Technical Report – Self-Data Protection: On the Usability of Security & Privacy Boxes

Rafael Tarek Bela Mäuer
rafael.maeuer@smail.th-koeln.de
Technische Hochschule Köln
Cologne, NRW, Germany

ABSTRACT

The goal of this work is to investigate the usability of Security & Privacy Boxes. For this purpose, a research question is posed to evaluate the usability of Privacy Boxes in the case that users want to protect themselves against unwanted use of their data as well as intrusions into their privacy. To answer this research question, the development of an own methodology for the usability investigation of Privacy Boxes becomes necessary, since no existing methodology can be found or adapted. Furthermore eight Privacy Boxes are ordered for a usability evaluation based on a market analysis. These are assigned to two user groups identified as relevant for Privacy Boxes by a target group analysis. An evaluation methodology for Privacy Boxes is developed, based on the feature model, the device pre-selection and the defined user types.

The methodology, which is based on common analytical evaluation methods and established usability and privacy heuristics, investigates the Out-of-Box Experience and required time during setup as well as usability and usable-privacy during usage of Privacy Boxes. The results of four tested devices show: the evaluation of a Privacy Box's usability depends on the respective user type. While users with average knowledge and motivation have difficulties in implementing effective self-data protection with Privacy Boxes, users with higher motivation succeed in this task. However, this is more due to the lack of available privacy functions than to the average usability. But a large number of privacy functions is only provided by Privacy Boxes that require more effort to put into operation.

Finally, usability can be identified as a decision criterion for successful self-data protection with Privacy Boxes, as well as the number of privacy functions supported by the specific device.

KEYWORDS

privacy, usability, usable privacy, usable security, privacy by design, privacy by default, privacy boxes, security & privacy boxes, data privacy, self-privacy, self-data protection, data protection

1 INTRODUCTION

With the growth of digital connectivity and the increased use of digital services in everyday life, the amount of personal data created and used has increased massively in recent years [70]. This trend is driven by the growing number of connected devices per person from the fields of *Internet of Things* (IoT), *Smart Home* and *Wearables*. The development of business models by large platforms such as *Google* and *Facebook*, which are based on collection and exploitation of user data, indicate a strong commercial interest in this field.

Today, it is hard to imagine everyday life without using these platforms. However, the collection and utilization of user data involves risks and dangers. To avoid such dangers, data protection must be properly understood and applied. On the one hand, there are government measures with laws, as shown by the GPDR, the CCPA or the LGPD. On the other hand, there are technical tools such as ad blockers, web filters and VPN services. The latest step in this development are Security & Privacy Boxes: these involve hardware that bundles many of those technical protection functions in a single device.

The purpose of this paper is an overview of the existing range of Security & Privacy Boxes (in the following just "Privacy Boxes"), to compare them with each other and to examine their usability for the end user. However, the work does not analyze whether the promised security and privacy goals of the devices are implemented properly. Thus, it is about the development of a new methodology for usability evaluation, but not about the evaluation of the current implementation status of existing Privacy Boxes.

2 BASICS ON PRIVACY AND USABILITY

With basics on security and privacy, relevant terms such as 'personal privacy' and 'identity' will be introduced. The focus is then moved to the user. The importance of data protection is highlighted on the basis of risks and dangers. These arise from the collection and analysis of personal data. This leads to the central topic of self-data protection, as a collective term for protective measures for users. Usability basics will then follow to prepare for the pending usability study of Privacy Boxes.

2.1 Terms and Definitions

After determining the Latin word origins of *sē-cūrus* as 'sorceless' for security and *prīvātus* as 'by oneself' for privacy, the model of *personal privacy* can be introduced with the help of different dimensions of privacy: Like an onion, the outermost rings, represented by society, state, and economy, provide the minimum level of privacy, with the innermost layer representing the highest amount of privateness and thus intimacy [55, p.16]. According to the UN's Universal Declaration of Human Rights, personal privacy is even a human right, which should protect the individual from improper intrusions [43, p.22].

With the definition of *identity* the value of personal privacy for being human, and also personal data can be determined: "Identity is the authenticity of a person as a union of his presence in the online and offline world" [43, p.22f.]. Regarding the protection of personal identity, it is necessary to define the terms *anonymity* as "not being known" and *pseudonymity* as "codename usage" too. These

definitions (partially having a legal basis) help in understanding why users are the focus of further attention.

2.2 Tracking and Data-Mining

Personal data (PD), according to General Data Protection Regulation (GPDR), are "any information relating to an identified or identifiable natural person" [20]. With the digital form of PD, disclosed information is no longer temporary, but is available permanently, over the long term, and can be indexed by search engines. It can be duplicated, assembled and removed from its original context at will. The Internet's lack of social, spatial, and temporal separation results in the loss of the various social contexts of the data. The publicity of this out-of-context data that can be reassembled and reinterpreted can lead to serious problems.

Governments, especially security and intelligence agencies, are highly interested in PD, because data means information and knowledge and properly used also power and control (surveillance programs like *PRISM*, *Tempora* and *XKeyscore* are worth mentioning at this point [45]). A large number of companies have specialized in making profit from reselling data and the analytics calculated from it (besides Google and Facebook, it is worth mentioning *Palantir*, *Acxiom* and *Segment*) [28].

The accumulation of left behind *data traces* of users through the use of electronic services in everyday life is summarized as *Big Data*. The observation of people's browsing, usage and consumption behavior is called *tracking* and is also characterized as *tracing* over longer periods of time or different locations. Besides, numerical estimation of a person's property is performed on mathematical-statistical analysis of empirical values, so-called *scoring*. The next obvious step is to create digital user profiles by classifying and evaluating personal characteristics [55, pp.21-24].

The data traces generated by users largely consist of information that is generated during the online use of digital services. The data is collected when visiting websites using *cookies*, *super cookies* and *fingerprinting* technologies. Furthermore, device-specific advertising IDs are used when using mobile apps on iOS and Android in order to be able to track users across applications [7, pp.13-22].

2.3 Risks and Threats for Users

"If you are not paying for it, you're not the customer; you're the product being sold." [59]. This phrase by user *blue_beetle* (Andrew Lewis) in the blog *MetaFilter* became famous as an Internet meme in 2010. It shows the awareness that is slowly forming that free offers on the Internet are paid for with personal data. Thereby, the concern about privacy increases with age, as shown at the TU Darmstadt in 2016 by Peter Buxmann [6].

There are many ways to determine the value of user data: from the bounty *Average Revenue per User* (ARPU), to ratio of users to financial valuation of the company, down to advertising revenue generated per user. The last value can be calculated on the basis of user rank and number of advertising networks to an average of 260 US dollars for a single user per day [43, pp.46-55].

One problem users may face as the result of digital data disclosure is *manipulation* through "behavioral targeting" and "persuasion profiling." In this process, users are manipulated with *Online Behavioural Advertising* (OBA) by companies in well targeted advertising campaigns. In the case of *persuasion profiling*, the mood or temperament of users is analyzed with the help of tracking methods in order to find psychological weaknesses and exploit them in a targeted manner [43, pp.108-120].

Another risk is *social discrimination*, which can occur when employees or supervisors are given access to people's private affairs. Based on this, decisions like employment, salary negotiation or even termination can be made. The Internet also offers an easy way to harm people through *reputational damage* by falsifying online traces. However, removing data once it is online is still a complicated process [43, pp.58-88].

The dangers mentioned so far are only exceeded by *identity theft*. This involves a person's identity being hijacked and taken over by unknown actors. Attackers can then use the accounts to act on behalf of the victim and in their own interests. The damage caused to the person concerned not only affects the financial situation, but both reputation and life of the victim can be damaged and destroyed in a long-term perspective [43, p.89].

Besides all these dangers, users generally care about protecting their privacy, but they do not transfer this to their actions. This phenomenon, known as the *privacy paradox*, has also been revealed in studies [39]. By highlighting concrete problems and risks for users through surveillance, manipulation, discrimination, loss of reputation and identity theft, the value of user data is once again clarified. It also serves as motivation to investigate appropriate measures that can be used to protect against these dangers.

2.4 Self-Data Protection

"Self-data protection" is the central topic of this work which roots go back to 1983, when the right to informational self-determination laid the legal foundation for data protection [48]. Since then, many EU directives have been approved, which are legally binding in their most current form with the GPDR. The latest proposal of the European Parliament (EP) of 2017 proposes an privacy related addition with an *ePrivacy Regulation* (ePR), which however, will not be effective before 2022 [34].

In addition to the legal basis for data protection, the *standard ISO/IEC 29100* provides eleven principles developed by different countries and international organizations. This general framework is intended to help in the development and integration of systems and solutions of the information and communication sector (ICS) to improve the protection of PD by using best practices [25, p.7].

Finally, a digital bill of rights is presented which was developed by Shane Green in 2012 together with data protection experts, advertising and Internet managers under the title *"A Digital Bill of Rights by the people, for the people"* [36]. These rights describing the application of self-data protection are still valid:

(1) **Right to transparency:** use, security and value of data
(2) **Right to privacy:** protection of privacy as default
(3) **Right to choice and control:** golden copy of own data
(4) **Right to safety:** security on storage and transport
(5) **Right to identity:** multiple personages and anonymity
(6) **Right to minimal use:** use for declared purpose only

In equating digital and physical identity for the purpose of legal and social equality, there is mention of the "untouchability of the

digital self". It can be seen as a parallel to one of the most important basic human rights – *the inviolability of human dignity* [32].

2.5 Seven Steps to Digital Self Defense

In addition to the legal and organizational actions resulting from basic digital rights, there are also technical measures that users can take on their own to protect themselves from unauthorized access to their data by others. Steffan Heuer describes four steps to digital self-defense [43, p.225f.], to which three additional steps are added. By placing them in order of application, the following seven steps to digital self-defense can be identified:

Preventive measures:

(1) **Preparing** for potential vulnerabilities and the data value
(2) **Preventing** threats through proactive protection measures

Operational measures:

(3) **Denying** personal information to data collectors
(4) **Obscuring** identity through pseudonyms and anonymity
(5) **Encrypting** private data and communications

Reactive and emergency measures:

(6) **Banning** digital services and technologies
(7) **Reducing** damage to reputation and identity

The application of the presented measures for digital self-defense can be described by the term *self-data protection*: "By self-data protection is meant the technical, organizational and legal measures taken by individuals to protect their fundamental data protection rights." [16]. Users can express their displeasure with the omnipresent monitoring of their behavior through the use of self-data protection techniques [41, p.148].

2.6 Usability and User Experience

Since this work specifically examines the usability of Privacy Boxes, it is necessary to introduce the main terms related to it. An important underlying term is *Ergonomy* which means 'teachings of work' and was coined by Wojciech Jastrzębowski in 1857. The standard *DIN EN ISO 6385* describes ergonomics as the optimization of well-being and performance in the human-computer interaction (HCI) [22, p.7]. Due to the increasing 'multifunctionality' of technical systems, and increasing complexity in their operation, the question of *user-friendliness* appeared [76, p.19].

