DEPARTMENT OF INFORMATICS

TECHNISCHE UNIVERSITÄT MÜNCHEN

Master's Thesis in Informatics: Information Systems

Privacy-Preserving Natural Language Processing: A Systematic Mapping Study

Felix Viktor Jedrzejewski

DEPARTMENT OF INFORMATICS

TECHNISCHE UNIVERSITÄT MÜNCHEN

Master's Thesis in Informatics: Information Systems

Privacy-Preserving Natural Language Processing: A Systematic Mapping Study

Privatsphäre erhaltende Verarbeitung natürlicher Sprache: Eine systematische Mapping-Studie

Author:	Felix Viktor Jedrzejewski
Supervisor:	Prof. Dr. Florian Matthes
Advisor:	Oleksandra Klymenko
Submission Date:	15.07.2021

I confirm that this master's thesis in informatics: information systems is my own work and I have documented all sources and material used.

Munich, 15.07.2021 Felix Viktor Jedrzejewski

Acknowledgments

I'd like to thank my family and friends for their support. I also want to thank my advisor Oleksandra for her guidance and patience with me.

Abstract

The introduction of the General Data Protection Regulation (GDPR) shifted the focus of interest towards the research field of privacy preservation techniques. This paper investigates challenges and solutions within the research field of Privacy-Preserving Natural Language Processing (NLP), an intersection between Privacy and Natural Language Processing (NLP) and privacy. Since this research field is beginning, we want to know which challenges and solutions it provides to deal with privacy-related challenges and if there is a possibility to categorize them. Furthermore, our goal is to overview this research field to support other researchers coordinating within the area. To achieve this goal, we apply a systematic mapping study focusing on the challenges and the solutions provided by the research field of Privacy-Preserving Natural Language Processing. We noticed two significant categories that interpret NLP either as a privacy enabler or as a privacy threat. To deepen our understanding of the privacy-related issues within the field, we also extracted use case categories and NLP-related features to map them on the privacy-related challenges and solutions. Finally, we offer an overview of privacy-related challenges in which use case categories they appear and how they are solved.

Kurzfassung

Die Einführung der General Data Protection Regulation (GDPR) hat das Interesse auf das Forschungsfeld der Techniken zur Erhaltung der Privatsphäre geweckt. Diese Arbeit untersucht Herausforderungen und Lösungen innerhalb des Forschungsfelds der privatsphäre-erhaltenden natürlichen Sprachverarbeitung, einer Kombination aus Datenschutz und natürlicher Sprachverarbeitung und Privatsphäre. Da dieses Forschungsfeld sehr jung ist, wollen wir wissen, welche Herausforderungen und Lösungen es für den Umgang mit privatsphäre-erhaltenden Herausforderungen bietet und ob es eine Möglichkeit gibt, diese zu kategorisieren. Darüber hinaus ist es unser Ziel, einen Überblick über dieses Forschungsfeld zu geben, um andere Forscher zu unterstützen, die sich auf diesem Gebiet orientieren wollen. Um dieses Ziel zu erreichen, wenden wir eine systematische Mapping Studie an, die sich auf die Herausforderungen und die Lösungen konzentriert, die das Forschungsfeld privatsphäre-erhaltenden natürlichen Sprachverarbeitung bietet. Dabei sind uns zwei Kategorien aufgefallen, die NLP entweder als Unterstützer der Privatsphäre oder als Bedrohung der Privatsphäre interpretieren. Um unser Verständnis der datenschutzrelevanten Themen innerhalb des Feldes zu vertiefen, haben wir außerdem Anwendungsfallkategorien und NLP-bezogene Merkmale extrahiert, um sie auf die privatsphäre-relevanten Herausforderungen und Lösungen abzubilden. Abschließend bieten wir einen Überblick über privatsphäre-relevanten Herausforderungen, in welchen Use-Case-Kategorien sie auftreten und wie sie gelöst werden.

Contents

Acknowledgments **iii**

Abstract **iv**

Kurzfassung **v**

1. Introduction **1**
1.1. Introduction . . . 1
1.2. Research Objectives . . . 3
1.3. Research Approach . . . 4
1.3.1. Systematic Collection of Potential Sources . . . 4
1.3.2. Inclusion and Exclusion Process . . . 5
1.3.3. Analysis of Included Sources . . . 5

2. Foundations **7**
2.1. Definitions . . . 7
2.1.1. Privacy . . . 7
2.1.2. Privacy Enhancing Technologies (PETs) . . . 8
2.1.3. Natural Language Processing . . . 9
2.1.4. Privacy-Preserving Natural Language Processing . . . 10

3. Related Work **12**
3.1. Systematic Mapping Studies Addressing Privacy . . . 12
3.1.1. Security and Privacy Concerns in Connected Cars . . . 12
3.1.2. Privacy-Related Challenges in mHealth and uHealth Systems . . . 13
3.2. Applying Natural Language Processing in the Legal Domain . . . 13
3.2.1. Natural Language Processing and Automated Handling of Privacy Rules and Regulations . . . 13
3.3. Surveys on Applying Privacy Preservation on Machine Learning and Deep Learning . . . 14
3.3.1. Privacy Preservation and Machine Learning . . . 15
3.3.2. Privacy Preservation and Deep Learning . . . 15
3.4. Workshops on Privacy in Natural Language Processing . . . 19
3.4.1. Papers from the ”PrivateNLP 2020@WSDM 2020” Workshop . . . 19
3.4.2. Papers from the ”PrivateNLP@EMNLP 2020” workshop . . . 20

4. Methodology **22**
4.1. Definition of Research Questions . . . 22
4.2. Search Process . . . 22
4.2.1. Search Queries . . . 23
4.2.2. Selection of Electronic Data Sources . . . 24
4.2.3. Result Filtering . . . 26
4.2.4. Validation of the Search Process . . . 27
4.3. Paper Screening for Inclusion or Exclusion . . . 28
4.4. Validation . . . 29
4.5. Keywording of Abstracts . . . 33
4.5.1. Subcategories Natural Language Processing as Privacy Enabler . . . 34
4.5.2. Subcategories Natural Language Processing as Privacy Threat . . . 40

5. Results **48**
5.1. Numbers of Publications per Year . . . 48
5.2. Numbers of Publications per Electronic Data Source . . . 48
5.3. What privacy-related challenges exist in the area of Natural Language Processing (NLP)? . . . 49
5.3.1. Challenges for NLP as a Privacy Enabler . . . 50
5.3.2. Challenges for NLP as a Privacy Threat . . . 56
5.4. What approaches are used to preserve privacy in and with NLP tasks and how can they be classified? . . . 58
5.4.1. Privacy Solutions Provided by NLP . . . 58
5.4.2. Solutions Provided for NLP Privacy Issues . . . 61
5.5. What are the current research gaps and possible future research directions in the area of privacy-preserving NLP? . . . 63
5.5.1. Research Gaps for NLP as a privacy Enabler . . . 63
5.5.2. Research Gaps for NLP as a privacy Threat . . . 64

6. Discussion **83**
6.1. Summary of Findings . . . 83
6.1.1. Main Privacy related Challenges for NLP as a Privacy Enabler . . . 83
6.1.2. Main Privacy related Challenges for NLP as a Privacy Threat . . . 84
6.1.3. Solutions supported by NLP as a Privacy Enabler . . . 85
6.1.4. Main Solutions for NLP as a Privacy Threat . . . 86
6.2. Limitations . . . 87

7. Conclusion and Future Work **89**
7.1. Conclusion . . . 89
7.2. Future Work . . . 89

A. General Addenda **91**
A.1. Work Sheets containing the analysis of the top categories 91
A.1.1. NLP as a Privacy Enabler Analysis Sheet 91
A.1.2. NLP as a Privacy Threat Analysis Sheet 98
A.2. Detailed Category Tables with Aggregation Mapping 102
A.2.1. Privacy Issue Solutions for NLP as a Privacy Enabler 102
A.2.2. Privacy Issue Solutions for NLP as a Privacy Threat 106
A.3. Figures for Mapping Results 108
A.3.1. Use Case Classification for NLP as a Privacy Treat 108

List of Figures **110**

List of Tables **112**

Acronyms **113**

Bibliography **114**

1. Introduction

The following chapter will elaborate the motivation of this research in section 1.2, the research objectives in section 1.2 and afterwards, in section 1.3, we illustrate how we intend to achieve these goals.

1.1. Introduction

One of the most crucial events in terms of privacy was the introduction of General Data Protection Regulation (GDPR) in 2016. The European Union adopted this law that is recognised across Europe. The member states had 2 years to adopt the law on their national level until May 2018. Now, an individual has legal protection for the data that were collected based on different factors (e.g behavior online, input data, etc.). This also means that there are crucial legally binding consequences for anyone who is not acting accordingly [1]. One main reason for this law is to protect the individual from the threats posed by Big Data and the insatiable hunger of companies collecting data in any possible manner [2]. Therefore, the GDPR enables the European Data Protection Authorities (DPA) to punish companies for a violation of this right with a payment of up to 4 percent of the annual income [3]. There are already several examples of EU member countries that prosecuted companies for GDPR violations. For instance, France suing Google for insufficient legal basis for data processing resulting in a fine of 50 million euros. The same scenario occurred to H&M in Germany and TIM(telecommunications operator) in Italy with fines of around 35 million and 27 million euros, respectively [4].

However, this was not the only reason for the increased interest for privacy, but rather the result of multiple events in the past that drew the attention of the public towards it. One of the aforementioned events is the Cambridge Analytica Scandal which only got disclosed to the public through whistleblower Christopher Wylie. He described how his former employer harvested data of Facebook users without their consent. With this data, Cambridge Analytica was able to analyze the behavior of a large amount of Facebook users and target those who were likely to change their mind and also convince others. This "service" was purchased by famous politicians to win voters for their side [5]. This is just one of many examples that got leaked, however, there are many more cases of data breaches and leaks.

Living in the time of Big Data, companies are collecting more and more data from everything possible we can get in order to analyze. This fact is reflected in the amount of publications in the area of big data which were made between 2000 and 2019, as can be seen in Figure 1.1 [6].

The collection of data happens automatically, therefore, it is imperative to also apply an automated approach to preserve the data privacy in order to protect not just the individual

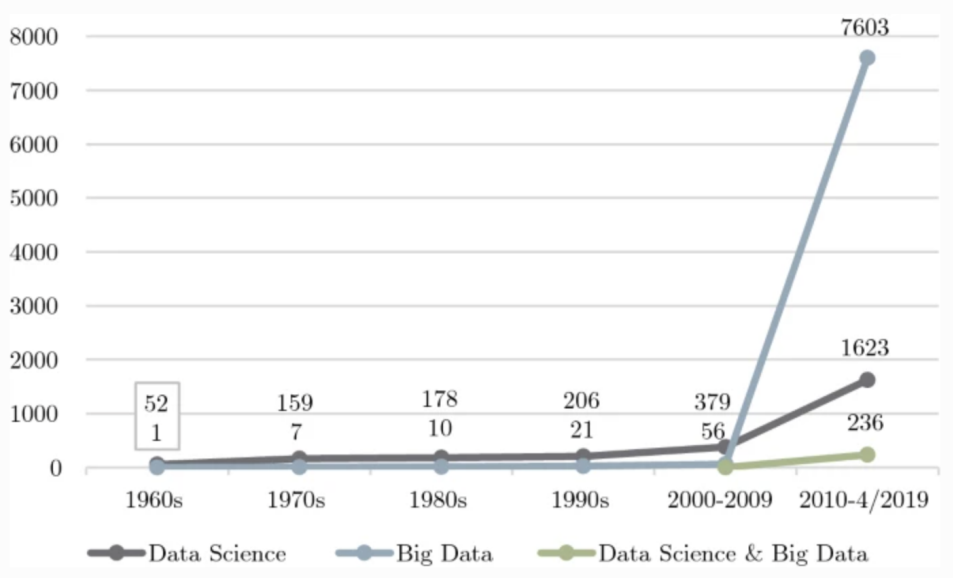


Figure 1.1.: Trend of the number of publications in data science and big data taken from [6]

but also companies intending to guarantee privacy of every involved individual and avoid tremendous penalty fines. However, data privacy has the main disadvantage of usability reduction which is a key issue and is being intensively researched. We decided to focus on the medium that incorporates and transmits private information, namely the natural language. The natural language occurs either in the form of voice or in written form.

Filtering out private information is a difficult tasks especially if the text is unstructured. There are several easily detectable pieces of sensitive information, namely email and local addresses, names, phone numbers etc., which embody some sort of uniqueness that can be solved with algorithms (e.g. a pattern matching). However, there are also some information types which require more sophisticated approaches in order to be detected. If the context or the user perception of the private information varies it is complex to devise an optimal solution because of the lack of flexibility of current methods [7]. An attempt is needed that is robust to varying complexity levels to find sensitive information and also capable to handling the amount of data. We consider Natural Language Processing (NLP) domain as an adequate fit for the aforementioned challenge.

Furthermore, we must point out that there are several vulnerabilities within the NLP domain. One paper demonstrates the ability to extract information about the training data used to train neural networks. This trait is called unintentional memorability. Additionally, a method is presented that can measure the unintended memorability of different neural networks. Thus, models save information from the training set. In our case, this is especially critical if the training set contains private information in the form of natural language [8]. Additional privacy leaks were also detected within language models. Successful attacks already have been constructed to demonstrate the exploitability of popular state-of-the-art language models, namely BERT, Transformer-XL, XLNet, GPT, GPT-2, RoBERTa, XLM, Ernie

2.0. Word embeddings are reverse-engineerable without any prior knowledge and attackers are able to retrieve up to 75 percent of the sensitive data they have been trained on [9]. Another research attempt could fully reconstruct 411 out of 600 patient data records that were anonymized before they were used to train the published word embeddings [10].

During our mapping study, we realized that there are two challenges that can be solved with NLP. On the one hand, we know that large unstructured text corpora can be automatically redacted by the application of NLP to extract or replace private information. There is a plethora of papers aiming at the aforementioned challenge, thus, we concluded that a structured overview for this domain will be essential to not just show what kind of research has already been done but also which gaps exist. On the other hand, it emerges the need to preserve privacy within the tasks broadly applied in the NLP domains. Furthermore, we discovered that plenty of papers address the problems caused by privacy policies. All the mentioned aspects encouraged us to aggregate it in one domain. This leads us to the domain of Privacy-Preserving Natural Language Processing (PP NLP).

1.2. Research Objectives

This thesis aims to provide a definition for PP NLP, since we realized that there will be multiple ways of interpretation of the term during our preliminary analysis. Additionally, we think it will helpful in the future of this research field to have a clear definition in order to avoid repetitive research. We will provide some additional information that are the answer to our research questions listed in Table 1.1.

ID	Research Question
RQ1	What privacy-related challenges exist in the area of Natural Language Processing (NLP)?
RQ2	What approaches are used to preserve privacy in and with NLP tasks and how can they be classified?
RQ3	What are the current research gaps and possible future research directions in the area of privacy-preserving NLP?

Table 1.1.: Table of Research Questions

In our overview of the research field of PP NLP, we include the privacy related challenges which exist in the context of NLP. Simultaneously, this is the answer of RQ1. This piece of information will support the community to see which challenges were already identified and also ease the process of finding new ones. In order to answer RQ1, we will scan all the papers we found in the search process for the problem statements that are trying to solve and summarize it. Then, we propose an aggregation scheme for the findings with the help of keywording [11]. This will ease the understanding of the research field since the aggregation scheme will map the papers to high level terms. Further, we define the term Privacy Preserving Natural Language Processing to clarify our understanding of the research field which we analyze.

After extracting and having an overview of the different privacy challenges within the NLP domain, we aim to figure out which approaches currently exist in order to preserve the privacy in NLP tasks and also how NLP concepts can be utilized to establish privacy. We expect to derive patterns from these findings indicating popular privacy enhancing technologies PETs to preserve privacy within which NLP concepts and which NLP concepts were used in order to introduce an increased level of privacy in a certain scenario. Here, we will categorize our findings and bring it in context with the findings of RQ1. Furthermore, our research will point out which trends are currently emerging.

After answering RQ1 and RQ2, we will provide an overview of the privacy challenges and their solution approaches. The answer to RQ3 will be the investigation of possible gaps within the current research state based on the aforementioned findings and imply which research streams are up-rising or even suggest new research streams. Additionally, other researchers are supported in discovering further research gaps.

Additionally, we would like to devise an overview of the research field of PP NLP. With this overview, we would like to graphically summarize the research field to ease the task to discover new research opportunities. Therefore, a categorization of different research streams is necessary to introduce in order to structure the overview better and improve the readability of the graphical representation. Furthermore, we will highlight resulting trends in the research area by showing how many papers contributed to the field.

1.3. Research Approach

Since we want to receive a broad overview over the research field of PP NLP and which challenges and solutions are prevalent, the application of a systematic mapping study (SMS) is suggested [12]. Therefore, we will describe the process roughly and in more detail in chapter 4. We chose the systematic mapping study, since it supports the idea of devising a classification scheme and structure of a software engineering field. According to Petersen, the mapping study roughly consists of three phases, namely planning, conducting, and reporting the mapping. The detailed process is displayed in Figure 1.2 and the process adaptations will be further explained in chapter 4 [11]. We will utilize the systematic approach of the SMS to conduct the collection process of papers addressing our definition in a reproducible way. Mainly, the aim of SMS is to categorize different research streams and the analysis of publication related information in a software engineering field of interest [13]. Instead of focusing on the data regarding the paper publication, we inspect the challenges and solutions in the area of PP NLP. This will be the main inspiration for the research approach of this thesis. The number of relevant papers in the different phases of the SMS, which are explained in the next sections, are displayed in Figure 1.3.

