailed analysis of specific anti-tracking add-ons.
[83] Firefox private browsing, https://www.mozilla.org/en-US/firefox/android/.
[84] Ghostery privacy browser, https://itunes.apple.com/us/app/ghostery-privacy-browser/id472789016?mt=8 .
[85] Maxthon Web Browser, https://play.google.com/store/apps/details?id=com.mx.browser&hl=en .
[86] Disconnect Privacy Pro, https://itunes.apple.com/us/app/disconnect-privacy-pro-entire/id1057771839?mt=8 .

Moreover, in some cases the use of anti-tracking tools might negatively influence the users' online experience (e.g. being blocked from different types of sites or content). These are both important elements to consider before selecting such a tool and users need to be appropriately informed. Thus, in order to offer a thorough understanding of the operation of anti-tracking tools, the assessment criteria are concerned with all the aforementioned issues, namely:

- Blocking of trackers.
- Data collection.
- Side effects.

In the next paragraphs we explain in detail each criterion and its relevant parameters and assessment points.

4.4.1 Blocking of trackers

Clearly, this is the most important criterion to assess under anti-tracking tools, as it is related to the core of their functionality, i.e. to block different types of trackers. A number of parameters that require more detailed attention are listed below.

General information
The first (and most important) aspect to consider under this parameter is the types of elements that an anti-tracking tool blocks, as well as whether the blocking is continuous for all types of elements. Moreover, it is interesting to examine the blocking mechanism used by the tool (e.g. tracker detection algorithms/heuristics, white/black listing or filtering rules), as this might influence both the effectiveness, as well as the overall operation of the tool. Finally, it is interesting to assess whether the tool has embedded Do Not Track (DNT) protection and how this is done[87].

Default settings
This parameter is focused on assessing whether the settings of an anti-tracking tool are set to the highest level of protection by default, i.e. blocking all possible trackers, without 'hidden' exceptions. It is clearly linked to the concept of data protection by design and by default in GDPR (art. 25).

- Blocking enabled by default: Due to the nature of this particular type of tool, users would probably expect that blocking is activated by default (i.e. upon installation of the tool) for all types of tracking elements. If this is not the case, users should be clearly informed about the elements that are not blocked by default, e.g. with the use of pop-ups or banners. Moreover, users should be offered the possibility to activate blocking, e.g. by clicking on a button or through the settings menu.

- Exceptions: Another important point is that users are also clearly informed in case that specific trackers (e.g. specific companies or groups of companies) are exempted from tracking by default. An example of such exception is the so-called 'acceptable ads' list[88], which may be supported by certain ad-blockers[89].

[87] The Do Not Track (DNT) header is the proposed HTTP header field that requests that a web application disable either its tracking or cross-site user tracking of an individual user, see in [61]. Although DNT is not widely employed by web services providers today, it can still be a very promising standard against online tracking, see https://www.eff.org/press/releases/coalition-announces-new-do-not-track-standard-web-browsing
[88] Advertising from companies which have signed the Acceptable Ads Manifesto, https://acceptableads.org/
[89] See for example: https://adblockplus.org/en/acceptable-ads

In cases of exempted trackers it is important that users are informed and provided with the possibility to activate tracking also for these trackers.

User choice

This parameter concerns the possible choices that the users have in configuring the anti-tracking tool to best match their preferences. In this respect it is interesting to assess the next points:

- Configuration options: Users might be offered the possibility to activate/deactivate the blocking of specific trackers or tracking elements, a feature that can be very useful, for example in order for the users to access certain types of sites or content. In such cases, it is also important to consider how activation/deactivation can be done (e.g. per tracker, for all trackers in a page, per domain, etc.).

- Information on risks: Another useful point is whether the tool informs the users about possible risks, e.g. in case of deactivation of blocking for certain tracking elements or trackers. Also, the way that this information is provided (e.g. warning message when user deactivates a blocked element).

Blocking information

This parameter is related to the information that the tool provides to the users about the blocked tracking elements/trackers. It concerns the information provided per browsing session and it may include e.g. identity of the tracker, types of elements blocked (per tracker), active processes, etc. Moreover, it also refers to whether a history of blocked elements/trackers is available (beyond particular browsing sessions) and how the user can access it (e.g. by clicking a button or through the settings menu).

4.4.2 Data collection

This criterion aims at assessing whether an anti-tracking tool collects and further processes any personal data of its users, taking into account the principles of the GDPR and ePrivacy Directive. As such, it is closely linked to the generic criterion of privacy policy implementation (see section 3.2) but aims at explicitly considering specific implementation aspects in the case of anti-tracking tools (e.g. with regard to data transfers and data recipients). To this end, the following parameters require more detailed attention.

Collection of personal data

In general anti-tracking tools are not expected to collect and further process any personal data. Still, it is interesting to analyze this parameter, as subtle collection of users' personal data might in fact hinder the very purpose of an anti-tracking tool. Some aspects to particularly consider are as follows:

- Types of personal data: Possible types of data include contact information, device/browser identifiers, IP address, URLs visited, etc.