In addition to the comfortable use of a technical system, nowadays support for the user in achieving his goals is also required, which makes the term *usability* necessary. Standard *DIN EN ISO 9241-11* defines usability as: "The extent to which a system, product, or service can be used by specific users in a specific context of use to achieve specific goals with effectively, efficiently, and satisfactorily" [23, p.15]. In order to achieve a high degree of usability in HCI, there are interaction principles, of which seven describe an implementation in the standard *DIN EN ISO 9241-110.* [26, p.11]:

(1) **Suitability for the task** (e.g. characteristic features)
(2) **Self-descriptiveness** (e.g. offer adequate information)
(3) **Conformity to expectations** (e.g. predictable behavior)
(4) **Learnability** (e.g. support discovery of capabilities)
(5) **Controllability** (e.g. control of the user interface)
(6) **Robustness against user errors** (e.g. avoid errors)
(7) **User binding** (e.g. promote continuous interaction)

Since usability describes only the process during HCI, there is the concept of *User Experience* (UX), which describes the complete process of HCI before, during and after use. The UX is defined in the standard *DIN EN ISO 9241-220* as "perceptions and reactions of a person resulting from the actual and/or expected use of a system, product or service" [24, p.11]. The UX therefore describes the complete experience that results from the interaction of a system's performance, function, and presentation with a user's personality, skills, and experiences.

2.7 Usability Engineering and Evaluation

After the introduction of usability and UX as quality and success criteria of systems and products, their integration during development and possibilities of verification are of interest. In order to ensure optimal usability, appropriate criteria must be taken into consideration when developing new, technical systems. This process is known as *Usability Engineering* and is described as iterative process in the standard *DIN EN ISO 9241-220* [24, p.21].

More interesting for this work, however, is the *Usability Evaluation*, which emerges as an important component in usability engineering, since it allows the evaluation of a system or product's usability. Two different approaches are available: *analytical methods* (expert-oriented) and *empirical methods* (user-oriented). For each approach there are different methods with varying pros and cons: effort and validity as well as objectivity and reliability are important quality criteria of usability evaluation methods [68, p.224].

The following examples are well-known and established methods for evaluating usability [68, p.234], [56, p.39]:

Analytical methods:

- **Cognitive Walkthrough:** acting out typical scenarios
- **Heuristic Evaluation:** validation by use of heuristics
- **Guideline Review:** design guidelines from ergonomics
- **GOMS:** Goals, Operators, Methods and Selection Rules

Empirical methods:

- **Hallway Test:** spontaneous and random interview
- **Usability Walkthrough:** workshops with users
- **Usability Survey:** standardized questionnaires
- **A/B-Test:** comparison of two solution alternatives
- **Usability-Test:** realistic monitored user tasks

2.8 Usable Privacy and Privacy by Design

To establish the connection between the three topics of privacy, security and usability, the terms *Usable Privacy* and *Privacy by Design* are introduced and explained. The progress of user-centered development can be shown by Saltzer and Schroeder's term *Usable Security* from 1975 [75, p.1283] and Zurko and Simon's paper *"User-Centered Security"* from 1996 [97, p.1]. The parallel trend towards *User-Centered Privacy* can be easily demonstrated using GPDR Article 25 Paragraphs 1 and 2 [19]:

- GPDR Art. 25 §1: "(...) designed to implement data-protection principles (...)" can be identified with *Privacy by Design*
- GPDR Art. 25 §2: "(...) by default, only personal data which are necessary (...)" can be assimilated to *Privacy by Default*

The duty to comply with data protection-friendly default settings therefore means that the data protection settings of a product or

service must be preset to a level that complies with the data protection principles without any action being required from the user. Privacy by Default aims to strengthen the data subject's self-data protection and thus his or her sovereignty [88, p.185].

Ann Cavoukian developed seven basic principles for Privacy by Design (PbD) in 2010, which are presented below [9, p.6]:

(1) **Proactive** not Reactive; **Preventative** not Remedial
(2) Privacy as the **Default Setting**
(3) Privacy **Embedded** into Design
(4) Full Functionality – **Positive-Sum**, not Zero-Sum
(5) End-to-End Security – **Full Lifecycle Protection**
(6) **Visibility** and **Transparency** – Keep it **Open**
(7) **Respect** for User Privacy – Keep it **User-Centric**

Even though these principles describe PbD in detail, there is no explanation of practical options for implementing suitable technical and organizational measures (TOM)s. Possible solutions to this problem are presented in section 4.

3 RELATED WORK

Besides various test reports on Privacy Boxes from different Tech Magazines in 2016-17 [2, 33, 79], the current state of research on this topic does not yet give much[1]. Therefore, this chapter presents related work with the greatest possible intersections to this work. The work considered can be divided into four major topics with direct relevance: 1. Tracking and Profiling, 2. Privacy in IoT and Smart Home, 3. Privacy and (Self-)Data Protection, and 4. Usability and Usable Privacy.

3.1 Tracking and Profiling

Research exists on the understanding of Online Behavioural Advertising (OBA) and Ad Blocking Tools (ABT) or Tracking Prevention Tools (TPT) by Chanchary et al [10]. Additionally, the willingness to disclose data to third parties is investigated. These showed that only a low awareness of users about tracking as well as protection by ABT or TPT exists. On the topic of *user profiling* and OBA, Trusov et al. present a scalable method that demonstrates effectiveness based on just a small amount of data [90]. The possibility of profiling based on user-generated visual content on social networks such as Pinterest can also be verified by You et al. [93].

The practical use of *blocking extensions*, their effectiveness against tracking and the decision criteria of users are investigated by Mathur et al. It was shown that users have a basic understanding but only limited mental models about online tracking and the use of blocking extensions [66]. Furthermore, Herrmann et al. show that threats to user's personal privacy exist with *behavioral tracking* that operate autonomously and are very difficult for the users to defend against [42, 54].

3.2 Privacy in IoT and Smart Home

Security experts' concerns about risks to user privacy from IoT highlight the need for protection of the many connected devices in *smart homes* [94]. Ziegeldorf et al. analyze privacy issues related to IoT based on the evolution of features, trends, and their privacy implications. They present an IoT threats model that identifies user profiling, identification and tracking as risks [96].

The vulnerability of smart homes to security and privacy issues are identified by Geneiatakis at al. as attacks like eavesdropping, identity theft, Denial of Service (DoS), or exploitation of software vulnerabilities, most of which can occur due to weak default passwords and low network protection [31]. Expectations, actions, and attitudes of smart home users about security and privacy are examined by Zeng et al. Interviews with smart home residents revealed incomplete mental models and a dangerous imbalance between administrators and residents of smart homes [94].

Most recently, Zheng et al. investigated user perceptions of privacy in smart home IoT devices, finding four recurring issues [95]:

(1) Desire for comfort to justify sacrifice of privacy
(2) Acceptance of data disclosure depends on the benefit
(3) Awareness and reputation influence the purchase
(4) No sense of privacy risks from connected devices

Recommendations to device designers, researchers, and industry are developed to better align device privacy features with the expectations and preferences of smart home owners.

3.3 Privacy and (Self-)Data Protection

The Platform for Privacy Preferences (P3P) project, involving Lorrie Cranor and the W3C, can be considered an origin of technical implementations for privacy concepts. The approach allowed users to configure their personal privacy settings in an P3P-enabled web browser. These could be processed in a standard computer-readable format when web pages are accessed. The project failed due to lack of implementations [14].

Another concept using Privacy by Design (PbD) as a guideline for translating complex social, legal, and ethical concerns into system requirements was proposed and later refined by Gürses et al. [37, 38]. The work is expanded by Jaap-Henk Hoepman, who developed eight data protection strategies with help of *DIN EN ISO/IEC 29100* standard. The strategies are divided in data-oriented (*minimize*, *hide*, *separate*, *aggregate*) and process-oriented strategies (*inform*, *control*, *enforce*, *demonstrate*) [44].

Motivated by the *privacy paradox*, Trepte et al. propose in their paper a comprehensive scale for measuring privacy literacy and its implementation in future research and policymaking (OPLIS) [89]. In response, Philipp K. Masur proposes a reconceptualization that takes into account not only factual knowledge about economic, technical, and legal aspects of online privacy, but also dimensions of privacy-related reflective and critical skills, as well as concrete privacy and data protection capabilities [65, 64].

The challenge of integrating privacy-enhancing technologies into the infrastructure of the Internet is presented by Harborth et al [40]. Other difficulties encountered in developing software systems when embedding privacy into applications are mentioned by Senarath and Arachchilage [83]. Coopamootoo et al. investigate why user privacy is often neglected [12] and Rudolph et al. further develop an intension model that can be used to explain why users often ignore privacy policies [72].

It can be concluded that the implementation of applicable data privacy and self-data protection does not work properly in many

[1] Results of searches on ResearchGate, ACM Digital Library, IEEE Xplore, SpringerLink and Microsoft Academic for the term "Privacy Box" and similar queries (as of 10/05/2020).

places yet. In numerous cases, privacy protection is ignored and data protection guidelines are dismissed.

3.4 Usability and Usable Privacy

One of the most well-known papers on the topic of usability in security tools is Whitten and Tygar's study of the email encryption tool *PGP 5.0 "Why Johnny Can't Encrypt"* [91]. Many other works followed over time, with the investigation of *PGP 9* by Sheng et al. [85] or the evaluation of the modern PGP client *Mailvelope* by Ruoti et al. [74]. The results showed that more than 15 years after the original study by Whitten and Tygar, modern PGP tools are still unusable for the masses.

In the privacy tools area, the usability of the P3P user agent *Privacy Bird* was investigated by Cranor et al. [15]. The performance of popular ad blockers, including *AdBlock Plus* and *Ghostery*, on a large number of news websites has been studied by Leon et al. later on [58]. One of the most recent studies on usability of the four popular browser add-ons *AdBlock Plus*, *uBlock Origin*, *Ghostery*, and *Privacy Badger* was conducted by Hubert et al. [46].

The presented work reveals that the underlying concepts of security and privacy tools are not understood by novice users and not clearly communicated by software vendors. Meaningful feedback mechanisms are needed so users are able to protect their privacy using TPT to effectively apply self-data protection.

In order to understand users' mental models Raja et al. and later Kang et al. studied users' mental models in relation to privacy and security decisions [71]. Despite different mental models, no direct relationship between users' technical background and the privacy protection measures taken could be identified [51].

The impact of browser extensions on users' awareness and concern about privacy was studied by Schaub et al. In addition to increased awareness about privacy, the study of the popular TPTs *Ghostery*, *DoNotTrackMe* (today *BLUR*) and *Disconnect* identified additional usability issues [78]. Another recent study of the browser extensions *DuckDuckGo Privacy Essentials Ghostery* and *Privacy Badger* by Corner et al. aimed, in addition to usability, at responses about trust, concern and control of users [13].

