"Do We Call Them That? Absolutely Not.": Juxtaposing the Academic and Practical Understanding of Privacy-Enhancing Technologies

Alexandra Klymenko*, Stephen Meisenbacher*, Luca Favaro, and Florian Matthes
Technical University of Munich
School of Computation, Information and Technology
Garching, Germany
{alexandra.klymenko, stephen.meisenbacher, luca.favaro, matthes}@tum.de

***Abstract*—Privacy-Enhancing Technologies (PETs) have gained considerable attention in the past decades, particularly in academia but also in practical settings. The proliferation of promising technologies from research presents only one perspective, and the true success of PETs should also be measured in their adoption in the industry. Yet, a potential issue arises with the very terminology of *Privacy-Enhancing Technology*: what exactly is a PET, and what is not? To tackle this question, we begin with the *academic side*, investigating various definitions of PETs proposed in the literature over the past 30 years. Next, we compare our findings with the awareness and understanding of PETs *in practice* by conducting 20 semi-structured interviews with privacy professionals. Additionally, we conduct two surveys with 67 total participants, quantifying which of the technologies from the literature practitioners consider to be PETs, while also evaluating new definitions that we propose. Our results show that there is little agreement in academia and practice on how the term *Privacy-Enhancing Technologies* is understood. We conclude that there is much work to be done towards facilitating a common understanding of PETs and their transition from research to practice.**

I. Introduction

The discussion of Privacy-Enhancing Technologies (PETs) very often focuses on the technology itself: a particular technology may be characterized by its unique approach to privacy protection, by which its inclusion under the umbrella of PETs may become readily apparent. The name *Differential Privacy* (DP), for example, may vouch for an immediate acceptance into the class of *Privacy*-Enhancing Technologies. *Homomorphic Encryption* (HE) and *Secure Multi-party Computation* (SMPC) often also receive this designation. In other circles, however, password managers and email encryption would likewise be classified as PETs. While the underlying goal of all these technologies may be aligned, it may become challenging to view them in the same light.

In order to tackle this lack of alignment, one might wish to rely on a common definition of what it means to be a PET, which would ideally contain a list of criteria with which one could make an informed decision: PET or not a PET. Alas, such a common understanding does not yet exist; there is no common understanding or generally accepted definition for Privacy-Enhancing Technologies. This fact is emphasized in the Privacy Tech Strategy Recommendations to the White House [1], claiming that in order to develop an effective national strategy on privacy tech, "there must be clarification and standardization of what [is] mean[t] by privacy tech, privacy enhancing technologies (PETs), and related terminology", implying the lack of a universally accepted definition.

The issue portrayed in this statement runs deeper, when one considers the practical side of PETs. In order for PETs to achieve their goal of privacy protection, they must exit the academic sphere and be implemented in real-world use cases. In crossing the academic-practical divide, though, the question becomes whether the practical perspective of what a PET is aligns with the academic view.

Thus, we make concrete two potential setbacks in the research and implementation of PETs: (1) an unclear definition of PETs in general, particularly from a theoretical perspective, and (2) a gap in awareness and understanding between the academic side researching PETs and the practical side implementing them. Furthermore, we posit that (1) could play a major role in exacerbating (2).

To investigate the prevalence of this issue, we first survey the academic understanding of PETs by exploring the key characteristics of PETs, as discussed in the literature, and how these characteristics have evolved over time. This is accomplished by conducting a Systematic Literature Review (SLR) of relevant PET literature from the past 30 years, dating back to the inception of the term *Privacy-Enhancing Technology*. In doing this, we hope to encapsulate the academic understanding of PETs, facilitating the following analysis.

The second phase of our work sets the scope to the practical side, where we aim to investigate the understanding

*Equal contribution.

Symposium on Usable Security and Privacy (USEC) 2025
24 February 2025, San Diego, CA, USA
ISBN 979-8-9919276-5-9
https://dx.doi.org/10.14722/usec.2025.23045
www.ndss-symposium.org, https://www.usablesecurity.net/USEC/

of PETs from the viewpoint of privacy professionals. Here, the goal becomes not only to investigate the term *PET* and the technologies themselves, but also to evaluate which of the identified aspects from the first phase are most relevant to practitioners. To foster this discussion, we conduct a two-sided, mixed methods study, first interviewing 20 privacy professionals and then conducting a two-phase survey study with 67 total participants. The primary goal of these two studies is to gain both qualitative and quantitative data which provide insights into the practical understanding of PETs, particularly in juxtaposition to the findings from our SLR.

Our findings include seven definitions, derived from 37 primary literature sources. These definitions shed light on the *building blocks* that have shaped the academic PETs thinking in the past three decades. We put these definitions under the microscope in our practice-oriented study, which ultimately validates the hypothesis that there is little agreement as to which technologies are PETs, and more importantly, what a common definition of PETs could be. Presented with this disparity in understanding, we propose an updated definition of PETs, which takes inspiration from our building blocks and fuses the feedback from practitioners. With this, we hope to take a first step in making the concept of PETs more available and understandable for practitioners in general.

Our work makes the following contributions to the field of Privacy-Enhancing Technologies:

1) We provide a comprehensive survey of PET definitions in the literature, uncovering seven foundational definitions, from which seven *building blocks* are derived.
2) We identify the list of technologies considered to be PETs in the literature and quantify their prevalence.
3) We probe the practical perspective on PETs, exploring the perceived gap between academia and industry.
4) We quantify the degree to which PETs stemming from the literature are considered PETs in practice.
5) We synthesize our findings to construct an updated definition of PETs, and evaluate the understandability, completeness, and scope of our proposed definition.

The structure of our work is as follows. In Section II, we introduce PETs and their rising prevalence. Section III outlines our methodology, divided into our conducted SLR, interviews, and surveys. Section IV begins our research findings with an overview of PET definitions and their corresponding building blocks. These become the basis for Section V, which reports the major findings of the semi-structured interviews and surveys. Section VI culminates in our proposed revised definition of PETs, which is followed by a discussion in Section VII. Finally, Section VIII highlights the practical relevance of our work, as well as suggestions for follow-up work on the topic.

II. Background and Related Work

The technological advancements of the past decades have led to ever-increasing amounts of data being processed on a daily basis. This, in turn, raises significant privacy concerns, as the potential presence of Personally Identifiable Information (PII) in a dataset can put the affected individuals at risk if a data breach occurs. It is, therefore, important to handle sensitive data in a privacy-preserving manner, considering both legal and technical aspects.

From the legal side, various legal frameworks and regulations, such as the General Data Protection Regulation (GDPR) or The California Consumer Privacy Act (CCPA), have been enacted to safeguard individuals' fundamental rights concerning the protection of personal data [2]. Such regulations are crucial in guiding organizations in ethical and responsible data management practices, establishing principles for data collection, sharing, storage, and usage.

In order to achieve compliance with the requirements set forth by these regulations, appropriate technical measures for privacy protection must be developed and integrated into software products and processes [3]. Serving as a technical approach to the preservation of privacy, a class of technologies known collectively as Privacy-Enhancing Technologies (PETs) has emerged in research. In essence, PETs encompass a range of technical approaches designed to allow deriving value from data while ensuring privacy protection; however, there is no universal definition.

Interestingly, the term Privacy-Enhancing Technologies did not originate in the academic environment; its first appearance dates back to 1995 when it was used in a report by the Dutch Data Protection Authority and the Ontario Information Commissioner, which explored a novel approach to privacy protection [4], [5]. Since then, the term has seemingly struggled to gain acceptance within the industry but instead began to attract attention in academia, resulting in a growing number of scientific publications on the subject. The exponential trend is illustrated in Figure 1, which shows the number of publications over the years with "Privacy-Enhancing Technologies" in the title or abstract.

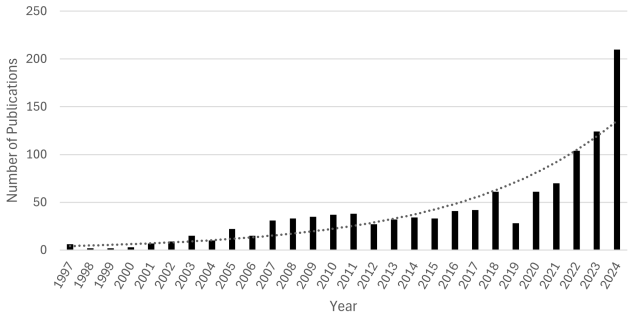

Fig. 1. Number of publications with "Privacy-Enhancing Technologies" in the title or abstract. Data source: Dimensions.ai

In a literature review conducted in 2020, Mangio et al. [6] categorized research on PETs into three distinct branches. The first branch encompasses studies within the field of economic research, which aim to understand the evolutionary dynamics of the PET market and identify the key technological and economic barriers that hinder the widespread adoption of these technologies. The second branch includes research in the field of ICT and information systems, focusing specifically on high-

tech aspects of PETs and evaluating their effectiveness and usability through technical advancements. The third branch relates to the history of end-user-focused information system research and comprises studies that aim to explore users' perspectives on adopting PETs, an area that is still relatively new. Multiple researchers have also attempted to categorize PETs, proposing different taxonomies of PETs based on involved entity [7], performed operation [8], privacy goals and requirements [9], technology maturity [10], effectiveness [11], and activities or layers [4].

Although numerous studies have previously asserted that there is no universally accepted definition for Privacy-Enhancing Technologies [12], [13], [14], to the best of authors' knowledge, there is no comparative study analyzing the available definitions and exploring why, after 30 years since its initial definition, the term remains unstandardized. The report that originally introduced the term PETs did not provide a formal definition; subsequently, numerous academic works attempted to clarify and formalize the concept, offering their own custom definitions, which will be presented in Section IV-A. The only identified comprehensive study on the topic, which also tried to introduce a new definition, is the Handbook of Privacy and PETs [15], which was published shortly after the original report [5]. In this work, the authors support their new definition by outlining seven principles, stemming from the evolution of the concept and the emergence of new techniques that align with the initial notion of an identity protector, as described in the first publication. The Handbook also describes legal foundations, along with state-of-the-art PET examples and active projects on the topic. The main limitation of this study arises from its publication year of 2003; at that time, numerous technologies that are currently recognized as privacy-enhancing were either in their early stages or not yet developed.

In this light, we revisit the topic of defining Privacy-Enhancing Technologies after twenty years since Borking [15], which has seen significant technological developments, immense changes in the regulatory landscape, and most importantly, the seemingly growing disparity in what it means to be considered a PET. This gap represents the motivation and starting point for our investigation.

III. Methodology

To guide our work we define the following research question as a basis for our investigation:

RQ: What is the operational definition of PETs in the literature, and how does this differ from what can be observed in the industry?

In order to realize the answer to this question, we naturally divide our work into two overarching studies. The first consists of a Systematic Literature Review (SLR), which aims to explore and systematize the definition of PETs in academic literature. In the second phase, we conduct semi-structured interviews and a survey, which have a two-fold goal: (1) to validate whether the definitions from our SLR are shared also in the industry, and (2) to evaluate the understanding of PETs in the industry, from the perspective of privacy practitioners.