- Purpose of data collection: Possible purposes can be data analytics (e.g. to improve the performance of a tool or provide statistics on its usage), commercial activity (e.g. selling users' behavioral patterns to advertising companies), the provision of added value services to users, etc.

- Information and consent: Users should be clearly informed and asked to provide their consent in case that processing of personal data is performed through an anti-tracking tool (for any of the aforementioned purposes). In this respect it is also essential to consider whether the tool provides the same functionality if consent is not granted, as well as if consent can be easily withdrawn.

Transfer of personal data

On top of the data collection addressed under the previous parameter, it is important to particularly consider if any personal data of the users are transferred to third parties. In this respect, the first aspect to assess is the recipients of the data. Possible recipients include advertising or analytics companies who might use the data to draw behavioral patterns or statistics. It is also interesting to consider whether the tool's provider has any business relationship with such companies (e.g. supporting the tool's underlying business model). Moreover, as in the case of data collection, the types of data, purpose of collection and users' information and consent should be assessed. On top of these, a particularly interesting point is to explicitly assess if anonymized data are transferred and, in such cases, what is meant by 'anonymization' (as it is often confused with simple de-identification or pseudonymization of data).

4.4.3 Side effects

As in the case of VPNs and anonymizing networks, anti-tracking tools may have certain side effects with regard to the user's overall use of internet, both in terms of limitations in accessing particular websites or content, as well as in performance.

Known side effects on users' online activity

There are different cases where users' online activity might be affected by the use of an anti-tracking tool, e.g. due to the fact that certain blocked elements are essential for accessing a particular site or content. It is, thus, important to assess if the tool offers relevant information to the users, as well as whether it is possible to overcome the problem (e.g. by activating certain elements in certain browsing sessions).

Known performance issues

Sometimes anti-tracking tools might also be associated with performance issues, e.g. slowing down page loading. Again user information and practical tips to solve the problem are interesting to consider.

4.4.4 Summary and assessment methods

Following the aforementioned analysis, Table 9 shows the assessment criteria, parameters and assessment points for anti-tracking tools.

PETS ASSESSMENT FRAMEWORK – ANTI-TRACKING TOOLS: SPECIFIC CRITERIA		
CRITERION	**PARAMETERS**	**ASSESSMENT POINTS**
Blocking of trackers	General information	Types of blocked elements
		Blocking mechanism
		Do Not Track
	Default settings	Blocking enabled by default
		Exceptions
	User choice	Configuration options
		Information on risks
	Blocking information	Information on blocked elements/trackers
		History of blocked elements/trackers
Data collection	Collection of personal data	Types of personal data
		Purpose of data collection
		Information and consent
	Transfer or personal data	Recipients of data
		Types of personal data
		Purpose of data collection
		Information and consent
Side Effects	Known side effects on user's online activity	List of issues and user information
	Known performance issues	List of issues and user information

Table 9: Assessment framework criteria for anti-tracking tools for online browsing

The starting point for the assessment of anti-tracking tools is to review publicly available documentation, such as the websites of the tools, published reviews, user forums/blogs, etc. Hands-on use and testing can also be very helpful, e.g. in assessing the default settings, user configuration options, and information provided to users. It is interesting to note that a number of available tools/websites can support testing, e.g. Panopticlick[90], Web browser security tools[91], Aloodo test[92], Do not track test[93], Am I unique[94], etc. More in-depth technical assessment (e.g. code review) could also reveal detailed information, especially with regard to the anti-tracking mechanism used and the possible collection and/or transfer of personal data.

[90] EFF Panopticlic, https://panopticlick.eff.org/ .
[91] BrowserLeaks.com, Web Browser Security, https://www.browserleaks.com/ .
[92] Aloodo, Tracking Protection Test, http://www.aloodo.org/test/ .
[93] Future of Privacy Forum, All About Do Not Track - DNT, https://allaboutdnt.com/
[94] Am I unique?, https://amiunique.org/

5. The PETs control matrix

The 'PETs control matrix' is the implementation of the proposed PETs assessment methodology (presented in the previous Chapters) into a practical tool that can be used for:

- Performing the assessment of a PET
- Presenting the results of the PET's assessment to any interested party
- Facilitating the comparative presentation of different PETs

As such, the 'PETs control matrix' comprises different sets of detailed assessment questions, each corresponding to the assessment criteria described under Chapters 3 and 4. In particular, for each criterion, specific questions are defined to address the different parameters and assessment points. In order to provide for standardized and comparable answers to the questions, for each question a set of possible answers is also defined (Yes/No or multiple choices). However, in some cases, where a closed set of answers is not possible, open questions (free text) are also defined. The aforementioned set of questions and answers is finally implemented in Excel to allow for a practical use of the overall method. Figure 6 shows a snapshot from the Excel-based 'PETs control matrix'.