Finally, both the background and experience of users determine the extent of their mental models. Since less detailed mental models can cause dangerous mistakes, the points of complexity and usability must be weighed against each other with great care, especially in the area of security and privacy.

4 PRIVACY BOXES

Ubiquitous tracking and profiling in all areas of private life requires protection against threats such as *manipulation*, *discrimination*, *identitytheft*, and *reputational damage*. The range of TOMs in which users can actively protect themselves can be identified in the technical measures at the network level. Privacy Boxes therefore are a promising solution for users to protect their privacy.

A Privacy Box combines various functions in one hardware product to enhance user security and privacy, where the term *"Security & Privacy Box"* comes from. It can be defined as follows:

> "A Privacy Box is an electronic device in the form of a hardware-software combination that provides maximum privacy when using the Internet." [77, p.100]

The goal of a Privacy Box is to empower and protect the security and privacy of the user in as many activities and operations on the Internet as possible.

4.1 Research Questions

Based on the findings of the previous basics and the current research state, the following research question is formulated:

Q *How should the usability of Privacy Boxes be evaluated if users want to protect themselves from unwanted use of their data as well as intrusions into their privacy?*

The research question aims to determine whether usability in the use of Privacy Boxes can help users to implement self-data protection. It is further specified:

Q1 *Is it possible for users to correctly connect and set up Privacy Boxes to protect their data and privacy?*

Q2 *Are users appropriately supported by the user interface of Privacy Boxes in typical application scenarios for self-data protection?*

As a result, the mentioned research questions mainly aim at investigating the usability of Privacy Boxes during their setup (Q1) and their usage (Q2).

4.2 Self-data Protection Tools

The following overview of 20 self-data protection tools summarizes important measures users can take to protect their privacy during activities on the Internet. The collection is inspired by *selbstdatenschutz.info* [63] and the chapter "Five levels of defense" by Steffan Heuer [43, p.228f.]:

Preventive measures

1) Awareness about PD's value: *calc.datum.org*
2) Know about the use of data: *youronlinechoices.com*
3) Detect weaknesses and threats: *haveibeenpwned.com*
4) Create and use of strong passwords: *lastpass.com*
5) Avoid privacy-critical services: *privacytools.io*
6) Self-reflect prior sharing: *ais.co.th/thinkbeforesocial/en*

Operational measures

7) Usage of blocker software: *privacybadger.org*
8) Prevent device fingerprinting: *mybrowseraddon.com*
9) Delete sessions and cookies: *github.com/Cookie-AutoDelete*
10) Use of pseudonyms on the web: *mysudo.com*
11) Use secure DNS/VPN services: *dnsforge.de / nordvpn.com*
12) Use of different browsers: *brave.com, waterfox.net*
13) Use transport encryption: *eff.org/https-everywhere*
14) Encrypt chats, emails and calls: *signal.org, jitsi.org*
15) Encrypting data and storage: *veracrypt.fr*

Reactive and emergency measures

16) Use privacy-friendly services: *qwant.com, joinmastodon.org*
17) Social cleanup & digital suicide: *socialsweepster.com*
18) Avoid and turn off technologies: *paysafecard.com*
19) Using the right to be forgotten: *support.google.com/legal*
20) Apply reputation management: *primseo.de*

For each of the self-data protection tools presented, a concrete example for realization was provided (link in *italics* behind).

The tools were then sorted into the *Seven Steps to Digital Self Defense* and evaluated in terms of their feasibility in Privacy Boxes:

		Feasibility of tool with Privacy Boxes	yes	pt.	no
Preventive	Prepare	T1 Awareness about PD's value		✓	
		T2 Know about the use of data		✓	
		T3 Detect weaknesses and threats		✓	
	Prevent	T4 Create and use strong passwords	✓		
		T5 Avoid privacy-critical services			✓
		T6 Self-reflect prior content sharing			✓
Operational	Deny	T7 Usage of blocker software	✓		
		T8 Prevent device fingerprinting	✓		
		T9 Delete sessions and cookies		✓	
	Obscure	T10 Use of pseudonyms on the web			✓
		T11 Use secure DNS / VPN services	✓		
		T12 Use of different browsers		✓	
	Encrypt	T13 Use transport encryption	✓		
		T14 Encrypt chats, emails and calls	✓		
		T15 Encrypting data and storage			✓
Reactive	Ban	T16 Use privacy-friendly services		✓	
		T17 Social cleanup & digital suicide			✓
		T18 Avoid and turn off technologies			✓
	Red.	T19 Using the right to be forgotten			✓
		T20 Apply reputation management			✓

Table 1: Self-data protection tools with Privacy Boxes

The measures in table 1 are rated as "yes", "pt." and "no", where "pt." means that realization with Privacy Boxes is only partially possible or with additional components (such as user feedback channels).

4.3 Market Analysis and Overview

To provide a current overview and classification of "Privacy Boxes" in the field of privacy and security hardware, a brief market overview follows. A division is made between wired solutions for stationary use and portable solutions for mobile use. In addition, there are commercial products for sale as well as open source and do it yourself (DIY) solutions.

Consumer Products (Stationary)

- **Bitdefender BOX 2:** Security center from Bitdefender GmbH, which promises improvements for user privacy and data protection in addition to enhanced security for all home network devices [5]
- **F-Secure SENSE:** Security router from F-Secure GmbH, designed to protect the Internet activity of all networked devices in the home from cyberattacks and block malicious websites and other threats [30]
- **TrutzBox Home:** Device from Comidio GmbH with a focus on data protection and privacy, which already becomes clear in the product slogan "back to privacy". Offers protection functions in five different areas [11]
- **Winston Privacy Filter:** Device from Winston Privacy LLC focused on Internet privacy. Provides protection against tracking and blocks advertising and malware [92]
- **RATtrap**: Device from IoTDefense Inc. that provides users increased security and privacy through privacy protection of all devices connected to the network [17]

Consumer Products (Portable)

- **Keezel 2.0:** Portable cyber security firewall that protects users on the go from phishing, malware, snoopers and hackers using VPN encryption [52]
- **InvizBox Go**: Portable device that protects users on the go from ads and malicious sites with VPN encryption of all traffic and AdBlocker [47]

Kickstarter Projects

- **anonabox Pro:** Kickstarter/Indiegogo project that redirects all network traffic over the TOR network or a VPN server in addition to web servers and file sharing [60]
- **Relaxbox/Tarnomat:** Box to protect against malware and Trojans with antivirus and improve privacy with content filtering and anti-fingerprinting techniques [53, 87]
- **eBlocker 2:** Device that prevents online tracking and advertising, protects against malware and Internet dangers, blocks harmful content, adds parental controls, and provides anonymity while surfing [27]
- **AKITA:** Network scanner for use with IoT or Smart Home devices. Protects users' security and privacy by monitoring the home network for unusual activity and blocking it immediately [1]

Open Source and DIY Products

- **Pi-hole 5:** *Raspberry Pi*-based solution for network-wide filtering of advertisements by DNS servers and extendable by a VPN service [61]
- **Syncloud:** A personal server for running your own web services from home such as ad blocking, VPN server, file sharing as well as private chats, calls and web meetings [62]
- **upribox 3:** Provides a way for more privacy on the Internet by preventing advertising and tracking or anonymizing Internet traffic through the TOR network [18]
- **FreedomBox:** A sort of private server where open source software is available for VPN servers, ad blockers, hosts for email, video conferencing, chats and more [67]
- **Anonymebox 3 Plus:** Raspberry Pi based anonymous access to the internet via TOR, encryption of internet communication and change of personal IP address at any time [4]

4.4 Device Functions and Pre-Selection

As the presented devices reveal, the functional scope of Privacy Boxes varies a lot. The identified self-data protection functions are grouped into six different areas:

(1) Security: *anti-virus*, *firewall*, *IoT monitor*, *password manager*
(2) Tracking: *content filtering*, *ad blocking*, *anti-tracking*, *DNS protection*, *VPN tunnel*, *privacy mesh*, *TOR network*
(3) Communication: *secure calls*, *private web meetings*, *secure chats*, *secure emails*, *private social networks*
(4) Cloud services: *notes*, *calendar*, *contacts Cloud Storage*, *web hosting*, *email server*, *git server*
(5) Trust and control: *open source code web dashboard*, *smartphone app*, *router*, *WiFi network*, *mobile protection*
(6) Cost: *purchase price*, *subscription price*

The number of supported functions serves as one parameter for determining a representative preselection for the study from the market overview. Further criteria are the representation of all product categories and the availability for ordering and use in Germany. As a result, eight devices remain as a representative pre-selection for the Privacy Boxes presented, which form the basis for the following chapters and the investigation:

Consumer Products (Stationary and *Portable*)
(1) Bitdefender BOX 2
(2) F-Secure SENSE
(3) TrutzBox Home
(4) RATtrap
(5) *Keezel 2.0*

***Kickstarter* and Open Source Products**
(6) *eBlocker 2*
(7) Syncloud R
(8) FreedomBox

5 METHODOLOGY

To begin with the development of a methodology for the usability evaluation of Privacy Boxes, the object of investigation is further specified. First, a feature model is created from the functional areas of Privacy Boxes already presented. This enables an assignment of self-data protection functions and tools in the second step.

5.1 Feature Model of Privacy Boxes

Figure 1 shows the feature model, the affiliation of the five areas to the three basic principles of Privacy Boxes is shown by the outer labeling: 1. *security* (dark red), 2. *privacy* (red and light red) and 3. *usability* (black). The color scheme is chosen to show the area of interest in black and all areas with Privacy Box functions or properties in red.

In addition to the five areas, the model also consists of three rings. The innermost ring defines the self-data protection goal of the respective area (*what* should be achieved?). The middle ring describes the effects of situations in which users want to achieve the goal (*when* should the goal be achieved?). The outer ring, contains concrete functions or attributes that can be used to achieve the goal of the area (*how* should the goal be achieved?).

The *security* is an important basis of Privacy Boxes as the first area of the model (cf. fig. 1 dark-red section). It represents an important, *preventive* measure for self-data protection and guards, for example, against misuse or theft of PD by third parties. The aim of the 'Security' area is to establish a private IT security management (*IT protection*).

The *privacy* is the second and most important basis of Privacy Boxes and determines the second, third and fourth sections of the model (cf. fig. 1 red and light red sections). Privacy is the main goal of a Privacy Box and can be additionally divided into *operative* (red) and *reactive* (light-red) areas of application.

The *operational* areas of privacy (cf. fig. 1 red sections) are determined by active self-data protection measures applied while using the Internet. *Anonymity*, as the first goal, provides users with more privacy while surfing as well as protection from OBA and unwanted tracking or tracing on the Internet. *Confidentiality*, as a second goal, provides secure and protected communication, between two ore more participants.