A. PETs Definitions in the Literature

A Systematic Literature Review was conducted according to the methodology proposed by Kitchenham et al. [16]. The SLR encompassed five databases, specifically IEEE Xplore, ACM Digital Library, ScienceDirect, Scopus, and SpringerLink, which rank among the top ten search engines for identifying relevant studies in software engineering [17]. For each database, the following search string was employed:

(Q1 OR Q2) AND Q3

Q1: *Privacy Enhancing Technologies* in title AND *privacy-enhancing technologies* in keywords
Q2: *Privacy Enhancing Technologies* in title AND *PET* in keywords
Q3: publication date $\geq$ 1995

The search string was carefully designed during the planning phase of the literature review. An important decision in the planning of the literature review was to focus solely on previous works that survey or investigate PETs *in general*, and not on specific PET implementations or methods. In this way, our goal was to consider papers that define or characterize **Privacy-Enhancing Technologies**, where this exact term is explicitly defined. Thus, this term becomes central to our search string for the literature review. This decision becomes especially important to the review when considering venues that specialize in featuring works that introduce *implementations* of PETs. Rather, we mainly consider works attempting to survey, analyze, systematize, or otherwise study PETs as a concept, not instances of PETs.

A decision was also made to exclude the term "PET" as a single search term due to its tendency to yield results unrelated to the field. Incorporating terms such as "definition" or "characterization" in conjunction with "PETs" likewise produced inconsistent results during the preliminary search. As such, a deliberate decision was made to opt for a broader query and focus on manual filtering and selection of relevant papers, according to defined quality and inclusion criteria, which primarily necessitated a focus on the definition or characterization of PETs from a technical perspective.

In order to fill potential gaps created by the exclusions discussed above, we performed forward/backward reference searching, based on the initial foundation of papers found by our search string. From the initial filtered set of 28 papers, we searched for previously not found relevant papers in the references of these 28 papers, as well as leveraged Google Scholar to find papers that cite these 28 works. These forward/backward results were filtered by title to achieve the final set of papers for the SLR.

Table I presents the number of identified research publications grouped by the search engine. The initial sample, comprising 140 publications, was obtained by applying the presented search string to the selected databases. Note that the initial sample may include duplicates, as no filtering was

performed at this stage. The final sample of filtered papers includes publications originating from additional sources identified from the forward and backward search.

The corresponding references for the papers contained in the final sample are presented in the last column of Table I.

TABLE I
SLR RESULTS AND REFERENCES.

Search Engine / Venue	Initial Sample	Final Sample	References
IEEE Xplore	11	3	[18], [13], [19]
ACM Digital Library	7	1	[20]
ScienceDirect	13	7	[21], [8], [4], [22], [23], [24], [25]
Scopus	85	6	[7], [14], [26], [27], [10], [28]
SpringerLink	22	11	[29], [30], [11], [31], [32], [9], [33], [34], [35], [36], [37]
PoPETs/PETS	2	1	[38]
USENIX Security	-	-	-
SOUPS	-	-	-
Other	-	8	[15], [39], [12], [5], [40], [41], [42], [43]

a) Analysis: The main goal in the analysis of the identified literature was to extract definitions of PETs as proposed by these sources. This process was performed in a collaborative manner, where one researcher reviewed the sources and extracted candidate definitions, while two additional researchers reviewed and verified these definitions. The result of this process is presented in Section IV.

B. Gaining Practical Perspectives on PETs

We conducted semi-structured interviews with experts in technical roles in the privacy field. The goal of these interviews was to assess the level of familiarity with PETs among these practitioners, as well as to gain insight into the level of adoption of PETs in the industry.

1) Design: The interview guide was set up to learn about the understanding of PETs from the perspective of the interviewee's role and experiences. A team of three researchers first drafted a set of interview questions, where the main focus was to inquire into a practitioner's familiarity with the concept of PETs, as well as the practical relevance of this term. In addition, we constructed a ranking exercise, based on the SLR definition findings. Finally, we focused on broader questions, asking about the practitioner's opinion on any perceived gap between industry and academia, as well as the merits of a more common understanding of PETs, if any.

This initial guide was piloted in the first conducted interviews, after which the research team discussed any potential ambiguities or confusing questions as perceived during the interview conduction. Following this, the only major change that was made was the manner in which the ranking exercise was administered (giving the option for offline completion), but otherwise, the final guide as presented in the Appendix very closely mirrors the initial draft.

After obtaining consent to conduct and record the interview, we first obtained background information on the interviewee. Next, questions revolving around the interviewee's practical understanding of PETs, including whether the term is used at all, were asked. This was followed by an interactive task, in the format of a survey, where the interviewee was asked to rank a list of definitions (from the SLR) from *most to least accurate* (Question 7), as well as complete a multi-choice question on the perceived most important aspects of PETs (Question 8). The interview was rounded out with general questions probing into the perceived gap between academia and industry, as well as possible ways to improve this, if at all.

All participants joined our study voluntarily. Participants were provided with relevant information regarding the study in advance, ensuring informed consent. We explicitly asked for consent to the recording, transcribing, and publishing of the results in anonymized form. Interviews remained confidential, with all PII being anonymized, thus also minimizing potential social harm to the person or company behind them. We considered the emotional well-being of the interviewees by conducting interviews in an appreciative manner, motivated by appreciative inquiry [44].

2) Candidate Acquisition: As we focused on the perspectives of technical practitioners, we sought out suitable interview candidates in technical roles involved with privacy, using LinkedIn as a basis. Search strings such as 'privacy engineer', 'privacy champion', 'requirements engineer', and 'privacy architect' were used to obtain a list of potential candidates. This list was sorted by examining each potential participant's profile and checking whether it explicitly mentioned PETs, cybersecurity, or information security. If so, these people were given a higher priority in the extraction. For people who did not mention PETs in their profile, we gave preference to candidates with more years of experience in the field and different roles held over the years. During the course of the interviews, candidates were also obtained via referral from earlier interviewees.

The relevant interviewee demographics can be found in Table V of the Appendix. Our interviewees work in small (n=3), medium (n=4), and large (n=12) companies (1 self-employed), within various industry domains. They are located on five different continents, primarily in Europe and the United States. Years of experience range from 1-3 (n=1), 3-5 years (n=4), 5-10 years (n=7), 10-20 (n=6), and 20+ years (n=2).

The candidate acquisition process was stopped after 20 interviews due to feedback from the interview insights that saturation had been reached. Two criteria quantifying saturation include a stabilization in the *rank* scores (Table II), as well as a more subjective perceived saturation of themes extracted from the interview data.

3) Analysis: Following the conclusion of each survey, a Qualitative Content Analysis [45] was conducted to extract findings from the unstructured transcript data. Firstly, the transcript was sectioned by interviewee response, and these responses were assigned to the original questions in our interview guide. Then, important excerpts were highlighted, focusing on extracting direct citations from the interviewee to avoid bias introduced by personal interpretation. In the case of the interactive tasks outlined above, the answers to these could be simply aggregated into quantitative data, i.e., a *rank* score. Thus, our analysis follows the guidelines of Mayring

[45], in the way that interview data is transformed both into qualitative data (excerpts, themes) and quantitative data (rank score, frequencies of themes).

In addition to the above, we mitigate researcher bias by collaboratively coding in a team of three researchers, where codes can be shared and verified. In particular, codes initially defined by the main researcher were reviewed and verified by two senior researchers. Furthermore, the transformation of interview data into quantitative results adds objectivity to the coding and analysis process, further reducing the effect of any potential personal biases.

The findings from our analysis serve as the basis for assessing the SLR PET definitions (Section IV) and for reflecting on the practical perspective of PETs (Section V).

C. Surveying PET Understanding

The goal of the survey study was to obtain a clearer picture of the understanding of PETs among practitioners. Specifically, the study was divided into two separate surveys:

- S1. (1) given a set of PETs from the literature, inquire which of these are considered PETs by practitioners, and (2) evaluate our newly proposed draft definition of PETs.
- S2. (1) after the incorporation of feedback from S1, evaluate an updated definition of PETs, in comparison to the two leading PET definitions from the literature.

1) S1 Design: After initial background questions, survey participants were presented with a list of PETs, and for each PET, a response of *Yes*, *No*, or *Not Sure* was prompted by: *Which of the following technologies do you consider a PET?*

Finally, the participant was presented with our proposed definition of PETs (Definition 1 discussed in Section VI), and prompted to rate the definition on a scale of 1-10 for *understandability* and *completeness*, with 10 being the best. Both of these terms were clearly defined in the survey form and are introduced in Section VI-B.

2) S2 Design: Following the same background questions as S1, survey participants were prompted to rate the *understandability*, *completeness*, and *scope* of three PET definitions – two definitions from the literature receiving the highest ranks from the interviews, as well as our updated Definition 2. In this survey, an additional metric of *scope* was introduced based on the feedback from S1.

Both surveys were administered via Google Forms. They were fully anonymous and no personal data was collected.

3) Participant Acquisition: To facilitate participant acquisition, we published calls for participation in two groups on LinkedIn: *IAPP* (57k+ members) and *Information Security Network* (600k+ members).

These calls were refreshed on a regular basis for a period of two months. The target group for the survey was professionals working in the privacy and security field. In addition to the above, the surveys were distributed directly to select individuals whose LinkedIn profiles closely matched our target profile (PETs somewhere in the profile), as well as to interviewees who also expressed interest in participating in the survey.

4) Participant Demographics: S1 elicited a total of 40 responses. The respondents are based in 16 different countries from five different continents, and work in 12 different industry domains, the most dominant ones being Information Technology (n=13) and Finance (n=7). In terms of years of experience, there is a relatively even distribution between *1-3* (n=4), *3-5* (n=8), *5-10* (n=10), *10-20* (n=9), and *20+* (n=9). To reflect the views of privacy professionals from various backgrounds, practitioners serving in technical (n=13), legal (n=5), consulting (n=7), and management (n=15) roles were included. Further details on the demographics of the first survey are presented in Table VI of Appendix A.

S2 elicited 27 responses. The respondents are based in 12 different countries across four continents, working in 11 different industry domains. Years of experience are well distributed with an emphasis on *5-10* (n=13), with other ranges including *1-3* (n=2), *3-5* (n=4), *10-20* (n=4), and *20+* (n=4). Role categories included technical (n=9), legal (n=8), consulting (n=2), and management (n=8) positions. Therefore, the demographics of the S2 respondents proportionally match those of S1 very closely, thus providing a similarly representative sample across domain, region, role, and experience. Demographic details of S2 participants can be found in Table VII of Appendix A.

D. Ethics Considerations

During the course of the study, we made sure to set guidelines on how we were to protect the privacy of the study participants, which included safeguarding the identities of the interview study participants in the data analysis and synthesis phases. We obtained informed consent both in written and oral (at the beginning of the interviews) form. Informed consent included a clear explanation of the background and purpose of the study, as well as how the interview data would be captured and used. Namely, the participants gave their consent for the audio to be recorded and transcribed, and for pseudonymized resulting data, including direct quotes, to be published in a scientific publication. All analyses on the interview transcripts were performed with pseudonymized versions, and no transcripts were ever shared outside of our research team. The two administered surveys were completely anonymous; no personally identifiable information was asked for or recorded.