ENISA'S PETS CONTROL MATRIX

TOOL/SERVICE NAME	Secure Messanger 1	*WEBSITE*	www.sm1.com
DEVELOPER	SM 1	*CONTACT EMAIL*	contact@sm1.com

Tool/service type Please click on the yellow cells to select		*Operating System Please click on the yellow cells to select*		*Please introduce the version of the tool/service*	
VPNs		*Android*	✓	version	
Secure Messaging	✓	*iOS*	✓	version	
Anonymizing (networks)		*Windows Phone*		version	
Anti-Tracking		*Windows*		version	
		Mac		version	
		Linux		version	
		Any OS (only for Anti-Tracking)			

GENERIC			SPECIFIC			
Maturity & Stability	Privacy Policy Implementation	Usability	VPNs	Secure Messaging	Anonymizing Networks	Anti-Tracking

The ENISA's PETs control matrix can help you analyse and present the different characteristics of a specific privacy-enhancing tool and/or service.

You can choose between four different types of tools/services: VPNs, Secure messaging, Anonymizing networks and Anti-tracking. Based on your choice you will be asked to answer a number of questions particular to the selected tool/service (under Specific tab above). For all cases you will be asked to answer a number of generic questions applicable to all types of tools/services (on Maturity and Stability, Privacy Policy Implementation and Usability under Generic tab above).

A glossary is provided for explanation of technical terms used within the questions.

This document should be filled under Excel versions 2007, 2010, or 2016.

If you would like to learn more about the ENISA's PETs control matrix and the overall framework for assessment of privacy tools, please visit: www.enisa.europa.eu

Figure 6: ENISA's 'PETs control matrix' (Excel – Windows version)

It should be mentioned that the 'PETs control matrix' at this stage does not include any scales for providing quantitative assessments of tools (e.g. a final grading, such as 'good, moderate or bad'). This choice was made due to the inherent difficulty of attributing specific weights and values to distinct controls related to privacy and data protection without missing critical information and/or edge cases. Moreover, as already mentioned, in many cases the answers to questions related to privacy and data protection are not 'clear cut' and more information is in many cases needed (which cannot be quantified under a limited set of choices). Therefore, the 'PETs control matrix' should mainly be seen as means that can facilitate *a standardized and clear presentation of different privacy tools*, rather than a tool that can directly offer comparative assessments. Still, by enabling the provision of the 'right' information, the 'PETs control matrix' can help users understand what

features are offered by different tools, thus indirectly also supporting comparative assessments for specific features of different tools.

Annex 1 to this document presents the questionnaires for all assessment criteria described in the previous Chapters. Annex 2 to this document is the final 'PETs control matrix' in Excel (the tool).

5.1 A case study: secure messaging apps

In order to provide for a more thorough understanding on the practical use of the 'PETs control matrix', in the course of this work we conducted a case study on secure messaging apps for mobile devices. After the completion of this exercise, it is interesting to note that, although the core functionality of the tools is the same, there are certain elements that differ and could in some cases influence the final users' choice. The 'PETs control matrix' could, thus, indeed support the presentation of these differences in a standardized way, so as to help users in their decision making process.

As already mentioned, the scope of this document is not to conduct a comparative evaluation of tools and, therefore, no specific details on the characteristics of different tools are provided herein. Some more general outcomes of our analysis are briefly presented below.

Selecting the 'best' solution

Although users are mostly interested to get precise guidance on which tool is 'the best', in practice our analysis showed that what is best is actually very much dependent on the users' needs. In that sense, there is not really one 'best' solution, but rather many solutions that offer different approaches towards the same issue, i.e. secure communication. Having said that, it is important to note that the notion of 'best solution' does not only rely on the technical characteristics of a tool, but also on the overall perception of how privacy and data protection are addressed by the provider of a secure messaging app/service[95]. Moreover, the notion of 'best solution' is very much influenced by publicity gained over the use of certain tools[96].

Same feature, different implementation

As expected, all secure messaging apps offer end-to-end encryption as their core functionality. Still, it is interesting to note that certain properties are implemented in different technical ways (that might lead to higher or lower level of security, depending on the particular implementation).

One notable example is the implementation of the property of 'forward secrecy', which is a fundamental property in end-to-end encryption, ensuring that past communications are not compromised if the encryption key is compromised. In most of the examined secure messaging apps forward secrecy is implemented by using a new encryption key (generated at the user's device) to encrypt/decrypt each message during a communication session and then immediately destroying the key. Variations of this approach can be found where the same key is used for a certain number of messages or time period. In some cases, however, a different implementation may be found: end-to-end communication is based on a static single key (generated at the user's device) for the whole communication session but a second level of protection is added at the transport layer, where the symmetric keys used are ephemeral.