1.3.1. Systematic Collection of Potential Sources

After the selection of the data bases which we involved in our search process defined in table 4.3, we needed to decide which search queries have to be executed. As a result, we selected

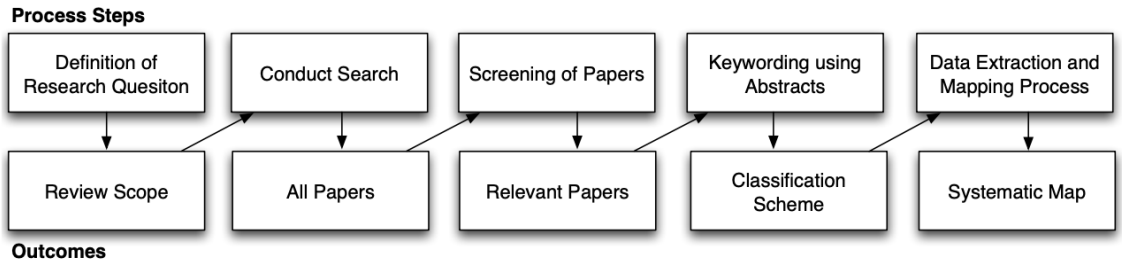


Figure 1.2.: Overview of the Systematic Mapping Study (SMS) taken from [11]

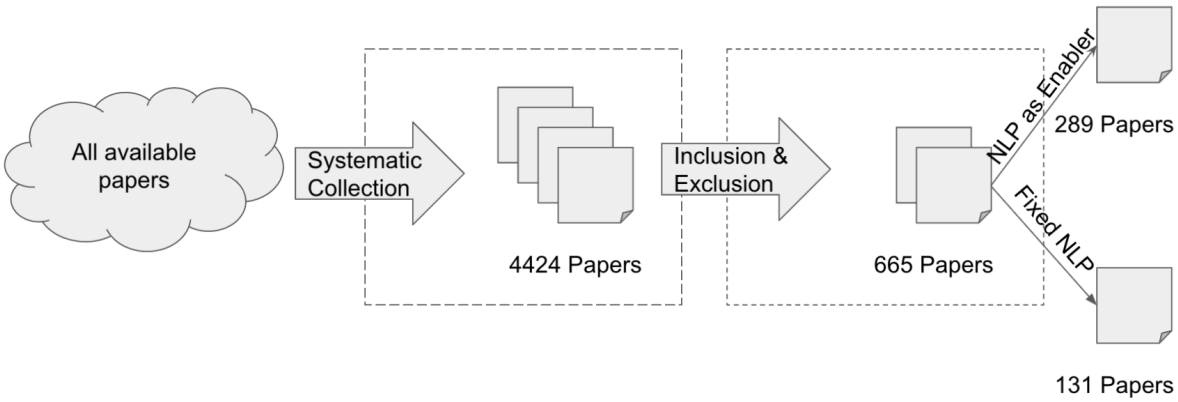


Figure 1.3.: Amount of papers during the different SMS phases

five search queries listed in Table 4.1. Every data base was confronted with each query which resulted in 4424 papers. In the next step, the collected papers need to be further examined, as suggested by Petersen [11].

1.3.2. Inclusion and Exclusion Process

After the collection of the relevant papers, we thought of inclusion and exclusion criteria which supported us to scan through the papers and sort those out that do not fit into our definition of PP NLP. Here, we applied the methodology of Petersen and inspected the title and the abstract of the collected papers and included or excluded accordingly to the criteria we agreed on [11]. At the end of this phase, 665 papers were left that addressed our topic of interest. Now, we analyze the remaining papers and start the categorization process.

1.3.3. Analysis of Included Sources

In the last phase of the mapping study, we sorted our findings into a classification scheme regarding the privacy related challenges and solutions according to Petersen [11]. For this purpose, we applied the keywording of abstracts displayed in Figure 1.4. During this process

we discovered two main streams within the selected papers, namely NLP as enabler for privacy preserving methods and also fixed privacy related issues within NLP concepts. The two main streams ended up to different amount of papers. NLP as enabler for privacy counts 304 papers and the second stream fixed privacy issues within NLP concepts 127 papers.

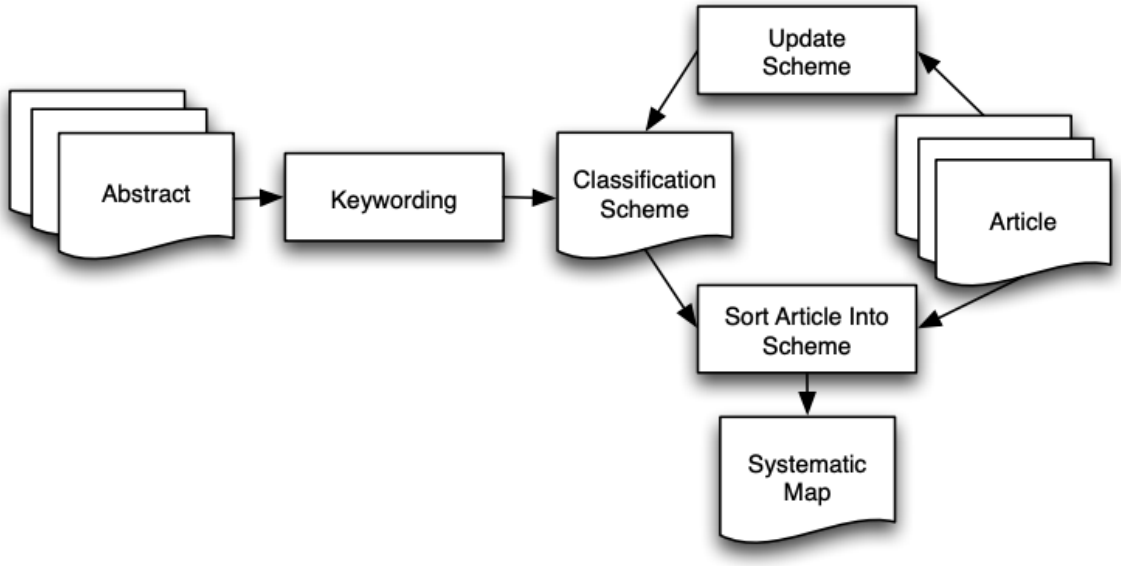


Figure 1.4.: Keywording abstracts to build classification schemes taken from [11]

2. Foundations

In this chapter we will define our area of research and the terms applied in this work to have the same understanding. Also, we want to propose a novel definition regarding Privacy-Preserving Natural Language Processing.

2.1. Definitions

This section contains the definitions of the key terms that are essential in the context of this thesis. First, the key terms privacy, its preservation techniques and Natural Language Processing are delineated. As part of our contribution, we also propose a definition for Privacy-Preserving Natural Language Processing.

2.1.1. Privacy

The definition of privacy is always a complicated endeavor, especially in the legal domain because it is a term that not just differs from country to country, but from individual to individual [14]. According to Westin, there are three levels of privacy, namely the political, socio-cultural and personal [15]. In this thesis, we will focus on the personal level. Every individual has a set of information that is clearly attributable to it, however, this set is dynamic and changes from context to context and from time to time [14]. In this thesis, we call this set of information personal data. According to the General Data Protection Regulation (GDPR), personal data, or Personal Identifiable Information (PII), is defined as any information about an identified or identifiable natural person, or data subject. Specifically, an identifiable natural person, is a person that can be identified directly or indirectly by direct identifiers like a name, an identification number or one or more factors referring to its physical, physiological, mental, economic, cultural, or social identity [16]. The legal definitions of Personal Identifiable Information (PII) differ from country to country. In this thesis we use the expansionism of the European Union towards the term PII instead of the very restricted definition of PII in the United States of America [17]. The European expanded definition of PII is, however, limited to the realistic possibility of linkability of the information to a data subject [16]. It is also proven that the concept of PII is not sufficient to protect the privacy of an individual, especially when the sophistication of tools capable of inferring further information with little to no previous knowledge is constantly improving [7]. Therefore, we need an improved categorization of information related to an identifiable natural person. Any piece of information that might lead to the revealing of the privacy of an individual based on its perception is also called Privacy Sensitive Information (PSI). The combination of PSI and PII forms the super set

Privacy Revealing Information (PRI). Most importantly, the avoidance of the mapping of PII to PSI needs to be guaranteed at any time [7].

2.1.2. Privacy Enhancing Technologies (PETs)

Same as Y. Shen and Pearson, our understanding of privacy enhancing technologies are applied in order to protect private information of a data subject [18]. This part will describe our understanding of privacy preserving techniques that will frequently appear in this thesis. Therefore, we need to define our understanding of a few terms in order to have the same theoretical foundation.

De-identification of Personal Information

The process of De-Identification focuses on the removal of identifying information within a data set. The data removed in this context is called Personal Information instead of Personal Identifiable Information (PII). According to Garfinkel et al., Personal Identifiable Information refers to information that is only attributable to one individual, however, information that can attribute any individual are left out, although they are also important. This refers to any kind of data type including structured and unstructured text or multimedia. After the removal of that information, the risk is reduced for an individual to be linked to the data set. The goal is to have an acceptable trade-off between privacy and usability, in other words, sharing a data set without disclosing any information that might disclose the identity of an individual. Furthermore, the terms ”de-identification” and ”anonymization” are commonly used interchangeably, but in general, they aim for the same aforementioned process [19].

Differential Privacy

Differential Privacy guarantees a certain level of privacy to an input of an individual to a (randomized) function or a series of functions. It was designed in order to protect the privacy of an individual or a small group of individuals in a statistical analysis. A tremendous benefit of Differential Privacy is that even if an adversary has a lot computational power and knowledge over the differential private data set it is impossible to re-identify the individuals [20].

Obfuscation

The paper by Pang, X. Xiao, and J. Shen, illustrates our understanding of obfuscation in a sense where the actual data within a text corpus like a search query is masked by for example injecting fake queries in order to blur the intentions of the searching user or in other words not to fully disclose the data to a third party [21].

Synthetic Data Generation

According to El Emam, the generation of synthetic data is based on statistical models that are reapplied in order to generate a new data set fitting into the statistical traits from the original model. This avoids the sharing of the actual data but still allows the recipient to conduct analysis on the synthetic data set [22].

Federated Learning

The general idea of Federated Learning is that the training of a model is not executed on a central server but is distributed among different parties, also called clients. Every client has a data set containing sensitive information that is not uploaded to a central server. Instead, the client trains the global model with his locally stored data set and updates the parameters of the model. The orchestration of the training model among the different clients is managed by one central server [23].

Secure Multiparty Computation

As the term implies, the calculation process of an agreed function f involves several parties . All parties are in possession of a secret x_i that they do not send to any other of the parties participating in the computation process but is used as input for the function f. Two attributes are essential for Secure Multiparty Computation, namely the correctness of the computation of f and the privacy of the input x_i [24].

Homomorphic Encryption

According to Fontaine and Galand, Homomorphic Encryption needs to satisfy the following equation [25]:

$$\forall m_1, m_2 \in M, \qquad E(m_1 \odot_M m_2) \longleftarrow E(m_1) \odot_C E(m_2)$$

Let M and C represent all sets of plaintext and ciphertext respectively. $\odot_M and \odot_C$ denote an operation that is validly executable on the respective plaintext or ciphertext. $\longleftarrow$ means that the same operation is computable like on the left side of the arrow. In other words, Homomorphic Encryption is the process of performing operations on encrypted data with decrypting it at any stage [25].

2.1.3. Natural Language Processing

Our understanding of NLP is equal to the definition by Liddy [26]. Through the application of computational techniques, naturally occurring text is analyzed on multiple levels of linguistic analysis in order to have a similar level of human-like language processing to preform a specific set of task on it [26].

This definition is further explained in the source since a few terms a rather vaguely formulated. By ”naturally occurring text” any text is meant that is spoken or written by a human. This language is then ”analyzed on multiple levels of linguistic analysis” to translate

the human language in a way that is also understandable for the computer to process it [26]. This is an essential aspect for this work because we inspect not just written but also spoken text. It is commonly known that written text is containing private information about us like our email or our local address or our name. All of those information lead to a unique mapping that points to an individual. But this also counts for uniqueness of our voice which is also used for biometric authentication systems.

One level of the aforementioned level of linguistic analysis is called phonology or speech processing. This area inspects the voice sounds by applying a set of rules in order to not just distinguish words in a sentence but also take into account that pronunciation differs from one to another. There are rules called phonetic rules concentrating on the sounds within a word. Then, there are phonemic rules when words are spoken together and their pronunciation differs. Prosodic rules aim for the fluctuation in stress and intonation in a sentence [26]. But there are also novel approaches for the generation of voices that is based on vectors and probabilistic models [27].

For the written text, there are multiple linguistic models that need to be considered. The first and very fundamental level is morphology. The main subject of this topic are morphemes the smallest particle or word chunks with meaning in linguistics [26]. Part of Speech Tagging (POS) is the process of assigning words in a sentence their role within it for example noun, verb, adverb etc. The tagging is based on the morphological analysis of words [28]. The word, the composition of morphemes and lemmas, itself and its meaning is inspected on the lexical level. If we take the verb ”deliver” as a lemma and combine it with some morphemes we receive ”delivers” or ”delivered” etc. [29].

According to Liddy, another level of analysis within the NLP domain is the semantic one. The main goal of it is to investigate the contribution of meaning of sentences in order to detect and solve the problem of disambiguity and larger text corpora taking into account the information delivered by context of a given corpus [26]. Frequently used in the domain of NLP is a task from information extraction called Named Entity Recognition (NER). NER is a way to introduce structure into an unstructured text document searching for a certain meaning on the semantic level. It is not just used in order to identify people, organizations and institutes, but to search for certain information within a text corpus [30].

2.1.4. Privacy-Preserving Natural Language Processing

This definition of privacy preserving natural language processing is inspired by the accepted papers from the workshop series ”PrivateNLP” [31, 32, 33]. During the mapping study, we discovered two major topics that are handled by PP NLP. The first area is the application of NLP in order to establish privacy in a certain scenario. Commonly, the scenario focuses on some forms of sharing or publishing unstructured data sets with third parties in different contexts or supports the process of coping with privacy policies or requirements. But this can not be done before a privacy preservation technique based on NLP is executed on the data set in order to protect the privacy of the data subjects. The challenge with privacy policies or requirements is that the language, in which they are written, is complex and not comprehensible at first sight. In context of agreeing on web site cookies, privacy related

documents frequently challenge the user with its length. Because of that, NLP is applied in order to ease the process of handling those kinds of documents in different ways, namely summarization or rephrasing of privacy policies or an automatic comparison of a privacy policy and privacy requirements. The second topic we recognized, is the privacy protection of the data involved within a NLP process. As already mentioned in the introduction, the exploitation of fundamental NLP concepts was demonstrated. Therefore, it is important to extend this definition by including also the statement of Q. Feng, D. He, Z. Liu, et al. claiming that NLP should not enclosing any information regarding the data it is trained on [34].

3. Related Work

In the following, we list research that is closely related to our work to stress the value of our contribution to the field. Since, to the best of our knowledge, there is no concrete definition for Privacy-Preserving Natural Language Processing, there are several papers interfacing the topic. In this chapter, we point out Systematic Mapping Studies and surveys that focus on privacy preservation techniques related to machine learning or deep learning. However, there are some papers about the combination of privacy preservation and specific natural language techniques. In the first part, we will have a look at Systematic Mapping Studies that are topicwise related to our research. Afterwards, we discuss the application of NLP in the legal domain. Then, we inspect surveys based on privacy preservation techniques and deep learning. At the end, we inspect a workshop series addressing the topics NLP and privacy.

3.1. Systematic Mapping Studies Addressing Privacy

To the best of our knowledge, there are no systematic mapping studies addressing privacy preservation and Natural Language Processing, but only surveys on PP ML or PP AI not NLP. We selected two Systematic Mapping Studies analysing privacy challenges and its solutions within a context that includes natural language.

3.1.1. Security and Privacy Concerns in Connected Cars

We chose this Systematic Mapping Study inspecting privacy and security challenges within the domain of connected cars [35]. All research questions of this work are comparable to ours. The first attempts to identify what kind of privacy and security-related issues were identified by the researchers in connected cars. Here, the problems identified towards identity management refer to unallowed access to the network and, simultaneously, to the personal data processed and stored within it. The vehicle provider does not provide any additional privacy measures within the network to secure the personal data in a malicious network intruder or an insecure central server. According to the paper, the solution to this threat is the implementation of privacy-preserving schemes like k-anonymity, encryption, bit-array encoding, or pseudonym-changing scheme [35]. Our work will focus on the privacy preservation of data in natural language in written or spoken form. Moreover, we analyze the role of NLP in providing privacy exclusively.

