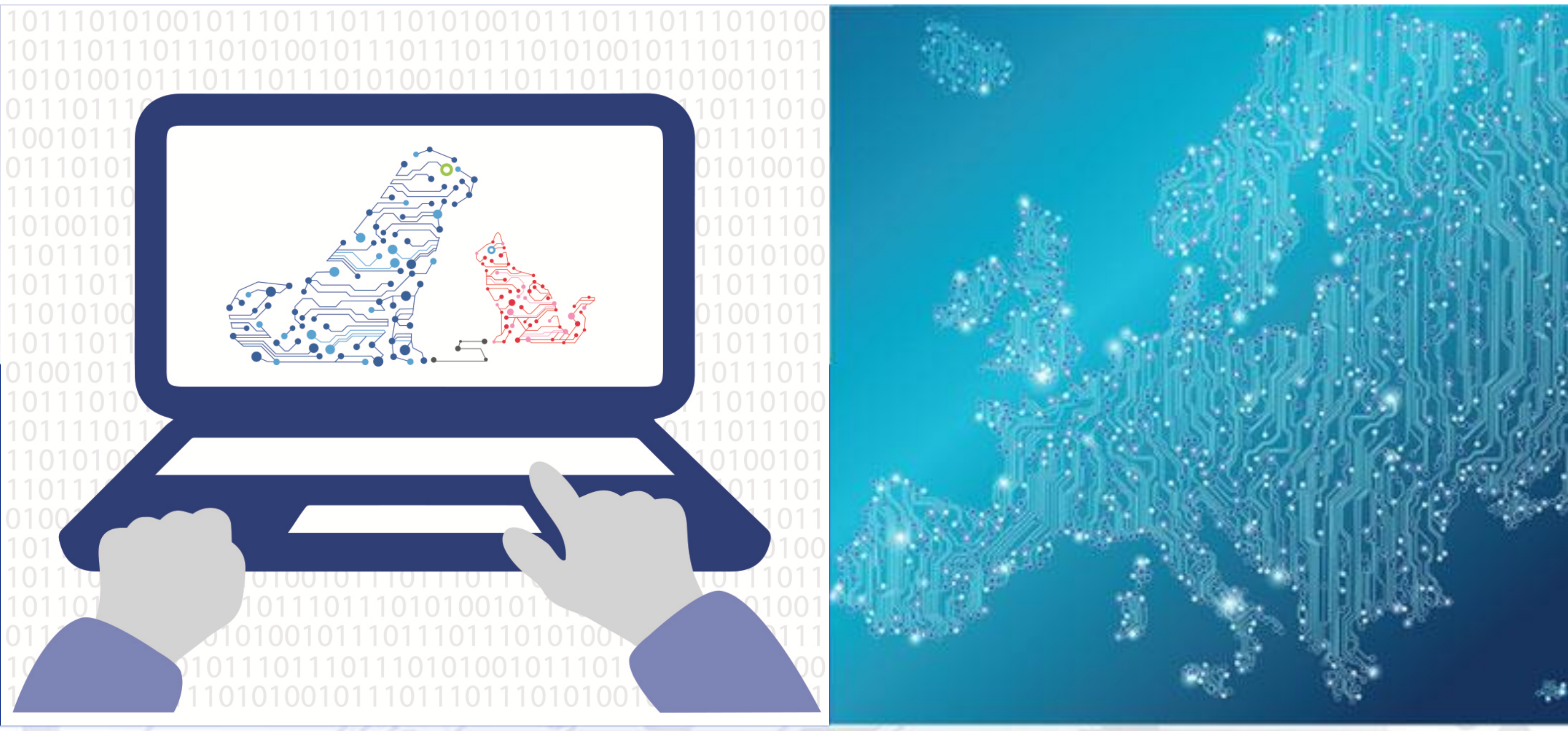


Online privacy tools for the general public

Towards a methodology for the evaluation of PETs for internet & mobile users

FINAL
1.0
PUBLIC
DECEMBER 2015

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.

Authors

Luis Hernández Encinas (CSIC-ITEFI), **Agustín Martín Muñoz** (CSIC-ITEFI), **Víctor Gayoso Martínez** (CSIC-ITEFI), **Jesús Negrillo Espigares** (CSIC-ITEFI), **José Ignacio Sánchez García** (CSIC-ITEFI), **Claude Castelluccia** (INRIA), **Athena Bourka** (ENISA)

Editors

European Union Agency for Network and Information Security
ENISA responsible officer: **Athena Bourka**
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 express our gratitude to the following individuals for providing valuable comments and support to this report:
Emiliano De Cristofaro (UCL), **Gwendal Le Grand** (CNIL), **Jean-Marc Manach** (freelance journalist), **Lothar Fritsch** (Karlstad University), **Simone Fischer-Hübner** (Karlstad University), and **Stefan Katzenbeisser** (TUD). Acknowledgement should also be given to **Glara Galan Manso** (ENISA) for her support and help in this report.

Legal notice
Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

ISBN: 978-92-9204-157-1, DOI: 10.2824/097859

Table of Contents

Executive Summary

Taking into account the increasing need for online data protection and the availability of numerous Privacy Enhancing Technologies[1] (PETs) for internet and mobile users, ENISA conducted, under its 2015 work programme[2], a study on online privacy tools, aiming at enhancing trust and assurance in their use by the general public. In particular, this study includes three parts: a) a review of existing web portals promoting the use of online privacy tools for the general public, b) a proposal for a methodology for evaluating the quality and functionality of PETs, and c) a pilot application of the proposed methodology in the area of anti-tracking browser extensions.

The review analysed several web portals that are listing and/or recommending the use of specific online privacy tools (e.g. for secure messaging, anti-tracking, encryption, etc.). The main focus was on the criteria applied for the selection (and further assessment) of these tools. The analysis showed that there are no commonly accepted methodologies and in most cases there is not even a description of the rationale used for selecting and recommending certain tools.

To this end, based on the results of the privacy portals' review, a number of criteria was defined relating to the reliability and usability of online privacy tools, especially when targeting the general public. These criteria set the basis for ENISA's proposal for a generic PETs evaluation methodology and are divided in three categories: basic, quality and functionality. The basic criteria are a preliminary set of fundamental characteristics that the tool should have (a threshold for proceeding with further analysis). They are related to the maturity and stability of a PET, overall maintenance (last update), reactivity to known vulnerabilities, ease of access and installation, availability of documentation. The quality criteria aim to assess generic quality features related to the reliability and usability of the tool. In that respect they include: background information for the tool, version history, transparency of installation and use, available public reviews, privacy by design and by default, ease of use, user interaction and side effects. Last, the functionality criteria assess whether the tool offers the promised functionality and features (in other words what the tool does and what it does not) and they differ for each area of privacy tools.

Following the proposed methodology, as part of the study, a pilot analysis of six popular anti-tracking browser extensions was also conducted. The results of the analysis is a comparative presentation of the tools, aiming at highlighting their differences and similarities and drawing relevant conclusions.

A generic methodology for evaluation of PETs

One of the main findings of this study is the need for a widely accepted methodology for the evaluation of PETs, which could enable a uniform presentation of their different aspects, thus supporting the general

[1] In the context of this report, PETs is also used to refer to privacy enhancing tools (or privacy tools).
[2] ENISA Work Programme 2015 including multi-annual planning, https://www.enisa.europa.eu/publications/programmes-reports/enisa-work-programme-2015

public 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 PET 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. Although only an in-depth technical analysis (e.g. code inspection) may provide certainty regarding a tool's functionality at a certain point in time, such a generic methodology could be very useful in evaluating PETs, serving as an indicator of their reliability and usability.

Criteria for evaluating PETs – open issues and further work

On top of the evaluation criteria already proposed in the report, several parameters still need to considered for a systematic assessment of PETs and there are extensive grounds for research and improvement in the field. A number of open issues where, thus, identified, for example relating to the assessment of privacy by design, the analysis of side effects (due to the use of PETs), the usability and accessibility assessment, performance and costs of PETs, relevant legal, ethical and societal aspects, etc. Taking into account the above points, this study should be seen as a step forward for opening this discussion and engaging all involved parties in it.

Providing guidance to the general public

A critical dimension of the proposed methodology is its' practical application and use for providing guidance to the general public. Several elements need to be discussed in this area, for example who is doing the evaluation, the extent that self-assessments (by PET developers) can be useful, visual and comprehensive presentation of results to internet and mobile users, maintenance of the information, etc. Awareness and education of the users is central in such an approach and different dissemination channels and methods can be applied, especially through social media platforms.

Building trust in online privacy: a combined effort

As a final remark, it should be noted that the promotion of online privacy enhancing technologies for the general public needs to be a combined effort of all involved stakeholders, such as the Data Protection Authorities, the privacy researchers, the independent privacy organisations and associations, the users of PETs, as well as the industry of PET developers. ENISA will continue its efforts in this field by bringing the different communities together and building the necessary expertise for this important task.

1. Introduction

Privacy and data protection are fundamental human rights and are strictly anchored within the EU legal framework[3]. Over the last years, ENISA has put considerable effort in these areas, providing technical guidance on key privacy technologies such as cryptographic techniques, trust frameworks and electronic seals, and supporting the ongoing discussions for the reform of the European data protection regime.

Following the recent revelations on mass surveillance of electronic communications[4], it is widely recognised that one of the most serious concerns today is the preservation of privacy when using internet and mobile applications. This concern has given rise to an increasing appearance of online tools, often open-source and/or freeware, affirming that they can offer certain privacy-preventive functionality for the average user, such as for example secure communication, protection against tracking, safeguarding of personal data, anonymous browsing, etc. However, in many cases the functionality of such tools is not as expected, for example due to lack of transparency on the tool's development and operation or lack of proper maintenance mechanisms. There are already a few known cases of tools declared as top privacy solutions that have been proven fraudulent[5]. Privacy enhancing technologies (PETs) that fail to offer what they promise can be very dangerous, as the false sense of protection can compromise the users' personal data and negatively affect or even put in harm's way their personal life.

Against this background, ENISA decided to carry out under its 2015 work programme a study in the area of PETs for the protection of online privacy (online privacy tools) with two main objectives: a) to define the current level of information and guidance that is provided to the general public and b) to provide a proposal for an assessment model for online privacy tools that could bring more assurance in their use, supporting their wider adoption by internet and mobile users. In particular, the study comprises three parts:

- A review of existing web portals promoting the use of online privacy tools by the general public.
- A proposed methodology for evaluating the reliability and usability of online privacy tools based on a set of predefined criteria.
- A pilot evaluation and comparative presentation of PETs in a specific privacy area.

[3] See the European Commission's data protection web site for a thorough overview of the underlying legal and regulatory framework, http://ec.europa.eu/justice/data-protection/index_en.htm; Also, the web site of the Article 29 Working Party for a list of opinions and other documents on specific data protection maters, http://ec.europa.eu/justice/data-protection/article-29/

[4] European Parliament, Committee of Civil Liberties, Justice and Home Affairs, "Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs", 2013, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2014-0139+0+DOC+PDF+V0//EN

[5] See for example: http://www.zdnet.com/article/charlatans-the-new-wave-of-privacy-profiteers/

In the following Chapters the three different parts of the study are described in detail. More specifically, Chapter 2 presents a number of initiatives listing and/or recommending the use of specific PETs, focusing especially on the scheme used for the selection of these tools. Based on the results of this review, Chapter 3 provides a proposal for an evaluation methodology for PETs, paying particular attention on their levels of reliability and usability. Chapter 4 then shows a practical application of this methodology in the area of anti-tracking browser extensions. Finally, Chapter 5 draws some conclusions and recommendations regarding the evaluation of online privacy tools, as a means for increasing trust and certainty in the field for the general public.

It should be noted that for the purpose of the study 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 considered in our work. Moreover, emphasis is mainly put on online privacy tools, i.e. tools designed to operate during an internet connection (e.g. anonymizers, secure instant messenger applications, etc.). Last, the study paid particular attention to open source tools, due to the fact that open software allows for independent evaluation by any interested party, thus increasing trust in the tool's functionality. Having said that, it is important to note that no in-depth security analysis of PETs (e.g. code inspection) has been part of this study. This is due to the fact that such an activity requires much specialised skills and at the same time it can only guarantee security at a certain point in time (and not beyond this). Still, such an analysis, whenever available, can provide useful input in the course of the methodology proposed in this document.

The target audience for this document includes all interested stakeholders in the area of privacy tools (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.

2. A review of web portals promoting online privacy tools

This review is the first part of our study and the basis to develop a methodology to evaluate online privacy tools. In particular, the scope of the review is to identify web portals promoting the use of selected PETs, analyse them against a set of parameters (relevant to the objectives of the study) and provide a comparative presentation of them, highlighting similarities, differences, strengths and weaknesses. The main focus of the analysis was on the methodology used for the selection of the proposed tools, as well as the overall quality and completeness of information offered to the general public. The review includes information gathered or elaborated by both public and private sectors in EU member states or third countries.

2.1 Identification of existing web portals

In order to identify initiatives which promote the use of privacy tools, a comprehensive review of websites and documents available online was made. The approach followed has been mainly based on web search, using several search engines to take advantage of different indexing methods. In addition, privacy and security experts from different domains (academia, industry, public sector) have been contacted to provide this review with specialised advice. Effort was made to reflect both European and international projects, as well as national initiatives in Europe and beyond.

Taking into account the objectives of the overall study, we considered explicitly initiatives fulfilling the following characteristics:

- Focusing on online privacy. This is the main topic of the review and most initiatives listed below fulfil this characteristic. Still in some cases privacy initiatives of broader scope were considered if they had an interesting evaluation/maintenance scheme for the selection and promotion of online privacy tools.
- Listing and/or recommending specific online privacy tools. This is a very important feature as it is closely related to the assurance level of PETs, especially if reviews and/or comparisons of tools are offered. As an example, a portal which includes reviews of certain PETs by privacy experts can enhance trust on the tools. As another example, a portal which enables users' reviews makes it easier also for other users to assess the usability and trust they can put on a certain tool.
- Targeting general public. Portals directed towards developers or similar specialised user groups are out of the scope.

Taking into account these characteristics, the most relevant web portals promoting the use of privacy tools identified through our review are provided in the Table 1 below (see Annex A for a more detailed description for each portal).

NAME/TITLE	ORGANISATION	URL	DESCRIPTION
Secure Messaging Scorecard	Electronic Frontier Foundation (EFF)	https://www.eff.org/secure-messaging-scorecard	A presentation and assessment of secure messaging apps and tools using a list of predefined criteria.
PRISM Break	Nylira (Peng Zhong)	https://prism-break.org	A selection of tools (per platform) against mass surveillance, such as encryption tools, anonymizers, etc.
Security in-a-box	Tactical Technology Collective and Front Line Defenders	https://securityinabox.org	General purpose security portal, including tools for the protection of privacy, such as encryption tools.
EPIC Online Guide to Practical Privacy Tools	Electronic Privacy Information Center (EPIC)	https://www.epic.org/privacy/tools.html	Offers lists of privacy tools classified under different areas (web browser add-ons, anonymizers, etc.).
The Ultimate Privacy Guide	BestVPN (4Choice Ltd)	https://www.bestvpn.com/The-ultimate-privacy-guide	General purpose security portal offering ratings for commercial VPNs. The privacy guide provides a list of tools classified per areas.
Free Software Directory	Free Software Foundation (FSF)	https://directory.fsf.org/wiki/Main_Page	General purpose portal for free software with specific area on security and privacy (main focus on encryption).
Privacytools.io	Privacytools.io	https://www.privacytools.io	Offers lists of privacy preserving tools, such as VPN, browser add-ons, etc.
Me & My Shadow	Tactical Technology Collective	https://myshadow.org	A portal focused mainly on digital traces and online tracking. It offers recommendations on various relevant tools.
Gizmo’s Freeware	Gizmo's Freeware	http://www.techsupportalert.com/content/free-windows-desktop-software-security-list-privacy.htm	General purpose freeware tools portal, offering also a list on open privacy tools.
Best Privacy Tools	Best Privacy Tools	http://bestprivacytools.com/	Offers list of privacy tools, especially chat apps, VPNs, secure browsing, etc.
Internet Privacy Tools	Internet Privacy Tools	http://privacytools.freeservers.com	Offers list of privacy tools, especially email filters, browser encryption, etc.
Reset The Net Privacy Pack	Fight for the Future and Center for Rights	https://pack.resetthenet.org	Offers list of free privacy tools and relevant advice (e.g. secure communication, anonymous browsing, etc.).

Table 1: Web portals promoting the use of online privacy tools for the general public

Apart from the web portals mentioned above, there are also many other internet sources where proposals for privacy tools can be found in a more generic way (for example as a special category of security software or as part of software directories[6]). Moreover, there are several private blogs that provide advice and recommendations on specific tools[7]. Last, plenty reports from various stakeholders (European institutions and agencies, Data Protection Authorities, independent privacy organisations, NGOs, etc.) advocate in favour of the wider adoption of online private tools by the general public, offering in some cases relevant recommendations and examples[8]. Although the content of such initiatives is very useful and relevant to our survey's objectives, we did not include them in our list, as the focus in only on dynamic material, presented in a structured way and offering specific recommendations and/or evaluations of different tools.

Moreover, it should be noted that there are many other quite advanced portals and web sites on information security, including portals from member states' public institutions, such as the ones of ANSSI (France), BSI (Germany) and INCIBE (Spain). Also several EU Data Protection Authorities have dedicated portals or web sites providing, among others, privacy recommendations and advice for the general public. Still such type of portals have not been considered in our review, since we are specialising explicitly in online initiatives promoting and/or recommending specific PETs.

It should also be mentioned that our analysis focused mainly on initiatives promoting open-source tools as it is possible to get more insight in their operation and they also offer the possibility for independent code review. Most of the initiatives listed in Table 1 have this characteristic. Still in some cases commercial portals with privacy tools were considered if they had an interesting evaluation/maintenance scheme for the selection of PETs.