Participation in the interviews was completely voluntary, and therefore, no compensation was offered. In conducting the interviews, we facilitated a welcoming and open environment by asking questions in an *appreciative* manner, inquiring about our participants' experiences and perspectives. The full interview guide was shared in the days before the interview, so that the interviewees felt prepared and confident to answer the questions; however, interviewees were free not to answer any questions. Time was always left before and after the interviews to allow for comments or concerns.

IV. The Academic Perspective

In the investigation of the academic perspective on PETs, we first begin with the SLR to identify literature where PETs

TABLE II
OVERVIEW OF PET DEFINITIONS. "SUP." DENOTES THE NUMBER OF CITING PAPERS WITHIN OUR SELECTED 37 SOURCES.

ID	Definition	Year	Ref.	Sup.	Rank ↓
DEF-1	Technologies to protect sensitive personal information, either by separating the user's identity from the use of the information system through an identity protector or without recording any identifying information at all.	1995	[5]	4	3.6
DEF-2	System of ICT measures protecting informational privacy by eliminating or minimizing personal data thereby preventing unnecessary or unwanted processing of personal data, without the loss of the functionality of the information system.	2001	[41]	8	3.5
DEF-3	Technologies to protect legitimate users' privacy against abusive companies or agencies, without helping criminals to perpetrate illegal actions with impunity.	2006	[34]	0	5.1
DEF-4	Technologies that help achieve compliance with data protection legislation and help meet business privacy requirements.	2012	[13]	0	4.5
DEF-5	Broad range of technologies and applications that are designed to enhance privacy and data security of both individual and corporate users in their online activities and communications.	2020	[36]	0	3.3
DEF-6	Group of systems, processes, and techniques that enable processing to derive value from data while minimizing the privacy and security risk to individuals.	2021	[8]	0	3.9
DEF-7	Promising technologies that fulfill users' requirements regarding privacy, especially with the emergence of privacy legislation while enabling service providers and third parties to provide optimal user experience and quality of service.	2022	[7]	0	4.3

are explicitly defined. We then perform a quantitative analysis to quantify the prevalence of various technologies that are referred to as PETs in the selected literature, including reviews and taxonomies of PETs.

A. Definitions of PETs

Within the final set of included publications, presented in Table I, 14 distinct definitions were identified. In the conducted SLR, the main point of concern was identifying literature in which a definition of Privacy-Enhancing Technologies, or PETs, was explicitly given. With the final set of 37 included literature sources, 14 distinct definitions were identified. Some of these definitions, however, were not completely relevant to our study, for reasons that are given in the full list of Table IX in the Appendix. Specifically, six definitions were excluded since they either (1) presented *no new aspects* to an earlier definition or (2) were *too broad*. After removing these, the final set contained seven remaining definitions.

This final set of seven definitions is presented in Table II, which includes the original definition, the year of its inception, originating source (*Ref.*), supporting references (*Sup.*) and *rank*. Rank refers to the average ranked position in the ranking task of the interviews, where a lower rank means that the definition was generally regarded as a better definition than others. Supporting references refer to works being published after a given definition, in which this definition is used exactly, or nearly identically.

Observing the definitions in Table II, one can detect a clear change in focus expressed in the individual definitions. This is plausible, as the rapidly changing technological sphere, as well as the rise of modern data privacy regulations, could have certainly had an effect on the formation of updated PET definitions. Taking an example, the definition of Pelkola [13] can be seen as a close predecessor to the omnibus GDPR drafted and enacted just a few years later. A similar analysis of the mapping from a shift in focus to a change in real-world events or shifting opinion would present an interesting study, but is outside of the scope of our work.

B. Uncovering the Most Predominant PETs

With the set of PET definitions, our next analysis performed as part of the SLR involved exploring which specific technologies were referred to as PETs by the SLR sources.

Table III presents the top 10 mentioned technologies from the 37 included papers in the SLR. In these papers, all mentions of technologies were identified and enumerated. In addition, a *weighted* score is calculated, which provides a better notion of the relative predominance with respect to time. For example, while Differential Privacy is only mentioned 8 times, it occurs with heavy frequency since its earliest mention in reviewed literature in 2020. Beyond the top 10 PETs, the full table of identified technologies, as well as the works in which they are mentioned, are listed in the Appendix.

Performing this analysis is useful as it sheds light on the academic understanding of PETs, namely from those who defined the term PET in the literature. Table III gives insight into the most prevalent PETs as seen by the *definers* of PETs. From this, one can begin to draw lines between a PET definition and its associated technologies. The challenges of attempting to do so, however, are discussed in Section VII.

V. PRACTICAL PERSPECTIVE

While PETs are rooted in academia, their true significance lies in their practical application for data protection. Hence, a clear understanding of these technologies and their potential is essential to facilitate their implementation in the industry. Having extensively covered the academic definitions and viewpoints related to PETs in Section IV, we now shift focus to the practical understanding of PETs in an industrial context. As a basis for our investigation, we rely on the conducted semi-structured expert interviews described in Section III-B.

TABLE III
TOP TEN TECHNOLOGIES CLASSIFIED AS PETS IN LITERATURE. "MENTIONS" DENOTES RAW NUMBER OF APPEARANCES IN THE LITERATURE, WHILE "WEIGHTED" DIVIDES MENTIONS BY THE NUMBER OF YEARS ELAPSED SINCE THE FIRST MENTION IN THE REVIEWED LITERATURE. THE WEIGHTED SCORE IS NORMALIZED FOR READABILITY.

Technology	Mentions	Weighted
Onion Routing	14	0.25
K-Anonymity	13	0.40
Homomorphic Encryption	11	0.33
Secure Multi-party Computation	11	0.33
Zero Knowledge Proof	10	0.20
Mix-Networks	10	0.16
Symmetric/Asymmetric Encryption	10	0.12
Anonymous Credentials	9	0.18
Digital Signatures	9	0.09
Differential Privacy	8	0.85

A. Definition of PETs in Practice

In this section, we briefly discuss the insights from the interview, namely practitioners' understanding and use of the term "PETs", as well as their encounters with these technologies.

While our interview study targeted technical professionals who deal with privacy matters on a daily basis, in their responses, we observed a degree of uncertainty and confusion regarding the term Privacy-Enhancing Technologies. For instance, I1, I5 and I15 admitted that they were not familiar with this term before the interview. On the other hand, others viewed the topic from a legal standpoint:

> *Technical and organizational measures [...] with a positive impact on the seven data protection principles.* (I3)
>
> *Technologies that we have to implement in our products, services, and processes to meet the requirements and legal obligation of articles 25 and 32 of the GDPR. (I7)*

Two definitions that are closely aligned with those from the literature were given by respondents with a strong academic background on the topic, namely I4 and I6, who described PETs as:

> *Technologies that help us manage information flows, particularly information flows that identify subjects.* (I4)
>
> *[A] set of technologies that help provide the necessary level of privacy according to the chosen adversary model.* (I6)

Arguably, the most precise definition was provided by I8, who holds a PhD in privacy protection and is actively involved in researching and developing PETs for a large organization:

> *Technologies which can be both software and hardware or a combination of both that increase the privacy of the user while still allowing for the use of existing services or applications.* (I8)

Interestingly, in providing a definition for PETs, many interviewees focused not necessarily on the nature of technology, but rather on the goal of PETs to allow individuals to exercise their right to privacy and empower them to control the usage of their data. This aspect introduces a user- and rights-centric definition that illustrates PETs as a *facilitator* of lawful and ethical data processing, something which is largely ignored by the selected literature.

> *[The] technology is there, for me, to provide [privacy] rights to individuals.* (I16)
>
> *PETs give data subjects the ability to understand and control the data being collected (...) and minimize the individual risk of that data being used incorrectly or unethically.* (I11)

Not all interviewees were able to formulate a definition for the term PETs, and some seemed to conflate the *privacy* and *security* aspects of data protection, as also observed by I14:

> *I don't have any technical term to refer to the PETs, but I hear some people in my field, they confuse the term PET with security controls or security measures.* (I14)

Nearly all interviewees unanimously agreed that the term itself is academic in nature. In addition, I19 mentioned that the term is most often encountered by practitioners at conferences, on certification exams, and through media outlets such as podcasts and LinkedIn posts. Accordingly, an important insight derived from our study is that the term PETs is not as prevalent in the industry. I12 sheds light on the sheer lack of usage of the term:

> *Yes, technically, there are Privacy-Enhancing Technologies, of course. Do we call them that? Absolutely not.* (I12)

Instead, other terminologies are often used to refer to the technologies used for privacy preservation:

- Privacy by design techniques (I2, I15, I17)
- Technical and organizational measures (I3)
- Privacy-Preserving Technologies (I6)
- Privacy management software (I13)

One further question posed to every candidate is whether they have encountered these technologies in practice. Some responses, such as I1, pointed out that the answer depends on one's definition of a PET. When provided with examples of technologies typically labeled as PETs, some participants demonstrated familiarity with them, thereby highlighting the issue of definitional ambiguity.

The results of our qualitative study unveil a notable lack of clarity in the terminology surrounding PETs. This confusion became apparent as interviewees struggled to define PETs, with some offering quite differing explanations. Furthermore, while the majority of interviewed privacy professionals appear to be aware of at least some of the most commonly recognized PETs, they often possess only a limited and indistinct comprehension of these technologies.

B. Practical Views on Academic Definitions

In this section, we discuss some of the opinions of practitioners on the academic definitions of PETs, introduced in Section IV-A. The feedback was obtained during the interviews after participants were tasked to rank the seven definitions presented in Table II based on their clarity and comprehensiveness. The *Rank* column of Table II presents

the average score received by each definition, serving as an indicator of its accuracy as seen by the interviewed privacy experts. The rank can vary from 1.0 if unanimously ranked as the best by the interviewees, to 7.0 if it is ranked the lowest by all.

The best-ranked definition was DEF-5, with an average score of 3.3. DEF-5 stresses the broad aspect of the term PETs, which was highlighted by numerous interviewees. DEF-3 received the lowest level of approval with an average rank of 4.9. Interviewees highlighted numerous concerns, starting from the choice of words *"legitimate users"*. This sentiment was also shared by I19, amongst others, who claimed that the distinction between legitimate and illegitimate users is not relevant, and the *"excuse of criminality"* is not a reason to preclude certain users from privacy protection.

Interestingly, DEF-4, which focuses on compliance with data protection legislation, elicited very mixed opinions, which varied regarding whether legislation should be prioritized over privacy or vice versa. For instance, I7 supports the first point of view saying that *"[...] achieving compliance with data legislation is the essence"*, while I6, I8, I9, and I10 see PETs as a concept that should be kept separate from data protection legislation, as *"privacy is something that is more fundamental than legislation"* (I9).

Other feedback includes the comment of I7 on DEF-6, who considered changing *individuals* to *data subjects* to include companies. In the same vein, other interviewees expressed the idea that the distinction between individual and corporate users lacks sense as *"we are all people with rights that are protected"* (I19), and therefore, all data subjects should be considered collectively.