[95] See for example the recent privacy concerns raised by WhatsApp's announcement about sharing of personal data with Facebook, http://www.reuters.com/article/us-privacy-whatsapp-europe-idUSKCN1141UW

[96] See for example publicity gained for Signal after Edward Snowden's revelation of the use of the particular tool, http://www.dailydot.com/layer8/edward-snowden-signal-encryption-privacy-messaging/

Another example is the authentication mechanisms applied. While in most cases an out-band authentication mechanism is used, different technical approaches might be implemented, such as for example public key fingerprint IP (hexadecimal string format) or scanning 2D codes (QR codes) values over a second communication channel (e.g. external scan, email or phone).

Different features

Despite the same core functionality, different tools may offer different supported features, which, depending on users' needs, might be more or less important.

Storage and encryption of communication data is a prominent case of such difference. For example, while all applications store data on the user's device (local storage), only some provide encryption of these data, each following a different method (e.g. the use of SQLcipher[97] or the use of passphrases provided by users upon installation) and encrypting different types of data (content or metadata or both). Communication data may also be stored at the provider's servers (sometimes in the cloud), providing the users remote access to these data from multiple devices. Again the types of data stored and/or encrypted, as well as access to the encryption keys vary. Overall assessment of this element is difficult and requires trust to the tool's provider (see also point on assessment limitations).

Another interesting example is that of self-signed certificates for users' authentication. Self-signed certificates may allow a decentralized mode of communication based on which users may deploy their own Instant Messaging (IM) server and install a self-signed certificate in the secure messaging application. Despite the flexibility that they offer, self-signed certificates are often associated, as mentioned earlier, with certain security threats (e.g. compared to certificates signed by a CA). Most secure messaging apps do not support self-signed certificates, allowing connection only to the server of the service provider. In some cases, however, this feature can be found, e.g. allowing users to deploy their own private IM XMPP server[98] and install their own self-signed certificate to communicate[99].

Default settings

While in most secure messaging apps end-to-end encryption is enabled by default, there are few examples where this is not the case. In these cases, the users may activate end-to-end encryption, e.g. using a 'padlock' or other similar icon on the screen. Still, it is important to note that for this particular type of application, privacy by default settings are essential to enable non-expert users to get the most out of the application. In this respect, the new GDPR provision on data protection by default may support this overall approach in the mobile sector, setting the apps to the highest possible level of privacy protection.

Understanding privacy policies

The privacy policies of secure messaging apps should in principle cover any type of processing of personal data associated with the operation of the app. From our analysis it is obvious that these policies in many cases differ, while at the same time the level of information and choice that is provided to the users varies also considerably.

[97] An extension to SQLite database platform that facilitates the creation of encrypted databases, https://sqlite.org/
[98] See more information on XMPP in https://xmpp.org/about/technology-overview.html
[99] For more information, see: http://arstechnica.com/information-technology/2014/03/how-to-set-up-your-own-private-instant-messaging-server/

A very interesting example in this respect relates to the processing of communication metadata by the messaging service providers, which takes place in the context of the operation of all secure messaging apps (as they are all based on the client-server scheme). While some apps have privacy policies which are clearly defining what data are being processed and stating that these data are not shared with any third party without users' consent, others many not provide any privacy policy at all. Still, the latter may in certain cases be due to the fact that the service is delivered through different service providers and, thus, the processing of personal data must abide by the privacy policies of these providers. In many cases a privacy policy is available (e.g. at the official site of the app) but is general and unclear, without providing any explicit information on what personal data are being processed on the service provider's server, the purpose of the processing and/or any relevant time periods.

Anonymous communication

An interesting finding in this area is that the term 'anonymity' is sometimes misused by secure messaging apps, providing in this way information that is misleading, e.g. confusing anonymous communication with the use of pseudonyms. According to our analysis, true anonymous communication is currently not offered by any of the tested applications. However, in some cases the app may be used in conjunction with other tools to provide this feature[100].

Even when anonymization is not offered, some secure messaging apps do offer some level of pseudonymization, as a means to protect the disclosure of users' identity to third parties. For example in some cases the user's personal data (e.g. telephone number and contacts) are hashed before being uploaded to the provider's server, although this approach does not offer strong pseudonymization[101]. In other cases users may select to register with a pseudonym to a server and use this account to also register to the application. Some apps may also directly allow for the creation of pseudonymous ID upon registration.

Limitations of the assessment

As a final point, it is important to note the limitations of the technical assessment of PETs. Indeed, although certain features may be technically assessed, an in-depth technical analysis is in many cases impossible (e.g. due to the fact that the software is closed source or due to the technical complexity of the assessment). Therefore, it is necessary to rely on the information provided by the developers/providers of the tools or on other existing technical reports. Still, in many cases (as demonstrated for example in the point about the privacy policies), this information is not enough to perform a thorough assessment and cannot efficiently contribute to more guidance towards the general public.

[100] See some relevant information in: https://www.eff.org/node/82654
[101] As the address space of phone numbers is relatively small and, thus, a dictionary attack may be used to invert the hashes.