2.2 Comparative analysis of web portals

Following the identification of the relevant web portals, we conducted, as part of this study, a more detailed analysis of each one of them, based on a set of predefined parameters. In particular, the parameters used are grouped under three different blocks, depending on their association with the site's content, the methodology followed for selecting or comparing the privacy tools, and the maintenance characteristics. Table 2 provides in more detail the aforementioned parameters and their descriptions.

[6] For example the Directory Mozilla (DMOZ), covering privacy among many other topics, www.dmoz.org

[7] As for example the blog of journalist and author Julia Angwin that provides tips about protecting online privacy and offers suggestions on the use of relevant protection tools, juliaangwin.com/privacy-tools

[8] See for example: European Parliament, Mass surveillance- part 1: risk, opportunities and mitigation strategies, 2015, http://www.europarl.europa.eu/RegData/etudes/STUD/2015/527409/EPRS_STU(2015)527409_REV1_EN.pdf

CATEGORY	PARAMETERS	DESCRIPTION
CONTENT	TYPE OF SITE	It describes the extent that the portal is dedicated to online privacy, e.g. whether it is explicitly addressing PETs (covering several topics or specializing in one or more privacy areas) or it is a general purpose security portal providing also guidance for privacy tools.
	TYPE OF MATERIAL	It indicates the type of information (on privacy tools) offered by the portal. As a minimum a list of PETs should be provided with a basic description of what the tool offers. A most interesting feature would be the provision of reviews and/or comparative assessments of privacy tools.
	PRESENTATION	It indicates how easy it is for the average user to browse the portal and find the desired information. This is obviously related both to the design of the user interface, availability of classifications per platforms and privacy areas, use of plain and understandable language, etc.
	NUMBER OF TOOLS	It indicates the number of privacy tools presented by the portal. This is of course related to the privacy areas that are covered by the tool and can be seen only as factor of providing greater choice to the general public.
	INTERACTION	It describes if users can provide their feedback to the portal and how this feedback is presented and taken into account. The most interesting feature in this perspective is the availability of active user forums where registered users can contribute with comments.
	OTHER FEATURES	It covers additional functionality not included under the previous parameters, e.g. availability of help wizard, multilingual support, etc.
METHODOLOGY	DESCRIPTION	It indicates if the portal includes a description of the methodology used for the selection/comparison of the listed privacy tools. The most interesting portals in that respect are those that do apply such a methodology and clearly describe it to anyone interested, thus allowing wider understanding regarding the choice of particular tools.
	EVALUATORS	It provides information on the persons that did the selection and evaluation of tools.
MAINTENANCE	FREQUENCY	It provides information on the maintenance effort exerted in order to keep the content up-to-date. Portals that are often updated (e.g. the last update is not later than six months ago) can offer more assurance regarding the proposed PETs.
	UPDATE DOCUMENTATION	It indicates the amount of information provided on the site about the last updates. The more information on updates is provided, the more trust a user can put on the content of the portal. Information can include list of added/removed PETs and the reasons for doing so.

Table 2: Parameters used for the analysis of web portals promoting the use of online privacy tools

Using the above criteria, we performed a more detailed analysis of each of the privacy tools initiatives. Based on this work, Table 3 below gives a comparative presentation of the different web portals.

	Content						Methodology		Maintenance	
Portal	**Type of site**	**Type of material**	**Presentation**	**No of tools**	**Interaction**	**Other features**	**Description**	**Evaluators**	**Frequency**	**Update documentation**
EFF Secure Messaging Scorecard	Online privacy (secure messaging apps)	Comparison of tools based on seven criteria (pass/fail)	Info on a single web page	More than 30 tools	No user forum, Contact EFF	N/A	Clear description of the criteria used	Names clearly described	Last update June 2015	Clear indication of updated material
PRISM Break	Online privacy, mass surveillance	List of privacy tools with short descriptions	Per platform and per type of tools	More than 30 tools	User forum	In 26 languages	No details on the criteria for selection of tools	No details provided	Last update Oct 2015	Clear indication of updated material
Security in-a-box	Security portal including privacy tools	List of privacy tools with descriptions and reviews (based on certain criteria)	Simple interface, info can be a bit complex to find	Less than 30 tools	No user forum	In 15 languages	Clear description of the criteria used	Names clearly described	Last update shown per tool	Sometimes update info is Included in the description of each tool
EPIC Online Guide to Practical Privacy Tools	Online privacy (several areas)	List of tools with short descriptions	Info on a single page	More than 30 tools	No user forum, contact via form	N/A	No details on the criteria for selection of tools	Names clearly described	Last update 2015	No indication of updated material
BestVPN Ultimate Privacy Guide	Security portal including privacy tools	List of tools with short descriptions	Info on a single page	More than 30 tools	No user forum, contact via form	N/A	No details on the criteria for selection of tools	Names clearly described	Last update of privacy guide in 2014	Some info on the changes is provided
Free Software Directory	Security portal including privacy tools	List of tools with short descriptions	Mainly for advanced users	More than 30 tools	User forum, libreplanet wiki	N/A	No details on the criteria for selection of tools	No details provided	Last update in 2015	Clear indication of updated material
Privacytools.io	Online privacy (several areas)	List of tools with description, (sometimes comparison)	Info on a single page	More than 30 tools	Via reddit	N/A	No details on the criteria for selection of tools	No details provided	No info on last update	No indication of updated material

	Content						Methodology		Maintenance	
Portal	**Type of site**	**Type of material**	**Presentation**	**No of tools**	**Interaction**	**Other features**	**Description**	**Evaluators**	**Frequency**	**Update documentation**
Me & My Shadow	Online privacy (several areas)	List of tools with short description	Simple interface, help wizard	More than 30 tools	No user forum	N/A	No details on the criteria for selection of tools	No details provided	No info on last update	No indication of updated material
Gizmo's freeware	Security portal including privacy tools	List of tools, sometimes with descriptions and links to external reviews	Info on a single page	More than 100 tools	User forum	N/A	No details on the criteria for selection of tools	Some names provided, no info on the contributors	Last update in 2015	Clear indication of updated sections in the portal
Best Privacy Tools	Online privacy (several areas)	List of tools with short description	Info on a single page	Less than 30 tools	No user forum	N/A	No details on the criteria for selection of tools	No details provided	No info on last update	No indication of updated material
Internet Privacy Tools	Online privacy (several areas)	List of tools with short description and sometimes reviews	Info on a single page	More than 30 tools	No user forum	N/A	No details on the criteria for selection of tools	No details provided	No info on last update	No indication of updated material
Reset The Net Privacy Pack	Online privacy (several areas)	List of tools with short description	Info on a single page	Less than 30 tools	No user forum	N/A	No details on the criteria for selection of tools	No details provided	No info on last update	No indication of updated material

Table 3: Comparative presentation of web portals promoting the use of online privacy tools

As expected, all the above mentioned web portals are focused on online privacy or have a specific section dedicated to it, although their approach towards selection of tools and maintenance of the site varies.

In particular, most portals provide a selection of tools with some description but without further analysis and/or comparison. Moreover, the rationale behind the particular selection of tools, so as to support the user's final choice, is usually not clearly explained. There are, however, a few cases were a specific methodology and/or set of criteria is applied, as for example the case of the EFF Secure Message Scoreboard where 7 criteria are used (and explained to the users) for the assessment of secure messaging applications. Another example is Security-in-a-box which provides a list of generic criteria that they apply for their selection, though without further detailing how these criteria have been taken into account in each of the selected tools.

Having said that, it is important to note that there is no uniform way of assessing online privacy tools even in the context of specific application areas, e.g. anti-tracking or encryption tools. Moreover, there is no uniform mechanism for the providers of such tools to offer relevant information about their products, e.g. in the form of PETs quality and functionality matrix. Such a facility could be of great use to the general public, as it would allow comparison of different online privacy tools, helping them to select the one that can be appropriate for their own case.

Another interesting element that came out of the review is the difficulty in maintaining the portal's information up-to-date and to accordingly inform the users about this. Although yearly updates seem to be feasible for most of the portals we examined, a complete changelog was available to the users only in a few cases. Still, this is an important element for building trust to the information provided, in particular the selection of online privacy tools.

Although not critical from the perspective of trust, the web portal's usability is another significant criterion for the overall promotion of privacy tools to the general public. As it has been shown in our review, many web portals promoting online privacy tools are not always user friendly, e.g. because of lack of plain language explanations or descriptions of tools. Classification of tools per platform and privacy area with short and to the point reviews can be of great help when presenting tools for wider public adoption. Another singificant element concerns the use of language on these resources: although English is the standard one, multilingual websites have a much greater chance to become practically of use to the general public.

Interaction with the users is also an essential element in the context of a privacy tools' web portal. The possibility of receiving feedback from users adds value to the content of the portal by addressing points of common interest, as well as by enhancing the portal's overall functionality. A suitable way to implement this could be to establish a procedure so that registered (and identified) users could contribute with suggestions, comments, and criticisms. That contribution, however, needs to be filtered before its publication in order to avoid inappropriate (e.g. offensive) content.

2.3 Requirements for an online privacy tools portal for the general public

Following the comparative analysis of web portals, it is clear that there are many interesting initiatives providing lists of online privacy tools for the general public. Still, we find that there is room for improvement both in providing more detailed guidance and analysis of specific tools, as well as presenting and maintaining the portal's material.

To this end, we list below the main characteristics that a privacy tools portal targeting the general public should ideally have:

- Guidance to the users
  The portal should offer proper guidance to the users for the selection and use of the online privacy tools, aiming at increasing their trust and assurance and supporting them in making an informed choice. Such guidance should include information on the privacy risks online, pointing to the different options of tools that can help mitigate these risks, as well as the criteria that the users should apply when making their choice. Moreover, it should offer reviews and/or comparison between different privacy tools (of the same category), highlighting pros and cons (weak/strong points) and providing subsequent information for their operation and use. It should ideally propose a list of recommended privacy tools (for different privacy areas). A list of non-recommended tools could also be a plus. As an additional element the PETs providers could also be invited to provide their own assessments for their tools using the same criteria (e.g. in the context of an open online PETs evaluation matrix). The methodology followed to perform the reviews and issue the recommendations must be adequately described, with a clear explanation of the evaluation criteria applied, as well as any other aspect relevant to the selection of certain tools. Moreover, adequate information should be offered about the experts who perform the selection and evaluation of the recommended tools.

- Maintenance
  The information provided, including the reviews and recommendations, should be frequently updated. Static information is soon useless. Furthermore, a log of changes should be provided, describing which tools have been added to or removed from the list of recommendations, and the reasons for doing so.

- User interaction
  The portal should enable feedback or even reviews by registered users or other external experts. This can be a very good way to actively involve the broader EU and international privacy community in the enhancement of the portal. Such contributions can improve the general knowledge about the tools, supporting the users to assess the usefulness and reliability of a given tool.

- Usability
  The portal should target the general public and, thus, it should be designed in a way that non-expert users can benefit from it. Proper classifications (e.g. per privacy area, per platform, etc.) and an easy to user interface could be very important elements for increasing usability, taking also into account wider web accessibility standards. The evaluations/reviews of the tools should also follow the same concept. Although the use of English language is usually the standard, providing multilingual content can be a plus for increasing general public involvement and awareness.

The above features can be used to enhance existing portals' functionality or in the framework of new initiatives in the field that are targeting the general public.

3. A methodology for the evaluation of online privacy tools

As shown in the privacy portals' review (Chapter 2), despite the availability of a great number of web resources listing online privacy tools, it is in many cases quite hard for the users to select among the variety of tools and even harder for them to assess whether the tools indeed offer what they promise. In order to provide further guidance and support internet and mobile users in selecting the right application, we find that there is a need for a generic methodology that could be used to review and/or compare different online privacy tools.

Having said that, it is important to note that evaluating PETs is not an easy thing. However, we find that, although only an in-depth technical analysis of the tools (e.g. code review) could provide a thorough insight on their functionality at a certain point in time, there are still a number of more generic elements that could be assessed, simply by using the tools and reviewing available public information. Such elements relate to the general quality and functionality characteristics of the tools, as for example information about their developers, the tools' maintenance level, their transparency regarding the processing of personal data, the provided documentation, etc. Although these elements alone cannot guarantee the trust level of a PET, they can still serve as indicators of the PET's overall operation, providing more confidence regarding what the tool does offer (and what it does not).

To this end, for the purpose of this study we propose an evaluation methodology for online privacy tools based on a set of general criteria that can be assessed by testing the operation of the PET in combination with publicly available information. No in-depth technical analysis is supposed to take place in the context of the methodology, although the results of relevant analysis for certain tools (if publicly available) could be a great source of information.

The scope of the methodology is threefold:

- Set a structured way for the evaluation of online privacy tools that can be used by privacy experts to provide relevant reviews/recommendations of tools (e.g. in the context of a web portal as the ones presented in Chapter 2).
- Allow the PETs developers to provide more structured information regarding their tools, using the proposed criteria, enabling in this way a uniform presentation of the different tools.
- Offer internet and mobile users the possibility to assess themselves the different criteria for their tool of interest before making their final choice.

The overall scope is, as already mentioned, to increase in one or more ways the availability of information/assessment of existing privacy tools, providing more guidance to the general public.

In the next paragraphs we first set a number of characteristics that are important for building trust in online privacy tools. Then, based on this set, we define the criteria for a PETs evaluation methodology with the above described aim and approach.

3.1 Building trust in online privacy tools

As a first step of defining the evaluation methodology, it is important to determine the parameters which could increase trust and assurance on a specific privacy tool, making it at the same time attractive for the general public. In other words it is important to outline what the desired characteristics of such a tool are in terms of reliability and usability, in order to have it further recommended to internet and mobile users.

In this context and taking into account relevant work of existing privacy tools initiatives[9], we define in the following list the most important generic quality features that an online privacy tool should have:

- Maturity and stability. It is very important for the tool to be mature and stable and to count with a responsible developer community. Tools that have been used for years in diverse environments or different operating systems (and versions) are usually more stable.
- Reactivity to vulnerabilities. A rapid reaction after the detection of a weakness or vulnerability is also important as an indicator of the level of reliability and security of a tool.
- Proper maintenance. The developers of a tool should provide an updated log of changes and improvements, showing clearly how bugs or other issues have been resolved, as well as what new features have been added to the tool.
- Adequate background information and documentation. The background of the entity proposing the tool or being responsible for its development should be available to the users. Also, technical documentation allows expert users to assess whether the best up-to-date technical criteria and parameters have been taken into account.
- Transparency. It should be clear from the provided information what the functionality of the tool is, i.e. what the tool does and does not offer. No software or other content should be installed without user consent. No personal data should be processed (e.g. transferred to other parties or used for analytics) without user's consent. Proper information regarding the processing of personal data is essential.
- Privacy by design and by default. The tool should follow the principles of privacy by design and by default. For example, personal data should be properly anonymised before further processed. As another example, the default settings of the tool should be preserving user privacy and its overall functionality should be well explained to the users.
- Positive public reviews. It is very useful to have positive public reviews on the tool, both by identified privacy experts and/or by the general public – end users. The reviews can provide good insights to the functionality of the tools, as well as identify potential drawbacks and considerations. The reviews should be as recent as possible.
- Usability. Several aspects can be considered under this feature:
  - Ease of installation: The installation process should be easy and straightforward, avoiding questions which can be a strong barrier for non-expert users.

[9] For example EFF Secure Messaging Scorecard and Security in-a-box web portals described in Chapter 2.

- User interaction: The existence of a reliable feedback mechanism for user contributions could help improve the functionality of the tool and support its user basis.
- User guidance: The tool should be accompanied with high-quality documentation (installation guide, user's manual, error guide, FAQ, etc.).
- User friendly: The use of the tool should be straightforward and should not require much training. No or very few technical support should be needed by the users.
- Multilingual: Although the use of the English language should be considered as a standard, including other languages would broaden the spectrum of potential users.
- Accessibility: the tool should be available to different categories of users (including elderly population and users with special needs), taking also into account relevant web accessibility standards.

In addition to the above generic features, an online privacy tool must also have the specific functional characteristics that it promises. These characteristics may vary considerably depending on the privacy area. The important element in that perspective is that the tool does not have any hidden functionality and that it is consistent regarding the privacy features that it claims to offer. Moreover, it is important that the tool does not have any security traps/bugs and that its use does not bring problems to the user (e.g. affecting other applications, very high utilisation of memory, etc.).

3.2 Criteria for the evaluation of online privacy tools

Following the desirable features of online privacy tools described above, we define in this section a set of criteria that can be used for the evaluation of PETs.

In particular, we define three broad groups of criteria:

- Basic criteria: a preliminary set of fundamental characteristics of a tool, setting the basis for evaluation.
- Quality criteria: criteria assessing generic quality features related to the reliability and usability of a tool.
- Functionality criteria: criteria assessing whether the tool offers the promised functionality and privacy features (differ for each category of privacy tools).

Table 4 provides an overview of the proposed basic and quality criteria, whereas Table 5 provides an example of functionality criteria in the area of anti-tracking browser extensions.

	CRITERION
BASIC CRITERIA	MATURITY AND STABILITY
	MAINTENANCE (LAST UPDATE)
	REACTIVITY TO PUBLICLY KNOWN VULNERABILITIES
	EASE OF ACCESS AND INSTALLATION
	DOCUMENTATION
QUALITY CRITERIA	BACKGROUND INFORMATION
	VERSION HISTORY
	TRANSPARENCY OF INSTALLATION AND USE
	PUBLIC REVIEWS
	PRIVACY BY DESIGN AND BY DEFAULT
	EASE OF USE
	USER INTERACTION
	SIDE EFFECTS
FUNCTIONALITY CRITERIA	TO BE SPECIFIED PER CATEGORY OF TOOLS

Table 4: Proposed criteria for the evaluation of online privacy tools

	CRITERION
FUNCTIONALITY CRITERIA FOR ANTI-TRACKING BROWSER EXTENSIONS (AN EXAMPLE)	TYPE OF BLOCKING/ ANTI-TRACKING BEHAVIOUR
	PROCESSING OF PERSONAL DATA
	FLEXIBILITY
	CHOICE
	ON/OFF
	HISTORY OF BLOCKED ELEMENTS
	BROWSER COMPATIBILITY AND SIGNATURE

Table 5: Functionality criteria for anti-tracking browser extensions

The above listed criteria are described in more detail in the next paragraphs.