3.1.2. Privacy-Related Challenges in mHealth and uHealth Systems

There was another Systematic Mapping Study that caught our attention that aimed for a subtopic of our research. Therefore, we thought it is noteworthy in the context of this work. The research of Iwaya, Ahmad, and Babar focuses on the security and privacy in systems considering the NIST 800-53 control families that handle natural language. More particularly, on the privacy and security of mobile Health (mHealt) and ubiquitous Health (uHealth) systems. The mapping studies filter out 365 papers that match their field of research. The main targets of the analysis phase were the identification of research themes, main challenges, and their most prominent solutions. Then, those findings were categorized and synthesized. An overview of the different solutions organized by themes stresses the illustration of the limitations of the current research status. Also, an evaluation phase is conducted to check the practicability of the existing solution approaches [36]. Our approach differs mainly on the broader scope that we decided to have. Also, our interest is on NLP based approaches for private data represented in natural language.

3.2. Applying Natural Language Processing in the Legal Domain

This section will disclose several research overview papers addressing the application of NLP in the context of law and privacy. We realized that NLP offers support in handling complex legal documents explaining the privacy rights or complying with it.

3.2.1. Natural Language Processing and Automated Handling of Privacy Rules and Regulations

There is considerable research conducted on the combination of the legal domain and NLP. Papanikolaou, Pearson, and Mont survey natural language understanding and the automated enforcement of privacy rules and regulations in the cloud [37]. Automatic extraction of information from legal, regulatory, or policy text in the form of privacy knowledge or rules and combination with compliance and enforcement. The paper's main objective is to guarantee privacy level for customer data stored and processed in a cloud environment of an enterprise. To achieve this goal, the application of semantic analysis on text with NLP concepts and enabling automatic rule enforcement is imperative. Four categories were introduced within the paper: parsing and fundamental analysis of source texts, knowledge extraction from texts and learning, semantic models and representations, and policy enforcement and compliance. The analysis and parsing of a source text embody similar and repetitive patterns in frequencies of different word clusters. Therefore, several tools exploit this trait of legal text. Knowledge extraction from text and learning applies several machine learning concepts to analyze the semantic representation of legal text on a higher level and extract rules. Semantic models and illustrations support the idea of setting up rules with a specific order on the semantic level. Thus, this section refers to a sophisticated framework of rules for the generation of legal items that are easier to comprehend. The last section within the paper, policy enforcement, and compliance highlights that there is no research so far that focuses

on the entire life cycle of natural language analysis in the context of privacy. In other words, research that not just focus on the generation of clear and easily comprehendible rules, but also its enforcement [37]. Our work is more abstract and does not focus on the legal domain specifically. We will graphically represent the status quo of the research in the legal field with the focus on privacy preservation with the involvement of NLP, not explicitly searching for a complete privacy life cycle. Not just the creation of privacy life cycles was investigated. Also, tools were developed to detect privacy violations in legal documents like online contracts. The paper by Silva, Gonçalves, Godinho, et al. applies commonly known tools like NLTK, spaCy, and Stanford CoreNLP to develop a new tool that supports companies to detect privacy violations within legal contracts. The fundamental NLP task executed here is Named Entity Recognition (NER). It automatically detects potential personal identifiable information (PII) in legal documents. The tool is then tested in an experiment to evaluate its accuracy [38]. This is a very particular example for the application of NLP paradigm of semantics analysis to preserve the privacy of data subjects within a legal document like a contract. A systematic mapping study has been rendered on NLP for requirements engineering [39]. The objective of the SMS is to inspect the status quo of the research of NLP for requirements engineering, short NLP4RE, and to detect the open challenges with the domain. The result of the research is the extraction of five significant findings. First, a lot of publications in the area indicated that the research area is thriving. The research methods applied within the publications in the area using either laboratory experiments or demonstrate an example application. Most of the publications focus on the analysis phase requirement specification and detection as central linguistic analysis tasks. Furthermore, an overview of the applied NLP tools and concepts within the NLP4RE domain was presented. The paper concludes that there is a gap between the state-of-the-art theory and practice. The developed view in papers and the lack of application of the concepts in the industry [39]. Our work focuses more on the privacy-related requirements and other application areas of NLP and also gives an overview of fixed privacy issues within the NLP domain.

3.3. Surveys on Applying Privacy Preservation on Machine Learning and Deep Learning

This thesis unites multiple research domains. Therefore, we considered a huge variety of papers from different disciplines applying similar methodologies. Because of that, we also took papers surveying on topics related to our research topic. For example, machine learning and statistical methods are frequently applied in the domain of NLP (e.g., in context of ambiguity of words) [40]. So, we also saw a relation between surveying privacy preservation techniques in the area of machine learning and deep learning and our work which are fundamental for the recent successes in the NLP research field.

3.3.1. Privacy Preservation and Machine Learning

This part of the thesis delineates related surveys on privacy-preserving machine learning in which way this research is similar to ours but also how our research contributes differently to the field. There are two surveys on the combination of privacy preservation techniques and differential privacy.

One paper by Z. Ji, Lipton, and Elkan surveys the impact of differential privacy on the training process of machine learning algorithms [41]. The application of differential privacy supports the idea of not disclosing private user data to the algorithm and still providing valuable information by sharing or publishing differential private data sets. Moreover, the paper analyzed what could be learned from a differential private data set and also which limits in terms of the loss function differential private algorithms contain [41]. This paper focuses on the possibilities of applying differential privacy in combination with data release and training potentials. In contrast, we are eager to acquire an overview of which privacy preservation challenges and solutions exist specifically in the NLP domain.

Gong, Xie, K. Pan, et al. survey different differential private approaches in combination with machine learning [42]. The paper identified two different categories. First, the combination of the non-private machine learning model with the calibrated noise and the second category perturbs the objective function with random noise. Within the paper, the challenges regarding the model privacy level, usability, and its applications are pointed out and evaluated [42]. Again, the privacy preservation techniques and their impact on the relying machine learning model are inspected, our interest targets the application scenarios of the different techniques.

3.3.2. Privacy Preservation and Deep Learning

Here, we discuss how the research landscape of deep learning in combination with privacy preservation is shaped in the form of surveys and also how our work differs from it. After inspecting a survey about collaborative deep learning, we will elaborate on applying deep learning techniques to preserve privacy.

Several surveys deliver an overview of a privacy preservation technique comparable to our work. For example, the paper by D. Zhang, X. Chen, D. Wang, and Shi elaborates potential problems that might come up in a collaborative privacy-preserving deep learning environment that enables the participants of a model to contribute their data without actually sharing it [43]. Thus, the data is not leaving the data owner. However, either the model is updated by every participant, or the user is provided with an API that takes the user's input and generates an output sent to the central server. Although this process sounds secure, it still covers some challenges that are also addressed by potential privacy preservation techniques. Three major problem scenarios were presented in the paper. The problem assumption is based on the idea that the participating unit is malicious, namely either the server or the user or both. To mitigate the aforementioned problems, the paper presents three common techniques for privacy preservation, namely secure multiparty computation (SMC), Homomorphic Encryption, and Differential Privacy. The paper elaborated that the privacy preservation techniques address two phases, namely training, and usage. In the

training phase, it is essential that the user's data is not visible to any of the participating parties. A homomorphic encryption technique is applied to execute the training. Still, some communication between the participating parties is needed, which is solved by SMC. Thus, curious but honest participants are not able to spy on the sent data. To avoid statistical attacks when a malicious server and user are collaborating, the idea of differential privacy on the user level is applied to defend against it. Then there is also indirect collaboration in the training phase, which changes the challenge for privacy preservation. The data needs to remain at the user's storage. Here, it is essential for the parameters that are sent around the participating parties that there can not be any statistical attacks on them. There is one solution that averages over multiple outputs from users. Another solution applies additionally differential privacy that is incorporated in algorithms of the training stage, and there is also an approach that distributes the processes across the participating parties. Changes were made on the server and client-side to form a pipeline. In the usage phase, the paper by D. Zhang, X. Chen, D. Wang, and Shi highlights the CryptoNet system that works with homomorphic encryption [43]. The user encrypts its data and sends it to the server. The server performs its algorithms and calculations on encrypted data and sends the results back to the user that decrypts the received result. This requires a few adaptations in the training stage of the neural network. The other solution avoids changes to the neural network training stage and applies additive homomorphic encryption. This solution represents an oblivious network that works with secrete sharing and garbled circuits in the usage phase. The final solution approach for the usage phase incorporates Private Aggregation of Teacher Ensembles (PATE) and introduces random noise into the strategy [43]. We figured that the applied privacy-preserving technologies are similar to the ones we discovered in the mapping study for fixing NLP issues within the tasks. Still, we will concentrate on the domain of NLP which also incorporates deep learning techniques. In our work, we attempt to give an overview of privacy preservation covered by NLP.

Another survey investigates deep learning techniques and compares their benefits and drawbacks [44]. In Figure 3.1 the graphical representation of the deducted classifications is represented. The methods are divided into two categories: classical privacy preservation and hybrid privacy-preserving deep learning, meaning that privacy preservation does not solemnly rely on one classical privacy preservation technique but at least two. As classical privacy preservation techniques, the paper lists homomorphic encryption (HE), differential privacy, Secrete sharing, oblivious transfer (OT), and secure multiparty computation (MPC). All of those methods do not apply any deep learning. The Hybrid Privacy-Preserving Deep Learning (PPDL) takes advantage of a mixture of classical privacy-preserving techniques and deep learning. According to Tanuwidjaja, Choi, and K. Kim, every category is represented by one or multiple papers to implemented a privacy preservation technique that will be evaluated by the metrics listed in Figure 3.2. The largest sub-category listed here are papers based on HE, namely HE + Convolutional Neural Network (CNN), HE + Deep Neural Network (DNN), HE + Discretized Neural Network (DiNN), HE + Neural Network (NN), and HE + Binary Neural Network (BNN). Then there are a few more categories like three-party Computation (3PC) + Garbled Circuit (GC) + Neural Network (NN), Oblivious Transfer (OT) + Secrete Sharing

+ Secure MPC + DNN and OT + Secure MPC + CNN. This followed by a paper mentioned by Tanuwidjaja, Choi, and K. Kim applying Differential Privacy and Generative Adversarial Network (GAN). The aforementioned metrics listed in Figure 3.2 measure the accuracy of the underlying algorithm after the privacy preservation technique was installed. The run time refers to the time the privacy preserved method needs to execute its particular task. Data Transfer inspects the amount of data sent from the client to the server. Privacy of Client (PoC) stands for the fact that no other party is able to see the data except the data owner. Privacy of model (PoM) means that neither the client nor any participant is aware of the model classifier in the server. The papers that are based on HE are evaluated and compared with each other with those metrics. This also happens for the papers based on differential privacy and SMC. The results of those comparisons are irrelevant for our work [44]. This work demonstrated a possibility to categorize and test different privacy-preserving techniques. This thesis will zoom out and give an overview of NLP and not compare different papers with each other based on metrics since we want to shape a landscape of privacy-preserving Natural Language Processing and point out the different challenges and solutions within the domain.

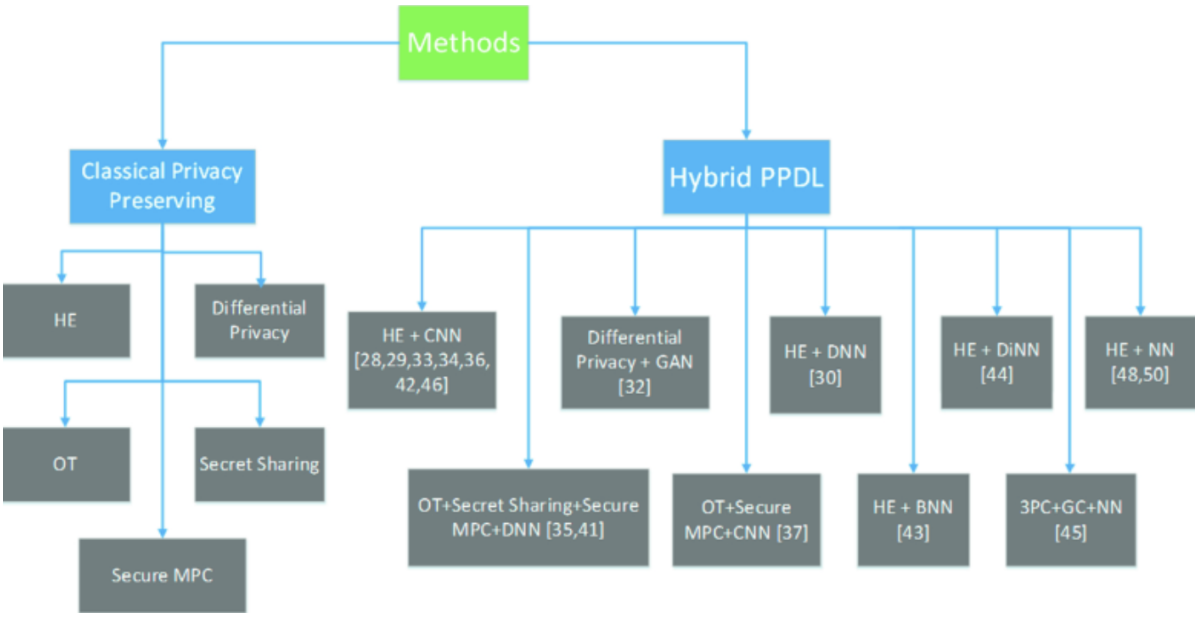


Figure 3.1.: Overview of privacy preservation methods in deep learning taken from [44]

The following paper discusses Privacy-Preserving Deep Learning (PPDL) in the research sector Machine Learning as a Service (MLaaS) and provides an overview [45]. At first, the paper points out the most classical approaches of PPDL and explains it. Then, fundamental conflicts of deep learning and adversarial models in privacy preservation are delineated. Finally, the paper offers a classification of the current PPDL techniques and a timeline of publications in a survey to follow the development better. Additionally, challenges and weaknesses of the state-of-the-art PPDL are displayed in Figure 3.3. The Figure displays two approaches of PPDL, namely the model parameter transmission and the data transmission

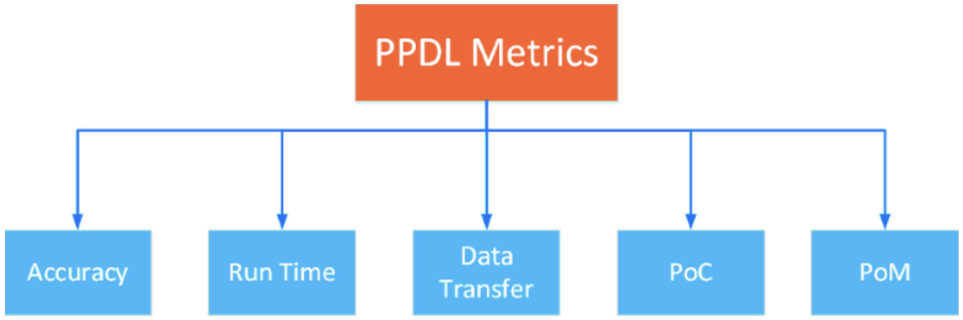


Figure 3.2.: Overview of privacy preservation metrics in deep learning taken from [44]

approach. Further, the approaches are then divided into the applied PPDL methods applied in the respective approach. For the model parameter transmission, it is federated learning and distributed machine learning having the weaknesses communication overhead, backdoor, and GAN attacks. The data transmission approach is solved by using either anonymization or homomorphic encryption or differential private-based PPDL. The main weaknesses for anonymization are homogeneity and background knowledge attacks. Homomorphic encryption-based PPDL is complex and comes with a slow training process. The problem of differential privacy-based PPDL is the central character having a central coordinator. Thus, a problem of a single point of failure [45]. Just as this thesis, privacy preservation techniques are inspected to shape an overview of the current approaches in a particular field of research. The difference to our work is not just the focus on NLP but also the more abstract interpretation of privacy-preserving NLP and the aggregation of challenges and their solutions within our definition of PP NLP. In contrast, this paper has a strong focus on the techniques themselves and their evolution, their challenges, and weaknesses.

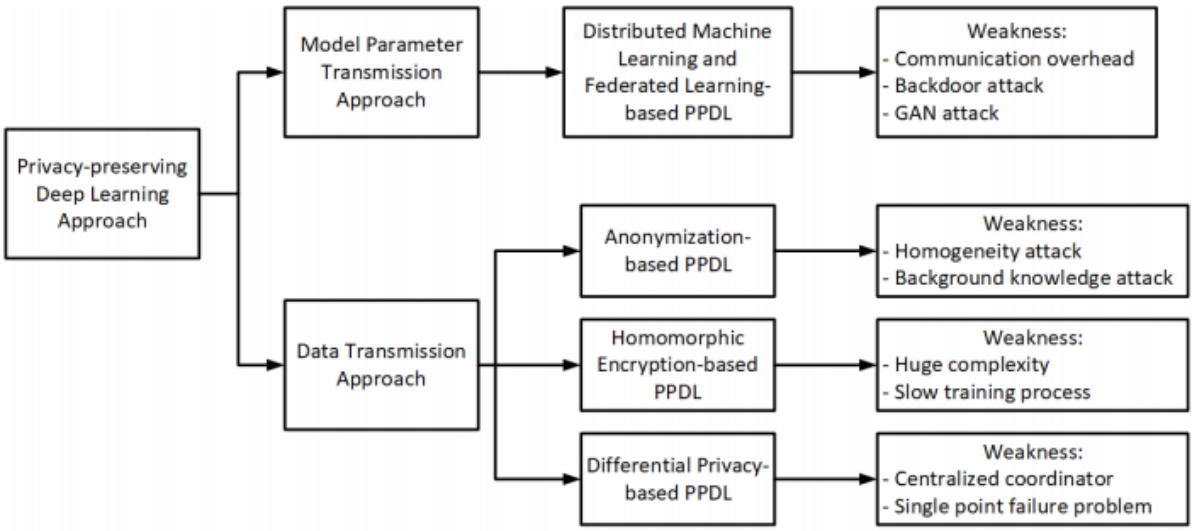


Figure 3.3.: Overview of privacy preservation challenges and weaknesses taken from [45]

Virtual assistants like Siri are commonly used by humans worldwide and in different languages, disclosing private information. One study focused its effort to analyze the literature prevalent in the topic of voice assistants and their impact on privacy and security. Those systems are frequently cloud-based [46].