Additional insights regarding the practical perspective on academic definitions stemmed from the question to the interviewees whether in their opinion, the presented definitions of PETs were missing any crucial aspects. Some of the proposed missing aspects include the idea of PETs enabling users to control their data usage (I1, I11), other theories of privacy such as contextual integrity [46] (I4), and personalization of protection to user preferences (I8).

C. The Gap between Academia and Industry

Most of the interviewed professionals agreed that there is a disparity between how academia and industry perceive PETs, or rather, *"the street and the books"* (I12). For instance, I1 pointed out that while researchers tend to explore new technologies and opportunities, the industry is primarily driven by business requirements. As a consequence, technologies like PETs are considered only when there exists clear potential business value:

> *But the truth is that there's such little focus spent on applying those technologies, because there's no profit."* (I12)
>
> *The biggest concern from the companies right now is the moment I established PETs, I'm going to lose the value from the data."* (I18)

As illustrated by I2, who defined PETs as *"academic approaches to privacy"*, some industry professionals view PETs as mere prototypes or concepts under development. However, many of them are, in fact, rather mature, and multiple out-of-the-box solutions exist [47], [48], [49], [50]. As pointed out by I19 with respect to the wording "promising technologies" of DEF-7, *"some people would argue that they [PETs such as Differential Privacy or Homomorphic Encryption] have already achieved their promise, lived up to the expectation."* I4 offered his view on this misconception:

> *For the traditional businesses probably it's not well understood or used. I don't think they understand or fully comprehend the capacities of Privacy-Enhancing Technologies.* (I4)

This perspective was further discussed with I5, who recognized regulatory gaps as a potential barrier to the comprehension and adoption of PETs in the industry:

> *The gap is between the regulatory and academic fields. I think the academic field provides theoretical knowledge [...] but then when you have to put that in practice you need to bind it with some regulation.* (I5)

I10 argued that academic work on PETs is overly centered on research-oriented tasks, making it difficult to apply them to real-world scenarios in the industrial context:

> *[I]n the academic world [...] the definition and the use cases that are contemplated tend to focus on research-oriented tasks. And what we find in the industry is there are a lot of different ways in which people might want to partner on data, and it's not static.* (I10)

On the other hand, other interviewees pointed to a gap originating from the practical side, claiming that *"you might find that some professionals are actually using PETs without even knowing that they're using them"* (I14), highlighting a lack of awareness.

D. Which PETs are PETs?

We now draw attention to the findings of our survey, specifically the responses to the question of *Which of the following technologies do you consider a PET?* Here, the list of all technologies extracted from the SLR (discussed in Section IV-B) were presented to the survey participants, with *Yes*, *No*, or *Not Sure* as answer options.

To allow for analysis, we employ the following scoring scheme: *Yes*=1, *Not Sure*=0, and *No*=-1. With these, an aggregated score can be achieved for each technology, which represents the "overall sentiment" towards a technology, With 40 survey participants, a score of 40 would mean complete agreement that something is a PET, while -40 would imply complete disagreement. To account for *Not Sure* responses not contributing to the score, an error bar is introduced in our reporting to represent this uncertainty.

The results of this analysis are presented in Figure 2. Positive scores are colored in black and are to the right of

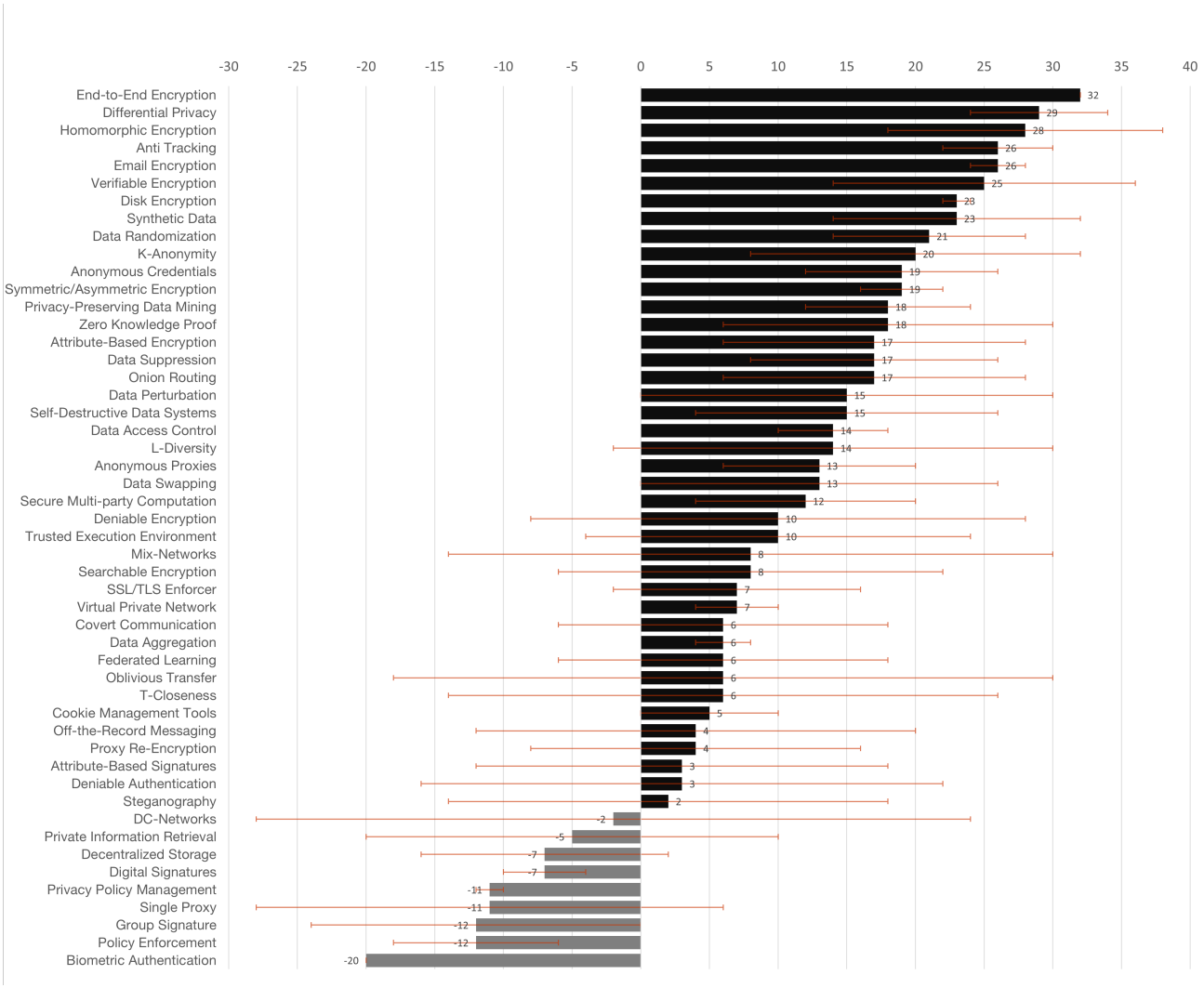

Fig. 2. Aggregated Scores (n=40) for the Question: *Which of the following technologies do you consider a PET?* The scoring scheme counts a *Yes* response as +1 and a *No* response as -1. Error bars indicate the number of *Not Sure* responses, thereby denoting the overall uncertainty expressed for a given technology.

the center axis, while negative scores are colored in grey and are to the left.

We note that the analysis of these survey results do not make the distinction between *correctness* and *awareness*. In other words, a *not sure* response may be given if the respondent is not aware of the given PET, or also if the respondent is simply not sure if the technology can be considered a PET or not. We consider this distinction outside of the scope of this work, but it nevertheless contributes to the limitations of the survey findings.

VI. Defining PETs

We now propose a new definition of PETs. To accomplish this, we first decompose the seven definitions from Table II to create the *building blocks* of PETs. Next, we look to the results of the two interactive tasks from our interviews to identify the most important aspects as seen by practitioners. Finally, we reconstruct a modified PET definition from our building blocks, guided by the practical insights.

A. The Building Blocks of PETs

As our first step in formulating a new definition for PETs, we deconstruct academic definitions into *primitives*, or rather constituent *building blocks* representing key aspects of the existing definitions.

We first define a *base block*, in line with the original definition of PETs, namely to *protect sensitive personal information* (BB-0). Further building blocks (BB1-6) are extracted by identifying the unique component introduced by a new definition, beyond the foundational understanding. For example, a foundational change can be observed from DEF-1 (identity protector) to DEF-2 (identity protector + data minimizer). Thus, BB-1 can be defined as *minimize, alter, or omit personal data*. Such analysis was performed to create the remaining building blocks, all of which can be found in Table IV.

As with the analysis of interview data, we perform the building block extraction process in a team of three researchers, where the blocks are proposed by the main researcher and

verified by two more senior researchers. The verification process primarily consisted of confirming that each new block: (1) correctly characterizes its originating definition, and (2) represents a distinct block not characterized by a previously identified block.

TABLE IV
BUILDING BLOCKS OF PETS.

ID	Building Block
BB-0	Protect sensitive personal information
BB-1	Minimize, alter, or omit personal data
BB-2	Protect only legitimate users without helping to perpetrate illegal actions
BB-3	Help to achieve compliance with data protection legislation
BB-4	Protect individual and corporate users
BB-5	Allow deriving value from data
BB-6	Allow improving the quality of service

1) Evaluation of the Building Blocks: In the second task presented to our interviewees, the goal was to prompt the participants to choose which of the aspects of PETs (building blocks) they view to be integral. In particular, the prompt read: *In your opinion, Privacy-Enhancing Technologies are technologies which...*, followed by a list of non-base building blocks (BB1-6). The interviewee could then pick multiple options, including none.

The results of this task are displayed in Figure 3, showing that BB3 (achieving compliance) received the highest number of votes. BB1, BB4, and BB5 were also strongly represented.

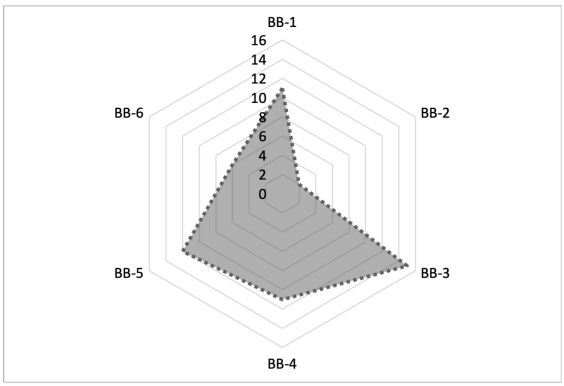

Fig. 3. Evaluation of the building blocks, showing a heavy preference for BB-3, followed by BB-5, then BB-1 and BB-4.

B. A New Definition

Looking at the aggregated results of the ranking task from the interviews (*Rank* in Table II), one can see that DEF-2 and DEF-5 were the highest ranked. These two definitions, therefore, served as the basis for our new definition. Looking to the interview task, all building blocks except for BB-2 and BB-6 received greater than 50% agreement, speaking to their candidacy for inclusion. Despite the poor performance of BB-2, the essence of DEF-2 was included in our definition, due to its strong rank in the first interview task.