3.2.1 Basic criteria

The basic criteria can be seen as the «first test» of a given tool against a set of preliminary necessary requirements that can be easily assessed based on existing publicly available information. The basic criteria can in fact serve as exclusion criteria: if even one of these requirements is not satisfied, the tool can be directly discarded with no further analysis of its quality or functionality. In other words, the basic criteria can be used to quickly reject certain tools without proceeding in a deeper evaluation. They can also be used (e.g. in the framework of a web portal as the ones presented in Chapter 2) as the threshold for providing lists of non-recommended tools.

In this context, we define the following list of basic criteria:

- **Maturity and stability**

  Maturity and stability are integral parameters for developing 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 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[10].

  In order to assess this criterion, it is important to evaluate both the time in the market but also the way the tool has evolved and improved over time. For example, a minimum period of three months would in most cases be considered necessary in order to test a tool's maturity and stability in the market. For a tool dating back a few years, the evolution of the tool (in terms of features added or removed over time, corrections of bugs, etc.) is a major element to assess. Public reviews of the tools can provide useful insight to this type of information.

- **Maintenance (last update)**

  The maintenance of tools is also a crucial parameter for trust, both in terms of security, as well as functionality. Updates need to be performed regularly, taking into account the type of the tool and the components that need to be maintained. For example in the case of browser plugins, often available in the area of anti-tracking tools, maintenance would naturally need to follow the latest versions of the relevant browser software.

  In order to assess this criterion, it is important to check the latest update of a tool, taking into account its overall functionality and dependency on other types of software.

- **Reactivity to publicly known vulnerabilities**

  This criterion is essential for the security of the tool to the extent that it can be assessed using publicly available information. As a first step, what needs to be assessed is whether any publicly known

[10] There is a lot of work in the area of maturity and stability evaluation for software, which could be taken into account in this respect. See for example: Justin Etheredge, "How Do We Measure Maturity In Software?," Code Thinked, http://www.codethinked.com/how-do-we-measure-maturity-in-software for a relevant discussion on the topic; Also ENISA's 2015 report on technology readiness for PETs, https://www.enisa.europa.eu/

vulnerabilities have ever been reported for a certain tool[11]. In case that a publicly known vulnerability is indeed found, what is important to assess is whether this vulnerability has been properly addressed, as well as the reaction time of the developers (between the discovery of the vulnerability and its resolution).

- **Ease of access and installation**

This criterion is related to the availability and usability of the tool and, in the context of this methodology, it is an important one for enabling use by the general public.

Ease of access refers to the effort needed by the user to locate and download the tool (and its potential updates). For example, it is preferable that the download page includes only the tool in study and it automatically selects the proper version of the tool based on the characteristics of the user's end device (operating system, 32/64-bit version, etc.). Tools that are hard to find and download will probably not be appealing to the general public.

Ease of installation is examined with regard to the effort and expertise that is expected from the user to install the tool (and its potential updates). In principle, the tool must have an installer or plugin directly available to the users, i.e. users should not be required to compile any source code before installing the tool.

Note that the overall usability of the tool is discussed later in the quality criteria. The reason that we address this particular point under the basic criteria is the fact that ease of access and installation might play a very critical role on the user's choice to further proceed with a tool. For example when the tool is not easy to find or when the configuration process is too complicated, the user would probably not consider the tool at all (no matter how good the offered functionality is). In that sense, it is a basic parameter that, in the context of our methodology, should be considered before addressing quality in detail.

- **Documentation**

Documentation is also an important element for enhancing use of the tool, as long as it is clear and understandable by the general public and is regularly updated. The assessment of this criterion should, thus, be based both on the availability of documentation, as well as its presentation (e.g. in the form of installation instructions, user guides, FAQs or Wikis).

[11] See for example CVE dictionary for publicly known security vulnerabilities and exposures, https://cve.mitre.org/

As already mentioned, the basic criteria should be checked as the first step of the assessment process. If a tool passes this test, then the criteria assessing its quality and functionality need to be applied.

3.2.2 Quality criteria

Quality aims at evaluating the overall reliability (in terms of privacy protection) and usability of the tools, taking into account that the scope of the assessment is to increase trust and assurance on the tools and putting special emphasis to aspects related to privacy and the protection of personal data.

In order to provide an objective and standardised assessment process, we propose a classification scheme for the evaluation of each criterion (Low (L), Medium (M), and High (H)). The scheme is based on quantitative information, wherever possible, so as to support the objectives of the evaluation, for example regarding the number of updates (in version history) or the availability of background information (yes/no). Still, in most cases a qualitative approach is needed, in the sense that the assessment cannot be solely based on a generic scale (such as for example the criteria on transparency or public reviews). Therefore, the classification mainly aims to provide possible scenarios or examples that could help the assessment. On top of this, we have tried to support the assessment process by providing guidance on the different aspects that need to be considered by the evaluator and the possible sources of relevant information.

To this end, the following list includes the proposed quality criteria:

- **Background information**

  User's choice of privacy tools may be supported by the provision of adequate background information regarding the tools' developers and/or the entities that are behind their overall maintenance and promotion. Although this criterion cannot be considered as directly affecting the reliability of a tool, still it is important for allowing the users to find useful information that could increase or decrease their level of trust on a certain tool (e.g. based on the expertise of the developers or the business model behind the operation of the tool).

  In the assessment of this criterion it is important to note that it is the availability and quality of clear background information that is being evaluated rather than the content of this information per se (e.g. no evaluation of the tool's developer's knowledge and expertise is taking place as part of this methodology).

  Classification/examples:

  - Low: no clear background information is provided regarding the entity that provides and supports the tool; no information regarding the tool's development and support team.
  - Medium: the organisation that provides the tool is well defined, without further information about the specific development and support of this tool.

- High: clear information is provided regarding both the tool's development, as well as the entity that is behind its' maintenance and support.

- **Version history**

A complete and documented version history is an important feature for building trust on a certain tool, as it permits potential users to check the evolution of the tool and, in some cases, understand how the developers have reacted to users' feedback or to the resolution of bugs. As part of this feature, it is also useful to provide update mechanisms that can inform the users about new versions and/or issues that have been added or resolved. This criterion is in fact a feature that can reveal the level and quality of maintenance of the tool.

Classification/examples:

- Low: there is no version history containing information about the new functionalities or the corrected bugs.
- Medium: some information on versioning is provided without specifically documenting the performed updates.
- High: a version history containing information about updated functionalities and corrected bugs is available; a mechanism for informing users about new updates is available.

- **Transparency of installation and use**

This criterion is mainly related to the transparency of the installation process, as well as the overall operation of the tool.

In particular during the installation process the user should be clearly informed whether any additional software is being installed (apart from the requested tool) or in general whether any other data is being stored and/or accessed in the user's terminal device (e.g. cookies). User's consent should be obtained before performing any relevant installation or access during the installation process of the tool or during its operation.

The user should also be clearly informed if any processing of his/her personal data takes place during the operation of the tool (e.g. transfer of user's personal data for analytics purposes). No processing of personal data should take place without prior user's consent.

Moreover, adequate information should be provided to the user regarding the functionalities of the tool (what it does and what is does not). Also, regarding the features that are enabled by default and those that the user needs to enable himself/herself.

In order to assess this criterion, it is important to check both the installation process and operation (default features, network traffic) of the tool, as well as the notice and information that is provided at the tool's web site.

Classification/examples:

- Low: the installation process and/or the operation of the tool are not transparent to the user. For example, it is not clear if changes to other applications or user settings are being performed during the installation process (e.g. changes in the selected search engine, homepage, tool bars, etc.). As another example, user's data are being further processed for analytics purposes without clear notice.
- Medium: the installation process is transparent to the user but the default operation of the tool is not as naturally expected. For example, a tool that is supposed to block advertising, it does not do so for certain companies without clearly informing the user about it.
- High: the installation process and operation of the tool are transparent to the user; the tool clearly informs the user about its default operation and the actions that need to be taken (if any) in order for the tool to reach its maximum privacy protection.

Note should be taken that for this particular criterion, the low value would imply possible unlawfulness of the tool and would, thus, directly exclude the tool from further being considered for evaluation.

- **Public reviews**

This is a special criterion as it can provide an overall insight of the reliability and usability of the tool based on feedback from other users. Its evaluation can in fact serve as input to the evaluation of all other criteria. Still, we preferred to address it separately as locating and assessing existing reviews is a special task in itself: it is not only important to identify relevant reviews but also to assess their quality, independence and accuracy. This is why this particular criterion is rather subjective as it is up to the evaluator to decide which information sources he/she can trust.

Reviews may come from specific experts or general users of the tool and they can take different formats (e.g. an article written by an analyst, an average rating provided by users at a software download centre, a prominent position at one of the existing portals promoting privacy tools). As already mentioned, it is the evaluator who will decide, based on his/her experience, if and how these reviews are worth being considered. Still what is most important to assess under this criterion is whether there are identified problems with a certain tool, especially hidden traps or information that is not directly available to the users (e.g. hidden monetization goals of anti-tracking tools whitelisting certain advertising companies or secretly selling users' personal data to advertisers). Also, public reviews can provide a useful criterion for the usability of the tool and the overall user satisfaction.

Classification/examples:

- Low: one or more public reviews outline a serious issue related to the installation or operation of the tool (e.g. possible hidden software installation, unlawful processing of users' personal data, functionality that is different than advertised/expected, etc.).
- Medium: some negative aspects can be found in public reviews but none of them is indicating any important functionality flaw (e.g. reviews are mostly about difficulty of use, complex interface, etc.).
- High: there are many reviews and most of them are positive; no or very few negative aspects can be found in public reviews e.g. indicating only minor usability problems.

Note that for this particular criterion, the low value could imply possible hidden unwanted functionality or even unlawfulness of the tool that could directly exclude the tool from further being considered for evaluation. This is of course very much dependent on the content and sources of the reviews and would, thus, need to be assessed separately for each different case.

- **Privacy by design and by default**

This criterion aims first of all to assess whether privacy and data protection have been considered in the overall design and implementation of the tool[12]. As outlined in the latest ENISA report in the field[13], privacy by design principles can be translated into certain design strategies, such as data minimization, anonymization, integration of proper notice and consent mechanisms, etc. Moreover, the purpose of this criterion is to assess whether the tool offers all its privacy preserving features by default, without the need for the user to configure it. Apart from the general configuration of the tool, what is also important to assess is the default behaviour of the tool and the particular features that the user needs to configure himself/herself so as to get the maximum privacy protection.

Classification/examples:

- Low: the tool asks users to provide their personal data in order to complete the installation although this is not necessary (e.g. in order to participate in a survey); the privacy features of the tool are not enabled by default.
- Medium: some privacy features are enabled by default but others need to be activated by the user through a complicated configuration process.
- High: the tool provides its maximum privacy preserving features without the need to configure it; no personal data are being collected and statistics are drawn only with the use of anonymous data.

[12] Privacy by design and by default have been introduced as new obligations for the data controllers and processors in the context of the European Commission proposal for the General Data Protection Regulation, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

[13] Privacy and data protection by design – from policy to enginnering, ENISA, 2014, https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design

- **Ease of use**

This criterion is aimed to cover the user friendliness of the tool, which directly affects its usability. Having said that, it is important to note that usability is related to the effectiveness, efficiency and user satisfaction[14] and, thus, it should in a way be assessed as part of most of the criteria already described. Although it is not the aim of this study to provide a detailed analysis for usability testing, it is important to note a number of parameters that need to be considered under the criterion for ease of use, such as the clarity of the user interface, the level of configuration that is needed by the users, the availability of customization options, etc. It is up to the evaluator (and his/her particular expertise) to address the above-mentioned parameters, taking into account the fact that the target group is the general public.

Classification/examples:

- Low: the tool requires complex configuration that is difficult for non-expert users; many of the tool's functionalities are hidden and not clearly explained.
- Medium: the main tool's functionality is achieved without need for further configuration but there are no customization options and/or the user has to spend a lot of time in order to find them.
- High: the main tool's functionality is achieved without need for further configuration; customization options are available and easy to configure; a help wizard or wiki can easily guide the user through the tool's functionality after installation.

It is important to note that usability of PETs is a topic that needs more thorough consideration, taking into account existing research in the field and addressing all relevant aspects. User accessibility (for example in relation to elderly users or users with disabilities) is also a core issue of usability, especially in the area of online privacy[15]. Another important aspect is to examine usability in relation to the reliability/trustworthiness of the tools, as it is not always easy to find the right balance between user friendliness and privacy protection. These issues have not been detailed in the context of our study and they should be subject of a specific analysis on the usability of PETs.

- **User interaction**

This criterion evaluates the support offered to the users of a tool, mainly in terms of addressing user comments, feedback mechanism, etc.[16]. It is important both for increasing the usability of the tool, as

[14] According to the International Standards Organization (ISO), usability refers to: "...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." See: ISO 9241-11:1998, "Ergonomic requirements for office work with visual display terminals (VDTs) -- Part 11: Guidance on usability," 1998, http://www.iso.org/iso/catalogue_detail.htm?csnumber=16883

[15] W3C Web accessibility initiative, "Introduction to web accessibility", https://www.w3.org/WAI/intro/accessibility.php

[16] Note that the availability and quality of documentation, which are also relevant to user support, are addressed under the basic criteria.

well as for integrating user comments and reviews as part of the tool's overall evolution. Moreover, well established user interaction mechanisms can help establish trust on the tool and create a supporting user community.

Classification/examples:

- Low: there is no way of user interaction with the developers/owners of the tool.
- Medium: users can submit comments/questions (e.g. by email or via web forms) but there is no active user forum where comments and relevant feedback are published.
- High: a well-established user interaction mechanism is available, including fast feedback mechanisms and an active user forum.

- **Side effects**

Another important criterion is the possible side effects that the tool's operation might have. These side effects can be twofold:

- Technical side effects for example related to the tool's CPU usage, possible overhead in network traffic, performance loss, possible false alerts in intrusion detection systems, etc.
- Blocking of access to certain web sites /services due to the use of a particular PET.

Although we find that this information is crucial for supporting an internet or mobile user to make his/her choice, we did not further address its practical assessment in our proposal, due to the fact that its analysis would probably require a deeper inspection of the tool's technical operation (especially in the case of technical side effects). Still, we tried to assess some of these aspects under the criteria of transparency and public reviews and we aim at further developing our methodology to better address this perspective.

On top of the criteria mentioned above, there are also some other parameters that, although they cannot be directly used as evaluation criteria, still they are quite important in the selection of a tool by the general public. These parameters are:

- Multilingual: Although English has been considered as a standard for the purpose of this study, it is still recognised that tools available also in other languages can increase adoption by the general public.

- Cross-platform: Tools available in multiple platforms can offer more options and flexibility to the users, making it easier for them to manage their privacy protection without the need to change their favourite applications. Depending on the specific tool, the software platform can be the operating system (as in the case of traditional applications), such as Windows, Mac, GNU/Linux, Android, iOS, or Windows Phone, or the web browser (as in the case of plugins or add-ons), e.g. Firefox, Chrome, Internet Explorer, Opera, or Safari.

Last, it should be noted that as part of the evaluation it is important to address what jurisdictions the tool is compliant with and in particular whether it is consistent with EU data protection legal framework. Also other legal considerations should be taken into account, for example regarding individual property rights or export restrictions if applicable.

3.2.3 Functionality criteria

Based on the functional privacy area which the tool belongs to, during the analysis it will be necessary to consider a specific set of criteria directly related to the functionality of the tool. This set of criteria will in fact assess to what extent the tool does what it claims in terms of protecting user privacy and personal data.

Clearly, functionality criteria will differ depending on the privacy area. To this end, it is first of all important to define the expected privacy features/characteristics of the tool. This will help determine its core functionality, as well as any optional/desirable functions that a tool (under a certain privacy area) could offer.

As an example we provide in the following a list of functionality criteria that we drew for the area of anti-tracking browser extensions (plug-ins/add-ons).

3.2.3.1 Example: Functionality criteria for anti-tracking browser extensions

Anti-tracking browser extensions (plug-ins/add-ons) aim at blocking attempts of certain websites to record the internet activity and other personal information of a web user (e.g. visited web page, user location, type of browser, etc.) and/or present content to the user. In particular, they are usually intended to block one or more of the following elements:

- Advertisements (e.g. in the form of a banner, images, etc.).
- Scripts (e.g. Java, JavaScript, and Flash scripts).
- Pop-ups.
- Cookies.
- Other elements (e.g. social buttons, such as Facebook, Google, Twitter, etc.).

Main functionality (type of blocking/anti-tracking behaviour)

In most cases, the tools block one or more of the above mentioned elements, providing also information to the user about the service that is trying to capture personal data, the processes and connections that are active and the number and types of elements that have been blocked. Besides, they can offer real-time information about user’s activity, the hosts and ports that are being used, etc.

Processing of personal data

An anti-tracking tool is expected to protect a user from being tracked when surfing the web, offering the functionality described above. It should not be used for the processing of user's personal data (e.g. online behaviour, favourite ads) for analytics or other purposes without user's consent. No hidden activities affecting users' personal data (e.g. by whitelisting specific advertising companies or secretly selling user's data to advertisers) should be acceptable.

Additional features

- Flexibility: The tool could allow users to personalize the way it is used, e.g. what and how is blocked (varying from single webpages to full domains). This option could be offered in various ways, e.g. white/black listing, filtering options, etc.

- Choice: The tool could provide the possibility for the user to temporarily block/unblock a specific element (emerging windows, advertising, trackers, etc.). This can be very useful, e.g. if the user would like to allow graphs from a certain company, while images from all other companies would be blocked.

- On/off: The tool could allow users to pause the blocking/unblocking process (as a whole and not only for a specific element).