The *reactive* area of privacy (cf. fig. 1 light-red section) concerns self-data protection measures that are often deployed after usage has already occurred (e.g., by switching from Gmail to a self-hosted mail service). *Autonomy* represents the goal of this area. It allows users to be independent from the services of large companies that may follow critical privacy practices.

The *usability* makes up the final basis of Privacy Boxes (cf. fig. 1 black section). Good *UX / usability* is considered the goal of this section, because intuitive setup and ease of use are key to successful self-data protection with Privacy Boxes. They concern the channels for user interaction and feedback which can be realized both in the form of *software interfaces* and *hardware interfaces*.

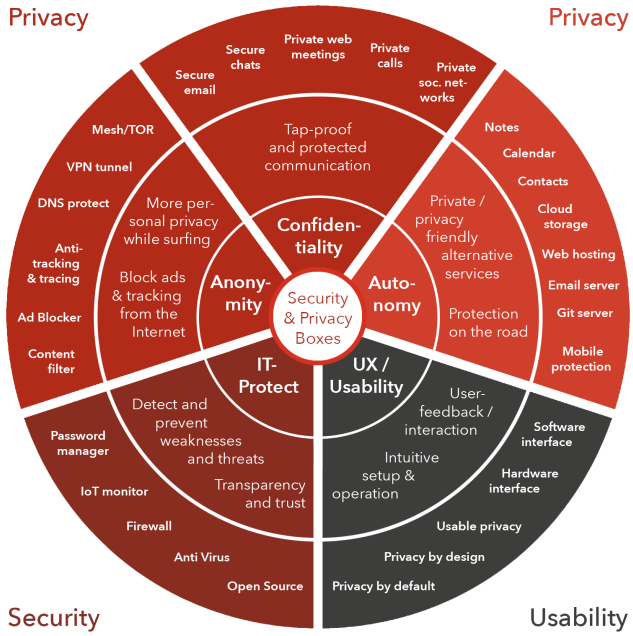

Figure 1: Feature model of Privacy Boxes

However, the assignment of features and functions to the five domains of the feature model is not exclusive, i.e., features can be applied in other domains as well as in several domains of the model. Using the feature model, self-data protection with Privacy Boxes can be described very clearly through the associated properties and functions.

5.2 Protection with Privacy Boxes

The maximum protection possible for users with the help of Privacy Boxes can be described as the highest match of privacy tools that can be realized with Privacy Boxes. To determine this match, a mapping of tools and functions to self-data protection is performed.

The mapping of privacy tools and features of Privacy Boxes results in ten matches, three of which required customization during the mapping process[2].

[2]Updates of tools in table 2 are marked with asterisk* and italic text

In addition, four properties of Privacy Boxes were identified that contribute to the quality and feasibility of self-data protection.

Tool 3*	Detect weaknesses and *prevent* threats
Tool 4	Create and use strong passwords
Tool 5*	Avoid *(privacy-)* critical services *and contents*
Tool 7	Usage of blocker software
Tool 8	Prevent device fingerprinting
Tool 9*	Delete sessions and *block* cookies
Tool 11	Use secure DNS / VPN services
Tool 13	Use transport encryption
Tool 14	Encrypt chats, emails and calls
Tool 16	Use privacy-friendly services
Prop. 1	Trust in product and vendor
Prop. 2	Mobile protection on the go
Prop. 3	Interfaces for interaction and feedback
Prop. 4	Interfaces and connectivity

Table 2: Maximum protection with Privacy Boxes

With this overview of tools and properties of Privacy Boxes for self-data protection, the definition of 'maximum protection' is sufficiently specified. It combines both 'maximum privacy' and 'maximum security', which is possible through the use of Privacy Boxes.

5.3 Target Group Definition

In order to determine the target group of Privacy Boxes, it is necessary to know and understand the differences in knowledge, experience and motivation of users with regard to security and privacy. For this purpose, the method *personas* is used. The basis for scientific personas in the field of privacy was developed by Alan F. Westin, already in the years from 1978 to 2004. In more than 30 surveys about privacy, three different user categories with varying levels of privacy awareness could be identified [57, p.5]:

(1) The privacy Fundamentalists (25%)
(2) The Pragmatic (57%)
(3) The Unconcerned (18%)

This categorization was further refined by Dupree et al.: the category of 'Pragmatic' is subdivided into the roles of *Lazy Experts*, *Technicians*, and *Amateurs* [21, p.5233f.]:

- **Fundamentalists** *(high knowledge, high motivation)*: No trust in security technologies, unique passwords, encryption of external storage, very concerned about their privacy, need fine-granular adjustment options due to knowledge
- **Lazy Experts** *(high knowledge, low motivation)*: Well-informed, convenience over security, socializing over privacy, believe not to be a target, strong passwords, use of advanced skills to reduce need of security-interaction
- **Technicians** *(medium knowledge, high motivation)*: Highly motivated, inform about security, understand before acting, personal passwords, privacy over online presence, concerns about safety can be postponed or forgotten
- **Amateurs** *(medium knowledge, medium motivation)*: Inform about security, not competent enough to distinguish good and bad advice, trust in foreign networks, multi-layer passwords, willing to protect if given enough information
- **Marginally Concerned** *(low knowledge, low motivation)*: Limited awareness of security concepts, knowledge from word of mouth, trust in pretended security, fallback authentication, single favored password, no worries about threats

Based on these descriptions, Rudolph et al. developed a classification according to the characteristics 'knowledge' and 'motivation' of the five user types [73, p.251]:

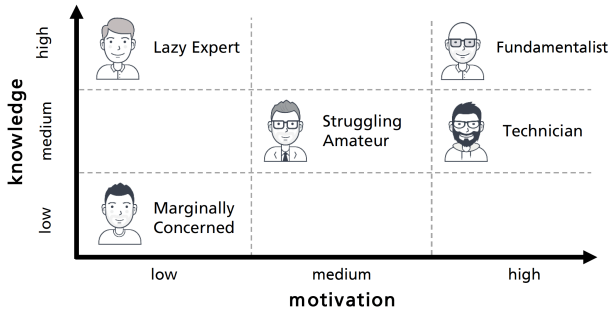

Figure 2: Knowledge vs. motivation of user types [73, p.251]

Considering the classification of these five user types (fig. 2), *Marginally Concerned* as well as *Lazy Experts* can be excluded from Privacy Boxes due to too low motivation for self-data protection. The *Fundamentalists*, on the other hand, do not rely on Privacy Boxes to implement successful self-data protection. This leaves the *Struggling Amateurs* and the *Technicians* as the target group for Privacy Boxes: willing to improve the protection of their security and privacy with help of a hardware device.

For users to effectively, efficiently, and satisfactorily implement self-data protection with Privacy Boxes, their motivation must be able to outweigh potential obstacles to setup and use. This requires good usability of the interaction and feedback channels between user and device. The *Struggling Amateurs* rely on products from the consumer sector, whereas *Technicians* can additionally use products from the DIY sector due to their higher motivation.

As a result of the different motivations within the target group, the Privacy Boxes in the pre-selection were assigned to the two identified user types on the basis of the effort required for initial startup. Only TrutzBox Home changes the original classification[3]:

Struggling Amateurs	**Technicians**
(1) Bitdefender BOX 2	(1) TrutzBox Home
(2) F-Secure SENSE	(2) eBlocker 2
(3) RATtrap	(3) Syncloud R
(4) Keezel 2.0	(4) FreedomBox

5.4 Application Scenarios

To identify typical application scenarios, frequently used Internet activities and measures against data misuse are analyzed. With their help, tasks that play a central role in the use of Privacy Boxes can be determined. For this purpose, two studies are used as a basis and the individual activities and measures are grouped into Privacy Box application areas. Weightings are then calculated, taking frequencies into account, which can be displayed.

[3]The ordered variant with WiFi for self-assembly is the reason for this

As the data from the first study [8, p.21f.] shows, about three quarters of typical user scenarios take place while 'Surfing the Internet' (red), so privacy measures aimed at *anonymity* are most frequently required. Just under a quarter of the user scenarios involve 'Web Communication' (orange), which means that the goal of *confidentiality* appears to be less relevant. The use of 'Cloud Services' (yellow), with a very small amount of user scenarios, however, shows that privacy measures aiming at *autonomy* have hardly any relevance for Privacy Boxes, similarly less than 'Other' (gray) activities (cf. fig. 3).

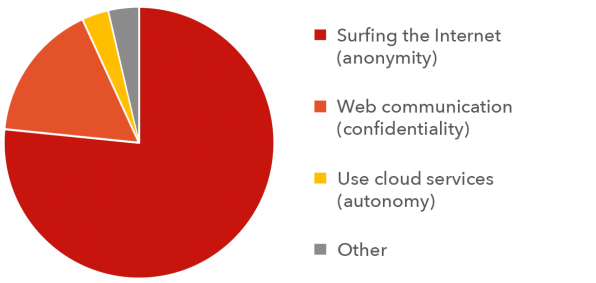

Figure 3: Internet activities for Privacy Box application

Data from the second study [86] shows that 'IT Security Management' (black) with the aim of private *IT Protection* takes up the largest part of the protective measures used (over one third). A similar relevance for users is represented by measures for 'Protection against Tracking/Tracing' (green) with the protection of *anonymity* (another third). *confidentiality* with measures to 'Protect Communications' (blue) seems to be less important to users (less than a quarter). 'Other' measures account for a small part (cf. fig. 4).

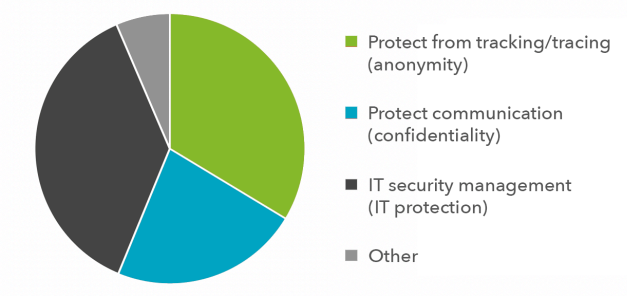

Figure 4: Protective measures for Privacy Box application

Finally, it can be noted that none of the activities mentioned address the area of 'Security' and none of the measures mentioned address the goal of *autonomy*. Thus, only data from the areas of 'Surfing' and 'Communication' are available for a comparison, which ratio is shown in fig. 5.

It can be demonstrated that only one third of the activities in *surfing the Internet* take place with a *protection from tracking* (green). Two thirds of the activities in *surfing the Internet* (red) are unprotected and represent a potential for improvement for Privacy Boxes in the area of 'Surfing'. For the activities of *web communication*, it can be shown that about only a quarter of the activities are performed with a *protection of communication* (blue). Three quarters of the *web communication* (orange) takes place without protection and also means a potential for improvement by Privacy Boxes in the area of 'Communication'.