Finally, it was originally decided to exclude BB-3 from the definition, as the role of PETs in achieving compliance was highly debated in the interviews. The most common argument against BB-3 was that privacy, and by association PETs, should not be coupled with legislation and compliance, as the pursuit of privacy should be undertaken regardless. Following the creation and evaluation of PET building blocks, we propose the following definition of PETs:

Definition 1 (Privacy-Enhancing Technologies)**.** *PETs are a system of ICT measures to protect the rights and freedom of data subjects in their online activities and communications by eliminating, altering, or minimizing the collection of personal data. These technologies, when properly implemented, can minimize the disclosure of PII and prevent correlation while allowing third parties to derive value from data.*

1) Definition 1 Evaluation: With the newly minted Definition 1 in hand, we asked participants of our survey to evaluate the proposed definition for *understandability* and *completeness*. For the purposes of the survey, these two terms were defined as:

- **Understandability**: how clear and easily comprehensible is the proposed definition?
- **Completeness**: to what extent does the definition cover the important aspects of PETs?

Each of these points was to be rated on an ordinal scale of 1-10, with 10 being the best. The *understandability* of Definition 1 received an average of **7.35** and median score of **8**. The *completeness* of the definition was rated with an average of **7.03** and a median score of **8**. This shows that in general, the respondents agreed that the proposed definition is quite understandable and complete.

Encouraged by the results of evaluating Definition 1 but recognizing the room for improvement, we crafted a second updated definition, this time revising key points introduced in the open-ended feedback of S1. The primary improvements include the removal of the term *ICT measures* due to its rare usage, generalization from PII to personal data, and for completion purposes, the addition of the compliance aspect. The updated definition, found in Definition 2, serves as the basis for survey S2, wherein this revised definition is evaluated for further feedback.

Definition 2 (Privacy-Enhancing Technologies, Revised). *Privacy-Enhancing Technologies (PETs) are a collection of technical measures to protect the rights and freedom of data subjects by eliminating, altering, or minimizing the processing of their personal data. These technologies, when properly implemented, can prevent direct or indirect linkage between data subjects and their data, while allowing processing entities to derive value from data in a way that is compliant with applicable data protection regulations.*

2) Definition 2 Evaluation: As with S1, we evaluated Definition 2 in S2, this time taking the form of a comparative evaluation with the top two definitions from the literature as ranked by our interviewees (DEF-5 and DEF-2). As introduced in Section III, we introduce a third metric in S2, namely *scope*, defined as follows:

- **Scope**: whether the scope of the definition is too narrow, too broad, or just right (=5).

The results of the survey are presented in the following, where the triples represent (*Understandability*, *Completeness*, *Scope*), with the subscript denoting the median score.

- DEF-2: (6.11_7, 6.04_6, 5.93_7)
- DEF-5: (7.85_8, 6.56_7, 6.15_6)
- Def. 2: (7.74_8, 7.67_8, 5.81_5)

One can see that DEF-5 achieved the best score in understandability, and Definition 2 achieved the best in completeness and scope. Looking to the median scores, our Definition 2 achieve equal or higher scores in all metrics. To view all three metrics holistically, we define the following composite score:

$$\textit{composite} = \frac{(\textit{understandability} + \textit{completeness}) - |5 - \textit{scope}|}{20}$$

This composite is derived to represent the percentage of the maximum score (20) achieved. With this, DEF-2 achieves a composite of **0.56**, DEF-5 a score of **0.66**, and Definition 2 a score of **0.73**.

VII. Discussion

The presented results of our study evoke numerous insights, which we attempt to narrate in the following.

We observe from the literature that numerous technologies are classified as PETs, and that definitions of the term PETs vary in scope. In evaluating academic definitions with practitioners, we observe that although some definitions are ranked higher on average, there is no clear winner. In fact, with the highest possible score of 1.0 and the lowest possible score of 7.0, all ranks are relatively close to the center, i.e., 4.0. One can imply from this that there is very little uniform agreement on a single PET definition. As such, PETs can be seen as serving a multitude of aims. These results are supported by the evaluation of the building blocks, as well as the evaluation of PETs (Figure 2) from the 40 surveyed practitioners. Finally, the lack of inter-respondent agreement in S1 and S2, despite the careful analysis and incorporation of practitioner feedback, suggests that finding common ground is not only difficult, but potentially not feasible. This result sheds light on the potential confusion and lack of knowledge of many PETs stemming from academia, which seemingly arise from the challenges discussed above.

With the term *Privacy-Enhancing Technologies* itself, a strong majority of the interviewees stated that it is both academic and not widely used in the industry at all. In fact, the term is seemingly reserved for "academic" outlets, such as conferences or certification exams. Beyond this issue, in practice, the concept to which PETs refers also goes by other terminologies, e.g., privacy by design. In general, regardless of the exact terminology used, interviewees explained the term in quite different ways, ranging from a technical focus to a more legal definition to a user-centric, rights-based definition. In naming specific examples of PETs, responses from the interviewees ranged from Differential Privacy and Homomorphic Encryption to cookie banners and privacy management providers such as OneTrust and TrustArc. All of these findings suggest a clear lack of common understanding when it comes to PETs.

In investigating the source of this lack of common understanding, we observed a common theme from the interviewees in asking them about any perceived gap between academia and industry. Many of the interviewed practitioners pointed to a concrete gap, citing the issues of unclear business value, lack of expertise and awareness, and lack of practical applicability of PETs, among others. Another insight extracted from multiple interviews illustrates the need from practitioners for PETs to be *tangible*. As a complement to a strong definition, several interviewees expressed the usefulness that concrete *examples* would carry, particularly in showcasing how a PET can be used in practice. Another suggestion was the introduction of more *"business-friendly"* (I20) names for PETs. From such statements, it is clear that a lack of harmony between research and practice may serve as a severe hindrance in both understanding and implementing PETs beyond the laboratory.

Beyond these challenges, the factor of "privacy culture" was often mentioned as an aspect missing in academia, as the general understanding of PETs can depend on someone's role and background; moreover, the general privacy readiness of a society or country in general, particularly the value placed upon privacy as a right, can affect the perception of PETs. This additional challenge introduced by the aspect of culture is made concrete by one interviewee:

> *Before you even tell people to use PETs, you have to first understand what privacy is. And we are still struggling as a country. I believe also other African countries are struggling with this, unlike other countries in Europe and the USA.* (I14)

The number of findings revolving around the academic nature of PETs, the multitude of technologies considered to be PETs, the gap between academic and industry, and the overall perceived lack of common understanding of PETs brings up one simple question: *so what?* In the course of many interviews, this became the ultimate question, usually in the form of *Do you believe we even need a common understanding?* We received nearly unanimous answers saying that a common definition is indeed needed, so as to increase awareness for the term and the field at large. Exploring deeper beyond a simple *yes* response, we received unique and varied opinions as to why such a definition would be needed, from which we present a few impactful statements that round out our findings:

> *It's very important in my opinion. It's important for us when we're talking about something, having at least an idea of what we're all talking about.* (I19)

> *I see there are a lot of definitions, so if we can come up with one, it also helps us as regulators (...) it will help us to give clear regulatory guidance.* (I14)

> *[The term PETs] is interchangeably used as of now (...) There should be a unified definition, rather than*

having multiple – it's really going to help to clear the understanding. (I13)

We want these technologies to be implemented on a broader sense (...) most people should have the ability to understand this [what PETs are]. (I18)

I think that whenever we as people have a collective understanding of one definition, that gives us a collective awareness of what that entails and what it does not entail. When there are slight changes in the definition, it creates opportunity for arbitrage and for taking advantage of those differences. That's why I think it's important to have a fundamental [definition] (...) just choose one and we'll all follow it. (I12)

The statements above collectively support the idea that a unified definition of PETs would be useful for practitioners. Furthermore, the usefulness of a unified *term* itself is aptly compared by I20 to that of *AI*: while not all AI is AI, having the "buzzword" creates a sense of demand for the term, but at the same time, it also creates

... some form of theory or a "body of knowledge" that can be referenced to say, okay, I have problem X, can I look at this reference material of all PETs out there to say which solution matches my problem. (I20)

Our findings suggest that while a common definition would not solve the challenges of understandability and usability of PETs, it would certainly help. In fact, the general lack of agreement between study participants on what PETs are supports the need for more awareness, providing a clear call for researchers in academia to lead the way in defining PETs and creating a "body of knowledge" that is understandable to a wider audience outside of academia.

At the same time, the insights gained from the practical perspectives also demonstrate possible weak points in current academic definitions. In particular, we observe that multiple interviewees focus on the human aspect of PETs, namely who is being protected and how these people can safeguard their rights via the usage of PETs. Furthermore, the business side of PETs is often emphasized, while such an aspect is largely ignored in the academic literature.

In the evaluation of our newly proposed Definition 2, we see an improvement as perceived by the S2 respondents, particularly in the *completeness* and *scope*. The composite score results show a clear progression in the right direction (especially over Definition 1), yet there is clearly room for improvement. From this and the practical perspectives gained, one might argue that the academic side of PETs also has some work to do, focusing on making PETs both practically usable but also practically *understandable*.

VIII. Conclusion and Future Work

In this work, we systematically analyze the breadth of Privacy-Enhancing Technology definitions, spanning the past 30 years. Representing the academic understanding of PETs, these definitions serve as the basis for the creation of PET building blocks and the quantification of the predominance of individual technologies. Leveraging these findings in combination with practical insights gained from industry experts, we uncover a clear gap in understanding from practitioners in the privacy field, as well as between academia and industry. In addressing this gap, we leverage our empirical results to propose and evaluate a new definition of PETs.

The implications of our works pertain to several stakeholder groups. Firstly, as stated previously, academic researchers are called to conduct further studies on the nature of PETs, particularly from a practice-oriented perspective. Likewise, our findings suggest that privacy practitioners would benefit from more interactions with the academic space, mainly in generating discussions to investigate not only the mutual understanding of PETs, but also ways forward to work together. This will help to bring a field of largely theoretical research to the forefront of practice. Finally, although we do not emphasize the legal perspective in this work, this aspect must not be ignored, as data privacy is inherently interdisciplinary [51]. Legal professionals may benefit from the findings of our work as day-to-day guidance in a world where digital privacy becomes increasingly important. This also carries implications for regulators and lawmakers, who must be informed about the state of Privacy-Enhancing Technologies when drafting crucial forward-looking regulatory or legal mandates.

The findings of our study make clear the significant influence of diverse factors such as culture, background, and other subjective criteria on the understanding of PETs. Such variability was mitigated by the diversity of our study participants, yet further research would be well served to increase the generalizability of our findings. A limitation in the methodology comes with the selection of survey participants; particularly in S1, no screener question (e.g., *Are you familiar with PETs?*) was asked, something which was only incorporated later in S2. A final limitation is the stopping criterion of our interview study; although we believe to have observed a saturation of themes, a potential limitation of our work comes with our decision to cease interviews after I20.

From our findings and the abovementioned limitations, we propose paths for future work. Firstly, we hope that future investigations will continue to study the intersection of PETs and practitioner perspectives, with the goal of making PETs more usable in practice. In addition, future work should focus on clearly defining the bounds of *Privacy-Enhancing Technologies*, which will serve to provide a scope for researchers seeking to make contributions to the field.