- History (of blocked elements): The tool could make it possible for the user to check what has been blocked. Although this is only informative, it may be very useful for users to be aware about the attempts of tracking their behaviour while surfing the web. It could be up to the user to define how the history of blocking is presented.

On top of the criteria mentioned above, there are also some more generic features that are applicable to browser plugins and add-ons and could be quite essential also in the case of anti-tracking tools. These are:

- Browser compatibility: The tool could be available as a plugin or an add-on in the corresponding official store of the evaluated platform (Firefox, Chrome, etc.). This may be seen as an additional guarantee that the tool is going to be downloaded from a safe place.

- Signature: Singed plugins (which can be found when using a plugin locator menu option) may provide additional security guarantees.

Following the criteria described above, in the context of the assessment of anti-tracking tools, the evaluator would first have to check the main functionality of the tool, trying to identify any issues affecting the user's privacy (e.g. due to lack of proper information or hidden operations of the tool). Then the other functional criteria would also be examined. The result of this evaluation would be a list of what the tool offers and what it does not offer, including ideally its pros and cons and outlining any serious functionality issues.

4. A pilot evaluation of anti-tracking browser extensions

4.1 Scope of the pilot

This chapter provides a pilot analysis of anti-tracking browser extensions (plug-ins/add-ons) following the methodology that we defined in Chapter 3. The focus is on applying the predefined assessment criteria on a number of well-known browser extensions that can be used for blocking online tracking, as well as provide a comparative presentation of the different tools. The aim of the pilot is to demonstrate the practical application of the proposed methodology, serving as the basis for evaluations of privacy tools in the future.

There is a great variety of anti-tracking tools today, offering different options and functionality. For the purpose of the study we selected six of the most popular anti-tracking browser extensions that are listed in many of the web portals we identified in Chapter 2. Our selection was based on the popularity of the tools, as well as the fact that they cover different types of functionalities in the field. In particular, the tools we considered were as follows:

- Ghostery[17]
- Disconnect[18]
- uBlock origin[19]
- Privacy badger[20]
- NoScript[21]
- AdBlockPlus[22]

All of the above-mentioned tools satisfy the set of basic criteria, as they date already some years with a specific development team, their latest updates where less than six months old at the time of our study, no publicly known vulnerability is reported, they are all easy to access and install and they provide relevant documentation. Therefore, in the context of our pilot we focused our analysis of the tools on the quality and functionality criteria described in Chapter 3.

It is important to note again that our analysis is based solely on criteria that can be evaluated via publicly available information and/or the test installation and use of the tool. Still, only an in-depth security analysis (e.g. code inspection) can guarantee the functionality of a tool at a certain point in time. Such an analysis was not part of our pilot.

[17] www.ghostery.com
[18] disconnect.me
[19] github.com/gorhill/uBlock
[20] https://www.eff.org/privacybadger
[21] noscript.net
[22] adblockplus.org

It must also be mentioned that for the scope of the pilot the only platforms that have been considered are Firefox and Chrome due to the fact that they have similar characteristics (e.g. official add-on store) and they represent an important percentage of the browsing quota today.

4.2 A comparative presentation of six anti-tracking browser extensions

Following the approach and analysis mentioned above, Table 6 resumes the main functionality and features of the six selected anti-tracking tools, whereas Tables 7 and 8 summarize their specific quality and functionality characteristics. Annex B provides a more detailed description per tool.

TOOL	WHAT IT DOES	ADDITIONAL FEATURES	CONSIDERATIONS
Ghostery	Blocks several types of elements (cookies, scripts, ad networks, social buttons, etc.). Trackers are classified in five categories (analytics, web beacons, privacy, advertising, and widgets). Shows what has been blocked in each site during the session. Has an editable whitelist.	Click-to-play functionality enables unblocking of useful widgets (e.g. a comments form or an embedded video player). Very efficient memory usage. Configuration tutorial after installation.	Blocking is not enabled by default (but needs to be activated by the user). The Ghostrank option, when activated, allows selling of info related to blocked ads to advertising companies. Evidon, the company behind Ghostery (also an advertising company) claims that no personal data are being processed. Still, this topic raises ethical issues for some users. Ghostrank is deactivated by default.
Disconnect	Blocks several types of elements (cookies, scripts, ad networks, social buttons, etc.). Presents trackers in four categories: advertising, analytics, social networking, and content, plus three specific buttons for Facebook, Google and Twitter. Shows what has been blocked in each site during the session. Whitelist available (not editable).	In Chrome, it shows users who is tracking them with a collusion graph. Automatically reloads the page after a change in the filtering options. The dashboard shows the time and bandwidth saved.	After installation, a tab asks for financial support without any «exit» or «no support» button (the only option to avoid it is to close the tab or to select the «Tour the interface» button). This can be confusing for non-expert users.
uBlock origin	By default it blocks advertising, malware domains and social buttons. By enabling more lists more elements can be blocked (e.g. analytics). Shows what has been blocked in each site during the session (through the requests register). Has an editable whitelist.	Great CPU and memory performance. Very fast page loading. Great customization capabilities (importing of host files, third party filters selection, editing user's filters and rules). It is possible to enable an option to stop WebRTC from revealing local IP addresses of VPN users.	Sometimes (and depending on how the strict blocking option is set), some sites cannot be accessed (although the user is informed, and buttons appear to allow him/her to change the configuration at a permanent- or temporary basis). A little bit difficult to configure by a non-expert user. To see what has been blocked it is necessary to go to the requests register.
Privacy Badger	Blocks several types of elements (cookies, scripts, ad networks, etc.)	Its dynamic blocking behaviour, increases ease of	Due to its way of operation, it requires browsing around several different websites to start blocking.

TOOL	WHAT IT DOES	ADDITIONAL FEATURES	CONSIDERATIONS
	It builds its blocking list as the user navigates through different pages (dynamic). In each session, it shows the potential trackers and whether they have been blocked or not. In the configuration it records all potential trackers identified and those which have been blocked so far. Has an editable whitelist.	use and requires very little user configuration. It can detect canvas based fingerprinting. More advanced integration of Do not Track (DNT) – compliance with EFF DNT. Shows a tutorial after installation.	If a site is included in the whitelist, the configuration button disappears from the user interface.
NoScript	Blocks scripts (it blocks advertising or any other element provided that they include script). Allows selecting whether to block JavaScript, Adobe Flash, Microsoft Silverlight and other similar programs. Shows what has been blocked in each site during the session Has an editable whitelist.	Great customization options It does not rely on a virus/vulnerability database (good for unknown threats). Prevents «Clickjacking» and cross-site scripting attacks. It can be configured to automatically reload the page after a change in the blocking options.	It only blocks scripts. Time-consuming setup, otherwise pages with many scripts can be not properly displayed. This can be hard for non-experts. Only available as an extension for Mozilla-based browsers.
AdBlock Plus	It is primarily an ad blocker rather than an anti-tracking tool. Ad blocking is done by default, except from ads coming from the «acceptable ads» whitelist. It can be configured to block trackers, social buttons, and malware domains. Different functionalities are available for Firefox and Chrome. It is possible to check what has been blocked, but only in Firefox. In Chrome it is only possible to check the number of blocked elements. Has an editable whitelist in Chrome.	Wild cards allow blocking of specific sections of a domain (granularity). It allows selecting third party filters, and edit user's filters. Via context menu, images in a page can be blocked. Additionally, (only in Chrome) specific elements can be blocked via context menu or through user interface.	The default operation only blocks advertising. Any other type of blocking needs to be activated by the user. If this activation is not done directly after installation (through a tab that is automatically opened), it is quite difficult to do it later. It includes an acceptable ads whitelist (include ads from Google and Microsoft), which is enabled by default. The user needs to deactivate it in order not to receive ads from the companies in the list. High RAM penalty and CPU intensive.

Table 6: Summary of tools' functionality

	GHOSTERY	DISCONNECT	UBLOCK ORIGIN	PRIVACY BADGER	NOSCRIPT	ADBLOCKPLUS
Background information	Originally developed by David Cancel, later acquired by Better Advertising and finally by advertising company Evidon. Since April 2014, it is Ghostery, Inc.	The company behind the product is Disconnect, the development team is well defined (disconnect.me/team).	The main developer is Raymond Hill (the original developer behind uBlock) (github.com/gorhill)	It is an EFF project. The current maintainers are Cooper Quintin and Noah Swartz (www.eff.org/es/about/staff/)	Its author is Giorgio Maone (maone.net)	Developed by eyeo (eyeo.com). Team led by W. Palant (eyeo.com/en/team).
Version history[23]	List of new versions and corrected bugs in Firefox store.	List of new versions and corrected bugs in Firefox store.	List of new versions and corrected bugs in Firefox store and in the developer's page at GitHub (for Firefox and Chrome).	List of new versions and corrected bugs in Firefox store and in the developer's page at GitHub (for Firefox and Chrome).	List of new versions and corrected bugs in Firefox store.	List of new versions and corrected bugs in Firefox store and at AdBlockPlus site (for Firefox and Chrome).
Transparency of installation and use	Installation and operation are transparent to the user. Participation in Ghostrank is asked in way that may be confusing for non-experts. Same is true for user participation in the Ghostery survey (after installation).	Installation and operation are transparent to the user. Once installed, a tab asks for financial support without any «exit» or «no support» button, which may be confusing for non-experts.	Installation and operation are transparent to the user.	Installation and operation are transparent to the user.	Installation and operation are transparent to the user.	Transparent installation process. Acceptable ads will not be blocked by default and user is not clearly asked to deactivate them.
Public reviews	It has good user reviews. The most important complaints made by users is the Ghostrank issue and bugs in the Android version.	It has good user reviews. The main complaints are related to the lack of updates and the failures when accessing some web sites.	It has good user reviews, highlighting its performance and the involvement of its developer in the tool's enhancement.	It has good user reviews. The most usual complaints are about the failure to manage correctly some web pages and the need to fine-tune its algorithm.	It has good user reviews. The main complaint is about its difficulty to use for non-experts, and the lack of a version for Chrome.	It has good user reviews as an ad blocker. The most serious users' complaint is about the «acceptable ads» policy.

[23] Analysed only for Firefox and Chrome.

	GHOSTERY	DISCONNECT	UBLOCK ORIGIN	PRIVACY BADGER	NOSCRIPT	ADBLOCKPLUS
Privacy by design and by default	Blocking is not enabled by default (needs to be activated by the user).	Blocking is enabled by default, except from the Content category that needs to be activated by the user.	Blocking is enabled by default.	Blocking is enabled by default.	Blocking is enabled by default.	Blocking of ads is enabled by default, except from the acceptable ads whitelist. The user needs to deactivate this list. Blocking of other elements is not enabled by default (the user needs to activate it).
Ease of use	Although the interface is not complicated, some configuration options could be difficult for non-expert users. Several customization options.	Easy and informative user interface. Several customization options.	Easy and informative user interface. Several customization options, including filter editing.	Easy and informative user interface. The tool learns and develops its anti-tracking features while the user browses through different web pages.	The tool is difficult to use by non-expert users, as they must take decisions about which scripts to enable in order to correctly view many websites.	Easy and informative user interface Blocking images is possible via the context menu – in Chrome, elements can be blocked via user interface. Customization options in Firefox.
User interaction	User forum. Interaction is also possible via a web form.	User forum. Also e-mail support.	User forum.	Two user forums for Firefox and Chrome. Also e-mail support.	User forum. Also e-mail support.	User forum. A blog is also available.
Other information	Available in more than 15 languages. Multiplatform (Opera, Firefox, Chrome, Safari, IE, Android and iOS).	Only in English. Multiplatform (Opera, Firefox, Chrome, and Safari).	Available in more than 30 languages. Multiplatform (Chrome, Firefox, Opera, and Safari).	Available in 5 languages. Available for Chrome and Firefox.	Available in more than 40 languages. Available for Mozilla-based browsers (e.g. Firefox).	Available in more than 25 languages. Multiplatform (Chrome, Firefox, IE, Safari, and Opera).

Table 7: Presentation of quality analysis of the tools

	GHOSTERY	DISCONNECT	UBLOCK ORIGIN	PRIVACY BADGER	NOSCRIPT	ADBLOCKPLUS
Flexibility	Editable white/black lists. Enabling or disabling different categories of trackers (as a whole).	White/black lists.	Editable white/black lists, filter editing and selection of third party filter lists.	Editable white/black lists.	Editable white/black lists, filter editing, and many other customization options.	White/black lists (only in Chrome), user's filter editing, and selecting third party filter lists. In Firefox filters can be enabled/disabled in a given list.
Choice	Possibility to block/unblock trackers. It is possible to unblock an element in a page, so that it is always enabled for that page (even if disabled for other pages).	Possibility to block/unblock trackers (classified under different categories). Specific block/unblock for Facebook, Google and Twitter.	Possibility to block/unblock trackers (interactively via context menu or user interface).	Possibility to block/unblock tracking domains (entirely or only their cookies).	Possibility to block/unblock scripts (interactively via context menu or user interface).	Possibility to block/unblock trackers (interactively via context menu or user interface – only for Chrome).
On/off	Possibility to pause blocking and unblocking (affecting all tabs).	Possibility to pause blocking and unblocking (for the full domain of the current page by means of the «Whitelist site» option).	Possibility to pause blocking and unblocking (for the full domain or only for the current page).	Possibility to pause blocking and unblocking (for the current page).	Possibility to pause blocking and unblocking (either for the current page, or for the full domain).	Possibility to pause blocking and unblocking In Firefox: only for current page, for the full domain, or for all tabs. In Chrome: only for the full domain.
History	Possibility to check blocked elements.	Possibility to check blocked elements.	Possibility to check blocked elements via the requests register.	Possibility to check blocked elements.	Possibility to check blocked elements.	Possibility to check blocked elements in Firefox.
Browser comp/bility signature	Plugins in official store (Chrome, Firefox), not signed.	Plugins in official store (Chrome, Opera, Firefox), signed for Firefox.	Plugins in official store (Chrome, Firefox), not signed.	Plugins in official store (Chrome, Firefox), not signed.	Plugins in official store (Firefox), not signed.	Plugins in official store for Firefox and Chrome, not signed.

Table 8: Presentation of functionality analysis of the tools (additional features)

With the help of the previous information, it can be said that there are no major functional differences between most of the analysed tools, in the sense that all of them protect user's privacy by preventing user's activities to be tracked. Ad, cookies and script blockers give the users control over their browsing experience. They can block ads on the visited sites and kill scripts and widgets that send users' data to unknown third-parties. Still some functional differences can be found, for example AdBlockPlus is primarily an ad blocker rather than an anti-tracking tool, uBlock origin also primarily works with ads (but not only), NoScript is only for preventing scripts from running while browsing.

All the tools are quite popular and provide plenty of support information (e.g. background information, version history), user forums, as well as many configuration options.

However, there are some differences regarding the default privacy preserving functionality and transparency to the user. For example, AdBlockPlus allows acceptable ads and this option is enabled by default, although the user is informed about this fact. Privacy Badger or Disconnect block tracking cookies and scripts from running by default, while Ghostery does not block any tracker by default (the functionality needs to be enabled by the user).

Also, there are differences regarding the way the different tools operate, but details are only for advanced users. As an example, Privacy Badger does not use standard lists but follows a behavioural blocking process (learning user preferences while browsing). This can very useful in some cases, as it could enable blocking of a tracker that is not included in standard lists. However, with this approach the tool might take longer to build its own anti-tracking list (because the user needs to browse around several different websites for the tool to learn what to block).

Differences can also be found regarding the overall performance of the tools. For example uBlock origin has very good CPU and memory utilization, whereas AdBlockPlus is CPU and RAM intensive. However, with uBlock origin some sites might not be accessed without proper configuration of the tool's properties.

Looking at Tables 6 to 8 it is possible to provide tips which can serve as guidance for different types of users. For example, advanced users interested in having the possibility of including filters, should select uBlock origin, NoScript or AdBlockPlus. Disconnect users who want to see in a collusion graph what connections are activated when a web page is visited and which of them are blocked, should install the Chrome version. Users aiming to use an online privacy tool but do not want to be worried about any configuration process (even though this can be assisted through a wizard) should use Disconnect or Privacy Badger. A user who is interested in defining white or black lists to improve his/her browsing experience could select any of the tools. Similarly, if temporary blocking/unblocking is needed, all tools could be used (uBlock Origin and the Chrome version of AdBlockPlus allows to select what to block via context menu or the user interface; context menu is also available for AdBlockPlus users in Firefox, but only to block images).

Available public reviews also provide tips and recommendations to help users decide which tool to choose. For example, a recent review[24] recommends using both, Ghostery and Disconnect. The reason is that, although Ghostery blocks more trackers, there are many (even popular) trackers that it misses which are actually blocked by Disconnect, and vice versa[25]. In the same review, Privacy Badger is also recommended, highlighting that none of the add-ons makes the other one redundant.

A general conclusion that can be drawn from our analysis is that a clear description of the functionalities of the tools is needed, in order for the user to understand what exactly he/she needs and make the best possible choice. In many cases, tools would need to be complemented in order to provide for maximum protection in a specific privacy area.

[24] A review on tracker and script blocker extensions for Firefox: log.add0n.com/2015/05/16/tracker-and-script%20blocker-extensions-for-firefox.html

[25] See also: The best browser extensions that protect your privacy: lifehacker.com/the-best-browser-extensions-that-protect-your-privacy-479408034

5. Conclusions

The goal of this report has been to support the protection of online privacy by using PETs. Despite the availability of different tools and technologies, information provided is not always sufficient to guide internet and mobile users and help them select the PET that is most appropriate for their needs. Following a review of existing web portals promoting PETs, this report sought to identify the elements that could build trust and assurance for the general public when making their choice. The conclusions of our work and relevant open issues are listed below.