6. Conclusions and recommendations

The scope of this study was to develop a framework and a practical mechanism for the assessment of online and mobile privacy tools based on pre-defined generic and (technology) specific criteria. Indeed, in the previous Chapters we presented in more detail the approach followed for the definition of a thorough PETs assessment framework, the rationale and specificities of the assessment criteria applied, as well as the actual conduction/presentation of the assessment in the form of the 'PETs control matrix'. Based on the aforementioned analysis, as well as the testing of different privacy tools, this Chapter draws a number of more general conclusions and subsequent recommendations to be considered by all involved stakeholders in the area of PETs.

What you see is not always what you get

Going back to the initial point of departure of this work, i.e. reliability and trustworthiness of PETs, one important conclusion is that users of PETs do not always get the functionality that is expected from these tools. This is not to say that there are not several very useful and trustworthy privacy tools available in the market today; however, in many cases the actual functionality of the tools is not clearly advertised to the users or the users need to get more involved/engaged in understanding how a tool really works (e.g. by tweaking the privacy settings). The most obvious example in this respect is the whole area of 'anonymous communication' where in many cases the term 'anonymous' is used to refer to the use of pseudonyms, rather than true anonymity of the communicating parties. It is, thus, essential that more transparency is provided with regard to the functionality of PETs, as well as the underlying business models of the PETs developers/providers (which in many cases play a critical role in the privacy settings of a tool).

The PET developers/providers should offer clear information about the actual functionality and attributes of their tools, as well as opt for privacy by default settings, taking into account the privacy and data protection expectations of their users.

The research community and security/privacy centred EU and national organisations should support PETs assessment frameworks aiming at addressing the technical details of different tools and offering clear information to end users.

Open and closed source software

When discussing transparency and assessment of PETs, a central element of consideration is the type of license that is used for a tool's development. In that sense, an open-source license clearly facilitates review and customisation of software, whereas a closed-source license does not provide this possibility. However, open source in itself cannot be considered as an indicator for a tool's trustworthiness: a company's overall reputation and capacity is also a defining parameter (and probably the most important one for the general public), especially with regard to issues such as maintenance and software updates. Still, it is important to note that open source can be a critical requirement if PET libraries should be re-used in third-party products, as developers (both commercial and non-commercial) would probably not be willing to use closed libraries and, thus, risk to have their applications potentially compromised.

The PET developers/providers should make available as much as possible information about the basic PET libraries used for the provision of privacy-enhancing features of their tools.

The European Commission, EU standardization bodies and security/privacy centred EU organisations should explore certification schemes for PETs based on commonly accepted assessment frameworks. Such schemes can build more certainty on the functionality of different tools, independently from the licensing type used.

Usability and privacy

Some problems often associated with PETs are low performance (e.g. low speed) and other possible side effects (e.g. difficulty in accessing certain online sites or content). This often leads to the perception that users have to trade off usability for privacy protection online, which in fact is one of the most important barriers against the wider adoption of PETs by the general public. Exactly for the aforementioned reasons we have considered (in the 'PETs control matrix') usability as one important criterion for PETs assessment. However, it should be mentioned that a lot of research is still needed in this field, both with regard to implementing privacy features in a user-friendly manner, as well as with regard to the assessment of 'user-friendliness' in a practical way (e.g. by number of clicks or pages loaded for the conduction of certain tasks). In this way the battle of 'usability versus privacy' can be shifted to a balanced approach of 'usable privacy' [50] [51] [52] for the benefit of all involved stakeholders.

PET developers/providers and the research community should invest more in 'usable privacy' and 'usable security', involving also end users in the assessment of tools. The European Commission should promote research in this field, as a key enabler of the adoption of privacy technologies in online and mobile environments.

PET developers/providers should provide clear information on known limitations/side effects of their tools to the general public.

Providing information to the general public

The ultimate scope of the 'PETs control matrix' presented in this document is to provide for more clarity and assurance regarding the functionality of different online and mobile privacy tools to the general public. At the same time most users usually prefer easy and fast information from trusted sources (e.g. recommendations from Data Protection Authorities or independent security/privacy organisations), rather than detailed technical information. How can the 'PETs control matrix' (or other similar assessment frameworks) then really contribute to enhancing user information and awareness?

One answer to this question could be the use of the 'PETs control matrix' as a self-assessment tool by the PETs developers/providers: while self-assessment still requires trust to the developer/provider (and, thus, cannot be considered as objective), the use of a common scheme for the presentation of different tools can facilitate to a certain degree transparency and support comparative evaluations of PETs. It is interesting to note that relevant initiatives are already available in other IT industry sectors[102], e.g. as part of relevant self-accreditation schemes. However, in order for such a scheme to be successful, it requires strong commitment from the industry, as well as the use of an independent platform (e.g. offered by an independent third party), where all self-assessments will be made available to the general public/end users. Moreover, it also requires the use of specific grading, scales and weights (not currently part of the proposed framework), which are very difficult to define and follow in the area of privacy and data protection.