We realize that our work but scratches the surface in the pursuit of insights into the academic and practical understanding of the nature and definition of PETs. Many of these points, as discussed in Section VII, present clear paths for future research on the topic. As the need for the study of Privacy-Enhancing Technologies continues to rise, the questions raised and the insights gained in this work are seen to be highly important to address going forward. With this, we call on researchers to continue the work set out here; with a common understanding and higher awareness, we may march on to the same beat in the pursuit of data privacy.

REFERENCES

[1] The Rise of Privacy Tech (TROPT), "TROPT's Privacy Tech Strategy Recommendations to the White House." 2022.

[2] A. Klymenko, S. Meisenbacher, A. A. Polat, and F. Matthes, "A systematic analysis of data protection regulations," *Proceedings of the 58th Hawaii International Conference on System Sciences*, 2025.

[3] O. Klymenko, O. Kosenkov, S. Meisenbacher, P. Elahidoost, D. Mendez, and F. Matthes, "Understanding the implementation of technical measures in the process of data privacy compliance: a qualitative study," in *Proceedings of the 16th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement*, 2022, pp. 261–271.

[4] G. M. Garrido, J. Sedlmeir, Ömer Uludağ, I. S. Alaoui, A. Luckow, and F. Matthes, "Revealing the landscape of privacy-enhancing technologies in the context of data markets for the iot: A systematic literature review," *Journal of Network and Computer Applications*, vol. 207, p. 103465, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1084804522001126

[5] R. Hes and J. Borking, "Privacy-enhancing technologies: The path to anonymity," 01 1995.

[6] F. Mangiò, D. Andreini, and G. Pedeliento, "Hands off my data: users' security concerns and intention to adopt privacy enhancing technologies," *Italian Journal of Marketing*, vol. 2020, no. 4, pp. 309–342, 2020.

[7] N. Kaaniche, M. Laurent, and S. Belguith, "Privacy enhancing technologies for solving the privacy-personalization paradox: Taxonomy and survey," *Journal of Network and Computer Applications*, vol. 171, p. 102807, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1084804520302794

[8] K. Asrow and S. Samonas, "Privacy enhancing technologies: Categories, use cases, and considerations," *Federal Reserve Bank of San Francisco*, 2021.

[9] M. Deng, K. Wuyts, R. Scandariato, B. Preneel, and W. Joosen, "A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements," *Requirements Engineering*, vol. 16, no. 1, pp. 3–32, Mar 2011. [Online]. Available: https://doi.org/10.1007/s00766-010-0115-7

[10] M. Hansen, J.-H. Hoepman, and M. Jensen, "Towards measuring maturity of privacy-enhancing technologies," 03 2016, pp. 3–20.

[11] J. J. Borking, *Why Adopting Privacy Enhancing Technologies (PETs) Takes so Much Time*. Dordrecht: Springer Netherlands, 2011, pp. 309–341.

[12] Y. Shen and S. Pearson, "Privacy enhancing technologies: A review," *Hewlet Packard Development Company. Disponible en https://bit.ly/3cfpAKz*, 2011.

[13] D. Pelkola, "A framework for managing privacy-enhancing technology," *IEEE Software*, vol. 29, no. 3, pp. 45–49, 2012.

[14] S. Jordan, C. Fontaine, and R. Hendricks-Sturrup, "Selecting privacy-enhancing technologies for managing health data use," *Front. Public Health*, vol. 10, p. 814163, Mar. 2022.

[15] J. Borking, P. Verhaar, B. Eck, P. Siepel, G. Blarkom, R. Coolen, M. Uyl, J. Holleman, P. Bison, R. Veer, J. Giezen, A. Patrick, C. Holmes, J. Lubbe, R. Lachman, S. Kenny, R. Song, K. Cartrysse, J. Huizenga, and X. Zhou, *Handbook of Privacy and Privacy-Enhancing Technologies The case of Intelligent Software Agents*, 11 2003.

[16] B. A. Kitchenham, D. Budgen, and P. Brereton, *Evidence-Based Software Engineering and Systematic Reviews*. Chapman & Hall/CRC, 2015.

[17] H. Zhang, M. A. Babar, and P. Tell, "Identifying relevant studies in software engineering," *Information and Software Technology*, vol. 53, no. 6, pp. 625–637, 2011.

[18] G. M. Garrido, K. Schmidt, C. Harth-Kitzerow, J. Klepsch, A. Luckow, and F. Matthes, "Exploring privacy-enhancing technologies in the automotive value chain," in *2021 IEEE International Conference on Big Data (Big Data)*, 2021, pp. 1265–1272.

[19] Y. Kang, H. Lee, K. Chun, and J. Song, "Classification of privacy enhancing technologies on life-cycle of information," in *The International Conference on Emerging Security Information, Systems, and Technologies (SECUREWARE 2007)*, 2007, pp. 66–70.

[20] K. P. Coopamootoo, "Usage patterns of privacy-enhancing technologies," in *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '20. New York, NY, USA: Association for Computing Machinery, 2020, p. 1371–1390. [Online]. Available: https://doi.org/10.1145/3372297.3423347

[21] J. Heurix, P. Zimmermann, T. Neubauer, and S. Fenz, "A taxonomy for privacy enhancing technologies," *Computers & Security*, vol. 53, pp. 1–17, 2015. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404815000668

[22] H. B. Wolfe, "Privacy enhancing technology," *Computer Fraud & Security*, vol. 1997, no. 10, pp. 11–15, 1997. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1361372397899514

[23] R. Ott, "Privacy enhancing technologies: Protecting information online," *Computer Fraud & Security*, vol. 2000, no. 1, pp. 11–12, 2000. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1361372300010186

[24] V. Seničar, B. Jerman-Blažič, and T. Klobučar, "Privacy-enhancing technologies—approaches and development," *Computer Standards & Interfaces*, vol. 25, no. 2, pp. 147–158, 2003. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0920548903000035

[25] J. R. Vacca, *Preface*, third edition ed., J. R. Vacca, Ed. Boston: Morgan Kaufmann, 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/B9780128038437050018

[26] R. Meis and M. Heisel, "Pattern-based representation of privacy enhancing technologies as early aspects," in *Trust, Privacy and Security in Digital Business*, J. Lopez, S. Fischer-Hübner, and C. Lambrinoudakis, Eds. Cham: Springer International Publishing, 2017, pp. 49–65.

[27] M. Hansen, J.-H. Hoepman, M. Jensen, and S. Schiffner, "Report on the workshop on assessing the maturity of privacy enhancing technologies," in *IFIP Advances in Information and Communication Technology*, ser. IFIP advances in information and communication technology. Cham: Springer International Publishing, 2016, pp. 97–110.

[28] E. Wästlund, P. Wolkerstorfer, and C. Köffel, "Pet-uses: Privacy-enhancing technology – users' self-estimation scale," in *Privacy and Identity Management for Life*, M. Bezzi, P. Duquenoy, S. Fischer-Hübner, M. Hansen, and G. Zhang, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 266–274.

[29] I. Kunz and A. Binder, "Application-oriented selection of privacy enhancing technologies," in *Privacy Technologies and Policy*, A. Gryszczyńska, P. Polański, N. Gruschka, K. Rannenberg, and M. Adamczyk, Eds. Cham: Springer International Publishing, 2022, pp. 75–87.

[30] H. Elmimouni, E. Shusas, P. Skeba, E. P. S. Baumer, and A. Forte, "What makes a technology privacy enhancing? laypersons' and experts' descriptions, uses, and perceptions of privacy enhancing technologies," in *Information for a Better World: Normality, Virtuality, Physicality, Inclusivity*, I. Sserwanga, A. Goulding, H. Moulaison-Sandy, J. T. Du, A. L. Soares, V. Hessami, and R. D. Frank, Eds. Cham: Springer Nature Switzerland, 2023, pp. 229–250.

[31] K. Schmidt, G. Munilla Garrido, A. Mühle, and C. Meinel, "Mitigating sovereign data exchange challenges: A mapping to apply privacy- and authenticity-enhancing technologies," in *Trust, Privacy and Security in Digital Business*, S. Katsikas and S. Furnell, Eds. Cham: Springer International Publishing, 2022, pp. 50–65.

[32] I. Kunz, C. Banse, and P. Stephanow, "Selecting privacy enhancing technologies for iot-based services," in *Security and Privacy in Communication Networks*, N. Park, K. Sun, S. Foresti, K. Butler, and N. Saxena, Eds. Cham: Springer International Publishing, 2020, pp. 455–474.

[33] J. Parra-Arnau, D. Rebollo-Monedero, and J. Forné, *Privacy-Enhancing Technologies and Metrics in Personalized Information Systems*. Cham: Springer International Publishing, 2015, pp. 423–442.

[34] Y. Deswarte and C. Aguilar Melchor, "Current and future privacy enhancing technologies for the internet," *Annales Des Télécommunications*, vol. 61, no. 3, pp. 399–417, Apr 2006. [Online]. Available: https://doi.org/10.1007/BF03219914

[35] J. Borking, *The Status of Privacy Enhancing Technologies*. Boston, MA: Springer US, 2003, pp. 211–246.

[36] F. Mangiò, D. Andreini, and G. Pedeliento, "Hands off my data: users' security concerns and intention to adopt privacy enhancing technologies," *Italian Journal of Marketing*, vol. 2020, no. 4, pp. 309–342, Dec 2020. [Online]. Available: https://doi.org/10.1007/s43039-020-00017-2

[37] M. Jaatun, I. A. Tøndel, K. Bernsmed, and Å. Nyre, *Privacy Enhancing Technologies for Information Control*, 01 2012, pp. 1–31.

[38] I. Goldberg, "Privacy-enhancing technologies for the internet, ii: Five years later," in *Privacy Enhancing Technologies*, R. Dingledine and P. Syverson, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003, pp. 1–12.

[39] I. C. Office, "Privacy enhancing technologies," 2023. [Online]. Available: https://cy.ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/privacy-enhancing-technologies/

[40] D. Harborth and S. Pape, "Examining technology use factors of privacy-enhancing technologies," 08 2018.

[41] J. Borking and C. Raab, "Laws, pets and other technologies for privacy protection." *Journal of Information, Law and Technology*, vol. 2001, 01 2001.

[42] I. Goldberg, D. Wagner, and E. Brewer, "Privacy-enhancing technologies for the internet," in *Proceedings IEEE COMPCON 97. Digest of Papers*. IEEE, 1997, pp. 103–109.

[43] I. Goldberg, "Privacy-enhancing technologies for the internet iii: ten years later," *Digital Privacy*, pp. 25–40, 2007.

[44] D. L. Cooperrider, J. M. Stavros, and D. Whitney, *The appreciative inquiry handbook: For leaders of change*. Berrett-Koehler Publishers, 2008.

[45] P. Mayring, "Qualitative content analysis: theoretical foundation, basic procedures and software solution," 2014.

[46] H. Nissenbaum, "Privacy as contextual integrity," *Wash. L. Rev.*, vol. 79, p. 119, 2004.

[47] G. M. Garrido, J. Near, A. Muhammad, W. He, R. Matzutt, and F. Matthes, "Do i get the privacy i need? benchmarking utility in differential privacy libraries," *arXiv preprint arXiv:2109.10789*, 2021.