The need for a widely accepted methodology for the evaluation of PETs

Assessment of online privacy tools and comparison between different tools of the same category can assist internet and mobile users in understanding the options they have and make an informed choice. Although there are several web portals listing and/or recommending privacy tools, there is no uniform methodology for assessing the selected tools (and in many cases there is no methodology at all). It appears that that the definition and adoption of such a methodology both by the PETs developers, as well as by the greater privacy community, could greatly support an objective evaluation of the tools' quality and functionality, providing valuable output for the general public. The methodology should be based on specific predefined criteria (e.g. in the mode of an evaluation matrix) that could be used to assess different aspects of an online privacy tool. It could be applied both by privacy experts providing reviews and/or comparisons of tools and/or by the PET developers (in the course of a self-assessment practice). More advanced users could also apply the criteria of the methodology to assess certain aspects of their preferred online privacy tools. Although only an in-depth technical analysis (e.g. code inspection) can provide certainty regarding a tool's functionality at a certain point in time, we believe that such a generic methodology can still be very useful in evaluating PETs, serving as an indicator of their reliability and usability.

Criteria for a generic methodology for PETs evaluation

In the context of this report we proposed a number of criteria that could be used to develop a generic methodology for the evaluation of online privacy tools (basic, quality and functionality criteria). Having said that, it is important to note that evaluating PETs is not an easy task. Several parameters need to be considered and there is a lot of area for research and improvement. To this end, our proposal should be seen as a step forward for opening this discussion and engaging all involved parties in it. Still, there are many questions that need to be answered and further detailed, such as:

- Trust on the authors/developers/providers of the tool: The access to background information relevant to the tool is in most cases easy to achieve. Still, how can we assess the expertise of the entity behind the tool and how much is this relevant to the tool's functionality? (e.g. if it makes any difference that the tool is created by a known privacy expert rather than an unknown developer and at what extent).

- Companion tools: In many cases a tool alone would not be enough to protect the user. Combined use of different tools would probably enhance full protection in a certain domain. Recommendations of tools should take this into account and, to this end, the evaluation methodology should define not only what tools offer but also what they do not offer. In what detail can this be done?

- Privacy by design: Although some elements might be easy to check, still further research is needed on the practical evaluation of whether privacy has been an integral design element of a specific tool. At what level can this be performed and how can it be connected to the relevant legal obligations for the protection of personal data?

- Side effects: Does the tool «break» other applications or does it invalidate certain functionalities? Does it introduce any security risk? These are only some of the possible side effects of the tool that would probably demand a more in-depth technical insight in its functionality.

- Exclusion: Does the use of tool prevent the user from accessing certain sites or services (e.g. certain anti-tracking tools being blocked by specific sites)? It is important to address the extent that this element can be assessed and whether any practical solutions or tips can be offered to the users.

- Technology readiness: The maturity level of the tool (e.g. prototype or commercial product) is another dimension that needs to be considered. ENISA has addressed this topic with a specific report in 2015 and the results of this work need to be taken into account also for the assessment of online privacy tools for the general public.

- Usability: Many different aspects need to be taken into account for a thorough assessment of usability in different phases, including installation process, update configuration, regular utilisation, and de-installation. Relevant research in the field (e.g. with particular user groups) needs to be considered, including also conformity with web accessibility standards. It is also of utmost importance to examine usability in relation with all the other parameters, as the most easy-to-use tools are not necessarily the best in terms of privacy protection (but still if not easy enough, they are useless for the general public). The right balance between usability and protection is an aspect for further consideration.

- Performance and costs: How well does the tool perform its tasks and what is the cost of using it (e.g. financial cost, CPU, battery, network traffic)? This is also an important dimension in terms of cost benefit analysis for a certain tool.

- Legal, ethical and societal aspects: Many issues need to be discussed under this area. For example, which privacy legislation was the tool designed for and does it comply with the EU data protection legal framework? Are there any other legal concerns regarding its use (e.g. intellectual property rights)? Is the use of the tool ethical? The answer to these questions might not be easy and would probably require additional testing against legal provisions and involvement of legal experts.

- Open code: Although the aim of the methodology would not be to promote only open source tools, it is widely recognised that the availability of open code can increase trust as it allows for independent reviews. It is important to explore this dimension further, considering also relevant performed code audits for certain privacy tools (if applicable).

Apart from the issues mentioned above, it is important to test the criteria and their practical applicability with specific tools. In the course of our study we were able to do so to a limited extent with the pilot on anti-tracking tools but more testing and in several privacy areas is required.

Providing guidance to the general public

Together with the generic methodology, another important aspect to consider is the way that the methodology can be used in practice, as well as the type of guidance to be provided for the general public. Several elements need to be considered in this area, such as:

- Evaluators: Who performs the evaluations of tools and how their level of independence can be guaranteed? This is an important issue and it requires synergies between involved parties (e.g. privacy web portals and known experts in the field). In case of self-assessments (performed by the PETs developers), how can the accuracy of the provided information be guaranteed? To what extent can self-assessments be useful in the context of evaluating PETs?

- Presentation: It is important to provide the information on different privacy tools in a way that the general public can really benefit from them. To this end, visual representations and graphics can greatly help, together with plain language and clear definition of functionalities of the tools.

- Maintenance: This is also of utmost importance, as evaluations can only show the tool's state at a certain point in time. How often should this information be updated and how are these updates presented to the general public?

On top of the above points, the involvement of the users is also critical in order to broadly engage them in the online privacy tools and allow them to reflect their opinions, comments and requests. In other words it is important to invest on the wider PETs user community, involving also non expert users that would like to address their worries and concerns. Awareness and education of the users is, thus, central in such an approach and different dissemination channels and methods can be applied, especially through social media platforms.

Having said that, it is also important to note that the use of PETs is sometimes presented to the general public as a deterrent to timely accessing critical information, e.g. in case of an emergency or in combatting terrorism. However, mass surveillance cannot be the response to these problems with a cost to everyone's private lives[26] and should not be the reason for discouraging users to apply online privacy tools. Security is a fundamental part of privacy, in the same way as privacy is a fundamental aspect of one's perception of security, especially in the evolving online and mobile information landscape.

Building trust in online privacy: a combined effort

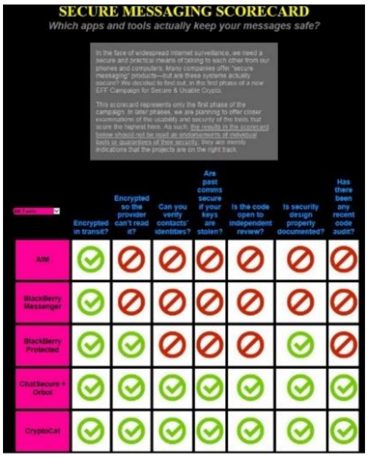
As a final conclusion, we find that the promotion of online privacy enhancing technologies for the general public needs to be a combined effort of all involved stakeholders, such as the Data Protection Authorities, the privacy researchers, the independent privacy organisations and associations, the users of PETs, as well as the industry of PET developers. It is for the mutual interest of all parties, and especially the internet and mobile users, to define and apply an objective way of assessing online privacy tools and openly presenting them in a comparable way. To this end, co-operation is important so as to bring the different perspectives and ideas on the table and to work towards a common approach on addressing the different characteristics of PETs. This could ideally lead to a widely accepted PETs evaluation/controls matrix open to the general public. ENISA will continue its efforts in this field by bringing the different communities together and building the necessary expertise for this important task.

[26] Article 29 Working Party, Opinion 4/2014 on surveillance of electronic communications for intelligence and national security purposes, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf

Annex A: Description of web portals promoting the use of online privacy tools

A.1 EFF Secure Messaging Scorecard

The Secure Messaging Scorecard website[27], launched in November 2014, represents the first phase of an Electronic Frontier Foundation (EFF) campaign in collaboration with Julia Angwin at ProPublica and Joseph Bonneau at the Princeton Center for Information Technology Policy. The goal of this initiative it to promote the use of secure and usable cryptography in secure messaging applications. EFF states that the results provided are not endorsements but indications about the correctness of the reviewed applications. Next phases of their campaign will analyse communication technologies, including chat clients, text messaging apps, email applications, and video calling technologies.



SECURE MESSAGING SCORECARD

Which apps and tools actually keep your messages safe?

In the face of widespread internet surveillance, we need a secure and practical means of talking to each other from our phones and computers. Many companies offer "secure messaging" products—but are these systems actually secure? We decided to find out, in the first phase of a new EFF Campaign for Secure & Usable Crypto.

This scorecard represents only the first phase of the campaign. In later phases, we are planning to offer closer examinations of the usability and security of the tools that score the highest here. As such, the results in the scorecard below should not be read as endorsements of individual tools or guarantees of their security; they are merely indications that the projects are on the right track.

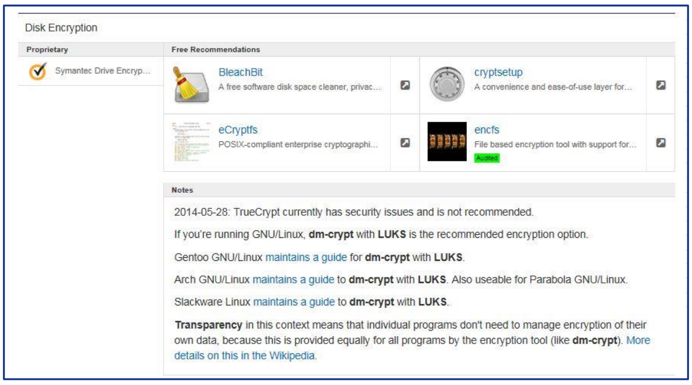
	Encrypted in transit?	Encrypted so the provider can't read it?	Can you verify contacts' identities?	Are past comms secure if your keys are stolen?	Is the code open to independent review?	Is security design properly documented?	Has there been any recent code audit?
AIM	✓	⊘	⊘	⊘	⊘	⊘	⊘
BlackBerry Messenger	✓	⊘	⊘	⊘	⊘	⊘	⊘
BlackBerry Protected	✓	✓	⊘	⊘	⊘	✓	⊘
ChatSecure + Orbot	✓	✓	✓	✓	✓	✓	✓
CryptoCat	✓	✓	✓	✓	✓	✓	✓

Figure 1: EFF Secure Messaging Scorecard

It is interesting to point out that the comparison contained in this website represents an updated version of the information displayed at the ProPublica website[28]. The website is structured as a single web page which includes a comparison table, information about the criteria used during the security assessment of the messaging applications and a detailed changelog.

A.2 PRISM Break

The PRISM Break project[29] is an initiative that advocates the right to privacy by using different open source applications against surveillance programs such as PRISM, XKeyscore or Tempora. In addition to covering a wide range of areas and including a lot of tools, it allows interaction with users via GitHub. As an example of this feature, the file Contributing.md includes guidelines for suggesting new software and, in case the suggestion is rejected, an explanation is given about the decision. The About tab includes an issues tracker link.



Disk Encryption

Proprietary	Free Recommendations	
Symantec Drive Encryp...	BleachBit A free software disk space cleaner, privac...	cryptsetup A convenience and ease-of-use layer for...
	eCryptfs POSIX-compliant enterprise cryptographi...	encfs File based encryption tool with support for... Audited

Notes

2014-05-28: TrueCrypt currently has security issues and is not recommended.

If you're running GNU/Linux, **dm-crypt** with **LUKS** is the recommended encryption option.

Gentoo GNU/Linux maintains a guide for **dm-crypt** with **LUKS**.

Arch GNU/Linux maintains a guide to **dm-crypt** with **LUKS**. Also useable for Parabola GNU/Linux.

Slackware Linux maintains a guide to **dm-crypt** with **LUKS**.

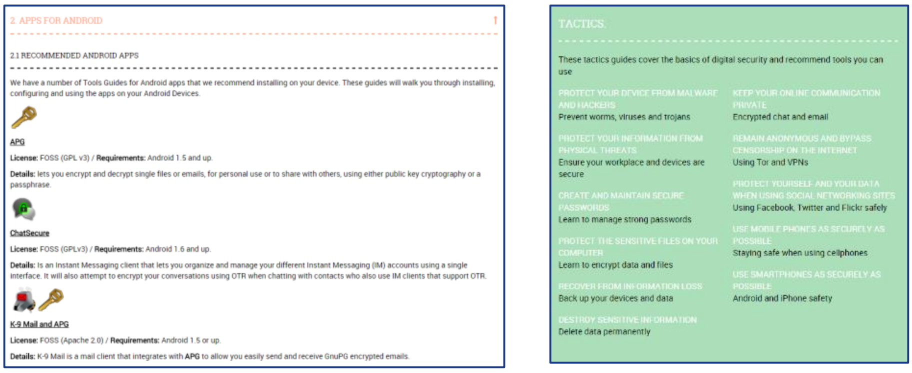
Transparency in this context means that individual programs don't need to manage encryption of their own data, because this is provided equally for all programs by the encryption tool (like **dm-crypt**). More details on this in the Wikipedia.

Figure 2: PRISM Break

[27] Electronic Frontier Foundation, Secure Messaging Scoreboard, www.eff.org/secure-messaging-scorecard
[28] Probublica, The best encrypted messaging programs, http://www.propublica.org/article/privacy-tools-the-best-encrypted-messaging-programs
[29] PRISM Break, https://prism-break.org/en/

A.3 Security in-a-box

Tactical Technology Collective is an organisation dedicated to the use of information in activism. Their digital security and privacy programme aims to build the digital security awareness and develop the skills of human rights defenders, independent journalists, anti-corruption advocates, and activists. Security in-a-box[30] is a guide about digital security and it has been jointly developed by Tactical Technology Collective and Front Line Defenders, along with a global network of many activists, trainers, and digital security experts.



2. APPS FOR ANDROID

2.1 RECOMMENDED ANDROID APPS

We have a number of Tools Guides for Android apps that we recommend installing on your device. These guides will walk you through installing, configuring and using the apps on your Android Devices.

APG

License: FOSS (GPL v3) / **Requirements:** Android 1.5 and up.

Details: lets you encrypt and decrypt single files or emails, for personal use or to share with others, using either public key cryptography or a passphrase.

ChatSecure

License: FOSS (GPLv3) / **Requirements:** Android 1.6 and up.

Details: Is an Instant Messaging client that lets you organize and manage your different Instant Messaging (IM) accounts using a single interface. It will also attempt to encrypt your conversations using OTR when chatting with contacts who also use IM clients that support OTR.

K-9 Mail and APG

License: FOSS (Apache 2.0) / **Requirements:** Android 1.5 or up.

Details: K-9 Mail is a mail client that integrates with **APG** to allow you easily send and receive GnuPG encrypted emails.

TACTICS

These tactics guides cover the basics of digital security and recommend tools you can use

PROTECT YOUR DEVICE FROM MALWARE AND HACKERS
Prevent worms, viruses and trojans

PROTECT YOUR INFORMATION FROM PHYSICAL THREATS
Ensure your workplace and devices are secure

CREATE AND MAINTAIN SECURE PASSWORDS
Learn to manage strong passwords

PROTECT THE SENSITIVE FILES ON YOUR COMPUTER
Learn to encrypt data and files

RECOVER FROM INFORMATION LOSS
Back up your devices and data

DESTROY SENSITIVE INFORMATION
Delete data permanently

KEEP YOUR ONLINE COMMUNICATION PRIVATE
Encrypted chat and email

REMAIN ANONYMOUS AND BYPASS CENSORSHIP ON THE INTERNET
Using Tor and VPNs

PROTECT YOURSELF AND YOUR DATA WHEN USING SOCIAL NETWORKING SITES
Using Facebook, Twitter and Flickr safely

USE MOBILE PHONES AS SECURELY AS POSSIBLE
Staying safe when using cellphones

USE SMARTPHONES AS SECURELY AS POSSIBLE
Android and iPhone safety

Figure 3: Security in-a-box

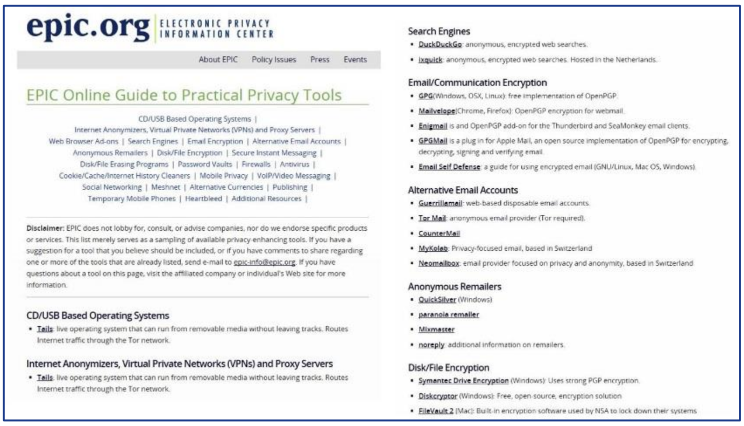
The site provides classifications for Windows and Android. The evaluation criteria, located at the About section include items such as if the tools are trusted (i.e., audited independently or anecdotal), matured (stable, with an active user-base community or a responsive developer community), open source or free, user friendly, multi-language, multi-platform, or if there is documentation available (source code, installation guides, usage notes, updates, etc.). Besides, the site references other similar projects promoting the use of privacy tools.

There is no information about the management of the website. Interaction with users or other experts is possible through a contact form.

[30] Tactical Technology Collective, securityinabox.org

A.4 EPIC Online Guide to Privacy Tools

EPIC is an independent non-profit research center based in Washington, DC. EPIC's goal is to protect privacy, freedom of expression, and democratic values, promoting the public voice in decisions concerning the future of the internet.



EPIC Online Guide to Practical Privacy Tools

CD/USB Based Operating Systems | Internet Anonymizers, Virtual Private Networks (VPNs) and Proxy Servers | Web Browser Ad-ons | Search Engines | Email Encryption | Alternative Email Accounts | Anonymous Remailers | Disk/File Encryption | Secure Instant Messaging | Disk/File Erasing Programs | Password Vaults | Firewalls | Antivirus | Cookie/Cache/Internet History Cleaners | Mobile Privacy | VoIP/Video Messaging | Social Networking | Meshnet | Alternative Currencies | Publishing | Temporary Mobile Phones | Heartbleed | Additional Resources |

Disclaimer: EPIC does not lobby for, consult, or advise companies, nor do we endorse specific products or services. This list merely serves as a sampling of available privacy-enhancing tools. If you have a suggestion for a tool that you believe should be included, or if you have comments to share regarding one or more of the tools that are already listed, send e-mail to epic-info@epic.org. If you have questions about a tool on this page, visit the affiliated company or individual's Web site for more information.