3.4. Workshops on Privacy in Natural Language Processing

In 2020 the first workshop was hosted, called ”PrivateNLP 2020@WSDM 2020”. In this workshop, several papers were presented addressing privacy-related challenges in NLP. The previous papers will be briefly mentioned in this section [33]. Furthermore, the second workshop of this series was held. The title of it was ”PrivateNLP@EMNLP 2020”. The papers accepted to this workshop are also part of the section [31]. Additionally, there will be a third workshop hosted named ”PrivateNLP 2021” [32].

3.4.1. Papers from the ”PrivateNLP 2020@WSDM 2020” Workshop

In this part of the thesis, we will elaborate on all the papers accepted by the ”PrivateNLP 2020” workshop. Since this workshop series is the first one discussing privacy and NLP, it is a relevant aspect for this thesis.

One topic mentioned within the workshop refers to an approach that introduces gaps instead of privacy-sensitive information within email texts inferred by an algorithm using a vector space trained on the email incoming box of the respective receiver. This method shall mitigate the disclosure of sensitive information caused by unintentionally send emails outside of the corporate environment [47]. Another user-centric approach presents a framework that works in the form of a plugin that warns the user about disclosing potentially sensitive data in his written text on, e.g., social media by analyzing its sentiment, authorship, and other linguistic tools [48]. The following paper introduces the combination of Recurrent Neural Networks (RNN) and homomorphic encryption to enable a user to use Machine Learning as a Service (MLaaS) without sending the plain text data. Still, an encrypted version [49]. At first sight, this approach seems to be susceptible to extended execution times. However, Podschwadt and Takabi prove that this is not the case with the same model working on plain text data. The comparison has been made with the IMDb movie review dataset [49]. The last paper of this workshop surveys privacy preservation techniques based on machine learning [50]. The result of the survey showed that there are two major streams represented in the literature. One is privacy-preserving machine learning, and the other one is mechanisms to control the data of users. The former category contains approaches that are related to artificial intelligence (AI). The main ideas of this research sector are the models and the training data. Both pillars are addressed by the literature, meaning that sensitive data sets are protected through applying the concept of differential privacy, and a distributed approach reinvents the concept of training a model without disclosing the sensitive data sets in the form of federated learning or Private Aggregation of Teacher Ensemble (PATE). Further, the mechanism to control users’ data incorporates the general idea of notifying or giving the user a choice.

In literature, this is primarily done by serving the extracted information from documents explaining the handling of the user's data. However, it is imperative to understand the general idea, is the applied language mostly either complex or ambiguous [50].

3.4.2. Papers from the "PrivateNLP@EMNLP 2020" workshop

The second workshop of the "PrivateNLP" series accepted six papers from different subjects enumerated here. One challenge in distributed or federated learning is that the potential of eavesdropping is high, but introducing a classic encryption scheme into the protocol might cause a significant increase in task performance. A proposed solution to this challenge is to introduce a small encryption step performed by the participants of the respective learning concepts. The encryption step is based on a "one-time secrete key". This encryption is then part of the training of pre-trained BERT. Both aspects are wrapped up in a framework called TextHide [51]. Another challenge within the privacy research field is privacy policies that every user should read before entering a website or downloading an app to identify third parties that collect data from the user. Privacy Policies are known to be long and complex; therefore, a team of researchers tackled this issue with a model that automatically extracts mentioned third parties out of them [52].

Further, the workshop accepted two papers that focus on detecting sensitive data or privacy-related settings with the assistance of semantic analysis [53, 54]. One example is the application of semantic analysis for content generated by users to avoid informational or emotional self-disclosure, which is frequently occurring in social media platforms [53]. Another approach is to utilize semantic analysis to locate settings relevant to the user's privacy setting. This supports the user to decide on its own privacy settings instead of sticking with the default settings of the developer [54].

Differential privacy is another major topic at the workshop and was also discussed by two papers [55, 56]. An advantage of differential privacy, especially in machine learning, is that users' privacy is ready to share sensitive information as training data can be protected. Still, the performance of language models that are trained on differential private data diminishes the model quality. Now, a few researchers discovered that differential private data is suitable for fine-tuning public base models [55]. Furthermore, there is also the possibility to apply differential privacy in privacy-preserving text analysis. Here, the concept of word embeddings is utilized. Specific words of the customer data are mapped into a continuous word embedding space which is then perturbed by applying a differential private algorithm. But Z. Xu, Aggarwal, Feyisetan, and Teissier discovered that some words in a sparse area of the word embedding space remained unchanged although a large scale of perturbation was selected. Therefore, a few researchers did design a new variant based on the Mahalanobis metric to solve the problem as mentioned earlier [56].

All in all, there are a lot of approaches addressing privacy and its preservation techniques. On the one hand, we have several papers summarizing certain types of privacy preservation techniques from different angles and discussing their challenges and solutions and also a few papers addressing specific privacy-related situations solved by or with NLP, but a summarization of privacy challenges and their solutions in the form of categories in the

context of NLP still needs to be done. On the other hand, there are also a few papers that apply NLP to ease the handling of privacy-related text documents like privacy policies, rules, or privacy requirements. Until now, there are a plethora of privacy topics applying NLP that needs to be summarized to receive an overview over the research field of Privacy-Preserving Natural Language Processing.

4. Methodology

We decided to conduct a systematic mapping study instead of a systematic literature review (SLR) in that we seek to acquire a broader scope of the research field of Privacy-Preserving Natural Language Processing [57]. Therefore, the following chapter will be structured according to the guidelines of Petersen to increase the comparability of the conducted systematic mapping study. This chapter will consist of a research question definition section in which we discuss the goals we are aiming for. Then, we will delineate the search process, the strategy behind it, and which results we received. Afterward, we screen through the papers to include or exclude them according to our criteria. Ultimately, we present our analysis and mapping results [11].

4.1. Definition of Research Questions

The classical approach of a SMS is to provide an overview of a research area and also illustrate current results and types of research [11]. We shifted our focus towards the challenges and their solutions in the domain of Privacy-Preserving Natural Language Processing. More specifically, we will illustrate how NLP supports us to protect our privacy and how NLP tasks can be secured from malicious users to exploit sensitive information they were trained on. These thoughts resulted in the research questions listed in table 1.1 which were explained in section 1.2. Usually, research questions answered by a SMS are accompanied by a character of high level and, therefore, they are amended during the process because a lot of findings cannot be foreseen before executing the study itself [12].

4.2. Search Process

This section elaborates the search strategy we applied to collect all papers that address our interests. Three significant decisions need to be made regarding the search process: the impact of completeness, the validation of the search process, and the appropriate mix of search methods. Since we conduct a mapping study on a relatively new topic, completeness is rather challenging to achieve and also not always a significant hallmark of a SMS. We decided to take the papers mentioned in a series of workshops addressing NLP and privacy to validate the completeness of our search process [12]. First, we explain our thoughts on why we chose our search queries and the electronic data sources. Then, we present the initial results of the search queries applied to the respective electronic data source and validate the search process.

4.2.1. Search Queries

We planned the queries that we would insert into the search bar of every electronic data source. All of our selected electronic data sources support the usage of boolean operator like in our case ”AND”, and ”OR”. The usage of ”AND” postulates that the results include all terms written on the right and left side of the operator. For the ”OR” operator this slightly differs because just one side needs to appear in the result list [58, 59, 60, 61, 62, 63, 64, 65]. The result of our thoughts are listed in table 4.1. We were aware of the fact that PP NLP is a very specific research field. Because of that we investigated how many papers address our topic directly in the very beginning of the mapping study. As shown in Figure 4.1, we divided our main term ”Privacy Preserving Natural Language Processing” into two parts and searched for synonyms or related terms that might be of our interest and are a foundation for the generation of our search queries. Q1 represents the equivalent of the research field we analyze consisting of two terms *”Privacy Preserving”* the operator *AND*, and *”Natural Language Processing”*. Q2 also includes potential synonyms for *”Privacy Preserving”*, namely *”Privacy Enhancing”* and *”Privacy Guaranteeing”*. Q3 aims for a very specific subtopic of our research field that investigates the interface between privacy and word embeddings. Q4 and Q5 address a wider scope of the research field. Q4 considers any kind of combinations of *”Privacy”* or *”Private”* and *”Natural Language Processing”* or *”NLP”*. The last search query is a construct of Q2 and the sub-fields of NLP handling either speech or text inspired by the work of Pandey [66].

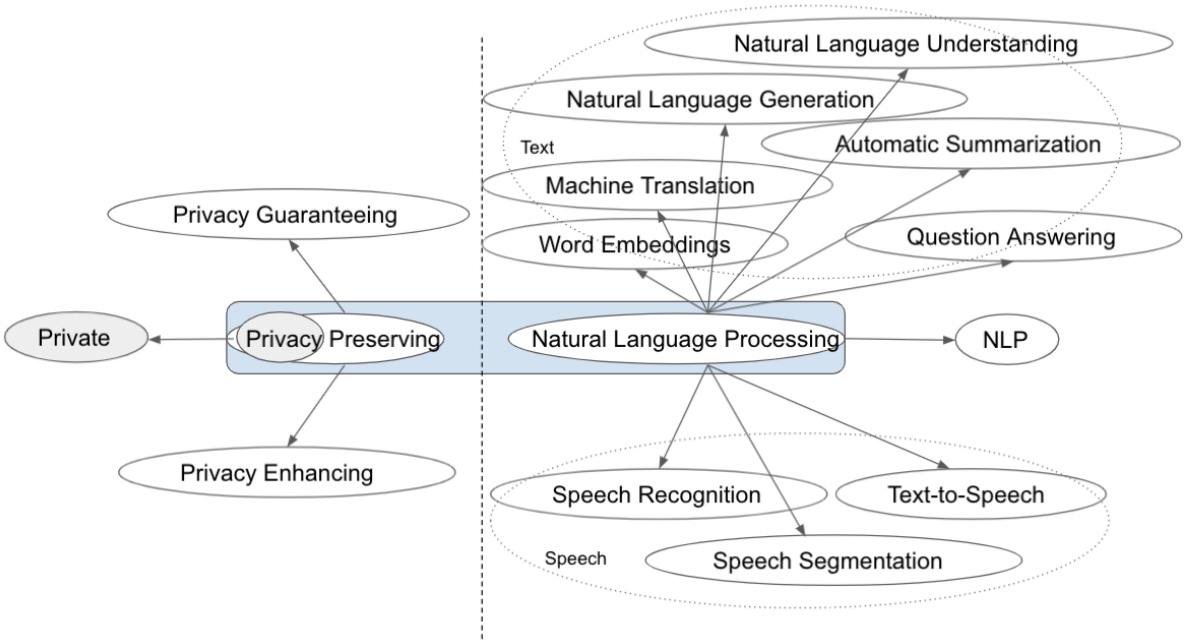


Figure 4.1.: Search Term Segmentation

In the next section, we will elaborate on the selection of electronic data sources, we decided

ID	Query
Q1	”Privacy Preserving” AND ”Natural Language Processing”
Q2	(”Privacy Enhancing” OR ”Privacy Guaranteeing”) AND ”Natural Language Processing”
Q3	(”Privacy” OR ”Private” OR ”Privacy preserving”) AND ”word embeddings”
Q4	(Private OR Privacy) AND (NLP OR ”Natural Language Processing”)
Q5	(”Privacy Enhancing” OR ”Privacy Guaranteeing” OR ”Privacy preserving”) AND (”Speech Recognition” OR ”Speech Segmentation” OR ”Text-to-Speech” OR ”Automatic Summarization” OR ”Machine Translation” OR ”Natural Language Generation” OR ”Natural Language Understanding” OR ”Question Answering”)

Table 4.1.: Table of all search queries applied in the search process

to consider within this thesis.

4.2.2. Selection of Electronic Data Sources

We agreed to select required sources from a selection of electronic data sources that provide a broad coverage, listed in Table 4.2 [67].

Electronic Data Source	Selected
IEEE Xplore	Yes
ACM Digital Library	Yes
EI Compendex & Inspec	No
ISI Web of Science	Yes
CiteSeer	No
Google Scholar	Yes
ScienceDirect	Yes
SpringerLink	Yes
Wiley InterScience	Yes
SCOPUS	Yes
Kluwer Online	No

Table 4.2.: Table of all electronic data sources elected by [67] and their selection status in this mapping study

Out of the eleven electronic data sources, we selected eight. There were several reasons why we did not proceed with some of the sources. EI Compendex & Inspec provides the only access to its database if the sales team is contacted [68]. Since we also have other sources to our disposition, we decided to exclude EI Compendex & Inspec. CiteSeer and Kluwer Online delivered empty result lists for a basic query *(privacy or private) AND (NLP OR ”Natural*

language processing"). Therefore, we implied that further consultation would be obsolete and stop proceeding with it.

In Table 4.3, we listed the selected electronic data sources and the corresponding Uniform Resource Locator (URL). The remaining eight electronic data sources were included in our mapping study, and all search queries from Table 4.1 were executed. We will present the results of each source in the next part according to the order of Table 4.3.

Electronic Data Source	URL
IEEE Xplore	`https://ieeexplore.ieee.org/Xplore/home.jsp`
ACM Digital Library	`https://dl.acm.org/`
Google Scholar	`https://scholar.google.de/`
SpringerLink	`https://link.springer.com/search`
ISI Web of Science	`https://apps.webofknowledge.com/`
Wiley InterScience	`https://onlinelibrary.wiley.com/action/doSearch?AllField=`
ScienceDirect	`https://www.sciencedirect.com/search`
SCOPUS	`https://www.scopus.com/search/form.uri?display=basic#basic`

Table 4.3.: Table of all electronic data sources selected for the mapping study

Exporting Query Results

To acquire a good overview of our findings, we utilized Google Sheets for our mapping study. Since it supports a variety of analytical tools, it is similar to Excel and allows us to cooperate [69]. Based on the selected tool, we needed to export the search query results in the form of a comma-separated value (CSV) or any similar format to insert it into our Google Sheets worksheet. As we experienced it, the only electronic data sources that did not support this format of exporting were ACM Digital Library, ScienceDirect, and Wiley InterScience. Instead, the exporting of search result lists in the form of BibTex files was possible. Because of that, we used JabRef, a free reference manager that allows us to import the exported BibTex files containing the search query results and export them in the form of a CSV file [70]. In the next part, we will discuss the overview of results we achieved after executing the search queries and inserting the acceptable format into our worksheet.

Query Results Overview

Here, we illustrate the results according to the consulted electronic data source. For this purpose, we generated Figure 4.2. In total, we received 6024 instances from all of the consulted electronic data sources. Most of the results were delivered by SCOPUS(1083), followed by Google Scholar(998) and ScienceDirect(956). Also, SpringerLink(881) and ACM Digital Library(822) contributed a significant amount of instances. The least amount of instances were contributed by Wiley InterScience(499), IEEE Xplorer(398), and ISI Web of Science(387). Technical issues occurred during the execution of Q4 for SpringerLink. Therefore, it was not possible to export the resulting list based. We contacted the support

team of the corresponding electronic data source. However, the issue was not resolved in time to include it in our mapping study. Next, we will explain how we filtered the initial results we acquired so far.