However, by comparing the areas 'surfing' and 'communication', it becomes clear that the potential for improvement by Privacy Boxes in *communication* is relatively high at three quarters, but only accounts for a smaller share (absolute) compared to the potential for improvement in *surfing*. Since the number of frequent activities in *surfing the Internet* is significantly higher in total, the relatively small improvement potential of one-third nevertheless accounts for the largest share (in absolute terms).

Consequently, the area of 'Protection from Tracking/Tracing' can be confirmed as the most important area of Privacy Boxes, offering the greatest potential for improvement that can be achieved by Privacy Boxes.

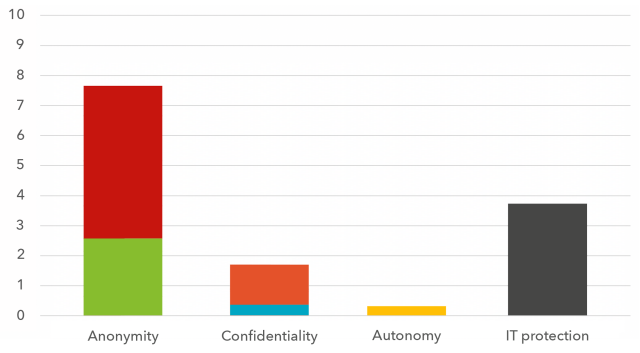

Figure 5: Relationship of activities to protective measures

Since the potential for improvement in the areas of 'Cloud Services' and 'IT Security' cannot be determined, the results of the comparison for the areas of 'Surfing' and 'Communication' can only be taken as a trend. To weight the relevance of all areas, therefore, a weighting based on the overall frequencies of activities and protective measures is used (rounded maximum values from fig. 5):

- **8** for *Surfing the Internet* (high count of frequent activities)
- **2** for *Web communication* (low count of frequent activities)
- **0** for *Use of cloud services* (too low count of freq. activities)
- **4** for *IT security management* (mid count of freq. measures)

5.5 Device Selection and User Tasks

Based on this weighting, promising devices can be identified from the representative pre-selection for comparison. A calculation is performed for the comparability of all Privacy Boxes. In the process, identical functions are counted for each device combination and weighted with the previously defined score. Accordingly, a higher value means the higher number of comparable functions with a high relevance due to the weighting.

In table 3 both the results from device comparisons of *struggling amateurs* (right/top), as well as the *technicians* (left/bottom)

are shown. A higher value here indicates greater significance in a usability evaluation.

–	BOX	**SENSE**	RATtrap	Keezel	*Amateur*
TrutzBox	–	**5**	2	2	**BOX**
eBlocker	**6**	–	3	2	SENSE
Syncloud	5	5	–	2	RATtrap
Free.Box	5	4	4	–	Keezel
Technician	**TrutzBox**	eBlocker	Syncloud	Free.Box	–

Table 3: Comparability of Privacy Boxes

For the suitable Privacy Boxes for *technicians*, a comparison of the devices 'eBlocker 2' and 'TrutzBox Home' with a score of 6 points seems particularly promising. In the case of devices for *struggling amateurs*, the comparison between 'F-Secure SENSE' and 'Bitdefender BOX 2' with a result of 5 points shows the most meaningful result. Therefore, the following device selection can be determined for the usability study:

Devices for Amateurs
- Bitdefender BOX 2
- F-Secure SENSE

Devices for Technicians
- TrutzBox Home
- eBlocker 2

With the intersection of common functions of the selected Privacy Boxes to be compared, the application scenarios to be analyzed can be defined for both user types. Here, the selection of user tasks is again performed according to the weighting. For the *technicians* all tasks from the area 'Surfing the Internet' can be chosen. Since the intersection of functions from this area is too small for the devices of *amateurs*, additional tasks from the next important area 'IT Security' are added:

Tasks for Amateurs
(1) Use of *VPN tunnel*
(2) Enable *content filters*
(3) Setup network *firewall*
(4) Setting up *Anti-Virus*
(5) Setting the *IoT monitor*

Tasks for Technicians
(1) Setup *anti-tracking*
(2) Setting *DNS protection*
(3) Use of *VPN tunnel*
(4) Configure *ad-blockers*
(5) Enable *content filters*

5.6 Evaluation Method

When choosing a suitable evaluation method for analyzing the usability of Privacy Boxes, an expert-oriented approach was chosen. Since there are no studies in this field of research yet, whose results could be elaborated with an empirical investigation, an analytical investigation is appropriate, since it allows the consideration of a broad range of usability aspects.

To answer the first research question (Q1), it is necessary to investigate the unpacking and setup of Privacy Boxes. Since this concerns a subset of the product life cycle, Out-of-Box Experience (OOBE) is selected from the field of UX methods. For this purpose, heuristics of OOBE are used as best practices [69, p.43], as well as an existing investigation method originally used for HDMs and PDAs [84, p.5]. Since the method was designed as an empirical study, it had to be adapted as an analytical method.

To answer the second research question (Q2), the analytical evaluation methods already mentioned in section 2.7 were analyzed regarding different quality criteria to determine the best method. For this purpose, reviews of the methods Guideline Review (GR), Goals, Operators, Methods and Selection Rules (GOMS), Cognitive Walkthrough (CW), and Heuristic Evaluation (HE) from four different papers [68, 56, 76, 50] were compared with each other.

The CW and HE emerged as the most promising methods from the comparison. Both are well-established methods, but the HE is not very structured, as the evaluator only has a list of usability heuristics for guidance. The CW, on the other hand, provides a very structured process since the execution is done using a list of user tasks. This, in turn, loses the exploration of a system, resulting in fewer problems being found.

To avoid the mentioned disadvantages and to combine the strengths of both methods, the Heuristic Walkthrough (HW) is used as a combination of both methods. It combines the free-form evaluation and usability heuristics from the HE with user tasks and questions about important parts of the interaction process from the CW [82, p.219].

The HW consists of two passes: In the first run, prioritized user tasks are completed while becoming familiar with the system (cf. section 5.5). In the second run, the system is evaluated using usability heuristics. Any established heuristic can be used here.

5.7 Usability Heuristics

As heursitic for the HW the usability principles of Granollers [35, p.62] are used. He combines two established and proven heuristics of Nielsen and Tognazzini with each other (cf. fig. 6).

Resulting Principles
1.- Visibility and system state
2.- Connection between the system and the real world, metaphor usage and human objects
3.- User control and freedom
4.- Consistency and standards
5.- Recognition rather than memory, learning and anticipation
6.- Flexibility and efficiency of use
7.- Help users recognize, diagnose and recover from errors
8.- Preventing errors
9.- Aesthetic and minimalist design
10.- Help and documentation
11.- Save the state and protect the work
12.- Colour and readability
13.- Autonomy
14.- Defaults
15.- Latency reduction

Figure 6: Granoller's usability heuristics [35, p.61]

Each of the 15 heuristics from fig. 6 additionally provides a set of concrete questions formulated in a way that is favorable for usability. This means an answer of 'Yes' (1 point) represents good usability of the feature – consequently 'No' (0 points) means the opposite. If the answer is ambiguous, 'Neither' (0,5 points) can be used to define a mean value. If a question is irrelevant to the feature, the answer 'Not applicable' (- points) serves to mark it as insignificant. This 4-option rating scale helps the evaluator from having to deal with rating the severity of issues on a scale during the study.

Finally, the method allows for a quantification of the results, which makes it possible to calculate the usability of the evaluated interface. This final value, called 'Usability Percentage' (UP), allows

to compare different User Interface (UI)s as well as the ratings of different evaluators.

5.8 Privacy Heuristics

To test the relevance of privacy heuristics for the usability evaluation of Privacy Boxes, three different approaches are reviewed, each based on *GPDR*:

Usable Privacy Criteria: Approach to usable-privacy evaluation combining privacy principles with usability criteria [49]. Built on: *GPDR*, *ISO/IEC 29100* and *ISO 9241-11*. Relevant and useful for a usability study of Privacy Boxes when investigating application scenarios where PD is collected, processed, or stored (e.g. user scenarios with protected communications and privacy-friendly alternative services). However, it is not applicable for the usability study of Privacy Boxes in the context of this work.

Privacy Design Strategies: Approach to close the gap between the legal framework of GPDR and available privacy design strategies and technological implementation measures (as of 2015) by combining Privacy with Usable Privacy [29]. Built on: *GPDR*, *ISO/IEC 29100* and *Seven Basic Principles of PbD*. Intersections can be identified in some principles to be realized using Privacy Boxes. Due to missing concrete scales, and little intersection with use cases, no added value is seen for the study.

Digital Privacy Nudges: Approach to help users make "better" privacy decisions using nudges [81]. Building on: *GPDR*, *BDSG*. Privacy nudging can have both positive and negative influences. Deriving six relevant dimensions of privacy nudges from current research: 1. default, 2. color elements, 3. information, 4. feedback, 5. time delay, 6. social norm. Thanks to illustrated examples, privacy nudges are seen as an additive value for the usability evaluation of Privacy Boxes therefore taken into account (cf. fig. 7).

Privacy Nudge	Example
Default	Privat Deine Channels werden standardmäßig als privat eingestellt. Geschlossene Channels sind nur auf Einladung zugänglich und erscheinen nicht in der Channel-Liste.
Color Elements	Privat Geschlossene Channels sind nur auf Einladung zugänglich und erscheinen nicht in der Channel-Liste.
Information	Im Durchschnitt können 38 Personen deine Nachrichten sehen.
Feedback	Du hast 80% deiner persönlichen Informationen angegeben
Time Delay	Die Nachricht wird in 5 Sekunden gesendet Bearbeiten Verwerfen Sofort senden
Social Norm	75 % deiner Kollegen geben ihre Telefonnummer nicht an.

Figure 7: Digital Privacy Nudges (mod. [81, p.332])

'Privacy nudges' are considered as heuristics for the intersection of usability and privacy in the scope of usability evaluation of Privacy Boxes for the rating of usable-privacy (cf. fig. 7). Additionally, there is a follow-up paper that evaluates the privacy nudges according to user acceptance [80] which is used for the score calculation later.

6 EVALUATION

The developed evaluation method for measuring the usability of Privacy Boxes is performed with the devices and user tasks mentioned in section 5.5.

6.1 Procedure, Pilot and Setup

The following schedule serves as a guideline for execution:

(1) Determination of OOBE using the heuristics of Moya and Burgess [69] and the questionnaires of Serif and Ghinea [84]
(2) Examination of usability with typical application scenarios and usability heuristics using HW by Granollers [35]
(3) Review of the implementation of privacy nudges according to Schomberg et. al [81] and evaluation according to the user ranking of Schöbel et al [80]
(4) Evaluation of results, calculation of UX, usability and privacy scores and interpretation using rating scales
(5) Result comparison with a device from the same user group

Prior to execution, the evaluation methodology is piloted using the remaining pre-selected devices 'RATtrap', 'Keezel 2.0' and 'Syncloud R' to find problems and optimize the method. In addition, an independent test network is set up with a separate router.