CD/USB Based Operating Systems

- Tails: live operating system that can run from removable media without leaving tracks. Routes Internet traffic through the Tor network.

Internet Anonymizers, Virtual Private Networks (VPNs) and Proxy Servers

- Tails: live operating system that can run from removable media without leaving tracks. Routes Internet traffic through the Tor network.

Search Engines

- DuckDuckGo: anonymous, encrypted web searches.
- Ixquick: anonymous, encrypted web searches. Hosted in the Netherlands.

Email/Communication Encryption

- GPG(Windows, OSX, Linux): free implementation of OpenPGP.
- Mailvelope(Chrome, Firefox): OpenPGP encryption for webmail.
- Enigmail is and OpenPGP add-on for the Thunderbird and SeaMonkey email clients.
- GPGMail is a plug in for Apple Mail, an open source implementation of OpenPGP for encrypting, decrypting, signing and verifying email.
- Email Self Defense: a guide for using encrypted email (GNU/Linux, Mac OS, Windows).

Alternative Email Accounts

- Guerrillamail: web-based disposable email accounts.
- Tor Mail: anonymous email provider (Tor required).
- CounterMail
- MyKolab: Privacy-focused email, based in Switzerland
- Neomailbox: email provider focused on privacy and anonymity, based in Switzerland

Anonymous Remailers

- QuickSilver (Windows)
- paranoia remailer
- Mixmaster
- noreply: additional information on remailers.

Disk/File Encryption

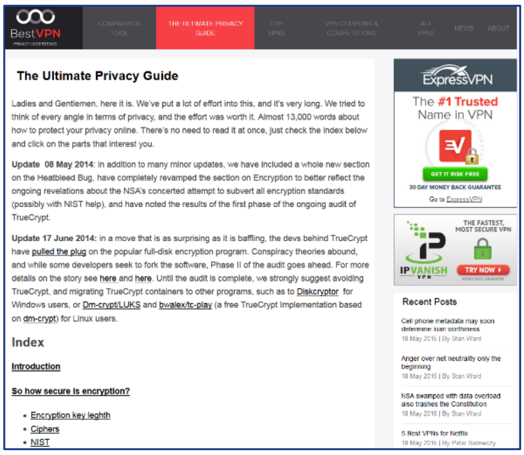
- Symantec Drive Encryption (Windows): Uses strong PGP encryption.
- Diskcryptor (Windows): Free, open-source, encryption solution
- FileVault 2 (Mac): Built-in encryption software used by NSA to lock down their systems

Figure 4: EPIC Online Guide to Privacy Tools

There is a list of privacy applications[31], where interested readers can also locate links to other similar initiatives.

The site is managed by an advisory board, whose details can be consulted in EPIC's website.

A.5 BestVPN: The Ultimate Privacy Guide



The Ultimate Privacy Guide

Ladies and Gentlemen, here it is. We've put a lot of effort into this, and it's very long. We tried to think of every angle in terms of privacy, and the effort was worth it. Almost 13,000 words about how to protect your privacy online. There's no need to read it at once, just check the index below and click on the parts that interest you.

Update 08 May 2014: In addition to many minor updates, we have included a whole new section on the Heatbleed Bug, have completely revamped the section on Encryption to better reflect the ongoing revelations about the NSA's concerted attempt to subvert all encryption standards (possibly with NIST help), and have noted the results of the first phase of the ongoing audit of TrueCrypt.

Update 17 June 2014: in a move that is as surprising as it is baffling, the devs behind TrueCrypt have pulled the plug on the popular full-disk encryption program. Conspiracy theories abound, and while some developers seek to fork the software, Phase II of the audit goes ahead. For more details on the story see here and here. Until the audit is complete, we strongly suggest avoiding TrueCrypt, and migrating TrueCrypt containers to other programs, such as to Diskcryptor for Windows users, or Dm-crypt/LUKS and bwalex/tc-play (a free TrueCrypt implementation based on dm-crypt) for Linux users.

Index

Recent Posts

Cell phone metadata may soon determine loan worthiness
18 May 2015 | By Stan Ward

Anger over net neutrality only the beginning
18 May 2015 | By Stan Ward

NSA swamped with data overload also trashes the Constitution
18 May 2015 | By Stan Ward

5 Best VPNs for Netflix
18 May 2015 | By Peter Selmeczy

Figure 5: Best VPN Ultimate Privacy Guide

BestVPN is a site created by 4Choice Ltd, a company located in the UK, and offers a review of over 50 VPN providers (most of them non-free). In addition to that, the site maintains a web page, The Ultimate Privacy Guide[32], which contains a list of privacy tools classified by areas.

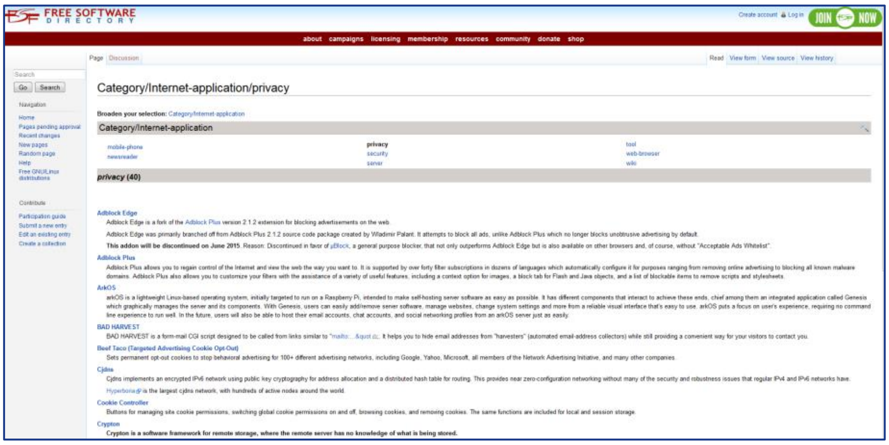
In the Write For Us area, readers are encouraged to contribute to the site, but in order to do so potential contributors must first contact BestVPN either by email or by filling in a form.

A.6 FSF Free Software Directory

[31] Electronic Privacy Information Center, EPIC Online Guide to Practical Privacy Tools, www.epic.org/privacy/tools.html

[32] Best VPN, Ultimate Privacy Guide, https://www.bestvpn.com/the-ultimate-privacy-guide/

The Free Software Foundation (FSF) is a non-profit organization with a worldwide mission to promote computer user freedom and to defend the rights of all free software users.



Category/Internet-application/privacy

Broaden your selection: Category/Internet-application

Category/Internet-application

mobile-phone
newsreader
privacy
security
server
tool
web-browser
wiki

***privacy* (40)**

Adblock Edge

Adblock Edge is a fork of the Adblock Plus version 2.1.2 extension for blocking advertisements on the web.

Adblock Edge was primarily branched off from Adblock Plus 2.1.2 source code package created by Wladimir Palant. It attempts to block all ads, unlike Adblock Plus which no longer blocks unobtrusive advertising by default.

This addon will be discontinued on June 2015. Reason: Discontinued in favor of µBlock, a general purpose blocker, that not only outperforms Adblock Edge but is also available on other browsers and, of course, without "Acceptable Ads Whitelist".

Adblock Plus

Adblock Plus allows you to regain control of the Internet and view the web the way you want to. It is supported by over forty filter subscriptions in dozens of languages which automatically configure it for purposes ranging from removing online advertising to blocking all known malware domains. Adblock Plus also allows you to customize your filters with the assistance of a variety of useful features, including a context option for images, a block tab for Flash and Java objects, and a list of blockable items to remove scripts and stylesheets.

ArkOS

arkOS is a lightweight Linux-based operating system, initially targeted to run on a Raspberry Pi, intended to make self-hosting server software as easy as possible. It has different components that interact to achieve these ends, chief among them an integrated application called Genesis which graphically manages the server and its components. With Genesis, users can easily add/remove server software, manage websites, change system settings and more from a reliable visual interface that's easy to use. arkOS puts a focus on user's experience, requiring no command line experience to run well. In the future, users will also be able to host their email accounts, chat accounts, and social networking profiles from an arkOS server just as easily.

BAD HARVEST

BAD HARVEST is a form-mail CGI script designed to be called from links similar to "mailto:...&quot;. It helps you to hide email addresses from "harvesters" (automated email-address collectors) while still providing a convenient way for your visitors to contact you.

Beef Taco (Targeted Advertising Cookie Opt-Out)

Sets permanent opt-out cookies to stop behavioral advertising for 100+ different advertising networks, including Google, Yahoo, Microsoft, all members of the Network Advertising Initiative, and many other companies.

Cjdns

Cjdns implements an encrypted IPv6 network using public key cryptography for address allocation and a distributed hash table for routing. This provides near zero-configuration networking without many of the security and robustness issues that regular IPv4 and IPv6 networks have.

Hyperboria is the largest cjdns network, with hundreds of active nodes around the world.

Cookie Controller

Buttons for managing site cookie permissions, switching global cookie permissions on and off, browsing cookies, and removing cookies. The same functions are included for local and session storage.

Crypton

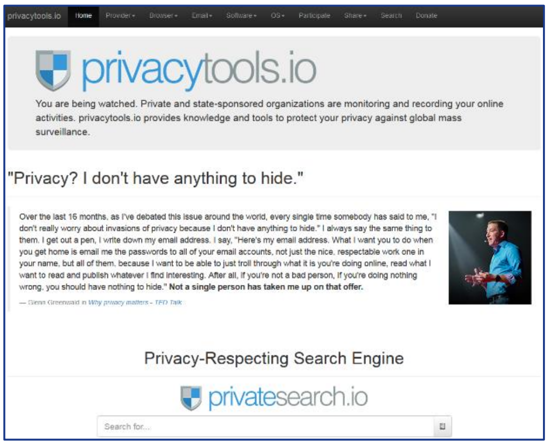
Crypton is a software framework for remote storage, where the remote server has no knowledge of what is being stored.

Figure 6: FSF Free Software Directory

The focus of this organization is thus free software rather than privacy. In this context, the FSF maintains the Free Software Directory[33], a catalogue of useful free software that runs under free operating systems, and that is collected by FSF staff and volunteers.

Among the different categories that can be found at the directory, there is one devoted to privacy. The directory includes a page where interested users can create an account and update or submit new entries. Updates and new submissions need to be approved by an administrator before they are added to the directory, where the changes approved and an updated track of the most recent changes are available in a changelog. The different FSF initiatives are maintained by FSF staff and volunteers.

A.7 Privacytools.io



You are being watched. Private and state-sponsored organizations are monitoring and recording your online activities. privacytools.io provides knowledge and tools to protect your privacy against global mass surveillance.

"Privacy? I don't have anything to hide."

Over the last 16 months, as I've debated this issue around the world, every single time somebody has said to me, "I don't really worry about invasions of privacy because I don't have anything to hide." I always say the same thing to them. I get out a pen, I write down my email address. I say, "Here's my email address. What I want you to do when you get home is email me the passwords to all of your email accounts, not just the nice, respectable work one in your name, but all of them, because I want to be able to just troll through what it is you're doing online, read what I want to read and publish whatever I find interesting. After all, if you're not a bad person, if you're doing nothing wrong, you should have nothing to hide." **Not a single person has taken me up on that offer.**

— Glenn Greenwald in *Why privacy matters - TED Talk*

Privacy-Respecting Search Engine

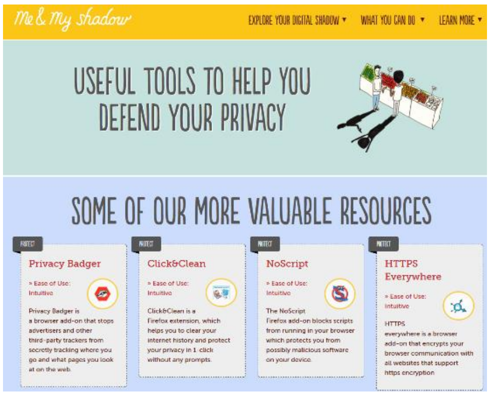
Figure 7: privacytools.io

Privacytools.io[34] is a socially motivated website that provides information for protecting internet users' data security and privacy. It is a community project that allows participation through a reddit discussion board.

[33] Free Software Foundation, Free Software Directory, directory.fsf.org

[34] Privacytools.io, www.privacytools.io

A.8 Me & My Shadow



Me & My shadow

EXPLORE YOUR DIGITAL SHADOW ▾ WHAT YOU CAN DO ▾ LEARN MORE ▾

USEFUL TOOLS TO HELP YOU DEFEND YOUR PRIVACY

SOME OF OUR MORE VALUABLE RESOURCES

PROTECT
Privacy Badger
» Ease of Use: Intuitive
Privacy Badger is a browser add-on that stops advertisers and other third-party trackers from secretly tracking where you go and what pages you look at on the web.

PROTECT
Click&Clean
» Ease of Use: Intuitive
Click&Clean is a Firefox extension, which helps you to clear your internet history and protect your privacy in 1 click without any prompts.

PROTECT
NoScript
» Ease of Use: Intuitive
The NoScript Firefox add-on blocks scripts from running in your browser which protects you from possibly malicious software on your device.

PROTECT
HTTPS Everywhere
» Ease of Use: Intuitive
HTTPS everywhere is a browser add-on that encrypts your browser communication with all websites that support https encryption

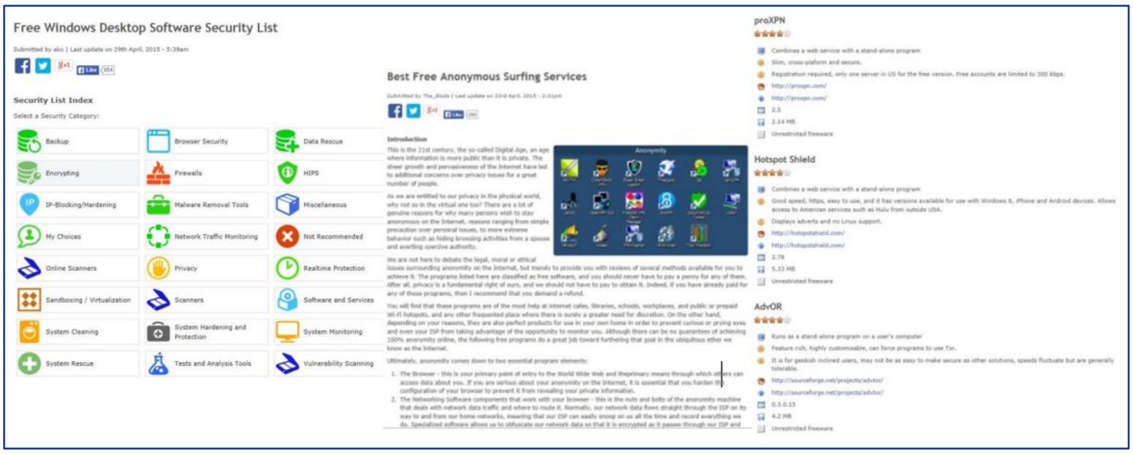
Figure 8: Me & My shadow

Me & My Shadow[35] is a project created in 2012 that helps to understand the concept of digital shadows, supporting users to minimise them. The site is maintained by Tactical Technology Collective, an international organisation dedicated to the use of information in activism (see also Security-in-a-box).

The site includes a page with several privacy applications, focusing especially on the protection against tracking.

A.9 Gizmo's Freeware

Gizmo's Freeware is a non-commercial community website composed of volunteers. Their goal is to help users select the best freeware products for a wide range of uses. Its staff is composed by volunteers with no commercial affiliations. Interested readers can contribute with short tips, how-to guides, tutorials or products reviews. In order to do that, it is necessary to register in the system, to send a proposal and to wait for its acceptance.



Free Windows Desktop Software Security List

Submitted by ako | Last update on 29th April, 2015 - 5:39am

Security List Index

Select a Security Category:

Backup	Browser Security	Data Rescue
Encrypting	Firewalls	HIPS
IP-Blocking/Hardening	Malware Removal Tools	Miscellaneous
My Choices	Network Traffic Monitoring	Not Recommended
Online Scanners	Privacy	Realtime Protection
Sandboxing / Virtualization	Scanners	Software and Services
System Cleaning	System Hardening and Protection	System Monitoring
System Rescue	Tests and Analysis Tools	Vulnerability Scanning

Best Free Anonymous Surfing Services

Submitted by The_Blade | Last update on 23rd April, 2015 - 2:31pm

Introduction

This is the 21st century, the so-called Digital Age, an age where information is more public than it is private. The sheer growth and pervasiveness of the Internet have led to additional concerns over privacy issues for a great number of people.

As we are entitled to our privacy in the physical world, why not so in the virtual one too? There are a lot of genuine reasons for why many persons wish to stay anonymous on the Internet, reasons ranging from simple precaution over personal issues, to more extreme behavior such as hiding browsing activities from a spouse and averting coercive authority.

We are not here to debate the legal, moral or ethical issues surrounding anonymity on the Internet, but merely to provide you with reviews of several methods available for you to achieve it. The programs listed here are classified as free software, and you should never have to pay a penny for any of them. After all, privacy is a fundamental right of ours, and we should not have to pay to obtain it. Indeed, if you have already paid for any of these programs, then I recommend that you demand a refund.

You will find that these programs are of the most help at internet cafes, libraries, schools, workplaces, and public or prepaid Wi-Fi hotspots, and any other frequented place where there is surely a greater need for discretion. On the other hand, depending on your reasons, they are also perfect products for use in your own home in order to prevent curious or prying eyes and even your ISP from taking advantage of the opportunity to monitor you. Although there can be no guarantees of achieving 100% anonymity online, the following free programs do a great job toward furthering that goal in the ubiquitous ether we know as the Internet.