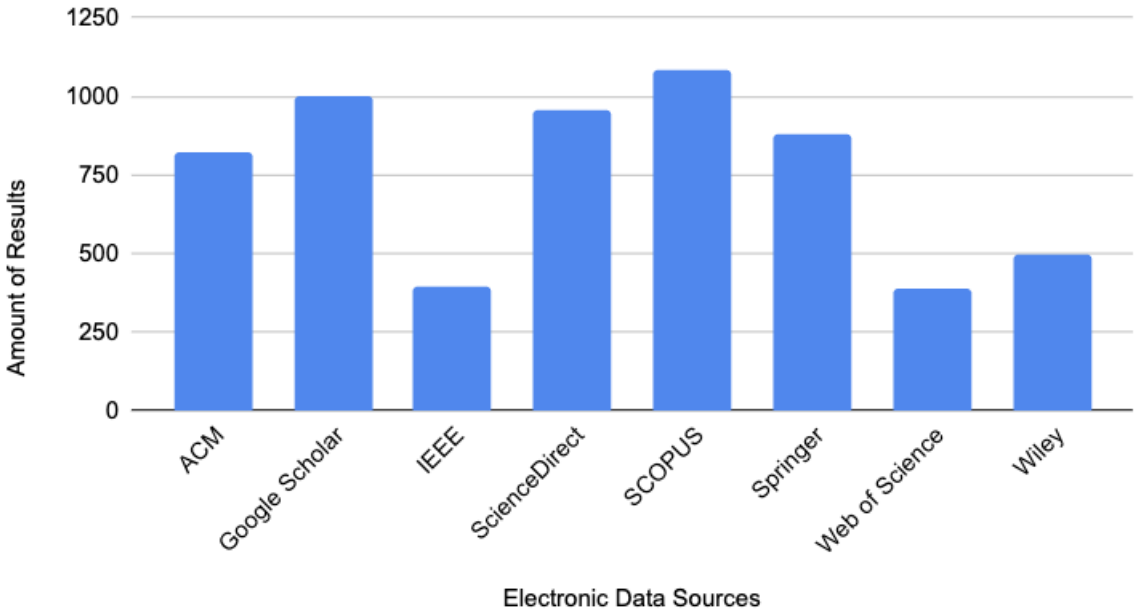


Figure 4.2.: Search Query Results

4.2.3. Result Filtering

As we had a look at the initial results, we realized that a lot of duplicates appear within it. Therefore we decided to apply several functions from Google Sheets, namely query and sort. COUNTUNIQUE allows us the count all those entries in a column that are unique [71]. Since all electronic data sources, we included had their own sheet to avoid any form of format issues or overwrite and keep an overview of which source delivered most of the results. The query function helped us to merge all sheets together without the risk of overwriting entries from other electronic data sources automatically. The function consists of two inputs, the first input specifies which data sheets are meant, and the second one is a query that works precisely like a database SQL request. In our case, the query was "select * where Col1 is not Null, or Col2 is not Null". "Col1" and "Col2" represented the paper title and the authors, respectively. If one of those was empty for one instance, then it wasn't included in the validation process because both columns are essential and indicate the completeness of a source [72]. The sortn function delivers n entries of a list after performing a specific sort task. This function is particularly vital for us because it helps us to eliminate duplicates that exist within the result list output by the query function with the Tie Mode 2 [73]. Since we wanted to have all entries of the resulting list output by the sortn function, we needed

to insert "9ĝ" since we did not know how many entries to expect [74]. After the execution of sortn, we received the following results that are observable in Figure 4.3. At first sight, the number of delivered results dropped significantly. In total, we observed the removal of 1600 duplicates. Most of the duplicates were part of the result list of SCOPUS (529), Google Scholar (390), and ScienceDirect(253), which is observable in the Delta column in Table 4.4 as the result of the difference of the Initial and the Filtered columns. Furthermore, we were interested in which electronic data source has the best ratio (so far) regarding the delivery of duplicates and all results of the respective electronic data source. According to our Table 4.4, Springer(93.98), IEEE(89.95) and ACM(89.29) embody the best ratio. After completing the search process, we face 4424 allegedly different papers in the paper screening phase of the mapping study, which we will further discuss in the next section.

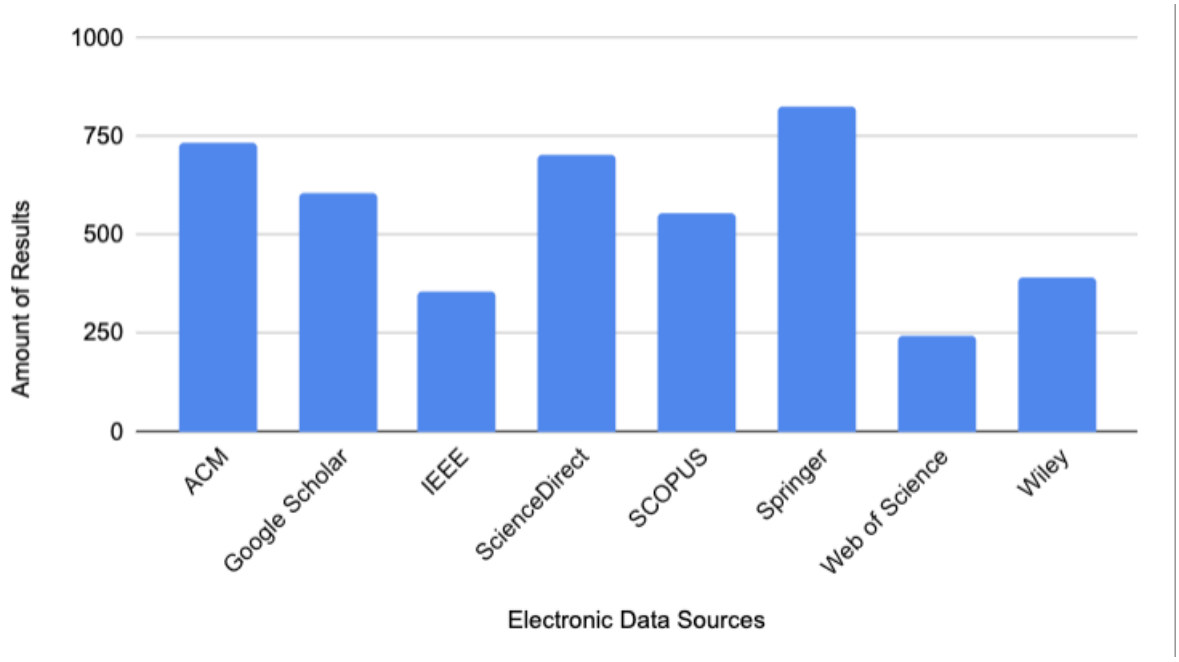


Figure 4.3.: Filtered Search Query Results

4.2.4. Validation of the Search Process

To validate the completeness of the search process, we apply a suggested method that requires us to select papers addressing PP NLP that were known by us based on our preliminary search [12]. We chose to utilize the papers mentioned in the workshop "PrivateNLP 2020@WSDM 2020" [33] because those workshops are the foundation of the research field investigated by us. In Table 4.5 we highlight that all papers covered by the workshop "PrivateNLP 2020@WSDM 2020" also appeared in the results of our search process without actually including specific terms within our search queries except for the term "word embeddings". Since we validated the results of our search process, we can now execute the paper screening process in which

Electronic Data Source	Initial	Filtered	Δ	Ratio (%)
ACM	822	734	88	89.29
Google Scholar	998	608	390	60.92
IEEE	398	358	40	89.95
ScienceDirect	956	703	253	73.54
SCOPUS	1083	554	529	51.15
Springer	881	828	53	93.98
Web of Science	387	247	140	63.82
Wiley	499	392	107	78.56
Total	6024	4424	1600	73.44

Table 4.4.: Table displaying the proportions after the filtering of the results

we decide which paper will be included in the mapping study or excluded from it.

Paper Title	Appearance
Privacy-Aware Personalized Entity Representations for Improved User Understanding [47]	Yes
Classification of Encrypted Word Embeddings using Recurrent Neural Networks [49]	Yes
A User-Centric and Sentiment Aware Privacy-Disclosure Detection Framework based on Multi-input Neural Network [48]	Yes
Is It Possible to Preserve Privacy in the Age of AI? [50]	Yes

Table 4.5.: Table of all papers selected for the search process validation

4.3. Paper Screening for Inclusion or Exclusion

This section will explain our self-defined criteria that determine whether a paper is included or excluded from our study. Furthermore, we will delineate the idea behind them. As a lone researcher with supervision, it is advised to go through the search query results multiple times in different orders and ask the supervisor to randomly select some papers to assess the quality and give some feedback. Since we have a tremendous amount of research papers that we consider to be a part of the research field of our interest, we just examined the paper title in the first round of validation and rarely the abstract if the title of the paper did not indicate its content [12]. After that, the screening is executed according to self-defined criteria that support the supervisor or other curious researchers to reproduce results of the validation phase [11]. In Table 4.6, the aforementioned inclusion and exclusion criteria are listed. We included papers that covered terms related to privacy preservation techniques in combination with NLP for natural language in the form of text or speech in their title or abstract. Then, if neither the title nor abstract delivered clear information about the content of the paper, we

inspected the keyword section if terms related to privacy or NLP appear. In general, we were interested in the synthetic generation of text or speech since this topic also contributes to our research field of interest. Ultimately, we also considered any type of involvement of NLP and the processing of privacy regulating documents like privacy policies or privacy policies and complying with them. We excluded every paper that neither mentioned privacy nor NLP in its title or abstract. Deliberately, we omitted papers handling steganography because we question its privacy sustainability. Additionally, we left out all papers that just processed privacy regulating aided with crowdsourcing. If an instance represented a conference or workshop summary, a content list, chapter overview, a book, or a patent, we also excluded it because we want to analyze papers reviewed by other researchers of the conference or workshop program committee. If there was no possibility to access the paper securely or at all or it was not written in English, we also excluded the paper from the mapping study. In the next part, we will present the results of the screening process.

Inclusion Criteria	Exclusion Criteria
The appearance of terms closely related to privacy preservation and NLP in the title or the abstract	Lack of privacy in the title or abstract
Privacy and Natural Language Processing or related terms appear in the keyword section	Lack of Natural Language Processing or its sub-domains in the title or abstract
Generation of speech or text synthetically	Conference or workshop summary, content list, chapter overview, books or patents
Processing of any privacy regulating document	Restricted access to the content
	Any topics related to steganography
	Insecure access to the paper
	Processing of Privacy Policies with crowdsourcing
	Papers not written in English

Table 4.6.: Table of all criteria applied in the screening process

After the screening of the results of the search process according to our criteria and the removal of additional duplicates, 666 papers (15.1 percent) remained within our mapping study, as you can see in Figure 4.4. The next step is to validate the screened papers.

4.4. Validation

To remove the bias within the mapping study and also assess the quality of the search process results, the advisor of this thesis validated the screened papers randomly because of the vast amount of papers potentially relevant for our work [12]. In this chapter, we will explain how we conducted the validation and which outcome we received.

Since we conducted the mapping study with the support of Google Sheets like [75], it was possible to share a link containing the sheet with the screened paper with the advisor to

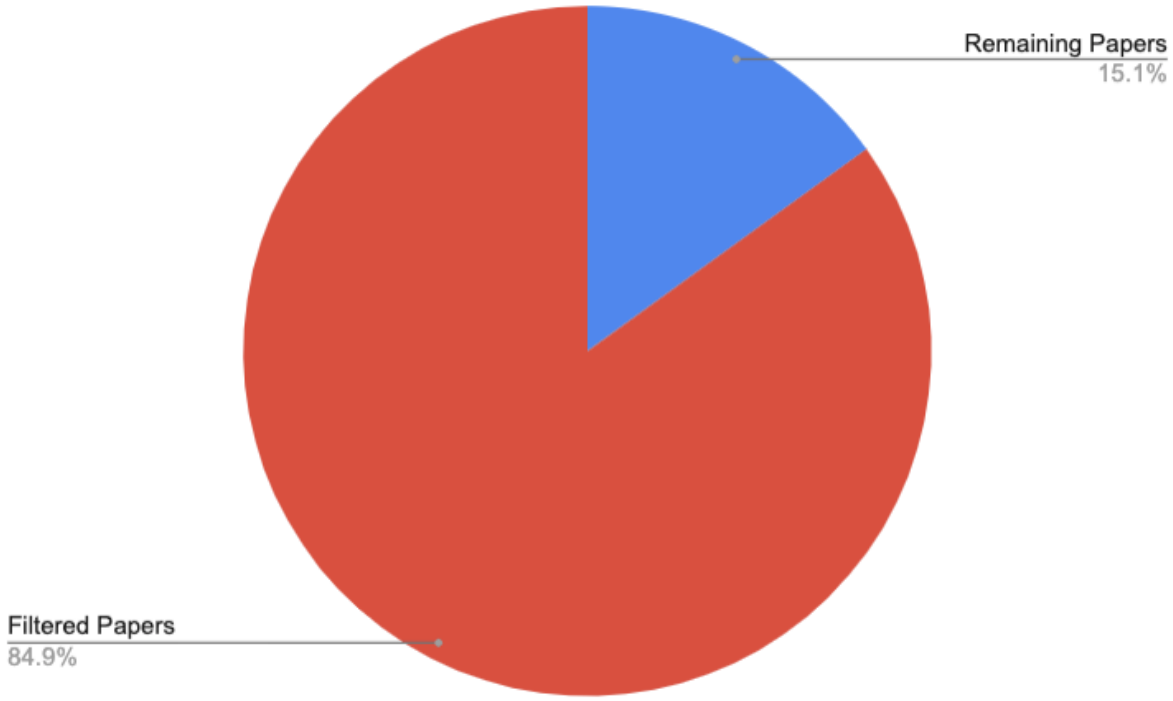


Figure 4.4.: Proportion of remaining papers

validate them. The advisor filtered the list to inspect just the screened paper that we consider valuable for the mapping study. We decided to communicate with three different categories in the validation process. Generally, we used ”1” as an equivalent for the inclusion of the paper in the mapping study or ”0” otherwise. Then, we applied the question mark (”?”) for uncertainty. Additionally, we commented on our decision for the options ”0” and ”?” in brackets after the corresponding sign. Table 4.7 displays an overview of the comments made by the advisor during the validation.

As you can observe in Table 4.7, the advisor had discovered ten uncertainties out of its 179 comments. Two uncertainties were caused by the papers with the title ”A DNS Tunneling Detection Method Based on Deep Learning Models to Prevent Data Exfiltration”[76] and ”A Full-Text Retrieval Algorithm for Encrypted Data in Cloud Storage Applications”[77]. The belonging of Zhang’s paper to our mapping study is indeed debatable. However, data traffic carries private information, and the developed data exfiltration prevention is based on NLP [76]. Song’s Team worked on an information retrieval algorithm on encrypted data avoiding the disclosure of private information in a cloud-based environment applying NLP [77].

The following comment in the table refers to questions the relevance to NLP and text data in Li’s review paper about applications applying federated learning [78]. After another review of the paper, we decided to exclude the paper from the mapping study because the focus did not highlight NLP related applications.

Meenakshi’s team published a paper reviewing security attacks and protection strategies for machine learning which lacked Privacy and NLP focus. Therefore, we agreed to exclude

Comment Types	Amount
? (addresses security issue)	2
? (does it mention NLP? / text data)	1
? (security rather than privacy issues)	1
? (security)	1
?	1
? (not textual data as far as I understand)	1
? (what data type do they work with?)	1
? (do they address privacy issues?)	1
? (what data type?)	1
0 (duplicate)	36
0 (no privacy?)	2
0 (doesn't address privacy issues?)	1
0 (doesn't seem to address privacy issues)	1
0 (spatial data)	1
0 (location data?)	1
0 (location privacy)	1
0 (not text?)	1
0 (not about NLP)	1
0 (doesn't seem to to talk about NLP/text data)	1
1	123
Total	179

Table 4.7.: Table of all comments made by the advisor during the validation

the paper from our work [79]. The same issue appeared for Liu's survey paper focusing on security threats and defensive techniques for machine learning having a data-driven perspective [80]. The fifth entry of the table states a general uncertainty towards the paper developing a flexible text corpus for specific linguistic research that did not address privacy [81]. The following comment of uncertainty questions the data sets worked on in the paper of Rashid's team. The data sets MIDUS and ADULTS contain personal information also in text form that is protected either by de-identification or differential privacy [82]. The comment asking for the data type used within the work of Tsai's team is not part of this thesis since it works with transactional data that does not include text [83]. The work of Ji's team does not address a privacy issue directly. The privacy issue causes a scarcity of data that impedes the development of the medical research area [84]. The last entry refers to the curiosity about the used data type within the paper, which is answered within the abstract that the approach to preserve privacy in linked data anonymization using queries is data-independent [85].

We continue with the comments that did not consider the selected papers to be a part of this work. 36 comments pointed out that the selected papers are duplicates which is true, and they were removed. This could easily happen caused by the number of papers being part of the screening process and was not filtered out beforehand. The next comment group mentioned

the lack of privacy issues relevant for the papers with the title "A multi-task learning-based approach to biomedical entity relation extraction"[86], "Towards Combining Multitask and Multilingual Learning"[87] and "DUT-NLP at MEDIQA 2019:An Adversarial Multi-Task Network to Jointly Model Recognizing Question Entailment and Question Answering" [88]. This paper was wrongly selected because of the applied shared-private model architecture, which refers to the visibility of the parameters within the system and not to our understanding of privacy in the sense of intentionally or unintentionally disclosing sensitive information to a third party [86]. The same issue also occurred for the second paper [87] and the third one [88]. Roberts' team paper is also motivated because there is a lack of data for the cancer research field caused by privacy issues. Therefore is the aim of the paper to propose annotations and a framework that works on the semantic level and, thus, introduce flexibility to the annotation scheme and an approach to preserve the privacy of annotated data sets [89]. Location-oriented privacy is describable in the form of numbers or words in the three comment types. Here the three papers with the title "SpatialPDP: A personalized differentially private mechanism for range counting queries over spatial databases" [90], "Towards privacy-driven design of a dynamic carpooling system" [91] and "Quantifying location privacy" [92]. The following comment assumes that there is not text data involved in the work of Gong's team, which is not provable because there is no access to the entire content of the paper [93]. The last two comment types question the focus of NLP in the papers, "Perceived privacy" [94] and "Distributed Latent Dirichlet allocation for objects-distributed cluster ensemble" [95]. Al-Fedaghi presents in his paper a model that connects privacy and security based on information exchange between two parties with measurable metrics for both domains. However, the application of NLP misses [94]. The second paper works on privacy preservation applying distributed Latent Dirichlet allocation, a topic modeling method, and was published at the International Conference on Natural Language Processing and Knowledge Engineering in 2008 [95].