For the usability study of the Privacy Boxes, a FRITZ!Box is used as a router for access to the Internet, network connections (LAN) and wireless network (WiFi). An iPhone 6S (iOS 14), a Galaxy A6 (Android 10) as well as an *ASUS laptop* (Windows 10, Ubuntu 18) and an *Apple MacBook* (macOS Catalina) are available. The study is then performed using the Privacy Boxes 'Bitdefender BOX 2', 'F-Secure SENSE', 'Trutzbox Home' and 'eBlocker 2' (cf. fig. 8 a-d).

(a) Bitdefender BOX 2 [5]

(b) F-Secure SENSE [30]

(c) TrutzBox Home [11]

(d) eBlocker 2 [27]

Figure 8: Privacy Boxes for evaluation

After calculating the UX, usability and privacy scores, the values have to be evaluated and interpreted with help of rating scales. For OOBE and usability, a scientifically collected rating according to System Usability Scale (SUS)-scale was used for this purpose [3, p.592]. Separate rating scales were defined for evaluating the time required for setup of the Privacy Boxes and the subsequently determined privacy nudges.

In addition, it was evaluated whether the user tasks could be completed successfully. These were carried out as part of the HW. The result provides information about the quality of the research conducted at the beginning or about the truthfulness of the manufacturer information.

6.2 Results and Comparison

Table 4 shows the evaluation results including the number of usability problems found. For the purpose of comparability, the results are presented without any deductions due to 'showstoppers' (superscripts) that occurred. This way, the Privacy Boxes in question are not disadvantaged in the comparison due to possibly only random problems. However, the 'showstoppers' are taken into account in the subsequent comparison.

User type	*Struggling Amateur*		*Technician*	
Privacy Box	**Bitdefen. BOX 2**	**F-Secure SENSE**	**TrutzBox Home**	**eBlocker 2**
OOBE-Rate	Very Good	Almost Perfect	Near Good[1]	Almost Very Good
OOBE-Time	OK	Near Good	OK[2]	Good
Tasks (Solved)	30%	30%	80%	100%
Tasks (Time)	01:02	00:45	03:15	02:35
Usability-Rate	OK[3]	Almost Very Good	Near Good	Very Good
Issues/Critical	2 / 1	– / –	15+ / 2	3 / –
Privacy-Rate	Poor	Poor	Near Good	Very Good

[1] The final evaluation is adjusted by two critical 'showstoppers' on *poor*.
[2] The result came with an 'USB3 stick', else the rating is seen as *worst imaginable*.
[3] The final evaluation is adjusted by one critical 'showstopper' on *poor*.

Table 4: Evaluation results of Privacy Boxes

As table 4 shows: with the *very good* to *almost perfect* OOBE of *Bitdefender BOX 2* (BOX) and *F-Secure SENSE* (SENSE) a lot of effort was put into optimizing this process by the vendors. The time required for this was *OK* to *nearly good*. There were difficulties with both devices when performing typical application scenarios, which result in only 30% solvability of the user tasks.

The usability evaluation shows that the rate *OK* of the BOX can be attributed to the integration of functions into the existing Bitdefender Central app. Therefore functions are neither prominently placed nor optimized for use. With the SENSE, on the other hand, a separate app was developed for setup and configuration. The result of *almost very good* usability makes it clear that the app is specifically designed for the use of the SENSE.

Two usability issues and one showstopper were found on the BOX, whereas no problems were detected with the SENSE. The implementation of privacy nudges was *poor* on both devices. Even without counting the critical 'showstopper', which significantly worsens the BOX' usability result (on *poor*), the SENSE achieves better results in all categories. Thus, the SENSE is the winner of the Privacy Box comparison for *Struggling Amateurs*.

When comparing *eBlocker 2* (eBlocker) and *TrutzBox Home* (TrutzBox), the eBlocker achieves the better result at the OOBE (*almost very good*) compared to the TrutzBox (only *near good*). The required time for the process ranges from *OK* to *good*, but in case of TrutzBox only by using a fast USB3-Stick during firmware installation (the result is rated as *worst imaginable* otherwise).

When performing typical application scenarios, it turns out that both TrutzBox and eBlocker deserve to be called a "Privacy Box". The high solvability of the examined user tasks with 80% and 100%, respectively, shows that the manufacturers mostly keep their promises about the implemented self-data protection features in the Privacy Boxes .

Even though 'showstoppers' are not as serious with *technicians* due to their higher motivation, two 'showstoppers' must be evaluated as a limiting barrier when setting up the TrutzBox. In addition, difficulties occur in some places during use, as evidenced by the number of usability problems found with the TrutzBox (15+). The complexity and amount of information presented can be challenging even for *technicians*. This is sufficient for *near good* usability, which concerns the implementation of privacy nudges too.

In contrast to TrutzBox, the eBlocker offers users just the right amount of information, which can be recognized by a *very good* usability and implementation of privacy nudges. Apart from three usability problems, however, no critical 'showstoppers' were encountered. By default, only necessary information is formulated in a short and simple way, which can have additional details and higher complexity if needed. In the direct comparison of all analyzed criteria, eBlocker emerges as the winner of the comparison of Privacy Boxes for *Technicians*.

7 CONCLUSION

To conclude this work by answering the research questions: If users want to protect themselves from unwanted use of their data as well as privacy intrusions, the evaluation of the usability of Privacy Boxes depends on the respective user type.

For the *Struggling Amateurs* it is possible to set up and use Privacy Boxes, as long as there are no critical errors that prevent the further process. However, the devices they can use do not provide sufficient privacy protection functionality. This makes effective self-data protection with Privacy Boxes difficult for this user group, despite average usability.

For *Technicians*, the setup and use of Privacy Boxes is possible, even if major errors occur in the process. The devices available to them offer a variety of privacy features, so effective self-data protection with Privacy Boxes is possible. Users in this group are supported by the devices with an average of more than good usability in typical application scenarios.

In this work, the basics of self-data protection were elaborated and, due to a lack of related work, an own method was developed to determine and evaluate the usability of Privacy Boxes. Frequent Internet activities and protection measures were taken into account in the selection of devices and user tasks to be investigated. Four devices for two user types were examined and evaluated for UX-usability and privacy criteria.

For the validity of the results, however, it is necessary to mention that while care was taken to ensure accuracy and objectivity in the conduct of the study, errors may have occurred in the collection and analysis of the results.

In addition, errors in the development of the methodology cannot be disregarded, such as incorrect aggregation of statistical data, wrong interpretations and simplifying of assumptions. For this reason, it is desirable that the developed methodology is critically examined in future work. Thereby, quality criteria such as correctness of the results, completeness as well as efficiency and reproducibility of the method can be examined.

REFERENCES

[1] Akita. *AKITA Amazon Shop | Instant WiFi Privacy Protection for Smart Home Devices.* en-us. 2020. URL: https://www.amazon.com/stores/AKITA/AKITA/page/B4C14F79-CBAC-409E-B237-258837C0C6E8 (visited on 10/07/2020).

[2] Arne Arnold. *Sicherheitsboxen im Test: Schutz oder Augenwischerei?* de-DE. Oct. 2016. URL: https://www.pcwelt.de/ratgeber/Sicherheitsboxen-im-Test-10059814.html (visited on 06/22/2020).

[3] Aaron Bangor, Philip T. Kortum, and James T. Miller. "An Empirical Evaluation of the System Usability Scale". In: *International Journal of Human–Computer Interaction* 24.6 (July 2008), pp. 574–594. ISSN: 1044-7318. DOI: 10.1080/10447310802205776.

[4] Maximilian Batz. *pi3g - Anonymebox 3 Plus.* de. 2020. URL: https://buyzero.de/products/anonymebox-anonym-frei-einfach (visited on 10/08/2020).

[5] Bitdefender. *BOX - Heimnetzwerksicherheit für alle Ihre vernetzten Geräte.* de_DE. 2020. URL: https://www.bitdefender.de/box/ (visited on 10/06/2020).

[6] Peter Buxmann. *Der Preis des Kostenlosen – Was sind unsere Daten wert? – Prof. Dr. Peter Buxmann.* de-DE. Aug. 2016. URL: https://www.peterbuxmann.de/2016/08/15/preis-des-kostenlosen/ (visited on 07/14/2020).

[7] BVDW. *Browsercookies und alternative Tracking-Technologien: Technische und datenschutzrechtliche Aspekte.* de. Whitepaper. Berlin: Bundesverband Digitale Wirtschaft (BVDW) e.V., Aug. 2015, p. 27.

[8] BVDW. *Digitale Nutzung in Deutschland 2018.* de. Marktforschung. Düsseldorf: Bundesverband Digitale Wirtschaft (BVDW) e.V., 2018, p. 100.

[9] Ann Cavoukian. "Privacy by Design - The 7 Foundational Principles". en. In: *Information and Privacy Commissioner of Ontario* (May 2010), p. 12.

[10] Farah Chanchary and Sonia Chiasson. "User perceptions of sharing, advertising, and tracking". In: *Proceedings of the Eleventh USENIX Conference on Usable Privacy and Security.* SOUPS '15. Ottawa, Canada: USENIX Association, July 2015, pp. 53–67. ISBN: 978-1-931971-24-9.

[11] Comidio. *Trutzbox - Ihre Privacy Box. Mehr Schutz im Internet.* de-DE-formal. 2020. URL: https://trutzbox.de/trutzbox/ (visited on 10/06/2020).

[12] Kovila P. L. Coopamootoo and Thomas Groß. "Why Privacy Is All But Forgotten: An Empirical Study of Privacy & Sharing Attitude". en. In: *Proceedings on Privacy Enhancing Technologies* 2017.4 (Oct. 2017), pp. 97–118. DOI: 10.1515/popets-2017-0040.

[13] Matthew Corner et al. "A Usability Evaluation of Privacy Add-ons for Web Browsers". en. In: *Design, User Experience, and Usability. Practice and Case Studies.* Ed. by Aaron Marcus and Wentao Wang. Lecture Notes in Computer Science. Cham: Springer International Publishing, 2019, pp. 442–458. ISBN: 978-3-030-23535-2. DOI: 10.1007/978-3-030-23535-2_33.

[14] Lorrie Faith Cranor. *Web Privacy with P3p.* English. 1st Edition. Beijing ; Sebastopol, Calif: O'Reilly Media, Oct. 2002. ISBN: 978-0-596-00371-5.

[15] Lorrie Faith Cranor, Praveen Guduru, and Manjula Arjula. "User interfaces for privacy agents". en. In: *ACM Transactions on Computer-Human Interaction* 13.2 (June 2006), pp. 135–178. ISSN: 1073-0516. DOI: 10.1145/1165734.1165735.