Another answer to this question is the use of the 'PETs control matrix' by independent experts or organisations in order to perform the assessments of different tools and accordingly present the results to the general

[102] See for example the Cloud Controls Matrix, established by the Cloud Security Alliance, in order 'to provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider; https://cloudsecurityalliance.org/group/cloud-controls-matrix/.

public. For example, the Data Protection Authorities could endorse (or the opposite) in this way the use of particular tools, e.g. as paradigms of data protection by design and by default in the course of implementation of GDPR. Having said that, it is important to acknowledge that such a task can be quite challenging, not only because of the level of technical expertise required and the overall difficulties associated with technical assessment, but also due to the fact that public organisations might not be in position of promoting (or rejecting) particular tools in the market. In that sense, civil society organisations might be better placed to offer detailed analysis of tools. Moreover, another point to consider is that each assessment is valid only at a certain point in time and, thus, an update mechanism is needed (which again requires a lot of effort and skills).

As a means to enhance transparency, PET providers/developers should make use of assessment frameworks/mechanisms (such as the 'PETs control matrix') and support relevant platforms/schemes to provide comparable presentations of the different features of their tools.

The research community and civil society organisations should engage in publishing technical reviews of PETs based on commonly accepted assessment frameworks.

The European Commission, security/privacy centred national and EU organisations, as well as national and EU privacy regulators/supervisors (e.g. Data Protection Authorities) should support platforms that can enable assessment of PETs (e.g. by independent privacy experts).

National and EU privacy regulators/supervisors (e.g. Data Protection Authorities) should provide more precise guidance on the use of PETs, as well as practical examples of the concepts of 'data protection by design and by default'.

Beyond PETs: a privacy assessment framework for online and mobile applications and services

The work presented in this study was focused on the assessment of PETs, i.e. tools that are already designed to protect users' privacy and personal data. A future (and quite interesting) step for the developed framework, would be its extension to conduct privacy assessments of different types of online and mobile tools that are widely used today by the general public in the context of their everyday activities (e.g. different categories of mobile apps). While utilizing many of the aspects addressed in the 'PETs control matrix', this extended assessment framework would actually go far beyond PETs, providing for a thorough scheme of technical evaluation of tools with regard to their privacy and security characteristics, as well as their overall compliance with relevant provisions of GDPR. Moreover, the framework could go a step further addressing aspects such as infiltration of apps in relevant marketplaces, as well as dynamic audit/control of apps on the fly in order to rectify identified privacy and data protection issues. An additional challenging requirement could be to include also scales for the grading of tools (in terms of their privacy and data protection performance). Such a framework could be very useful to the regulators/supervisors (e.g. Data Protection Authorities), as well as the users themselves, taking into account the considerations mentioned earlier in this section.

The research community, security/privacy centred national and EU organisations, as well as national and EU privacy regulators/supervisors (e.g. Data Protection Authorities) should co-operate and define a generic framework for privacy and data protection assessments of different types of online and mobile tools. Such a framework could on one hand enhance users' information and awareness regarding the privacy policies of different tools, while on the other hand it could contribute to the practical implementation of GDPR by application and service developers/providers.

7. Bibliography

[1] ENISA, "Online privacy tools for the general public: towards a methodology for the evaluation of PETs for internet & mobile users", 2015. [Online]. https://www.enisa.europa.eu/publications/privacy-tools-for-the-general-public

[2] ENISA, "Readiness analysis for the adoption and evolution of privacy enhancing technologies", 2015. [Online]. https://www.enisa.europa.eu/publications/pets

[3] Electronic Frontier Foundation. [Online]. https://www.eff.org/secure-messaging-scorecard

[4] Electronic Frontier Foundation. [Online]. https://ssd.eff.org/

[5] Privacy Rights Clearinghouse, "Privacy aware mobile application development". [Online]. https://www.privacyrights.org

[6] The Network Computing, "How to keep enterprise apps secure", 2013. [Online]. http://www.networkcomputing.com/wireless/how-keep-enterprise-mobile-apps-secure/647409173

[7] UK Information Commissioner's office (ICO), "Privacy in mobile apps. Guidance for app developers", 2013. [Online]. https://ico.org.uk/media/1596/privacy-in-mobile-apps-dp-guidance.pdf

[8] GSMA, "Privacy Design Guidelines for Mobile Applications", 2012. [Online]. http://www.gsma.com/publicpolicy/wp-content/uploads/2012/03/gsmaprivacydesignguidelinesformobileapplicationdevelopmentv1.pdf

[9] European Commission, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC", 2015. [Online]. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

[10] European Commission, "Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data," 1995. [Online]. http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf

[11] European Commission, "Directive 2002/58/EC of the European and of the Council of 12 July 2012 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)", 2002. [Online]. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002L0058:20091219:EN:PDF

[12] ENISA, "Privacy and data protection by design", 2014. [Online]. https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design

[13] Justin Etheredge, "How Do We Measure Maturity In Software? ", *Code Thinked*. [Online]. http://www.codethinked.com/how-do-we-measure-maturity-in-software

[14] ISO, "ISO/IEC 14764:2006 Software Engineering — Software Life Cycle Processes — Maintenance", 2011.