The last comment type remaining is the approving one. The advisor approved 123 papers. However, 118 papers made it in the end into the mapping study. Here, we will explain all those papers that we did not include in the mapping study. One out of the five papers was excluded because it was based on evaluating the numerical input of employees to investigate their stance on privacy by letting them choose from different levels of privacy in exchange for a payment. Here, the connection to NLP is not present [96]. Hakkani-Tur's team developed a patent for a privacy-preserving database that cooperates with natural language. However, we are interested in papers from conferences and workshops [97]. Another paper with the title "Identifying textual personal information using bidirectional LSTM networks" sounded promising, but just the title and the abstract were written in English. The rest was in Turkish [98]. The last two papers with the titles "Reasoning about unstructured data de-identification" [99] and "Towards Efficient Privacy-Preserving Personal Information in User Daily Life," [100] did fit this thesis. Still, there was no access to the full content.

All in all, Table 4.8 illustrates the consensus between the paper screening phase and the validation. Out of the 128 accepted papers, 118 were included in the mapping study resulting in an inclusion rate of 95.6 percent. Also, just one out of the 46 excluded papers is a part

of the mapping study, and three papers out of the ten uncertain ones take part in the next stage of this thesis. During the validation process of the advisor, the author conducted further analysis tasks on the screened data in which a few alterations occurred that led to a slight diversion. Still, all the mentioned results in the table highlight that the advisor and the author of the thesis have the same understanding of the research field of interest. In the next part of the thesis, we enter the keywording phase.

Comment Category	Amount	Coverage in SMS	Ratio (%)
1 (Inclusion)	123	118	95.9
0 (Exclusion)	46	1	21.7
? (Uncertainty)	10	3	30.0

Table 4.8.: Overview of all comment categories and their coverage within the mapping study

4.5. Keywording of Abstracts

In the process of keywording, the author inspects the abstracts of the validated and evaluates suitable categories and schemes based on the findings. If the abstract of a paper does not deliver sufficient information, the introduction or the conclusion part of the paper can be used for the keywording process [11]. This part will focus on the results which were extracted out of the keywording process. One key outcome of a mapping study is to give an overview of a specific area by classifying the articles. There are two types of classification schemes, the topic dependent one and the independent topic one. We decided to stick with a topic-dependent one with a focus on issues and their solutions [13]. The complete analysis tables are located in section A.1 the appendix of this thesis.

At the very beginning of this process, we realized that we need to distinguish two top categories for privacy-preserving NLP, namely NLP as a privacy enabler and also a privacy threat as privacy enabler NLP introduces privacy into a data set or an activity. As a privacy threat NLP endangers the privacy of data engaging with it. Both top categories need to deliver an appropriate answer to the research questions from Table 1.1. With RQ1, we desire to know which challenges exist for NLP that are privacy-related. With RQ2, we attempt to display the solutions for the corresponding problem within the domain of Privacy-Preserving Natural Language Processing. After answering RQ1 and RQ2, we will have an overview of the research field and can detect gaps within the landscape of Privacy-Preserving Natural Language Processing.

Since we utilized Google Sheets for this thesis, we inserted columns that were mainly provided by the export function of the corresponding electronic data source, namely title, author, abstract, and year. In addition to the basic columns within our worksheet, we inserted the following columns to the corresponding top category to answer the research as mentioned earlier questions displayed in Table 4.9.

NLP as Privacy Enabler	NLP as Privacy Threat
Domain (RQ1)	Domain(RQ1)
Classification of Use Cases (RQ1)	Use Case Classification (RQ1)
Generalized Privacy Issue (RQ1)	Data Type(RQ1)
Generalized Privacy Issue Solution (RQ2)	Generalized Issue/Vulnerability solved for NLP(RQ1)
Generalized Category of Applied NLP Concept(RQ2)	PETs(RQ2)
NLP Method Type(RQ2)	

Table 4.9.: Table of all sub-categories with the addressed research question

For both top categories, we will observe the domain they engage with to better classify the different privacy challenges. We expect that the top category, which utilizes NLP as a privacy enabler and as a privacy threat, to contain a wide variety of use cases that will help to delineate also the potential of the inspected research field. Then, we highlight the prevalent privacy issues that are solved by the application of NLP. Also, for the category in which NLP is a threat, we will point out which data type is more affected by NLP, and we will also provide an orientation for the different privacy challenges within this top category in the form of an overview with aggregated issue schemes. To answer RQ2, we propose an aggregated scheme to display which privacy issue solutions exist in both top categories. To solve the privacy issues caused by NLP, privacy-enhancing techniques (PETs) are applied [101]. For the other top category, we wanted to aggregate the different solutions in which NLP was involved and also which NLP concept and method type were applied. The following two subsections will specify which terms were applied within the categories according to the top category it appears in.

4.5.1. Subcategories Natural Language Processing as Privacy Enabler

In this part, we will delineate all the terms appearing in each subcategory. The worksheet for the corresponding top category is located in subsection A.1.1. We will start with the terms from the domain and continue with the use case classification and the general privacy issues. Afterward, we explain the terms included in generalized privacy issue solution part, the category addressing the applied NLP concepts, and the NLP method type category.

Domain

The domain column in our work sheet supports our idea to classify the different validated papers from our mapping study. This will give us the opportunity to structure the overview better and also provide the option to the recipient of this study to pay attention to a specific area of expertise. A domain is well defined on Merriam Webster describing it as a sphere of knowledge [102]. Table 4.10 displays all the major domains appearing within the validated papers. We observed a high frequency of papers that conducting research either on privacy

policies [103, 104] or other privacy regulating documents [105, 106], or on data from the medical area [107, 108, 109, 110]. Also, mobile applications [111, 112] and social networks [113, 114] were addressed by multiple papers which is reasonable, since those topics are omnipresent for the most of us in our daily routine. Then, we realized that there are several papers either addressing a rather specific topic like privacy preserving mining of search queries [115], big data [116] and finance [117] which we categorized as "Other" or the papers worked on a generic topic which we then classified as "General" [118, 119]. Next, we will specify the use case classification.

Domain
Law
Medicine
Mobile Application
Social Network
General
Other

Table 4.10.: Table of all terms occurring in the category Domain, a subcategory of NLP as a privacy enabler

Classification of Use Cases

Same as the domain category, we attempt to dive deeper into the classification of the papers and extract the different use cases applied within the papers we extracted from our search. Other than the domain part, the use case classification will help us to grasp which scenario is supported with NLP to guarantee privacy. As you can see in Table 4.11, we decided to apply two layers of generalization to keep the extracted information, because of the tremendous amount of papers within this top category. The more specific layer of abstraction is depicted in the column "Use Case Classes" and the more generalized version is the second column "Generalized Category". We tried to position a key word in front of the term in order to map them better to aggregated schemes if it was possible.

The first more generalized category in the table is the category "Annotations and Training Data" aggregating all use cases aiming for the improvement of the annotation process or to collect training data. The improvement is realized in form of the automatization or support [118] or revision [120] of the annotation process. Also annotations or specific data sets like privacy policies were collected to accelerate the research in a certain field [121] or a gold standard was developed [122].

The next category in the second column is "Automation". Here, we extracted two directions, namely the automation of flexible rule enforcement [123] and the automation of privacy regulations [124]. The following two categories were specific enough and did not embody any further specifications, namely "Browsing in a private manner"[125, 126] and "Definition of privacy requirements"[127, 128].

One major generalized category is the simplification of privacy related regulations. We discovered several approaches in this area range from the simple comprehension of privacy regulating documents [129, 130] to the comparison [131], compliance [132], writing [133] and implementation process [134].

Another category is related to investigations mostly aiming for mobile applications or related topics expose or check their privacy impact [135]. Especially, the rightfulness of access privileges and their coverage with the app description is inspected [136].

The next two categories work on the measuring of the compliance of apps to a privacy regulating document with a metric [117] and mining according to rules that guarantee privacy [137].

Another category focuses on the increase of attention towards privacy policies [103] and we observed that some papers also combine this use case with the comprehension of privacy policies [138].

Then, there is a common category aiming for a privacy preserving way to share data with third parties [139, 140, 141, 107]. We also did not specify this category more, because the added value would be negligible.

Further, there is another major category within the table that specifies the protection of sensitive information in unstructured textual data in general [142], in the clinical context [143] or on social media platform [144]. Here, we distinguished between the protection of the patient privacy and the privacy of medical unrelated privacy. The next generalized category is searching in a privacy preserving manner.

An additional section, we introduced voice related services that either protect the voice in public [145] or preserve the privacy of the user voice during a voice based assistance service [146] predominated by the health sector [147, 148].

The last general category in the table is dedicated to the services that require cooperation with the voice.

Since we gathered now enough categories describing the domain in which a specific scenario takes place, we require the privacy issue appearing within a scenario in a certain domain.

Generalized Privacy Issue

With this column we attempt to extract the privacy issue tackled within a paper in a generalized manner. For this purpose, we re-applied parts from the privacy issues specified by Boukharrou for cloud based home assistance and Internet of Things (IoT) devices, a topic closely related to ours. Boukharrou divides privacy issues in context of speech based systems processing user request in form of natural language in five categories. Three of them have proven useful to this thesis, namely identification, profiling and data linkage. Identification alludes to all information that are unique to an individual and might be sufficient to identify a person. Profiling outlines the possibility of collecting information about a person to increase the predictability of its actions and behavior. Data linkage refers to aspect that information about an individual could be combined with other available data and lead to conclusions of other facts. Those three terms are part of scheme listed in Table 4.12 [146].

Moreover, we extracted several more privacy issues within our results. One of these privacy issues handles the topic of disclosure of sensitive data for analysis [82, 149] or other reasons, intentionally [150, 146] or unintentionally [151, 152]. Then, we explored a high density of the issue of complexity of privacy policies [141, 153, 103, 129] and difficulties with the compliance with requirements [154, 155, 156]. We are aware of the fact that the issues with requirements compliance is caused by the complexity of privacy policies, but we observed a high frequency of this topic, therefore, we want to highlight this fact in our work. Then, there is a group of terms that represents privacy issues that are caused by the possession of sensitive data by a third party and a potential secondary use [107, 157]. The term "secondary use of unstructured clinical data" was taken from [158]. Here, not just the handling of those data needs to be regulated [142, 159], but also the misusage of sensitive data needs to be pointed out [160, 161]. Inflexibility of annonymization tools [162] is another term within Table 4.12 which is the outcome of the keywording session that caught our attention. We observed also that annotations and their quality were frequently mentioned by the literature we collected [122, 163, 121]. A more fundamental topic within the papers we found is the fact that sensitive information are contained by unstructured data sets [164, 165, 166].

So far, we invented categories depicting privacy related challenges solved with NLP, now, we attempt to devise a similar approach for the solution of the aforementioned privacy issues. The next category we introduce aims for the generalization of privacy issue solutions.

Generalized Privacy Issue Solution

Same as for the privacy issue, we also require a generalized approach towards solving those issues. We attempt to map privacy issues, and their solution approaches in an overview to ease the extraction of patterns. Since we observed a wide variety of use cases within Privacy-Preserving Natural Language Processing, we deepened our investigation of the privacy solutions and introduced the category which stands for the applied NLP concepts and method type, explained in the subsequent sections. Same as for the use case classification, we discovered a variety of solutions. Thus, we will provide a two-level abstraction approach again to structure the overview better. The mapping of this aggregated view and which specific terms we found are located in subsection A.2.1. Table 4.13 displays the top level of the extracted terms.

We observed that a plethora of papers tried to solve the privacy issues with automation. Not just the enforcement of privacy policies [123, 37, 167] and access control is desirable to be automatized, but also the analysis of privacy policies [168] and the compliance check [154, 169, 132]. Also, the anonymization of written text without any user interaction. Another interesting category was the collection of annotated corpora for different purposes [104, 170].

We detected also another niche within the validated literature and it focuses on the privacy analysis of mobile application code [155, 171, 172]. One of the largest section we found focused on de-identification of text data, mainly in the medical area to protect the patient privacy [107, 108, 109, 110], or the obfuscation of authorship [173, 174] . There is one paper that demonstrates potential threats within a fitness application [175].

Another big block in the privacy issue solution category is dedicated to the design of search

engines[176, 177], metrics [117], frameworks [178, 48] or algorithms to protect the privacy of an acting user for example gender [179] or the data subject within a data set.

The next entry in Table 4.13 is "Detection". Specifically, the search for irregularities within privacy regulating documents[180, 181] and the actual behavior or description. On top of that, there is the aim of detecting sensitive data within unstructured data [182] or activities [183].

A smaller part is the interest of encryption based solutions within our findings [139, 184].

Another upcoming topic within this category is the generation of artifacts[185, 186] or synthetic data [187, 188] based on data sets or a privacy regulating document. Then, we observe the interest of the information extraction topic. The most frequent goal is to extract information out of privacy policies [189, 190].

Another trend is to map the content of privacy policies to different metrics [191, 106] or other privacy policies like General Data Protection Regulation (GDPR) [192, 193]. Additionally, ontology based solutions focusing on privacy in general to shape a more universal approach to cope with the topic [194, 195].

A huge variety is also present in the aggregated scheme of overviews that are present in the literature we extracted from the search. The most frequent topics of the overviews is about applied methods of handling medical data in a privacy preserving manner [196, 197] or research field [198, 199].

The following aggregated term points out the solutions based on semantic level. In order to extend the application domain of developed solutions and tools [200], the semantics of language is utilized caused by its universal attitude [136].

Earlier, we mentioned the de-identification of textual data, however, there is also research conducted in the area of speech de-identification in which the content of a speaker is needed in order to execute a task , however, the voice is negligible [148, 201].

The last category within the Table 4.13 is the suggestion of security and privacy requirements in different ways and for diverse targets [202, 203, 204].

The next section will elaborate the different levels from NLP applied to solve the privacy issues.

Generalized Category of Applied NLP Concept

In order to compare the extracted information precisely with each other, we are obligated to map our findings to an equal level. Thus, we were curious about the applied NLP concepts within our findings. We define an NLP concept same as Liddy in his work described as "Levels of Natural Language Processing" [26], he distinguishes between several levels based on the investigated linguistic domain, also discussed in this thesis in subsection 2.1.3, namely morphological, semantic, phonological (speech processing). We understand that the morphological analysis focuses on the extraction of those morphems that carry the meaning of a word or to remove all those parts of the word that blur its shape. The semantic analysis is dedicated to the meaning of a word more than its shape. Speech processing is a topic for itself, since voice is based on sound, however, it does communicate words in which we are interested [26].

In Table 4.14 we see all the applied concepts, we discovered within the selected literature. Some papers did not apply any of those concepts because they just pointed out some possible improvements for privacy requirements or possible threats like the work of Ye that extracted different privacy and security challenges that occur when dealing with chatbots [205]. Morphological analysis is exemplified in the work of Fujita who developed a framework of rules in which privacy policies are parsed in order to increase the readability [153]. Semantic analysis is conducted in Hasan's work who used neral network and word embeddings in order to capture the semantic relationship between words to detect sensitive information and annonymize it [206]. Di Martino's paper shows a good example of the combination of morphological analysis and semantic analysis by applying Part of Speech (PoS) tagging and Named Entity Recognition (NER), respectively, to build an automated annotation tool to annonymize sensitive information in documents in the Italian law domain [207]. The creation of a corpus with annotations containing privacy policies like Wilsons' work illustrates the combination of the application of a morphological in form of Part of Speech (PoS) tagging, semantic with Named Entity Recognition (NER) and syntactic analysis by the identification of sentence boundaries [208]. We also distinguish between speech processing as a lone category if just the voice is de-identified in order to keep the patient's voice private as it is transmitted via internet or a phone call, but there is still the possibility to detect symptoms of depression [148]. A paper that just contributes to speech processing and the morphological analysis is the work of Boukharrou's paper that injects random noisy speech requests, also utilizing Part of Speech (PoS) tagging in a smart home environment in order to avoid the profiling or possible linkage [146]. Semantic analysis and speech processing are well represented in the work of Ye who developed a system that covers and identifies sensitive information with Named Entity Recognition (NER) so that people in public cannot read the text on the smart phone screen through peeking, however, when the smart phone owner require the covered text the system provides is able to read the actual information applying a text-to-speech approach [151]. The combination of three different concepts within our validated paper was observable in the work of Qian who conducts research on privacy preserving speech data publishing, because it is not just sufficient to de-identify the voice, it is also important to protect the content of the voice data [140].

Furthermore, we classified also the different approaches in which NLP was applied, further discussed in the next section.

NLP Method Type

In Liddy's work also the different approaches used to analyze text, were delineated. He divided it in three different parts symbolic (rule-based), statistical and the connectionist approach which corresponds with the today's understanding of neural networks [26]. We introduced this category in order to structure the overview better and track the applied technologies within the privacy solution domain in context with NLP. In Table 4.15 eight different combinations of NLP method types. The first one is "None" because there is none applied. "NN" stands for neural network and refers to the papers that apply deep learning like Hassan's paper detecting sensitive data in unstructured text by the application of word

embeddings [206]. Tesfy and his team investigated and presented the existing challenges in detecting sensitive information in unstructured data sets without applying any NLP concepts or methods [7]. Clearly, rule based approaches like Olsson's paper designing a framework for a more efficient way of annotating corpora [118]. A rule based and neural network based approach is shown in Ravichander's work by collecting a question and answering corpus with 1750 questions about privacy policies of mobile applications annotated by 3500 expert answers [209]. The mix of a rule-based and a statistical based approach is exemplified Deleger's work to set up an annotation gold standard and evaluating it with a statistical model to prove its value [163]. In general, we consider all papers applying the Natural Language Tool Kit (NLTK) or similar auxiliaries as part of the "Rule based & Statistical" category, since all of them offer support based on rules or statistical concepts. There is a the The Stanford CoreNLP natural language processing toolkit which embodies all three categories [210], therefore we consider every paper that uses this tool or similar ones to be a part of the respective category like Pan's paper that investigates the information flow of android applications to detect privacy violations [211]. A purely statistical approach is used within Neto's paper which is investigating the mining of personal query logs without taking into account work-unrelated queries [115]. The combination of statistical and neural network based approaches is well illustrated within the work of Lindner and his team that applies both categories in order to analyse the coverage of privacy policies and the privacy policies presented on websites [129]. The next section will describe the other subcategories for the category addressing NLP as a privacy threat.