[16] Der Sächsische Datenschutzbeauftragte. *Selbstdatenschutz.* de. Jan. 2012. URL: https://web.archive.org/web/20120105070747/http://www.saechsdsb.de:80/datenschutz-fuer-buerger/112-selbstdatenschutz (visited on 07/21/2020).

[17] IoT Defense. *RATtrap - Technology.* en-US. 2020. URL: https://www.myrattrap.com/technology/ (visited on 10/06/2020).

[18] Markus Donko-Huber. *Usable Privacy Box - Privatsphäre im Internet.* 2020. URL: https://upribox.org/ (visited on 10/08/2020).

[19] Art. 25 DSGVO. *Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen.* de. May 2018.

[20] Art. 4 DSGVO. *Begriffs-bestimmungen.* de. May 2018.

[21] Janna Lynn Dupree et al. "Privacy Personas: Clustering Users via Attitudes and Behaviors toward Security Practices". en. In: *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems.* San Jose California USA: ACM, May 2016, pp. 5228–5239. ISBN: 978-1-4503-3362-7. DOI: 10.1145/2858036.2858214.

[22] DIN e.V. *2016-12:DIN EN ISO 6385, Grundsätze der Ergonomie für die Gestaltung von Arbeitssystemen; Deutsche Fassung.* de. Norm. Beuth Verlag GmbH, Dec. 2016, p. 26. DOI: 10.31030/2429191.

[23] DIN e.V. *2018-11:DIN EN ISO 9241-11, Ergonomie der Mensch-System-Interaktion - Teil 11: Gebrauchstauglichkeit: Begriffe und Konzepte; Deutsche Fassung.* de. Norm. Beuth Verlag GmbH, Nov. 2018, p. 46. DOI: 10.31030/2757945.

[24] DIN e.V. *2020-03:DIN EN ISO 9241-210, Ergonomie der Mensch-System-Interaktion - Teil 210: Menschzentrierte Gestaltung interaktiver Systeme; Deutsche Fassung.* de. Norm. Beuth Verlag GmbH, Mar. 2020, p. 47. DOI: 10.31030/3104744.

[25] DIN e.V. *2020-09:DIN EN ISO/IEC 29100, Informationstechnik - Sicherheitsverfahren - Rahmenwerk für Datenschutz; Deutsche Fassung.* de. Norm. Beuth Verlag GmbH, Sept. 2020, p. 34. DOI: 10.31030/3174636.

[26] DIN e.V. *2020-10:DIN EN ISO 9241-110, Ergonomie der Mensch-System-Interaktion - Teil 110: Interaktionsprinzipien; Deutsche Fassung.* de. Norm. Beuth Verlag GmbH, Oct. 2020, p. 47. DOI: 10.31030/3147467.

[27] eBlocker. *eBlocker Open Source: Kostenlos anonym surfen. Plus Ad-Blocker. Schützt alle Geräte.* de-DE. 2020. URL: https://eblocker.org (visited on 10/07/2020).

[28] Jasmine Enberg. *Global Digital Ad Spending 2019.* 2020. URL: https://www.emarketer.com/content/global-digital-ad-spending-2019 (visited on 07/07/2020).

[29] ENISA. *Privacy and data protection by design - from policy to engineering.* en. LU: Publications Office, Jan. 2015.

[30] F-Secure. *SENSE - Sicherer Router und sichere App.* de. 2020. URL: https://www.f-secure.com/de/home/products/sense (visited on 10/06/2020).

[31] Dimitris Geneiatakis et al. "Security and privacy issues for an IoT based smart home". In: *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO).* Opatija, Croatia: IEEE, May 2017, pp. 1292–1297. ISBN: 978-953-233-090-8. DOI: 10.23919/MIPRO.2017.7973622.

[32] Art. 1 GG. *Die Grundrechte.* de. May 1949.

[33] Hauke Gierow. *Privacy-Boxen im Test: Trügerische Privatheit - Golem.de.* de-DE. Apr. 2016. URL: https://www.golem.de/news/privacy-boxen-im-test-truegerische-privatheit-1604-120250.html (visited on 06/22/2020).

[34] PROLIANCE GmbH. *Neue ePrivacy Verordnung.* de. Nov. 2019. URL: https://www.datenschutzexperte.de/blog/datenschutz-und-eu-dsgvo/review-was-bringt-die-neue-eprivacy-verordnung/ (visited on 09/08/2020).

[35] Toni Granollers. "Usability Evaluation with Heuristics, Beyond Nielsen's List". In: Mar. 2018, pp. 60–65. ISBN: 978-1-61208-616-3.

[36] Shane Green. *Revisiting a crowdsourced Digital Bill of Rights "by the people, for the people" from SXSW 2012.* en. Dec. 2018. URL: https://shanegreen.org/2018/12/20/revisiting-a-crowdsourced-digital-bill-of-rights-by-the-people-for-the-people-from-sxsw-2012/ (visited on 07/16/2020).

[37] Seda Gürses, Carmela Troncoso, and Claudia Diaz. "Engineering Privacy by Design". en. In: (Jan. 2011), p. 25.

[38] Seda Gürses, Carmela Troncoso, and Claudia Diaz. "Engineering Privacy by Design Reloaded". en. In: (Sept. 2015), p. 21.

[39] Kai Haller. "Sicherheitsbewusstsein bei der Nutzung von Apps". In: *mediaTest digital* (Sept. 2013).

[40] David Harborth et al. "Integrating Privacy-Enhancing Technologies into the Internet Infrastructure". In: *arXiv:1711.07220 [cs]* (Nov. 2017).

[41] Dominik Herrmann. "Notwehr oder notwendiger Ungehorsam? Wirksamer Selbstdatenschutz geht manchmal zulasten anderer". In: *digma: Zeitschrift für Datenrecht und Informationssicherheit* (Sept. 2014), pp. 148–152.

[42] Dominik Herrmann et al. "Behavior-based tracking of Internet users with semi-supervised learning". en. In: *2016 14th Annual Conference on Privacy, Security and Trust (PST).* Auckland, New Zealand: IEEE, Dec. 2016, pp. 596–599. ISBN: 978-1-5090-4379-8. DOI: 10.1109/PST.2016.7906992.

[43] Steffan Heuer. *Mich kriegt ihr nicht!: Die wichtigsten Schritte zur digitalen Selbstverteidigung.* Deutsch. 1st ed. Murmann Publishers GmbH, 2019.

[44] Jaap-Henk Hoepman. "Privacy Design Strategies". en. In: *ICT Systems Security and Privacy Protection.* Ed. by Nora Cuppens-Boulahia et al. IFIP Advances in Information and Communication Technology. Berlin, Heidelberg: Springer, 2014, pp. 446–459. ISBN: 978-3-642-55415-5. DOI: 10.1007/978-3-642-55415-5_38.

[45] Martin Holland. *NSA-Überwachungsskandal: PRISM, Tempora und Co. - was bisher geschah.* de. Oct. 2013. URL: https://www.heise.de/newsticker/meldung/NSA-Ueberwachungsskandal-PRISM-Tempora-und-Co-was-bisher-geschah-1909702.html (visited on 07/22/2020).

[46] Marvin Hubert, Joachim Griesbaum, and Christa Womser-Hacker. "Usability von Browsererweiterungen zum Schutz vor Tracking". de. In: *Information - Wissenschaft & Praxis* 71.2-3 (Apr. 2020), pp. 95–106. ISSN: 1619-4292, 1434-4653. DOI: 10.1515/iwp-2020-2075.

[47] InvizBox. *InvizBox Go | Award winning portable VPN Router.* en-US. 2020. URL: https://www.invizbox.com/products/invizbox-go/ (visited on 10/07/2020).

[48] Autorenteam iRights.Lab. *Das Recht auf informationelle Selbstbestimmung | bpb.* de. Oct. 2017. URL: https://www.bpb.de/gesellschaft/digitales/persoenlichkeitsrechte/244837/informationelle-selbstbestimmung (visited on 07/16/2020).

[49] Johanna Johansen and Simone Fischer-Hübner. "Making GDPR Usable: A Model to Support Usability Evaluations of Privacy". In: *arXiv:1908.03503 [cs]* 576 (2020), pp. 275–291. DOI: 10.1007/978-3-030-42504-3_18.

[50] Philipp Jordan. "Auswahl einer geeigneten Methode zur Usability Evaluation". de. In: *KTD* (2008). DOI: 10.13140/RG.2.1.2956.9448.

[51] Ruogu Kang et al. "'My Data Just Goes Everywhere:' User Mental Models of the Internet and Implications for Privacy and Security". en. In: 2015, pp. 39–52. ISBN: 978-1-931971-24-9.

[52] Keezel. *Keezel – Online Security for Everyone.* en. 2020. URL: https://eu.keezel.co/ (visited on 10/06/2020).

[53] Kickstarter. *RelaxBox - a box to thouroughly secure your internet access.* de. Oct. 2015. URL: https://www.kickstarter.com/projects/470304262/relaxbox-a-box-to-thouroughly-secure-you-internet (visited on 10/07/2020).

[54] Matthias Kirchler et al. "Tracked Without a Trace: Linking Sessions of Users by Unsupervised Learning of Patterns in Their DNS Traffic". en. In: *Proceedings of the 2016 ACM Workshop on Artificial Intelligence and Security - ALSec '16*. Vienna, Austria: ACM Press, 2016, pp. 23–34. ISBN: 978-1-4503-4573-6. DOI: 10.1145/2996758.2996770.

[55] klicksafe. *Privatshphäre und Big Data*. de. Lern-Baustein. Medienanstalt Rheinland-Pfalz (LMK) und Landesanstalt für Medien NRW, May 2015, p. 52.

[56] KUM. *Methodenhandbuch zur nutzerzentrierten Entwicklung*. de. Handbuch. Kompetenzzentrum Usability für den Mittelstand, July 2015, p. 59.

[57] Ponnurangam Kumaraguru and Lorrie Faith Cranor. "Privacy Indexes: A Survey of Westin's Studies". en. In: (Dec. 2005), p. 22.

[58] Pedro Leon et al. "Why Johnny can't opt out: a usability evaluation of tools to limit online behavioral advertising". In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI '12. New York, NY, USA: Association for Computing Machinery, May 2012, pp. 589–598. ISBN: 978-1-4503-1015-4. DOI: 10.1145/2207676.2207759.

[59] Andrew Lewis. *blue_beetle - User-driven discontent - MetaFilter*. Aug. 2010. URL: https://www.metafilter.com/95152/Userdriven-discontent#3256046 (visited on 07/07/2020).

[60] Anonabox LLC. *Anonabox | Privacy Protected | Tor Router | VPN Router | Access Deep Web*. en-US. 2020. URL: https://www.anonabox.com/ (visited on 10/07/2020).

[61] Pi-hole LLC. *Pi-hole - Network-wide Ad Blocking*. en-US. 2020. URL: https://pi-hole.net (visited on 10/08/2020).