Ultimately, anonymity comes down to two essential program elements:

1. The Browser - this is your primary point of entry to the World Wide Web and theprimary means through which others can access data about you. If you are serious about your anonymity on the Internet, it is essential that you harden the configuration of your browser to prevent it from revealing your private information.
2. The Networking Software components that work with your browser - this is the nuts and bolts of the anonymity machine that deals with network data traffic and where to route it. Normally, our network data flows straight through the ISP on its way to and from our home networks, meaning that our ISP can easily snoop on us all the time and record everything we do. Specialized software allows us to obfuscate our network data so that it is encrypted as it passes through our ISP and

proXPN
★★★★☆
- Combines a web service with a stand-alone program
- Slim, cross-plaform and secure.
- Registration required, only one server in US for the free version. Free accounts are limited to 300 kbps.
- http://proxpn.com/
- http://proxpn.com/
- 2.5
- 2.14 MB
- Unrestricted freeware

Hotspot Shield
★★★★☆
- Combines a web service with a stand-alone program
- Good speed, https, easy to use, and it has versions available for use with Windows 8, iPhone and Android devices. Allows access to American services such as Hulu from outside USA.
- Displays adverts and no Linux support.
- http://hotspotshield.com/
- http://hotspotshield.com/
- 2.78
- 5.33 MB
- Unrestricted freeware

AdvOR
★★★★☆
- Runs as a stand-alone program on a user's computer
- Feature rich, highly customisable, can force programs to use Tor.
- It is for geekish inclined users, may not be as easy to make secure as other solutions, speeds fluctuate but are generally tolerable.
- http://sourceforge.net/projects/advtor/
- http://sourceforge.net/projects/advtor/
- 0.3.0.15
- 4.2 MB
- Unrestricted freeware

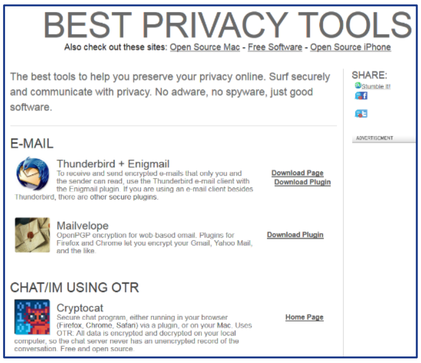
Figure 9: Gizmo's freeware

The site contains a specific section with a long list of privacy tools classified by areas[36] without further descriptions. In addition to that, privacy applications can be located at the sections devoted to each

[35] Tactical Technology Collective, Me & My shadow, myshadow.org
[36] Gizmo's freeware, Free Windows Desktop Software Security List – Privacy, www.techsupportalert.com/content/free-windows-desktop-software-security-list-privacy.htm

operating system (Windows, Mac, GNU/Linux, Android, and iOS). In some cases, a link to an external review is located next to the name of the tool. Finally, as an interesting feature, the site provides a list of non-recommended applications.

A.10 Best Privacy Tools



BEST PRIVACY TOOLS

Also check out these sites: Open Source Mac - Free Software - Open Source iPhone

The best tools to help you preserve your privacy online. Surf securely and communicate with privacy. No adware, no spyware, just good software.

SHARE:
Stumble It!

ADVERTISEMENT

E-MAIL

Thunderbird + Enigmail
To receive and send encrypted e-mails that only you and the sender can read, use the Thunderbird e-mail client with the Enigmail plugin. If you are using an e-mail client besides Thunderbird, there are other secure plugins.
Download Page
Download Plugin

Mailvelope
OpenPGP encryption for web-based email. Plugins for Firefox and Chrome let you encrypt your Gmail, Yahoo Mail, and the like.
Download Plugin

CHAT/IM USING OTR

Cryptocat
Secure chat program, either running in your browser (Firefox, Chrome, Safari) via a plugin, or on your Mac. Uses OTR: All data is encrypted and decrypted on your local computer, so the chat server never has an unencrypted record of the conversation. Free and open source.
Home Page

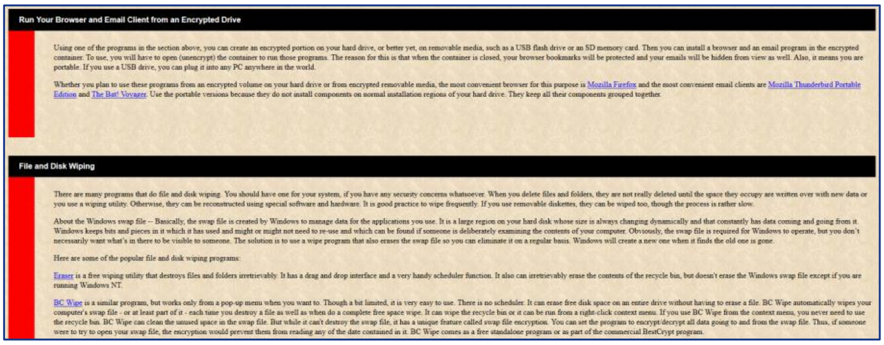
Figure 10: Best Privacy Tools

Best Privacy Tools[37] offers help for preserving privacy online. The site provides a simple list of resources that can be extended by users interested in collaboration.

The content is divided in areas (email, chat/IM, web browsing, etc.), with a few selected tools appearing in each section.

A.11 Internet Privacy Tools

Internet Privacy Tools[38] is a website that identifies some of the major areas of interest regarding the protection of private data and communications, like for example encrypted email, file and disk encryption and wiping, anonymous browsing or encrypted chat.



Run Your Browser and Email Client from an Encrypted Drive

Using one of the programs in the section above, you can create an encrypted portion on your hard drive, or better yet, on removable media, such as a USB flash drive or an SD memory card. Then you can install a browser and an email program in the encrypted container. To use, you will have to open (unencrypt) the container to run those programs. The reason for this is that when the container is closed, your browser bookmarks will be protected and your emails will be hidden from view as well. Also, it means you are portable. If you use a USB drive, you can plug it into any PC anywhere in the world.

Whether you plan to use these programs from an encrypted volume on your hard drive or from encrypted removable media, the most convenient browser for this purpose is Mozilla Firefox and the most convenient email clients are Mozilla Thunderbird Portable Edition and The Bat! Voyager. Use the portable versions because they do not install components on normal installation regions of your hard drive. They keep all their components grouped together.

File and Disk Wiping

There are many programs that do file and disk wiping. You should have one for your system, if you have any security concerns whatsoever. When you delete files and folders, they are not really deleted until the space they occupy are written over with new data or you use a wiping utility. Otherwise, they can be reconstructed using special software and hardware. It is good practice to wipe frequently. If you use removable diskettes, they can be wiped too, though the process is rather slow.

About the Windows swap file -- Basically, the swap file is created by Windows to manage data for the applications you use. It is a large region on your hard disk whose size is always changing dynamically and that constantly has data coming and going from it. Windows keeps bits and pieces in it which it has used and might or might not need to re-use and which can be found if someone is deliberately examining the contents of your computer. Obviously, the swap file is required for Windows to operate, but you don't necessarily want what's in there to be visible to someone. The solution is to use a wipe program that also erases the swap file so you can eliminate it on a regular basis. Windows will create a new one when it finds the old one is gone.

Here are some of the popular file and disk wiping programs:

Eraser is a free wiping utility that destroys files and folders irretrievably. It has a drag and drop interface and a very handy scheduler function. It also can irretrievably erase the contents of the recycle bin, but doesn't erase the Windows swap file except if you are running Windows NT.

BC Wipe is a similar program, but works only from a pop-up menu when you want to. Though a bit limited, it is very easy to use. There is no scheduler. It can erase free disk space on an entire drive without having to erase a file. BC Wipe automatically wipes your computer's swap file - or at least part of it - each time you destroy a file as well as when do a complete free space wipe. It can wipe the recycle bin or it can be run from a right-click context menu. If you use BC Wipe from the context menu, you never need to use the recycle bin. BC Wipe can clean the unused space in the swap file. But while it can't destroy the swap file, it has a unique feature called swap file encryption. You can set the program to encrypt/decrypt all data going to and from the swap file. Thus, if someone were to try to open your swap file, the encryption would prevent them from reading any of the date contained in it. BC Wipe comes as a free standalone program or as part of the commercial BestCrypt program.

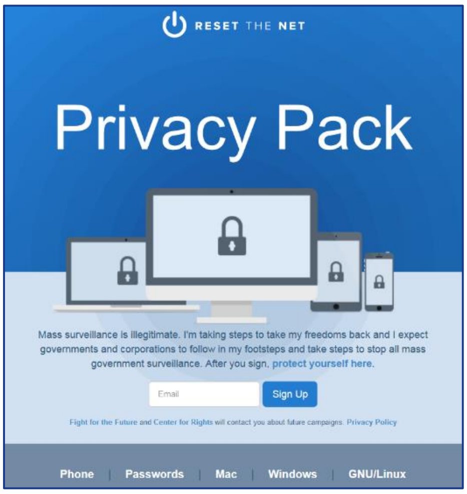
Figure 11: Internet Privacy Tools

Under each of these areas some tools are selected, including a brief description or (sometimes) a more comprehensive review. No detailed information about who promotes the initiative, the updating process, the level of expertise behind the comments, or the maintenance plan is provided.

[37] Best Privacy Tools, bestprivacytools.com
[38] Internet Privacy Tools, privacytools.freeservers.com

A.12 Reset The Net

Reset the Net[39] is an initiative led by Fight for the Future and Center for Rights (in consultation with technologists and activists at the Electronic Frontier Foundation) against mass surveillance and for defending internet users' right to privacy.



Mass surveillance is illegitimate. I'm taking steps to take my freedoms back and I expect governments and corporations to follow in my footsteps and take steps to stop all mass government surveillance. After you sign, protect yourself here.

Fight for the Future and Center for Rights will contact you about future campaigns. Privacy Policy

Figure 12: Reset the Net

Reset the Net aims at selecting software and providing tips regarding computers, phones, and tablets for regular users, offering at the same time additional tools and instructions for more technical users.

The website offers, under what they call "Privacy Pack", free software tools (they claim that it is a way to make it easy for outsiders to verify and improve their security) for Windows, Mac, GNU/Linux, Android, and iOS devices, covering different privacy areas like instant messaging, anonymous browsing or email encryption.

[39] Reset The Net, www.resetthenet.org

Annex B: Analysis of six anti-tracking browser extensions

B.1 Ghostery

Ghostery[40] blocks a number of elements, including tracking cookies, scripts, ad networks and social buttons. It is available for most PC browsers and also for the Android version of Firefox.

It allows users to check what trackers are following them and decide which ones to allow and which ones to block. Besides, the tool shows the elements that have been effectively blocked in the user interface and also in a separate window, depending on the configuration. Through click-to-play content replacement, if a user finds he/she is missing elements on a page, he/she can access a small ghost image informing him/her about the elements that were blocked from his/her view. The tool has an option to ignore first party trackers (also known as direct trackers, e.g. the DoubleClick tracker on doubleclick.com).

It is important to mention that if the «GhostRank» option is activated, anonymous information about the elements encountered and blocked is sent to the Evidon's servers (the company behind Ghostery) to be sold to advertising companies. According to Evidon, the tool does not collect any information which could be used to identify users or target ads specifically at individual users.

Ghostery is an open source tool whose usage is limited by a private license, meaning that users can review the code but they are not allowed to modify or use it in any other non-authorized way[41]. The source code is only available for Firefox[42]. The tool provides an email address (info@ghostery.com) and a forum[43] for user support. Regarding the documentation, the tool has a FAQ page[44].

Quality criteria

- Background information: The tool was originally developed by David Cancel[45], but in January 2010 Ghostery was acquired by the advertising company Better Advertising, which later on became Evidon. In April 2014 Evidon and Ghostery became Ghostery Inc.
- Version history: In the Firefox store there is a list of versions, with the new functionalities and corrected bugs of each version, when applicable[46].
- Transparency of installation and use: The installation process is transparent to the user. Still, just after the installation, a new tab is opened to configure the tool where the user is asked if he/she wants to participate in Ghostrank and the button for doing so is highlighted in green (it must be noted that the «next» button requires to select an option to be enabled). If this tab is closed, the Ghostrank option gets

[40] www.ghostery.com
[41] addons.mozilla.org/es/firefox/addon/ghostery/license/5.4.8.1
[42] addons.mozilla.org/en/firefox/files/browse/312088/A
[43] getsatisfaction.com/ghostery
[44] www.ghostery.com/en/faq
[45] http://www.davidcancel.com
[46] addons.mozilla.org/es/firefox/addon/ghostery/versions

unchecked and the default configuration is used. The default configuration does not activate the anti-tracking capabilities of the tool but this is clearly explained to the user in the tool's tutorial.

It is worth mentioning that the installer opens automatically another tab for the user to participate in a Ghostery Install Survey (which asks for some personal details, such as the age, gender, or employment status.) Although it is possible to avoid participation in the survey by closing the tab, the way the presentation is done (automatically opened tab which directly shows the first question to the survey) may be confusing and/or misleading for some non-experts users. Moreover, although the installation does not seem to include any third party software, if the survey is completed the last page suggests the user to register (for free) in a third party surveying service.

- Public reviews: The average rating at Mozilla's add-ons site is 5 over 5 (1195 reviews), and at Google Chrome's add-ons site is also 5 over 5 (7958 reviews). It is included in the Me and My Shadow and Best Privacy Tools websites. In addition to that, there are several external reviews, most of them positive and in general without outlining any major problem[47]. One point that is noted, though, is the Ghostrank option and the ethical issues surrounding its function.
- Privacy by design and default: When it is installed, an assistant with basic configuration options is executed. In addition to that, there are other advanced configuration options. It is important to mention that no tracker is blocked by default, so users have to activate that functionality by selecting the corresponding option (either during the initial configuration phase, or at any moment once the tool is installed). This can be easily made through the tool's options page.
- Ease of use: The tool is moderately easy to use for non-experts due to its complex configuration options.
- User interaction: A quite active forum is available[48] where users' comments are published. In addition, there is a web form where comments, suggestions and doubts can be sent[49].
- Other aspects: The tool is available in more than 15 languages and it is multiplatform, being available for the browsers Opera, Firefox, Chrome, Safari, Internet Explorer, and for the mobile systems Android and iOS (in Android users can choose the plugin for Firefox or the Ghostery browser).

Functionality criteria

- General functionality: Blocks trackers, cookies, pixels beacons, and social network indicators. Trackers are classified in five categories (analytics, web beacons, privacy, advertising, and widgets). The tool allows the blocking history to be reviewed during each session.
- Processing of personal data: If users activate the Ghostrank option, anonymous information about the browsing history and the blocked elements is sent to the company's servers to be sold to advertising

[47] Some example reviews can be found in: venturebeat.com/2012/07/31/ghostery-a-web-tracking-blocker-that-actually-helps-the-ad-industry, http://www.bestvpn.com/blog/10401/ghostery-a-great-web-extension-but-shady-business-practices, longhandpixels.net/blog/2014/05/protect-your-privacy-ghostery, www.thewindowsclub.com/ghostery-review

[48] getsatisfaction.com/ghostery

[49] www.ghostery.com/en/about-us/contact-us

companies. However, the company claims that no personal data that could identify the users are collected.

- Flexibility: The tool does allow to define white/black lists. Also, it allows enabling/disabling of different categories of trackers.
- Choice: It is possible to temporarily block and unblock specific elements. In addition to that, by clicking a button, it is possible to allow an element in the current page, in a way that it is always enabled for that page even if it is disabled for all the other pages.
- On/off: The tool allows to pause the blocking (affecting all tabs).
- History (of blocked elements): It is possible to check what has been blocked in each page while it is opened.
- Plugins are available in the Chrome and Firefox official stores, but they are not signed (as on 10/15/2015).

B.2 Disconnect

Disconnect[50] is an anti-tracking tool available for Mac (version 10.7 and above), Windows (version 7.0 and above), Android (version 4.0 and above), and iOS (version 7.1 and above). It allows first party trackers by default, and detects when the user's browser tries to make a connection to anything other than the site he/she is visiting. By checking and unchecking the corresponding box, it allows to block and unblock trackers of different categories (Advertising, Analytics, Social Networking, and Content), plus three specific trackers which are shown separately (Google, Facebook, and Twitter). The tool can be found in a free version (its source code can be found on GitHub) and a premium (paid) version. Both versions show users who is tracking them. Besides, it allows to manage white/black lists.
It is not necessary to make a great effort in the configuration process to achieve its total capacity, as the tool has very intuitive configuration options. In this sense, it is worthwhile to mention the graphic interface for Chromium-based browsers that, with a glance, permits to see what connections are activated when a web page is visited and which of them are blocked.

The source code is available at the Firefox store and from GitHub[51] (though it does not seem to be maintained anymore).

The tool offers a forum[52] and an email address[53] for contacting the developers. Besides, the documentation includes a FAQ[54] and a user manual[55].

[50] disconnect.me
[51] github.com/disconnectme/disconnect
[52] github.com/disconnectme/disconnect/issues
[53] support@disconnect.me
[54] disconnect.me/help#disconnect-private-browsing-browser-extension_faq
[55] disconnect.me/disconnect

Quality criteria

- Background information: The team in charge of the tool's maintenance is well identified[56]. The company behind the product has the same name (Disconnect).
- Version history: In the Firefox store there is a list of versions, with the new functionalities and corrected bugs of each version, when applicable[57].
- Transparency of installation and use: The installation process is transparent. The operation of the tool (default functionality and options) is also transparent to the users. The tool does not seem to include third party software or modify other applications or user configurations.