4.5.2. Subcategories Natural Language Processing as Privacy Threat

Here, we will specify the terms appearing in the other subcategories from the second top category. The work sheet for the corresponding top category is located in subsection A.1.2. Again, we start with the terms within the domain subcategory, then, the data type and the generalized privacy issue solved for NLP subcategory. The last terms delineated in this part are within the PET subcategory.

Domain

This category is similar to the one mentioned in the other top category in section 4.5.1. We orient ourselves according to the definition of the domain by the website of Merriam Webster and see it as a sphere of knowledge [102]. We distinguished between five different domains listed in Table 4.16. We discovered a plethora of papers that referred to the cloud computing domain [212, 77, 213, 214]. Then, we noticed the presence of home automation [215, 216]. This top category also embody "Medicine" as a domain [217, 218]. Same as in section 4.5.1 we introduce the domains "General" and "Other". "General" has a more generic approach to solve a problem for which we could not find a adequate domain like [219, 220] and the domain "Other" contains domains that are very specific [221, 222]. The next subcategory we will delineate is data type.

Data Type

The data type is relevant to us, because we attempt to know, if there is a prevalent focus on text (”Written”) or rather on ”Speech” data present within the research field of Privacy Preserving Natural Language Processing. On top of that, we want to discover the different use cases and how the issues were solved for NLP and cluster these solutions.

Use Case Classification

We choose to extract use case categories as well, to support the understanding of potential scenarios in which NLP preserves privacy and improve the orientation of this mapping study. Table 4.17 displays an aggregated overview from the more detailed use case list located in subsection A.2.2.

A frequent use case appearing in the papers we found is the classification of documents without the data disclosure [223] or it was based on encrypted data [49]. Another block within our categorization in this section was dedicated to the investigation of the impact of NLP concepts like word embeddings [9] or collaborative deep learning [224] on privacy. Additionally, we introduced a term that specifies model training without the necessity to contribute the actual data because the neural network is separated in two parts where on part of the network containing sensitive information in its parameters is located on the client side and the other part is then on the server side [225] or the concept of federated learning is applied [226, 227]. Another topic which we discovered is the privacy utility trade-off that applies a privacy preserving concept on neural text representations [228] or word embeddings [229] in order to protect the privacy of the data subjects, but still enough information is left to render an analysis on the respective data. Moreover, we noticed also the a group of papers about secure communication without the necessity to disclose sensitive information [47] or every feature of your voice [230]. Then, we noticed a niche referring to similarity detection without exposing the data to the analysing party [231, 232]. One of the largest segments in this section is dedicated to speech related services like emotion recognition [233], speech transcription [234] or speech verification [235] avoiding the complete disclosure of all features of the voice to a third party. Ultimately, we devised a category focusing on storing and searching Data without its exposure, mostly rendered on encrypted data [236, 237] and the summarizing without the document disclosure [238]. The next section is dedicated to the generalization of issues or vulnerabilities for NLP.

Generalized Issue/Vulnerability solved for NLP

The generalized view on privacy issues caused by the involvement of NLP support our idea to provide a better orientation for the recipients of this mapping study. As you can see in Table 4.18 this category was inspired by the research about the vulnerabilities of word embeddings, information leakage in language and the unintended memorization of neural networks conducted by Pan [9], Koppel [239] and Carlini [8], respectively.

The paper by X. Pan, M. Zhang, S. Ji, and M. Yang describes the exploitability of the learning parameters applied in word embeddings which allows the attacker to reverse-engineer those

parameters and extract the data used for the training of those word embeddings [9]. An example for this category is the work of Podschwadt and Takabi who applies homomorphic encryption in order to protect the sensitive information of a user attempting to train a Recurrent Neural Network (RNN) by using encrypted word embeddings [49].

According to Koppel, Argamon, and Shimoni, it is feasible to apply simple lexical operations in order to determine the gender of a the author who wrote a certain text [239]. The work of Beigi, Shu, R. Guo, et al. exemplifies a case of this category by pointing out the fact that simple tweets might lead to the disclosure of identity [221].

The paper by Carlini, C. Liu, Erlingsson, et al. describes the possibility to exploit neurons within a neural network. Every neuron is trained on data and carries parameters that can be exploited [8]. One example for this category is presented by Shao, S. Ji, and T. Yang which elaborates on the mitigation of the leakage for neural rankings [231].

Furthermore, we include two additional terms that differ from the three aforementioned ones. The first one is the disclosure of sensitive data to NLP model for training purposes like the work of Feyisetan's team developing an active learning approach to reduce the required amount of annotated training data but still achieve acceptable model performance [240]. The second term we would like to introduce is the general disclosure of sensitive data to an NLP task to process it. An example for this classification is Reich's paper about the privacy-preserving classification of personal text messages meaning that the classification model does not learn anything about the input of the author's message that was classified but also the author of the message doesn't have any access to the classification model except the resulting output [223]. Also, with this category, we try to point out current trends within the research field and visualize their maturity. After the classification of the privacy issues, we attempt to investigate if there is a particularly preferred solution to a specific privacy issue within the NLP domain.

PETs(RQ2)

We realized that Dilmegani published a very thorough overview of applied privacy enhancing technology examples which we will instrumentalize within this thesis for the classification in category PET. He lists Differential Privacy (DP), Federated Learning, Homomorphic Encryption (HE), Obfuscation, Secure Multiparty Computation and Synthetic Data Generation as PETs. Table 4.19 displays all classifications we encountered during the keywording phase [101]. Significantly, we noticed that there are also mixed PET that appear in our selected literature. For instance, we realized that the Pathak's work combines secure multi-party computation (SMC) and differential privacy in order to publish classifiers trained on sensitive data [241]. Furthermore, we detected a high frequency of papers that combine federated learning (FL) and differential privacy (DP) for NLP based on text [226, 242] and speech [243]. The last combination, we extracted from the literature applied homomorphic encryption (HE) and federated learning by analyzing the concept regarding its security and efficiency [244]. In addition to that, we realized that there are some papers that rise the attention towards vulnerabilities without solving the issue [245, 224] or suggesting concepts in order to preserve the privacy of data [246, 247]. After the extraction and the mapping of the

relevant information, we will be able to analyze which solutions were applied for which issue answering RQ2 with it. In the following section, we will discuss the results of the mapping phase.

All in all, we extracted information from the papers we collected in the previous phases as described by Petersen [11]. We detected two different top categories and several subcategories. In some, we needed a two-layer abstraction scheme to structure our resulting schemes better. The two top categories interpret the role of NLP in two different ways, namely as a privacy enabler or as a privacy threat. Therefore, the subcategories needed to be different because we proceed with different purposes by setting up the subcategories. For NLP as a privacy enabler, we wanted to know which use cases are affected by it, in which domain does it appear, which solutions and its NLP method types or analysis levels were applied. For NLP as a privacy threat, we also attempt to investigate which domain or use cases are affected by this and which solutions were applied. Since we have our categories yet, we continue to analyze the mapping results in the next chapter.

Use Case Classes	Generalized Category
Annotation automatization Annotation collection Annotation process support Annotation revision Annotations for research acceleration Annotations with gold standard Collection of privacy policies	Annotations and Training Data
Automated and flexible rule enforcement Automatic modeling of privacy regulations	Automation
Browsing in a private manner	Browsing in a private manner
Definition of privacy requirements	Definition of privacy requirements
Ease the automation process of privacy regulating documents Ease the comparison of privacy policies Ease the compliance process through automation Ease the comprehension of privacy policies Ease the comprehension of privacy related user reviews for developers Ease the implementation of written privacy policies Ease the writing process of privacy policies based on code	Simplification of privacy related regulations
Investigating the access legitimacy of smart phone apps Investigating the impact of GDPR with privacy policy analysis Investigating the permission usage coverage of app descriptions Investigating the potential privacy impact of smart phone apps	Investigations
Measuring the Compliance of apps	Measuring the compliance of apps
Mining according to privacy policies	Mining according to privacy policies
Paying more attention to privacy policies Paying more attention to privacy policies & Ease the comprehension of privacy policies	Increase attention towards privacy policies
Privacy preserving information sharing	Privacy preserving information sharing
Protecting patient privacy in unstructured clinical text Protecting sensitive information in unstructured text Protecting sensitive information on social media platforms	Protecting sensitive information in unstructured data
Searching in a private manner	Searching in a private manner
Voice protection in public Voice-based assistance in a privacy preserving manner Voice-Based healthcare in a private manner Voice-based service in a private manner	Voice related services

Table 4.11.: All terms occurring in the Classification of Use Cases

Generalized Privacy Issue
Data Linkage
Identification
Profiling
Disclosure of sensitive Data
Disclosure of sensitive data for analysis
Unintended data disclosure
Complexity of Privacy Policies
Compliance with Requirements
Handling of sensitive data by applications
Misusage of Sensitive Information by Data Collector or Adversary
Secondary use of unstructured clinical data (Research)
Inflexibility of annonymization tools
Annotations and their Quality
Sensitive Information in unstructured Data

Table 4.12.: All terms occurring in the category of Generalized Privacy Issue, a subcategory of NLP as a privacy enabler

Generalized Privacy Issue Solution Overview
Automation
Code-based Analysis
Collect annotated corpus
De-identification
Demonstration of Threats
Designing
Detection
Encryption based Solutions
Generation
Information Extraction
Mapping
Ontology based Solutions
Overviews
Semantic Solutions
Speech de-identification
Suggestions

Table 4.13.: All terms occurring in the category of Generalized Privacy Issue Solution, a subcategory of NLP as a privacy enabler

Generalized Category of Applied NLP Concept
None
Morphological Analysis
Semantic Analysis
Semantic Analysis & Morphological Analysis
Semantic Analysis & Morphological Analysis & Syntactic Analysis
Speech Processing
Speech Processing & Morphological Analysis
Speech Processing & Semantic Analysis
Speech Processing & Morphological Analysis & Semantic Analysis

Table 4.14.: All terms occurring in the category of Generalized Category of Applied NLP Concept, a subcategory of NLP as a privacy enabler

NLP Method Types
None
NN
Rule based
Rule based & NN
Rule based & Statistical
Rule based & Statistical & NN
Statistical
Statistical & NN

Table 4.15.: All terms occurring in the category of NLP Method Types, a subcategory of NLP as a privacy enabler

Domain
Cloud Computing
Home Automation
Medicine
General
Other

Table 4.16.: All terms occurring in the category of domain, a subcategory of NLP as a privacy threat

Use Case Category
Classification without Data Disclosure
Investigating the Impact of NLP related Concept on Privacy
Model Training without Sharing Data
Privacy-Utility-Trade-off for NLP related Concept
Private Communication
Similarity detection without Data Exposure
Speech related Service without complete Voice Feature Disclosure
Storing and Searching Data without Data Exposure
Summarization without Document Disclosure

Table 4.17.: All classes occurring in the category of use case classification, a subcategory of NLP as a privacy threat

Generalized Issue/Vulnerability solved for NLP
Exploitability of Word Embeddings
Information Disclosure by Statistical Language Models
Memorizability of Neural Networks
Direct Disclosure of Sensitive Data for NLP Model Training
Direct Disclosure of Sensitive Data for NLP Tasks

Table 4.18.: All classes occurring in the category of use case classification, a subcategory of NLP as a privacy threat

Privacy Enhancing Technology (PET)
Differential Privacy (DP)
Federated Learning
Homomorphic Encryption (HE)
Obfuscation
Secure Multiparty Computation
Synthetic Data Generation
Differential Privacy (DP) & Secure Multiparty Computation
Federated Learning & Differential Privacy (DP)
Federated Learning & Homomorphic Encryption (HE)
None

Table 4.19.: All classes occurring in the category of Privacy Enhancing Technology 1 and 2, a subcategory of NLP as a privacy threat

5. Results

Since we have the categories and the schemes, we start to extract the information from the validated papers and map it accordingly [11]. In the following sections, we will present the outcome of the mapping phase and explain the results. We will start with the mapping results showing us the distribution of publications regarding our topic in general and divided them into the two top categories over the years. For each electronic data source, as it is suggested by the paper by Kitchenham, Budgen, and Brereton[12]. Then, we present the mapping results of the two top categories in which we see NLP as a privacy enabler and iterate through the subcategories to answer the research questions RQ1 and RQ2. Afterward, we repeat this procedure for the second top category in which NLP is determined as a privacy threat. All plots are based on the findings listed in the worksheets located in subsection A.1.1 and subsection A.1.2.

5.1. Numbers of Publications per Year

Before answering the research questions, we first want to stress the interest of PP NLP in the research community by pointing out the number of publications per year as it is suggested by Kitchenham [12]. Since we discovered two major top categories in the research field of our interest, we were curious about the publications each year for those two categories. Figure 5.1 stresses the fact that the topic we are interested in continuously gains more attention and also its substreams. We assume that the increase is caused by multiple factors like the introduction of GDPR on the European level in 2016 and the adjustment on the national level two years later, which legally bind the private and public sectors.

Since the search process was completed at the beginning of March, the amount of publications in 2021 is limited. We could not manage to find a publication year for the publications with the title "Towards integrating the FLG framework with the NLP combinatory framework" [248] and "Privacy-Preserving Character Language Modelling" [249].

5.2. Numbers of Publications per Electronic Data Source

According to Kitchenham, it is an interesting piece of information to point out the electronic data source that delivered the most publications [12]. The resulting Figure 5.2 depicts an overview of the electronic data sources and their contribution with publications to this mapping study. Most of the publications were delivered by Google Scholar. However, it searches through the web for academic publications in other electronic data sources [250]. Therefore, we thought that we would distinguish this fact as well in the chart above by

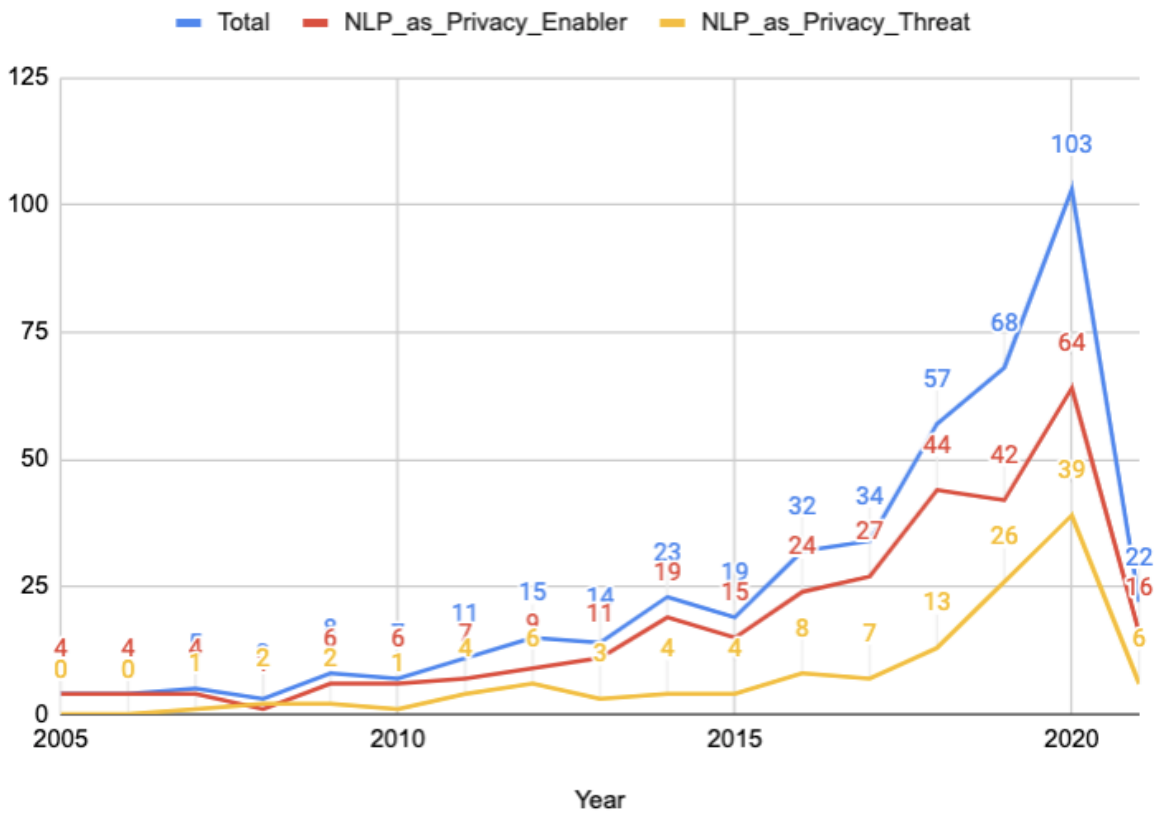


Figure 5.1.: Publications per year

representing the distribution of papers contributed with one category including Google Scholar and the other one excluding Google Scholar and redistributing the papers to their sources or assigning it to the category "Other" if the original data source is not represented within our selection of electronic data sources.