[48] K. D. Albab, R. Issa, A. Lapets, P. Flockhart, L. Qin, and I. Globus-Harris, "Tutorial: Deploying secure multi-party computation on the web using jiff," *2019 IEEE Cybersecurity Development (SecDev)*, pp. 3–3, 2019.

[49] M. Stopar, M. Bizjak, J. Modic, J. Hartman, A. Žitnik, and T. Marc, "emmy - trust-enhancing authentication library," in *Trust Management XIII: 13th IFIP WG 11.11 International Conference, IFIPTM 2019, Copenhagen, Denmark, July 17-19, 2019, Proceedings 13*. Springer, 2019, pp. 133–146.

[50] X. Liu, T. Shi, C. Xie, Q. Li, K. Hu, H. Kim, X. Xu, B. Li, and D. Song, "Unifed: A benchmark for federated learning frameworks," *arXiv preprint arXiv:2207.10308*, 2022.

[51] A. Klymenko, S. Meisenbacher, and F. Matthes, "The structure of data privacy compliance," *CIISR*, p. 85, 2023.

[52] OECD, "Inventory of privacy-enhancing technologies (pets)," 2002. [Online]. Available: https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?doclanguage=en&cote=dsti/iccp/reg%282001%291/final

[53] ENISA, "Privacy enhancing technologies," 2020. [Online]. Available: https://www.enisa.europa.eu/topics/data-protection/privacy-enhancing-technologies

APPENDIX

INTERVIEW PARTICIPANTS

TABLE V
INTERVIEW STUDY PARTICIPANTS.

ID	Role	Industry Domain	Org. Size	Country	Exp.
I1	Senior Privacy and Security Architect	IT Services and Consulting	Medium	Finland	10-20
I2	Senior Privacy Engineer	Software Development	Medium	Germany	5-10
I3	Privacy Engineer - Consultant	IT Consulting	-	Germany	5-10
I4	Senior Requirements Engineer	IT Services	Small	United Kingdom	5-10
I5	Staff Site Reliability Engineer	Software Development	Large	Netherlands	5-10
I6	Senior Privacy Researcher and Developer	IT Services	Medium	Spain	3-5
I7	Principal Privacy Engineer	Online Retailing	Medium	Germany	20+
I8	Senior Privacy Engineer	Telecommunications	Large	Germany	3-5
I9	Privacy Director	IT Services and Consulting	Large	Germany	10-20
I10	Product Manager - PETs	Software Development	Small	United Kingdom	1-3
I11	Privacy Engineer	IT Services	Self-employed	United States	3-5
I12	Chief Privacy Officer	IT Services	Large	United States	10-20
I13	Privacy Integration Specialist	Finance	Large	India	5-10
I14	Cybersecurity Officer	Regulatory Body	Small	Uganda	3-5
I15	Information Security and Privacy Manager	Finance	Large	Brazil	5-10
I16	Privacy Engineer	Energy	Large	United States	5-10
I17	Group Chief Privacy Officer	Finance	Large	South Africa	10-20
I18	Senior Data Privacy Program Manager	FinTech	Large	United States	10-20
I19	Senior Director of Global Information Security	Entertainment	Large	United States	20+
I20	Group Director - Customer Data Platform	Retail	Large	United States	10-20

INTERVIEW GUIDE

Disclaimer

Before we start the interview, I would like to mention that this interview will be recorded for subsequent transcription. The transcription itself and any findings within will be utilized for research purposes and for publication in a scientific work. Any personally identifiable information will be anonymized, and the final results will be shared in the end. Could you please confirm your consent to these terms?

Background

1. What is your position and role?
2. How many years of experience in this field and in this company do you have?
3. In which domain are you currently working?
4. What is the size of your company?

Privacy-Enhancing Technologies

5. Have you heard of the term Privacy-Enhancing Technologies (PETs)?
6. What is your practical understanding of Privacy-Enhancing Technologies?
7. In practice, is the term *Privacy-Enhancing Technologies / PETs* used? Is there some alternative term which is more prevalently used?
8. Have you encountered these technologies in practice?
    a) If so, can you describe your experience?

[NOTE: Questions 9-11 were presented to the interviewees in a survey format.]

9. [Rank] Give your personal ranking from the most to the least accurate definition:
    - Technologies to protect sensitive personal information, either by separating the user's identity from the use of the information system through an identity protector or without recording any identifying information at all.
    - System of ICT measures protecting informational privacy by eliminating or minimizing personal data thereby preventing unnecessary or unwanted processing of personal data, without the loss of the functionality of the information system.
    - Technologies to protect legitimate users' privacy against abusive companies or agencies, without helping criminals to perpetrate illegal actions with impunity.
    - Technologies that help achieve compliance with data protection legislation and meet business privacy requirements.
    - Broad range of technologies and applications that are designed to enhance privacy and data security of both individual and corporate users in their online activities and communications.
    - Group of systems, processes, and techniques that enable processing to derive value from data, while minimizing the privacy and security risk to individuals.
    - Promising technologies that fulfill users' requirements regarding privacy especially with the emergence of privacy legislation while enabling service providers and third parties to provide optimal user experience and quality of service.
10. [Multiple Choice] In your opinion, Privacy-Enhancing Technologies are technologies which...
    - Allow deriving value from data.
    - Allow improving the quality of service.
    - Help to achieve compliance with data protection legislation.
    - Minimize, alter or omit personal data.
    - Protect individual and corporate users.
    - Protect only legitimate users without helping to perpetrate illegal actions.
11. [Text] Which further aspects would you consider necessary for a comprehensive definition?
12. Given what you saw in the survey, do you see any gaps in the academic view on PETs and the practical one, from your experience? Is there something missing?
13. Do you think that the academic understanding of PETs should be augmented with more practical insights or vice versa?

Other

14. Is there any aspect on this topic we may have missed?
15. Can you refer anyone who would also be able to contribute to this discussion?

SURVEY S1

1. [Dropdown] Where do you currently reside?
2. [Short-answer Text] What is your position and role?
3. [Multiple Choice] In which sector do you work?
4. [Multiple Choice] How many years of experience in this field do you have?
5. [Multiple Choice Grid] Which of the following technologies do you consider a PET?

- Anonymous Credentials
- Anonymous Proxies
- Anti Tracking
- Attribute-Based Encryption
- Attribute-Based Signatures
- Biometric Authentication
- Cookie Management Tools
- Covert Communication
- Data Access Control
- Data Aggregation
- Data Perturbation
- Data Randomization
- Data Suppression
- Data Swapping
- DC-Networks
- Decentralized Storage
- Deniable Authentication
- Deniable Encryption
- Differential Privacy
- Digital Signatures
- Disk Encryption
- Email Encryption
- End-to-End Encryption
- Federated Learning
- Group Signature
- Homomorphic Encryption
- K-Anonymity
- L-Diversity
- Mix-Networks
- Oblivious Transfer
- Off-the-Record Messaging
- Onion Routing
- Policy Enforcement
- Privacy Policy Management
- Privacy-Preserving Data Mining
- Private Information Retrieval
- Proxy Re-Encryption
- Searchable Encryption
- Secure Multi-party Computation
- Self-Destructive Data Systems
- Single Proxy
- SSL/TLS Enforcer
- Steganography
- Symmetric/Asymmetric Encryption
- Synthetic Data
- T-Closeness
- Trusted Execution Environment
- Verifiable Encryption
- Virtual Private Networks
- Zero Knowledge Proofs

   "PETs are a system of ICT measures to protect the rights and freedom of data subjects in their online activities and communications, by eliminating, altering or minimizing the collection of personal data. These technologies, when properly implemented, can minimize the disclosure of PII and prevent correlation while allowing third parties to derive value from data."

6. [Linear Scale 1 - 10] How would you rank the above definition for PETs in terms of understandability?
   Understandability: how clear and easily comprehensible is the proposed definition.
7. [Linear Scale 1 - 10] How would you rank the above definition for PETs in terms of completeness?
   Completeness: to what extent does the definition cover the important aspects of PETs.
   Note: This question is optional.
8. Is there anything we may have missed or that you would like to share?

SURVEY S2

1. [Dropdown] Where do you currently reside?
2. [Short-answer Text] What is your position and role?
3. [Multiple Choice] In which sector do you work?
4. [Multiple Choice] How many years of experience in this field do you have?
5. [Multiple Choice] Are you familiar with the term *Privacy-Enhancing Technologies*?

   Privacy-Enhancing Technologies (PETs) are "a system of ICT measures protecting informational privacy by eliminating or minimizing personal data thereby preventing unnecessary or unwanted processing of personal data, without the loss of the functionality of the information system."

6. [Linear Scale 1 - 10] How would you rank the above definition for PETs in terms of understandability?
   Understandability: how clear and easily comprehensible is the proposed definition.
7. [Linear Scale 1 - 10] How would you rank the above definition for PETs in terms of completeness?
   Completeness: to what extent does the definition cover the important aspects of PETs.
8. [Linear Scale 1 - 10] How would you rank the above definition for PETs in terms of scope?
   Scope: whether the scope of the definition is too narrow, too broad, or just right (=5).

   Privacy-Enhancing Technologies (PETs) covers "a broad range of technologies and applications that are designed to enhance privacy and data security of both individual and corporate users in their online activities and communications."

9. [Linear Scale 1 - 10] How would you rank the above definition for PETs in terms of understandability?
   Understandability: how clear and easily comprehensible is the proposed definition.
10. [Linear Scale 1 - 10] How would you rank the above definition for PETs in terms of completeness?
    Completeness: to what extent does the definition cover the important aspects of PETs.
11. [Linear Scale 1 - 10] How would you rank the above definition for PETs in terms of scope?
    Scope: whether the scope of the definition is too narrow, too broad, or just right (=5).

    Privacy-Enhancing Technologies (PETs) are "a collection of technical measures to protect the rights and freedom of data subjects by eliminating, altering, or minimizing the processing of their personal data. These technologies, when properly implemented, can prevent direct or indirect linkage between data subjects and their data, while allowing processing entities to derive value from data in a way that is compliant with applicable data protection regulations."

12. [Linear Scale 1 - 10] How would you rank the above definition for PETs in terms of understandability?
    Understandability: how clear and easily comprehensible is the proposed definition.
13. [Linear Scale 1 - 10] How would you rank the above definition for PETs in terms of completeness?
    Completeness: to what extent does the definition cover the important aspects of PETs.
14. [Linear Scale 1 - 10] How would you rank the above definition for PETs in terms of scope?
    Scope: whether the scope of the definition is too narrow, too broad, or just right (=5).
15. [Paragraph] Is there anything we may have missed or that you would like to share?

S1 Survey Participants

TABLE VI
S1 survey study participants.