  It is interesting to mention that, once installed, a tab asks for financial support without any «exit» or «no support» button (the only option to avoid supporting the tool is to close the tab or to select the «Tour the interface» button, which provides a complete tutorial of the tool). This tab also invites to test the premium version.
- Public reviews: The average rating at Mozilla's add-ons site is 4 over 5 (152 reviews), and at Google Chrome's add-ons site is 4.5 over 5 (2386 reviews). It is included in the PRISM Break, EPIC, Best VPN and Privacy Tools websites[58].
- Privacy by design and by default: Its' privacy features are enabled without the need of user configuration. By default, Disconnect blocks all network requests in each category except Content. Content is unblocked by default because it often includes network requests that, if blocked, would deteriorate the browsing experience.
- Ease of use: The tool is easy to use for non-experts due to its simple and very informative interface.
- User interaction: There is a forum where users' comments are published[59]. There is also a support e-mail[60].
- Other aspects: The only language available is English. The tool is multiplatform. Versions for Opera, Firefox, Chrome, and Safari browsers are available.

Functionality criteria

- General functionality: The tool blocks and unblocks trackers of different categories (Advertising, Analytics, Social Networking, and Content). In addition it shows separate buttons to manage the blocking of three specific trackers (Google, Facebook, and Twitter).

[56] disconnect.me/team

[57] addons.mozilla.org/es/firefox/addon/disconnect/versions

[58] Some example reviews can be found in: techcrunch.com/2013/04/17/disconnect-2-brings-more-privacy-to-your-browser-lets-you-block-2k-sites-from-tracking-your-activity-online, archive.wired.com/geekdad/2011/01/plug-ins-for-privacy-disconnect-and-adbloc, techmaza.org/protect-internet-browsing-using-disconnect, www.download3k.com/articles/Disconnect-a-Browser-Extension-to-Stop-Websites-Tracking-While-You-Gain-Browsing-Speed-00925

[59] github.com/disconnectme/disconnect/issues

[60] support@disconnect.me

- Processing of personal data: According to the available information, during the tool's update procedure, the requests for the configuration files may include anonymous data about when the tool was last updated in the user's browser, but logs containing the user's IP address or other personal information are never sent when the tool's servers are contacted.
- Flexibility: The tool does allow to define white/black lists.
- Choice: It is possible to temporarily block and unblock specific elements.
- On/off: The tool allows to pause the blocking process for the full domain (site) of the current page, by means of the «Whitelist site» option.
- History (of blocked elements): It is possible to check what has been blocked.
- Plugins or add-ons are available in the corresponding official store for Opera, Chrome, and Firefox. The plugin is signed for Firefox (as on 10/15/2015).

B.3 uBlock origin

uBlock origin[61] is a general purpose blocker for Chrome and Firefox designed to work with custom rules and filters. The default behavior of uBlock origin is to block ads, trackers and malware sites, through the lists EasyList, Peter Lowe's Adservers, EasyPrivacy, various lists of malware sites, and uBlock origin's own filter lists. More lists are available to block trackers, analytics, and other elements.
The tool can load and enforce filters used by other popular adblockers such as AdBlock Plus or Disconnect. The control interface is minimal and very intuitive. It is important to mention the ability for creating «cosmetic» filters, that is filters used to delete something on a page which will not be displayed in subsequent visits, as well as the ability to pause the activity in a single page or in all of them.

The source code is available at GitHub and support is provided through a forum[62]. With regards to the documentation, it has a wiki[63]. Also a user manual is available[64].

Quality criteria

- Background information: Raymond Hill (the responsible for uBlock origin and the original developer behind uBlock) transferred ownership of the original uBlock project in 2015. After that, Hill forked uBlock into uBlock origin, a personal fork for which he's been releasing builds and providing support[65].
- Version history: In the Firefox store there is a list of versions, with the new functionalities and corrected bugs of each version, when applicable[66]. In the developer's page at GitHub[67] the same information can be found for Firefox and Chrome.

[61] github.com/gorhill/uBlock
[62] github.com/gorhill/uBlock/issues
[63] github.com/gorhill/uBlock/wiki
[64] github.com/gorhill/uBlock/blob/master/README.md
[65] https://github.com/gorhill
[66] addons.mozilla.org/es/firefox/addon/ublock-origin/versions
[67] github.com/gorhill/uBlock/releases

- Transparency of installation and use: The installation process is transparent. The tool is also transparent regarding the use and default functionality. It does not seem to include third party software or modify other applications or user configurations.
- Public reviews: The average rating at Mozilla's add-ons site is 5 over 5 (212 reviews), and at Google Chrome's add-ons site is also 5 over 5 (3767 reviews). It is included in the PRISM Break and Privacy Tools websites[68].
- Privacy by design and by default: After installation, enabled privacy features ensure a good protection capacity. It is possible to obtain a better performance of the tool by means of the advanced configuration, which allows to manage third-party filters, own filters (server name or a filter compatible with Adblock Plus), rules of dynamic filtering, and a whitelist (uBlock origin will be disabled for server names included in that list).
- Ease of use: The tool is easy to use for non-experts. By using the mode to select individual elements (element picker mode, also accessible with the right button of the mouse), adding a filter for that element is straightforward.
- User interaction: There is a forum[69] where users' comments are published.
- Other aspects: The tool is available in more than 30 languages. It is multiplatform. There are versions for Chrome, Firefox, Opera, and Safari browsers.

Functionality criteria

- General functionality: It blocks advertising, malware domains, social trackers and scripts. It blocks ads through its support of the Adblock Plus filter syntax (and with other custom rules and filters), and imports malvertising filter lists. Allows blocking images via the context menu.
- Processing of personal data: According to the available information, no personal data is processed. It is worth mentioning that it is possible to enable an option to stops WebRTC from revealing local IP addresses of VPN users (if the user is not behind any VPN or proxy, his/her ISP-provided IP address will be visible regardless of this setting).
- Flexibility: The tool allows to define white/black lists, to import third-party filters, and to edit user's filters.
- Choice: It is possible to temporarily block and unblock specific elements.
- On/off: The tool allows to pause the blocking capabilities for the full domain or only for the current page.
- History (of blocked elements): It is possible to check, in the requests register, what has been blocked (not easy to find).
- The tool is available in the Chrome and Firefox official stores, but it is not signed (as on 10/15/2015).

[68] Some example review can be found in: www.maketecheasier.com/ublock-origin-better-than-adblock-plus, xvblog.wpengine.com/internet-privacy/reviews/ublock-origin/?domain=www.expressvpn.com, blog.desdelinux.net/ublock-alternativa-libre-y-super-liviana-a-adblock-plus, www.news47ell.com/reviews/ublock-origin-review-adblock-plus-alternative, ohax.fr/oubliez-pachydermique-adblock-plus-ublock-origin-est-arrive

[69] github.com/gorhill/ublock/issues

B.4 Privacy Badger

Privacy Badger[70] is a browser add-on that blocks cookies, spying advertisers and invisible trackers. It works by creating a list of the third-party domains that embed images, scripts and ads as the user visits different pages across the Web. If the tool finds out that there are companies tracking the user on multiple websites, the loading of content from that source will be blocked in the future. It is not necessary to make any configuration process to achieve its total capacity. Currently supported browsers are Firefox and Chrome. The source code is available at GitHub[71].

Quality criteria

- Background information: It is a project of the Electronic Frontier Foundation (EFF). The current maintainers of this project are the EFF Technologists Cooper Quintin[72] and Noah Swartz[73].
- Version history: In the Firefox store there is a list of new versions, with the new functionalities and corrected bugs of each version, when applicable[74]. In the developers' page at GitHub[75] the same information can be found for Firefox and Chrome.
- Transparency of installation and use: The installation process is transparent. The tool is also transparent regarding the default operation and use. It does not seem to include any third party software or modify other applications or user configurations. It is interesting to remark that just after the installation a tab is opened with a quite detailed tutorial.
- Public reviews: The average rating at Mozilla's add-ons site is 4 over 5 (69 reviews), and at Google Chrome's add-ons site is also 4 over 5 (398 reviews). It is included in the PRISM Break, Me and My Shadow, and Best Privacy Tools websites[76].
- Privacy by design and by default: All its' privacy features are enabled without the need of user configuration.
- Ease of use: The tool is easy to use for non-experts due to its dynamic operation (the tool learns what to block as the users visit different pages across the Web).

[70] https://www.eff.org/privacybadger
[71] github.com/EFForg/privacybadgerchrome and github.com/EFForg/privacybadgerfirefox
[72] http://www.eff.org/es/about/staff/cooper-quintin
[73] www.eff.org/es/about/staff/noah-swartz
[74] addons.mozilla.org/es/firefox/addon/privacy-badger-firefox/versions
[75] github.com/EFForg/privacybadgerchrome/blob/master/doc/Changelog, github.com/EFForg/privacybadgerfirefox/blob/master/doc/Changelog
[76] Some example reviews can be found in: http://www.genbeta.com/web/la-eff-prueba-privacy-badger-una-nueva-extension-para-bloquear-anuncios-que-vulneren-nuestra-privacidad, http://www.pcworld.com/article/2961068/privacy/eff-tracker-smashing-privacy-badger-exits-beta.html, http://www.makeuseof.com/tag/block-online-tracking-privacy-badger/, icloak.org/privacy-badgers-triple-play-online-privacy-protection/

- User interaction: Two different forums are available for Firefox and Chrome [77] where users' comments are published. E-mail support is also provided by the staff in charge of the project[78].
- Other aspects: The tool is available in five available languages (English, German, French, Dutch and Swedish). There are versions for Chrome and Firefox browsers.

Functionality criteria

- General functionality: It blocks spying ads and trackers, also detect canvas based fingerprinting and blocks third party domains that use it. Privacy Badger sends the Do Not Track header with each request and evaluates the likelihood that the user is still being tracked. If a domain appears to be tracking a user on multiple websites, the tool automatically blocks the user's request from being sent to the tracking domain.
- Processing of personal data: According to the available information, no personal data is processed.
- Flexibility: The tool allows to define white/black lists.
- Choice: It is possible to temporarily block and unblock individual domains (entirely or only their cookies).
- On/off: The tool allows to pause the blocking process for the current page.
- History (of blocked elements): It is possible to check what has been blocked.
- Plugins are available in the Chrome and Firefox official stores, but they are not signed (as on 10/15/2015).

B.5 NoScript

NoScript[79] is an extension that provides protection for Firefox, Seamonkey, and other Mozilla-based browsers by blocking scripts. It allows JavaScript, Java, Flash and other plugins to be executed only when browsing trusted web sites, according to the users' choice. The tool has a clear and very informative website with FAQ and a forum, as well as a quite detailed changelog informing about the tool updates, fixed bugs, etc., but it is necessary to access the add-on register of Mozilla to find the dates of the versions. The source code is available at the Mozilla store[80]. There are two support channels: email[81] and forum[82]. Besides, the documentation consists in a FAQ[83] which contains the installation instructions.

[77] github.com/EFForg/privacybadgerfirefox/issues, github.com/EFForg/privacybadgerchrome/issues
[78] cjq@eff.org and noah@eff.org
[79] noscript.net
[80] addons.mozilla.org/es/firefox/files/browse/328048
[81] software@informaction.com
[82] forums.informaction.com/viewforum.php?f=3
[83] noscript.net/faq

Quality criteria

- Background information: Its author is Giorgio Maone[84], who develops software at InformAction[85] since 1998.
- Version history: In the Firefox store there is a list of new versions, with the new functionalities and corrected bugs of each version, when applicable[86]. A version record with the same information can also be found in the Noscript site[87], but without dates.

  Transparency of installation and use: The installation process is transparent. The tool is also transparent on its default operation and use (it starts blocking scripts as soon as it is installed). It does not seem to include any third party software or modify other applications or user configurations. It is good to know that after installation a tab is opened with several elements (button for donations and an advertisement of a commercial VPN, among others).
- Public reviews: The average rating at Mozilla's add-ons site is 5 over 5 (1498 reviews). It is included in the PRISM Break, Security in a Box, EPIC, Best VPN, Privacy Tools, Me and My Shadow, and Reset the Net websites[88].
- Privacy by design and by default: After installation, all the JavaScript, Java, Flash, and Silverlight scripts are blocked by default. Several configuration options (e.g. add domains to the whitelist) are available, although due to their complexity they are difficult to understand for non-experts.
- Ease of use: The tool is difficult to use by non-expert users, as they must take decisions about which scripts to enable in order to correctly view most websites.
- User interaction: There is a forum where comments from the users are published[89]. In addition to that, e-mails for software development & support[90] and for general information[91] are available.
- Other aspects: There are more than 40 available languages. The tool is only available for Mozilla-based browsers like Firefox.

Functionality criteria

- General functionality: It blocks JavaScript, Java, Flash and other executable content. Sites can be allowed to run scripts temporarily via the context menu.
- Processing of personal data: According to the available information, no personal data is being processed.

[84] maone.net
[85] www.informaction.com
[86] addons.mozilla.org/es/firefox/addon/noscript/versions
[87] noscript.net/changelog
[88] Some example reviews can be found in: www.miguelms.com/noscript.htm, securityinabox.org/en/guide/firefox/windows, venturebeat.com/2014/03/10/why-edward-snowden-gave-a-shoutout-to-the-noscript-add-on-for-firefox, www.ghacks.net/2014/02/10/firefox-noscript-guide-waiting, norfipc.com/internet/usar-noscript-para-navegar-internet-mas-limpio-rapido.php
[89] forums.informaction.com/viewforum.php?f=3
[90] software@informaction.com
[91] info@informaction.com

- Flexibility: The tool allows to define white/black lists and filters, and has a lot of customization options (e.g. embedded objects, exceptions to the XSS protection, etc.).
- Choice: It is possible to temporarily block and unblock specific elements.
- On/off: The tool allows to pause the blocking process, either for the current page, or for the full domain (site).
- History (of blocked elements): It is possible to check what has been blocked.
- The plugin is available in the Firefox official store, but it is not signed (as on 10/15/2015).

B.6 AdBlockPlus

AdBlockPlus[92] blocks ads by default, though it is initially configured to allow what they call «non intrusive advertising» (i.e. advertising from companies which have signed the acceptable ads manifesto with AdBlockPlus). It is necessary to configure the tool in order to eliminate these acceptable ads. In addition to that, it can be configured to block trackers, social buttons, and malware domains. There is quite a lot of documentation accesible to users (first steps, how-to-use tutorials, how to allow acceptable advertisements, FAQ, and an advanced document about how to create filters, preferences, interfaces, etc.). The source code is available for both Firefox and Chrome[93]. The available support channels are a forum[94], and an email address[95]. The documentation is clear and it consists of a FAQ[96] and additional information[97].

<u>Quality criteria</u>

- Background information: This tool is a spin-off of the former tool Adblock. The company which develops it is eyeo, and the developing team, led by Wladimir Palant, is well defined[98].
- Version history: In the Firefox store there is a list of new versions, with the new functionalities and corrected bugs of each version, when applicable[99]. At the Adblock Plus site, it is also possible to find records of changes made in files of successive versions of Adblock Plus (for both Firefox and Chrome).
- Transparency of installation and use: The installation process is transparent, and the tool offers its basic functionality (ad blocking) by default as soon as it is installed. Still, advertisements from the acceptable ads list will not be blocked and this is not clearly indicated to the users.

  The tool does not seem to include third party software or modify other applications or user configurations. Once installed, a tab is opened allowing to configure the tool for enabling malware blocking, social buttons elimination, and trackers blocking (all these options are disabled by default). It is interesting to mention that if this configuration is not made through that tab, it is not possible to do it

[92] adblockplus.org
[93] github.com/adblockplus
[94] adblockplus.org/forum
[95] info@eyeo.com
[96] adblockplus.org/faq
[97] adblockplus.org/en/android-config and adblockplus.org/en/getting_started
[98] eyeo.com/en/team
[99] addons.mozilla.org/es/firefox/addon/adblock-plus/versions, hg.adblockplus.org/adblockplus/log

through the tool's options menu (it is necessary to do it through the features option in the developer's website).

- Public reviews: The average rating at Mozilla's add-ons site is 5 over 5 (4947 reviews), and at Google Chrome's add-ons site is also 5 over 5 (86235 reviews). It is included in the Security in a Box, EPIC, Best VPN, Me and My Shadow, and Reset the Net websites[100].
- Privacy by design and by default: The tool provides adequate capacity as ad-blocker. In order to use additional privacy capabilities, it is necessary to complete a configuration process. As mentioned above, the difficulty to access these configuration options depends on whether they were activated during the initial configuration phase. Also, the acceptable ads option needs to deactivated by the user.
- Ease of use: The tool is generally easy to use for non-expert users. Blocking of images can be done via the context menu (in Chrome), also individual elements can be blocked via the user interface.
- User interaction: There is a forum[101] where users' comments are published. A blog[102] is also available to users.
- Other aspects: There are more than 25 available languages. The tool is multiplatform. There are versions for Chrome, Firefox, Internet Explorer, Safari, and Opera browsers.

Functionality criteria

- General functionality: The tool is primarily an ad blocker and not an anti-tracking tool. It blocks ads by default. It is initially configured to allow acceptable ads list (this can be changed in the options menu). It can also be configured to block trackers, social buttons, and malware domains.
- Processing of personal data: According to the available information, no personal data is processed.
- Flexibility: The tool allows to define white/black lists (only in Chrome), and to edit filters.
- Choice: It is possible to temporarily block specific elements.
- On/off: The tool allows to pause the blocking process. In the case of Firefox the options are: only for current page, for the full domain (site), or globally (for all tabs). In the case of Chrome, the option is to enable or disable blocking for the full domain.
- History (of blocked elements): It is possible to check what has been blocked, but only in Firefox. In Chrome it is only possible to check the number of blocked elements.
- The plugin is available in the official Firefox store, but it is not signed (as on 10/15/2015).

[100] Some example reviews can be found in: www.pcmag.com/article2/0,2817,2476293,00.asp, ajr.org/2015/05/08/adblock-plus-test, techcrunch.com/2013/10/07/adblock-plus-whitelist-acceptable-ads-numbers, arstechnica.com/business/2015/02/over-300-businesses-now-whitelisted-on-adblock-plus-10-pay-to-play

[101] adblockplus.org/forum

[102] adblockplus.org/blog

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 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

TP-02-15-957-EN-N

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

ISBN: 978-92-9204-157-1
DOI: 10.2824/097859