[15] Cochin University of Science and Technology, Department of Computer Applications, "Measuring the Maturity of Open Source Software for Digital Libraries: a Case Study of DSpace", 2015. [Online]. https://dyuthi.cusat.ac.in/xmlui/bitstream/handle/purl/5012/Dyuthi-T2079.pdf?sequence=1

[16] Common Criteria. [Online]. https://www.commoncriteriaportal.org/products/

[17] Article 29 Data Protection Working Party, "Opinion 15/2011 on the definition of consent", 2011. [Online]. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf

[18] ISO, "ISO 9241-11, Ergonomic requirements for office work with visual display terminals (VDTs)-Part 11: Guidance on usability", 1998.

[19] W. Quesenbery, "What does usability mean: Looking beyond 'Ease of use'", in *Proceedings of the 48 annual Conference, Society for Technical Communication*, 2001, pp.1-5. [Online]. http://www.wqusability.com/articles/more-than-ease-of-use.html

[20] J. Nielsen, "Finding usability problems through heuristic evaluation", in *Proceedings of the SIGCHI conference on Human factors in computing systems*, 1992.

[21] J. Nielsen, "Heuristic evaluation", in *Usability Inspection Methods*. New York: John Wiley & Sons, 1994.

[22] C. Hochleitner, P. Wolkerstorfer, J. Angulo, S. Fischer-Hübner, E. Wästlund C. Graf, "Towards Usable Privacy Enhancing Technologies: Lessons Learned from the PrimeLife Project ", in *Deliverable D4.1.6 of the EU Privacy and Identity Management in Europe for Life*, 2011.

[23] L. Santos, and P. Lew L. Olsina, "Evaluating Mobileapp Usability: A Holistic Quality Approach", in *Proceedings of the 14th International Conference on Web Engineering (ICWE)*, 2014, pp. 111-129.

[24] Alfred Menzies and Paul C. van Oorscot, "Handbook of Applied Cryptography", CRC Pres, 1997.

[25] IETF, "RFC 2246, The TLS Protocol, Version 1.0", 1999. [Online]. http://www.ietf.org/rfc/rfc2246.txt; RFC 5246

[26] IEFT, "RFC 7469", 2015. [Online]. https://tools.ietf.org/html/rfc7469

[27] ISO, "ISO/IEC 9797-1:2011- Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 1: Mechanisms using a block cipher", 2011.

[28] ISO, "ISO/IEC 9797-2:2011 - Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 2: Mechanisms using a dedicated hash-function", 2011.

[29] QuarksLab SAS, "ChatSecure security assessment", 2015. [Online]. http://blog.quarkslab.com/resources/2015-06-25_chatsecure/14-03-022_ChatSecure-sec-assessment.pdf

[30] WhatsApp, "WhatsApp encryption overview", 2016. [Online]. https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf

[31] Telegram, "Secret chats, end-to-end encryption". [Online]. https://core.telegram.org/api/end-to-end

[32] Wickr, "Wickr messaging protocol", 2015. [Online]. https://www.wickr.com/uploads/files/700869603163179165-wickr-whitepaper-final.pdf

[33] Threema, "Threema cryptography whitepaper", 2016. [Online]. https://threema.ch/press-files/cryptography_whitepaper.pdf

[34] C. Mainka, C. Bader, F. Bergsma, J. Schwenk, and T. Holz T. Frosch, "How Secure is TextSecure?", Cryptology ePrint Archive, Report 2014/904 2014. [Online]. https://eprint.iacr.org/2014/904.pdf

[35] Rolf Oppliger, "Internet security: firewalls and beyond," *Communications of the ACM* , vol. 40, no. 5, pp. 92-102, 1997.

[36] IETF, "RFC 6973 - Privacy Considerations for Internet Protocols", 2013. [Online]. https://tools.ietf.org/html/rfc6973

[37] Alexandros Kapravelosy, Wouter Joosen, Christopher Kruegely, Frank Piessens, Giovanni Vigna Nick Nikiforakis. Cookieless Monster: Exploring the Ecosystem of Web-based Device Fingerprinting. [Online]. https://lirias.kuleuven.be/bitstream/123456789/393661/1/;%20https://securehomes.esat.kuleuven.be/~gacar/persistent/the_web_never_forgets.pdf

[38] Article 29 Data Protection Working Party, "Opinion 9/2014 on the application of Directive 2002/58/EC to device", 2014. [Online]. http://www.dataprotection.ro/servlet/ViewDocument?id=1089

[39] ENISA, "Algorithms, key size and parameters report", 2014. [Online]. https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014/at_download/fullReport

[40] Michael Reed, Paul Syverson David Goldschlag, "Onion Routing for Anonymous and Private", *CACM*, 1999. [Online]. https://www.onion-router.net/Publications/CACM-1999.pdf

[41] E. Erdin, M. H. Gunes, G. Bebis, T. Shipley B. Li, "An overview of anonymity technology usage", *Computer Communications 36*, pp. 1269-1283, 2013.