ID	Role	Industry Domain	Country	Exp.
S1	Senior Privacy and Regulatory Counsel	Legal Services	United States	20+
S2	Senior Legal Counsel	Legal Services	Mexico	5-10
S3	Barrister	Legal Services	Ireland	10-20
S4	Privacy Engineer	Retail	Germany	5-10
S5	Policy Officer	Information Technology	Belgium	3-5
S6	Advocate	Information Technology	United States	10-20
S7	Data Protection Specialist	Finance	Bulgaria	5-10
S8	Software Engineer	Information Technology	United Kingdom	10-20
S9	Senior Security Consultant	Information Technology	India	20+
S10	Engineer	Automotive	Germany	5-10
S11	Software Developer	Information Technology	Argentina	5-10
S12	Account Executive	Information Technology	United Kingdom	1-3
S13	Software Release Manager	Education Technology	Portugal	10-20
S14	PhD Candidate	-	Germany	3-5
S15	Global Privacy Consultant	Management Consulting	United Kingdom	5-10
S16	Data Protection Officer	Finance	Poland	3-5
S17	Legal Consultant Data Privacy	Information Technology	Romania	10-20
S18	Privacy Officer	Healthcare	United States	20+
S19	Data Protection Auditor & Consultant	Consulting	Germany	5-10
S20	Information Security Specialist	Finance	Croatia	1-3
S21	Director	Consulting	United Kingdom	10-20
S22	Privacy Engineer	Information Technology	Germany	10-20
S23	Data Security and Privacy Consultant	Automotive	Romania	1-3
S24	Privacy Engineer	Information Technology	United States	3-5
S25	Sr. Director, Security Consulting & Data Privacy Officer	Information Technology	United States	10-20
S26	Privacy Integration Specialist	Finance	India	5-10
S27	Cybersecurity Officer	Information Technology	Uganda	3-5
S28	Partner Manager	Information Technology	Germany	3-5
S29	Counsel	Legal Services	United States	20+
S30	Privacy Lead	Travel and Tourism, Aviation	United States	3-5
S31	Group Director, Product Management - Customer Data Platform	Retail	United States	20+
S32	Program Manager, Privacy Compliance	Information Technology	United States	5-10
S33	Admin Director Privacy	Healthcare	United States	20+
S34	Privacy Analyst	Education	United States	5-10
S35	Group Chief Privacy Officer	Finance	South Africa	20+
S36	Cybersecurity and Privacy Manager	Finance	Brazil	20+
S37	Manager: Information Governance	Education	South Africa	1-3
S38	Senior Privacy Program Manager	Finance	United States	10-20
S39	Senior Consultant - Cyber Security	Consulting	Ireland	3-5
S40	Director	Entertainment	United States	20+

S2 Survey Participants

TABLE VII
S2 survey study participants. '-' denotes that no information was provided.

ID	Role	Industry Domain	Country	Exp.
S1	Data Protection Officer	Manufacturing	Netherlands	5-10
S2	Data Protection Officer	Government	Belgium	5-10
S3	Product Manager	Information Technology	United Kingdom	5-10
S4	Senior Consultant	Healthcare	Croatia	1-3
S5	Consultant	Information Technology	United States	3-5
S6	Sr. Director, Security Consulting & Data Privacy Officer	Information Technology	United States	10-20
S7	Cybersecurity Officer	Information Technology	Uganda	3-5
S8	Privacy Engineer	Energy	United States	5-10
S9	Information Security	Information Technology	United Kingdom	10-20
S10	Privacy Engineer	Automotive	Switzerland	5-10
S11	Director of Privacy, Compliance & Group DPO	BioTech	United Kingdom	5-10
S12	Data Privacy Officer	Energy	Germany	20+
S13	Group Chief Privacy Officer	Finance	South Africa	10-20
S14	Director	Entertainment	United States	20+
S15	Privacy Engineer	Healthcare	Germany	1-3
S16	Data Protection and Privacy Officer	Finance	United Kingdom	5-10
S17	Senior Machine Learning Engineer	Information Technology	United States	20+
S18	Privacy Manager	Retail	United Arab Emirates	5-10
S19	Group Director - Customer Data Platform	Retail	United States	10-20
S20	Chief Privacy Officer	Government	United States	20+
S21	Privacy Engineer	Information Technology	United States	5-10
S22	Privacy Engineer / Senior Consultant	Information Technology	Nigera	3-5
S23	-	-	Germany	3-5
S24	Data Protection Officer	Business Services	Romania	5-10
S25	Senior IT Compliance Analyst	Finance	United States	5-10
S26	Senior Privacy Engineer	Information Technology	United States	5-10
S27	Head of Privacy Operations	Information Technology	United Kingdom	5-10

THE COMPLETE LIST OF PETS

TABLE VIII
THE COMPLETE LIST OF TECHNOLOGIES CLASSIFIED AS PETS IN THE LITERATURE.

Name	References
Anonymous Credentials	[29], [7], [21], [4], [20], [9], [40], [25], [34]
Anonymous Proxies	[7], [24], [34], [36]
Anti Tracking	[7], [21], [20], [33], [36]
Attribute-Based Encryption	[29], [7]
Attribute-Based Signatures	[7]
Biometric Authentication	[15], [39], [13], [8], [25]
Cookie Management Tools	[7], [19], [23], [24], [25]
Covert Communication	[29], [9], [25]
Data Access Control	[15], [13], [4], [9], [5], [34]
Data Aggregation	[29], [18], [7], [4], [32], [25]
Data Perturbation	[29], [7], [12], [4], [33]
Data Randomization	[29], [4], [32], [25]
Data Suppression	[29], [32]
Data Swapping	[29], [4], [32], [25]
DC-Networks	[29], [9], [34]
Decentralized Storage	[31], [8]
Deniable Authentication	[29], [9]
Deniable Encryption	[29], [21], [9]
Differential Privacy	[29], [18], [39], [7], [31], [8], [4], [14]
Digital Signatures	[15], [31], [8], [4], [5], [24], [25], [35], [41]
Disk Encryption	[21], [8], [25]
Email Encryption	[21], [25]
End-to-End Encryption	[7], [8], [20], [25]
Federated Learning	[29], [18], [39], [31], [8], [4], [14]
Group Signature	[29], [7], [21], [34]
Homomorphic Encryption	[29], [18], [39], [7], [31], [8], [4], [14], [9], [33], [25]
K-Anonymity	[29], [18], [7], [12], [21], [31], [8], [4], [32], [9], [26], [10], [25]
L-Diversity	[29], [7], [12], [21], [4], [9], [10], [25]
Mix-Networks	[29], [15], [12], [21], [19], [9], [10], [25], [34], [35]
Oblivious Transfer	[29], [7], [21], [4], [14], [9], [25]
Off-the-Record Messaging	[29], [9], [43]
Onion Routing	[29], [15], [7], [12], [21], [31], [4], [9], [40], [25], [35], [36], [37], [43]
Policy Enforcement	[12], [4], [9], [25]
Privacy Policy Management	[15], [12], [31], [4], [9], [24], [34], [35]
Privacy-Preserving Data Mining	[4], [9]
Private Information Retrieval	[29], [7], [12], [21], [9], [33], [25], [34]
Proxy Re-Encryption	[29], [21], [25]
Searchable Encryption	[29], [21], [31], [9]
Secure Multi-party Computation	[29], [18], [39], [7], [12], [21], [31], [8], [4], [14], [9]
Self-Destructing Data Systems	[7]
Single Proxy	[29], [9], [25], [34]
SSL/TLS Enforcer	[21], [43]
Steganography	[29], [21], [9], [24], [25]
Symmetric/Asymmetric Encryption	[29], [15], [31], [8], [4], [9], [22], [24], [25], [35]
Synthetic Data	[29], [18], [39], [8], [4], [14], [32]
T-Closeness	[29], [7], [21], [4], [10], [25]
Trusted Execution Environment	[29], [18], [39], [31], [4]
Verifiable Encryption	[29], [9]
Virtual Private Network	[15], [7], [30], [4], [25], [36]
Zero Knowledge Proof	[29], [18], [39], [7], [31], [8], [4], [14], [25], [34]

EXCLUDED DEFINITIONS

TABLE IX
THE COMPLETE LIST OF EXCLUDED PET DEFINITIONS. IN ADDITION TO YEAR PUBLISHED AND THE SUPPORTING REFERENCE, WE PROVIDE A REASON FOR EXCLUSION FROM OUR FINAL SET OF DEFINITIONS.

ID	Definition	Year	Ref.	Exclusion Reason
D1	Wide range of technologies that help protect personal privacy.	2002	[52]	no new aspects
D2	Means to protect privacy of the individuals or the information contained within privacy.	2007	[19]	no new aspects
D3	Technologies that are enforcing legal privacy principles in order to protect and enhance privacy of users of information technology (IT) and/or data subjects.	2017	[25]	no new aspects
D4	Broad range of technologies that are designed for supporting privacy and data protection.	2020	[53]	too broad
D5	Technologies designed to protect personal and sensitive data in use by minimizing their exposure to potential malicious entities.	2021	[41]	no new aspects
D6	Technologies that embody fundamental data protection principles by minimizing personal data use, maximizing data security, and/or empowering individuals.	2023	[39]	no new aspects

TABLE X
THE SURVEY RESULTS, AS DESCRIBED IN SECTION V-D AND FIGURE 2.

Technology	**Yes**	**No**	**Not sure**
Anonymous Credentials	**26**	7	7
Anonymous Proxies	**23**	10	7
Anti Tracking	**31**	5	4
Attribute-Based Encryption	**23**	6	11
Attribute-Based Signatures	14	11	**15**
Biometric Authentication	10	**30**	0
Cookie Management Tools	**20**	15	5
Covert Communication	**17**	11	12
Data Access Control	**25**	11	4
Data Aggregation	**22**	16	2
Data Perturbation	**20**	5	15
Data Randomization	**27**	6	7
Data Suppression	**24**	7	9
Data Swapping	**20**	7	13
DC-Networks	6	8	**26**
Decentralized Storage	12	**19**	9
Deniable Authentication	12	9	**19**
Deniable Encryption	16	6	**18**
Differential Privacy	**32**	3	5
Digital Signatures	15	**22**	3
Disk Encryption	**31**	8	1
Email Encryption	**32**	6	2
End-to-End Encryption	**36**	4	0
Federated Learning	**17**	11	12
Group Signature	8	**20**	12
Homomorphic Encryption	**29**	1	10
K-Anonymity	**24**	4	12
L-Diversity	**19**	5	16
Mix-Networks	13	5	**22**
Oblivious Transfer	11	5	**24**
Off-the-Record Messaging	14	10	**16**
Onion Routing	**23**	6	11
Policy Enforcement	11	**23**	6
Privacy Policy Management	14	**25**	1
Privacy-Preserving Data Mining	**26**	8	6
Private Information Retrieval	10	**15**	**15**
Proxy Re-Encryption	**16**	12	12
Searchable Encryption	**17**	9	14
Secure Multi-party Computation	**22**	10	8
Self-Destructive Data Systems	**22**	7	11
Single Proxy	6	**17**	**17**
SSL/TLS Enforcer	**19**	12	9
Steganography	13	11	**16**
Symmetric/Asymmetric Encryption	**28**	9	3
Synthetic Data	**27**	4	9
T-Closeness	13	7	**20**
Trusted Execution Environment	**18**	8	14
Verifiable Encryption	**27**	2	11
Virtual Private Networks	**22**	15	3
Zero Knowledge Proofs	**23**	5	12