[62] Syncloud Ltd. *Syncloud - Ihr persönlicher Server*. de. 2020. URL: https://syncloud.org/ (visited on 10/21/2020).

[63] Markus Mandalka. *Digitale Selbstverteidigung für Eilige*. 2020. URL: https://www.selbstdatenschutz.info/digitale_selbstverteidigung (visited on 07/03/2020).

[64] Philipp K. Masur. "How Online Privacy Literacy Supports Self-Data Protection and Self-Determination in the Age of Information". en. In: *Media and Communication* 8.2 (June 2020), pp. 258–269. ISSN: 2183-2439. DOI: 10.17645/mac.v8i2.2855.

[65] Philipp K. Masur. "Mehr als Bewusstsein für Privatheitsrisiken. Eine Rekonzeptualisierung der Online- Privatheitskompetenz als Kombination aus Wissen, Fähig- und Fertigkeiten". de. In: *M&K Medien & Kommunikationswissenschaft* 66.4 (2018), pp. 446–465. ISSN: 1615-634X. DOI: 10.5771/1615-634X-2018-4-446.

[66] Arunesh Mathur et al. "Characterizing the use of browser-based blocking extensions to prevent online tracking". In: *Proceedings of the Fourteenth USENIX Conference on Usable Privacy and Security*. SOUPS '18. Baltimore, MD, USA: USENIX Association, Aug. 2018, pp. 103–116. ISBN: 978-1-931971-45-4.

[67] Eben Moglen. *FreedomBox - Personal Server at Home*. en. 2020. URL: https://freedombox.org/ (visited on 10/08/2020).

[68] Christian Moser. "Usability Testing". de. In: *User Experience Design: Mit erlebniszentrierter Softwareentwicklung zu Produkten, die begeistern*. Ed. by Christian Moser. X.media.press. Berlin, Heidelberg: Springer, 2012, pp. 219–242. ISBN: 978-3-642-13363-3. DOI: 10.1007/978-3-642-13363-3_10.

[69] Cathy Moya and Susan Burgess. "Out of Box and First Time User Experiences". en. In: (2011), p. 45.

[70] PricewaterhouseCoopers. *Datenkonsum - German Entertainment & Media Outlook 2018-2022*. de_de. Oct. 2018. URL: https://www.pwc.de/de/technologie-medien - und - telekommunikation / german - entertainment - and - media - outlook-2018-2022/datenkonsum.html (visited on 07/17/2020).

[71] Fahimeh Raja, Kirstie Hawkey, and Konstantin Beznosov. "Revealing hidden context: improving mental models of personal firewall users". en. In: *Proceedings of the 5th Symposium on Usable Privacy and Security - SOUPS '09*. Mountain View, California: ACM Press, 2009, p. 1. ISBN: 978-1-60558-736-3. DOI: 10.1145/1572532.1572534.

[72] Manuel Rudolph, Denis Feth, and Svenja Polst. "Why Users Ignore Privacy Policies – A Survey and Intention Model for Explaining User Privacy Behavior". en. In: *Human-Computer Interaction. Theories, Methods, and Human Issues*. Ed. by Masaaki Kurosu. Lecture Notes in Computer Science. Cham: Springer International Publishing, 2018, pp. 587–598. ISBN: 978-3-319-91238-7. DOI: 10.1007/978-3-319-91238-7_45.

[73] Manuel Polst Rudolph, Svenja Polst, and Denis Feth. "Usable Specification of Security and Privacy Demands: Matching User Types to Specification Paradigms". en. In: *Proceedings of the Mensch und Computer 2019 Workshop on Usable Security und Privacy*. Hamburg: Gesellschaft für Informatik e.V., 2019, pp. 248–255. DOI: 10.18420/MUC2019-WS-302-05.

[74] Scott Ruoti et al. "Why Johnny Still, Still Can't Encrypt: Evaluating the Usability of a Modern PGP Client". In: *arXiv:1510.08555 [cs]* (Jan. 2016).

[75] J.H. Saltzer and M.D. Schroeder. "The protection of information in computer systems". en. In: *Proceedings of the IEEE* 63.9 (Sept. 1975), pp. 1278–1308. ISSN: 1558-2256. DOI: 10.1109/PROC.1975.9939.

[76] Florian Sarodnick and Henning Brau. *Methoden der Usability Evalution: Wissenschaftliche Grundlagen und praktische Anwendung*. Deutsch. 3. unveränd. Bern: Hogrefe AG, 2015. ISBN: 978-3-456-85597-4.

[77] Hermann Sauer. "TrutzBox Kompendium Version 6.3". de. In: *Comidio GmbH* (Aug. 2020), p. 213. URL: https://trutzbox.de/trutzbox/#support (visited on 09/28/2020).

[78] Florian Schaub et al. "Watching Them Watching Me: Browser Extensions Impact on User Privacy Awareness and Concern". en. In: *Proceedings 2016 Workshop on Usable Security*. San Diego, CA: Internet Society, 2016. ISBN: 978-1-891562-42-6. DOI: 10.14722/usec.2016.23017.

[79] Mattias Schlenker. *Privacy-Boxen im Test: Trutzbox, Eblocker und Co. - PC Magazin*. de-DE. May 2017. URL: https://www.pc-magazin.de/testbericht/privacy-boxen - test - trutzbox - eblocker - pihole - upribox - 3197771.html (visited on 06/22/2020).

[80] Sofia Schöbel et al. "Understanding User Preferences of Digital Privacy Nudges – A Best-Worst Scaling Approach". en. In: Maui, Hawaii, USA., Jan. 2020, pp. 3918–3927. DOI: 10/1/JML_769.pdf.

[81] Sabrina Schomberg et al. "Ansatz zur Umsetzung von Datenschutz nach der DSGVO im Arbeitsumfeld: Datenschutz durch Nudging". de. In: *Datenschutz und Datensicherheit - DuD* 43.12 (Dec. 2019), pp. 774–780. ISSN: 1862-2607. DOI: 10.1007/s11623-019-1204-5.

[82] Andrew Sears. "Heuristic Walkthroughs: Finding the Problems Without the Noise". en. In: *International Journal of Human-Computer Interaction* (Nov. 2009). DOI: 10.1207/s15327590ijhc0903_2.

[83] Awanthika Senarath and Nalin A. G. Arachchilage. "Why developers cannot embed privacy into software systems?: An empirical investigation". en. In: *Proceedings of the 22nd International Conference on Evaluation and Assessment in Software Engineering 2018 - EASE'18*. Christchurch, New Zealand: ACM Press, 2018, pp. 211–216. ISBN: 978-1-4503-6403-4. DOI: 10.1145/3210459.3210484.

[84] T Serif and G Ghinea. "HMD vs. PDA: A Comparative Study of the User Out-of-Box Experience". en. In: (Sept. 2009), p. 27.

[85] Steve Sheng, Levi Broderick, and Colleen Alison Koranda. "Why Johnny Still Can't Encrypt: Evaluating the Usability of Email Encryption Software". en. In: (2006), p. 2.

[86] Statista. *Einsatz von Maßnahmen zum Schutz vor Datenmissbrauch im Internet 2017*. de. 2017. URL: https://de.statista.com/statistik/daten/studie/28771/umfrage/haltung-zu-sicherheitsrisiken-im-internet/ (visited on 11/10/2020).

[87] Tarnomat. *Wechselangebot für Relaxbox-Kunden*. de-DE. 2020. URL: https://www.tarnomat.com/relaxbox/ (visited on 10/07/2020).

[88] Laura F. Thies et al. "Anforderungs- und Entwurfsmuster als Instrumente des Privacy by Design". de. In: *Die Fortentwicklung des Datenschutzes: Zwischen Systemgestaltung und Selbstregulierung*. Ed. by Alexander Roßnagel, Michael Friedewald, and Marit Hansen. DuD-Fachbeiträge. Wiesbaden: Springer Fachmedien, 2018, pp. 175–191. ISBN: 978-3-658-23727-1. DOI: 10.1007/978-3-658-23727-1_10.

[89] Sabine Trepte et al. "Do People Know About Privacy and Data Protection Strategies? Towards the "Online Privacy Literacy Scale" (OPLIS)". en. In: *Reforming European Data Protection Law*. Ed. by Serge Gutwirth, Ronald Leenes, and Paul de Hert. Law, Governance and Technology Series. Dordrecht: Springer Netherlands, 2015, pp. 333–365. ISBN: 978-94-017-9385-8. DOI: 10.1007/978-94-017-9385-8_14.

[90] Michael Trusov, Liye Ma, and Zainab Jamal. "Crumbs of the Cookie: User Profiling in Customer-Base Analysis and Behavioral Targeting". In: *Marketing Science* 35.3 (Apr. 2016), pp. 405–426. ISSN: 0732-2399. DOI: 10.1287/mksc.2015.0956.

[91] Alma Whitten and J. D. Tygar. "Why Johnny can't encrypt: a usability evaluation of PGP 5.0". In: *Proceedings of the 8th conference on USENIX Security Symposium - Volume 8*. SSYM'99. USA: USENIX Association, Aug. 1999, p. 14.

[92] Winston. *Privacy Filter | Online privacy protection for your entire home*. en. 2020. URL: https://winstonprivacy.com/pages/technology (visited on 10/06/2020).

[93] Quanzeng You, Sumit Bhatia, and Jiebo Luo. "A picture tells a thousand words-About you! User interest profiling from user generated visual content". In: *Signal Processing* 124.C (July 2016), pp. 45–53. ISSN: 0165-1684. DOI: 10.1016/j.sigpro.2015.10.032.

[94] Eric Zeng, Shrirang Mare, and Franziska Roesner. "End user security & privacy concerns with smart homes". In: *Proceedings of the Thirteenth USENIX Conference on Usable Privacy and Security*. SOUPS '17. Santa Clara, CA, USA: USENIX Association, July 2017, pp. 65–80. ISBN: 978-1-931971-39-3.

[95] Serena Zheng et al. "User Perceptions of Smart Home IoT Privacy". en. In: *Proceedings of the ACM on Human-Computer Interaction* 2.CSCW (Nov. 2018), pp. 1–20. ISSN: 2573-0142, 2573-0142. DOI: 10.1145/3274469.

[96] Jan Henrik Ziegeldorf, Oscar Garcia Morchon, and Klaus Wehrle. "Privacy in the Internet of Things: threats and challenges: Privacy in the Internet of Things: threats and challenges". en. In: *Security and Communication Networks* 7.12 (Dec. 2014), pp. 2728–2742. ISSN: 19390114. DOI: 10.1002/sec.795.

[97] Mary Ellen Zurko and Richard T. Simon. "User-centered security". en. In: *Proceedings of the 1996 workshop on New security paradigms*. NSPW '96. Lake Arrowhead, California, USA: Association for Computing Machinery, Sept. 1996, pp. 27–33. ISBN: 978-0-89791-944-9. DOI: 10.1145/304851.304859.