[42] C. Palmer D. Kesdogan, "Technical challenges of network anonymity", *Computer Communications 29*, pp. 306–324, 2006.

[43] K. Matsuura. F. Feng, "Stronger Bridge Mechanisms of Tor which Take into Consideration Exhaustive Adversarial Models", *Journal of Information Processing*, vol. 23, no. 5, pp. 646-654, 2015.

[44] I. Goldberg T. Wang, "Improved website fingerprinting on Tor", in *Proceedings of the 12th ACM workshop on Workshop on privacy in the electronic society*, 2013, pp. 201-212.

[45] A. Khurshid, J. Juen, M. Caesar, N. Borisov P. Mittal, "Stealthy Traffic Analysis of Low-Latency Anonymous Communication Using Throughput Fingerprinting", in *Proceedings of the 18th ACM conference on Computer and Communications Security*, 2011, pp. 215-226.

[46] P. Eckersley, "How Unique is your Browser?", in *Proceedings of the Privacy Enhancing Technologies Symposium (PETS)*, 2010.

[47] M. Juarez, N. Nikiforakis, C. Diaz, S. Gürses, F. Piessens, B. Preneel G. Acar, "FPDetective: dusting the web for fingerprinters", in *Proceedings of the ACM SIGSAC Conference on Computer & Communications Security*, 2013, pp. 1129-1140.

[48] Walter Rudametkin, Benoit Baudry Pierre Laperdrix, "Beauty and the Beast: Diverting modern web browsers to build unique browser fingerprints", in *37th IEEE Symposium on Security and Privacy*, San Jose, United States, 2016.

[49] C. Eubank, S. Englehardt, M. Juarez, A. Narayanan, C. Diaz G. Acar, "The Web Never Forgets: Persistent Tracking Mechanisms in the Wild", in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, Scottsdale, Arizona, United States, 2016, pp. 674-689.

[50] The Telegraph. Balancing security and usability: it doesn't have to be a trade-off. [Online]. http://www.telegraph.co.uk/connect/media-and-technology/security-versus-usability-ux-debate/

[51] National Research Council, "Towards better usability, security and privacy of information technology," 2010. [Online]. http://www.stern.nyu.edu/networks/Toward_Better_Usability_Security_and_Privacy_of_Information_Technology.pdf

[52] The usable privacy policy project. [Online]. https://www.usableprivacy.org/

[53] ENISA, "Good Practice Guide on Vulnerabilities Disclosure. From Challenges to Recommendations", 2015. [Online]. https://www.enisa.europa.eu/publications/vulnerability-disclosure

[54] Article 29 Data Protection Working Party, "Opinion 02/2013 on apps on smart device", 2013. [Online]. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf

[55] Jergej Dechand, Joseph Bonneau, Sacha Fahl, Henning Perl, Ian Goldberg, Matthew Smith Nik Unger. SOK: Secure Messaging. [Online]. http://cacr.uwaterloo.ca/techreports/2015/cacr2015-02.pdf

[56] D. Crawford, "A Complete Guide to IP Leaks, BESTVPN Guide 2015", 2015. [Online]. https://www.bestvpn.com/blog/31750/a-complete-guide-to-ip-leaks/

[57] M. V. Barbera, G. Tyson, H. Haddadi, and A. Mei C. Perta, "A Glance through the VPN Looking Glass: IPv6 Leakage and DNS Hijacking in Commercial VPN clients", in *Proceedings on Privacy Enhancing Technologies*, 2015, pp. 77–91.

[58] D.G. Kourie, J.H.P. Eloff V.D. Izadinia, "Uncovering identities: A study into VPN tunnel fingerprinting", *Computers & Security 25* , pp. 97–105, 2006.

[59] Article 29 Data Protection Working Party, "Opinion 5/2014 on anonymization techniques". [Online]. http://www.cnpd.public.lu/fr/publications/groupe-art29/wp216_en.pdf

[60] J. Parra-Arnau, C. Castelluccia J.P. Achara, "MyTrackingChoices: Pacifying the Ad-Block War by Enforcing User Privacy Preferences", *Cryptography and Security*, 2016.

[61] W3C Tracking Protection Working Group, "Tracking Preference Expression (DNT), W3C Candidate Recommendation", 2015.

[62] Article 29 Data Protection Working Party,"Opinion 02/2010 on online behavioural advertising", 2010. [Online]. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf

ENISA

European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vasilissis Sofias
Marousi 151 24, Athens, Greece

TP-07-16-139-EN-N

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-198-4
doi: 10.2824/475340