We observed that the 127 publications contributed by Google Scholar contained 53 publications that were part of an electronic data source from our selection, but 74, a majority, were from other sources. As you can see, 14 publications were a part within ACM, which Google Scholar also found, which represents the highest ratio with 240 percent of otherwise assigned papers. 22, 6, 10, and 1 publications from IEEE, ScienceDirect, Springer, and Wiley, respectively, were assigned to Google Scholar. Without those publications, Google Scholar would still be in third place regarding the contribution behind SCOPUS and IEEE.

5.3. What privacy-related challenges exist in the area of Natural Language Processing (NLP)?

In this section, we will attempt to answer the first research question. In the keywording phase, we realized that there is the need to distinguish between two categories to answer this,

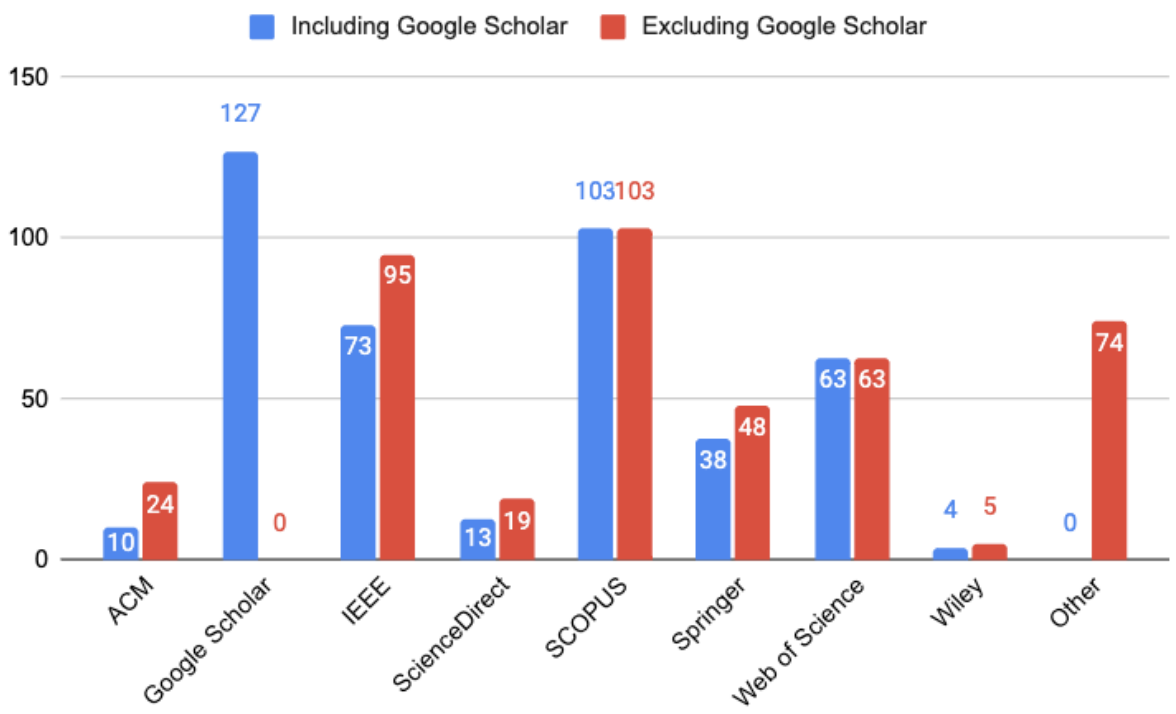


Figure 5.2.: Publications per electronic data source

namely NLP as and privacy enabler and as a privacy threat. Hence, we have different views. First, we will present our results for the privacy enabling part and then for the privacy threat part.

5.3.1. Challenges for NLP as a Privacy Enabler

In this section, we will answer RQ1 for the top category with the mapping results we collected in the following sections. First, we want to acquire an overview of the domains interested in the application of NLP as a privacy enabler. Then, we will inspect the distribution of use case classes discussed within the publications we selected. After having a better understanding of the environment NLP is utilized as a privacy enabler, we will present the fundamental privacy-related challenges this top category faces. Afterward, we map the use case categories and the domains on the privacy issues. At the end of this section, we will have a look at the timeline, including the privacy issues mapped on a timeline, to observe the development of privacy issues solved with NLP.

Domain Mapping Results

The mapping results in Figure 5.3 regarding the domain part for NLP as a privacy enabler displays 58.2 percent of the papers we found either contribute to the topic ”Law” or ”Medicine”.

28.6 percent of the papers in this part addressed either a particular topic or conducted research on a generic or theoretical topic. 8.9 percent of the paper we extracted focused on social networks, and the minor party in the chart is represented by mobile applications. In the next part, we will present the mapping results for the use case categories we collected.

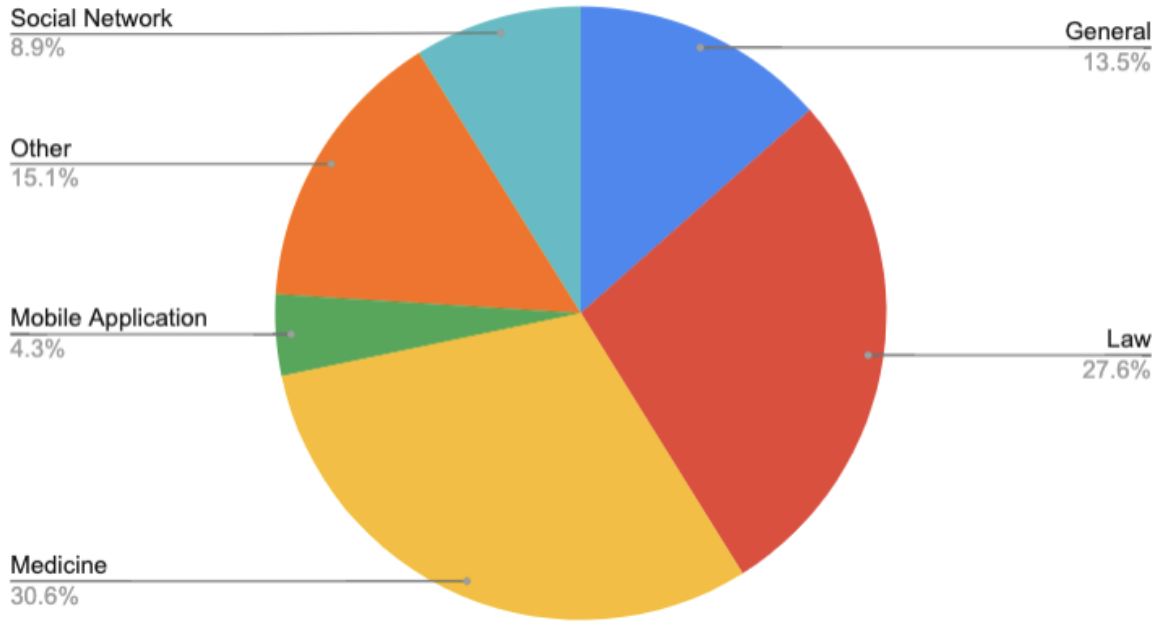


Figure 5.3.: Mapping Results for the Domain category in the top category NLP as a Privacy Enabler

Classification of Use Cases Mapping Results

Figure 5.4 represents the distribution of papers among the classes of use cases we delineated in section 4.5.1. We decided to depict the results with a bar chart to understand better the popularity of use cases among the literature we extracted in the earlier parts of the thesis. The top three consist of the topics ”Protecting sensitive information in unstructured data” with 81 papers, ”Privacy Preserving Information Sharing” with 73 papers, and the ”Simplification of privacy-related regulations” with 50 papers. Followed by 20 from ”Investigations” and 17 papers from ”Annotations and Training Data”. ”Voice related services”, ”Searching in a private manner” and ”Increase Attention towards Privacy Policies” received 15, 14, and 14 papers, respectively. Twelve papers were mapped to the ”Automation” category and 10 to ”Mining according to privacy policies”. Less attention was gained by the topics ”Definition of Privacy Requirements”, ”Browsing in a private manner”, ”Measuring the Compliance of apps” collecting with five, three and two papers, respectively. In the following section, we will present the mapping results from the privacy issue section of the top category NLP as a privacy enabler.

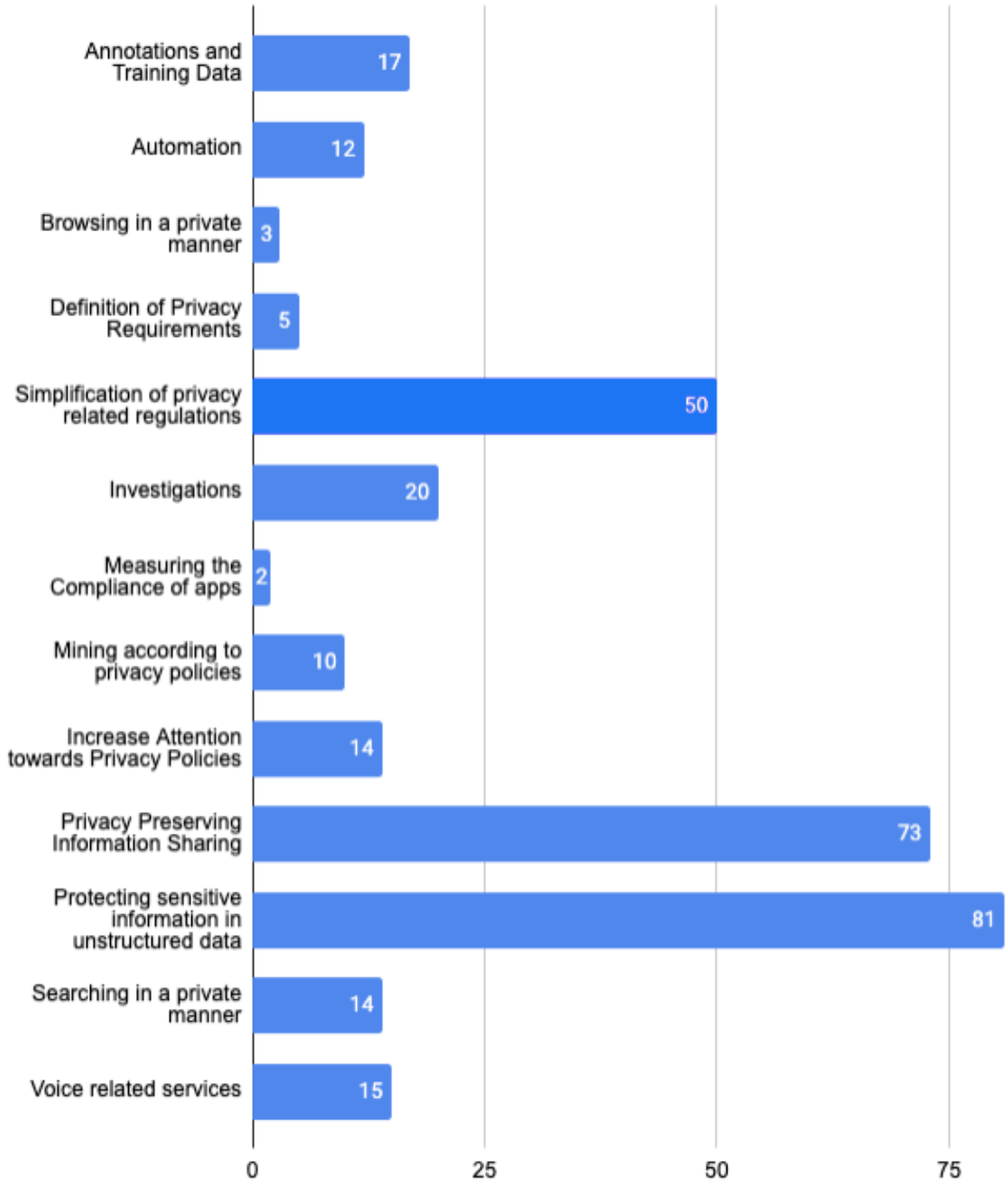


Figure 5.4.: Mapping Results for the Use Case Classification category in the top category NLP as a Privacy Enabler

Generalized Privacy Issue Mapping Results

In this section, we will discuss the mapping results for the privacy issues that are handled with the support of NLP. In Figure 5.5, we can observe a clear dominance of the secondary usage

of unstructured clinical data, primarily for research reasons and the complexity of privacy policies. Considerable popularity was also dedicated towards the topics ”Unintended data disclosure, ”Profiling’,’ and ”Compliance with Requirements”. Essential privacy issues in this section are also ”Identification”, sensitive information in unstructured data, and the handling of sensitive information by applications. Less frequently mentioned within the literature, we identified were the topics ”Disclosure of sensitive data analysis”, ”Data Linkage”, ”Misuse of Sensitive Information by Data Collector or Adversary”, ”Disclosure of sensitive Data” and ”Annotations and their Quality”. Next, we will display the results, which will show us the mapping of use case classes on privacy issues.

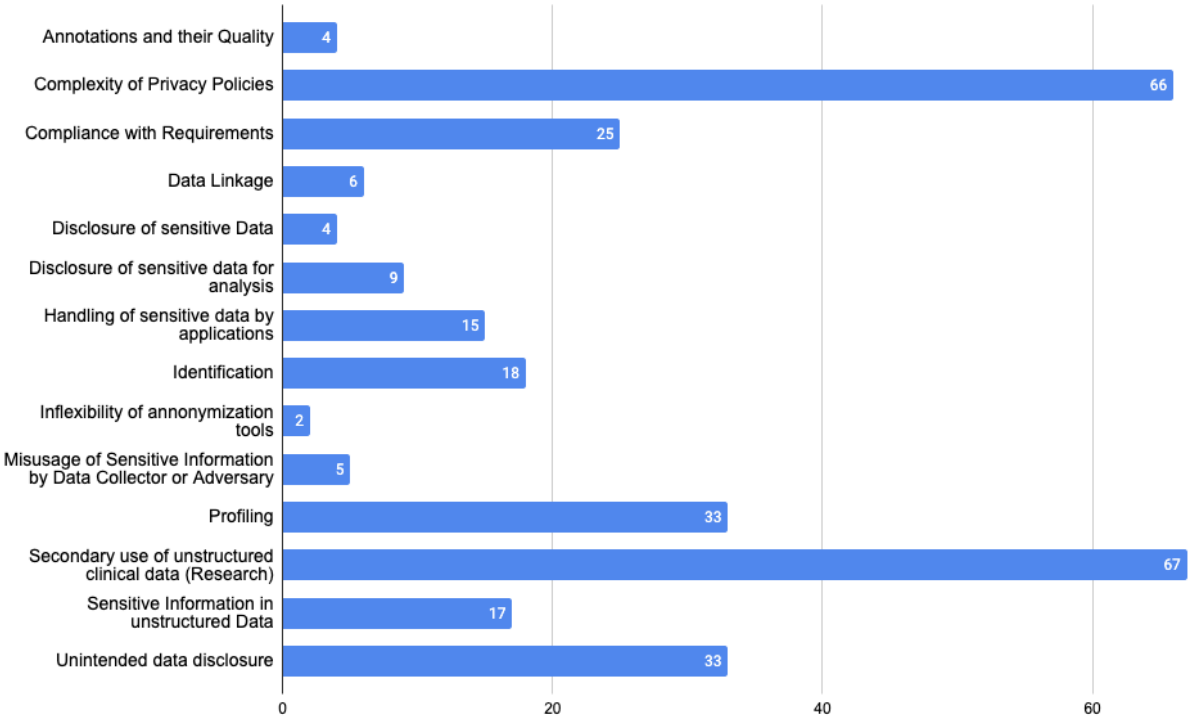


Figure 5.5.: Mapping Results for the Generalized Privacy Issue category in the top category NLP as a Privacy Enabler

Use Cases requiring NLP as a Privacy Enabler

Figure 5.6 delivers an aggregated overview over the constellation between the privacy issues and the corresponding use cases appearing in or which they cause. On the left of the graph are the privacy issues listed. The bar next to it displays the distribution of use cases, with the corresponding color on the right of the graph, addressing the respective privacy issue. If a privacy issue contains a use case category, the order is set by the order given on the right of the graph. This means, if a privacy issue category contains one publication addressing it for each use case category, the graph will depict a bar with 13 boxes, each filled with a ”1”. At

the bottom of the graph, a percentage is given to illustrate the proportion of use cases within publications. The numbers in the bar next to a privacy issue correspond to the number of contributions addressing a specific use case category.

For instance, we investigate which use cases address the privacy issue ”Complexity of Privacy Policies”. Six use cases are part of the category addressing ”Annotations and Training Data”, two ”Automation”, one ”Browsing in a private manner”, 13 ”Increase Attention towards Privacy Policies”, nine ”Investigations”, one ”Privacy-Preserving Information Sharing” and one ”Protecting sensitive information in unstructured data”. 33 contributions or 50 percent of the use cases addressing the complexity of privacy policies are dedicated to the simplification of privacy regulating documents.

This graph provides an overview of all the privacy issues and the use cases they occur in or they cause. Because of the annotation quality, issues regarding the scarcity of data or the training of sensitive data detection models occur in use cases related to the annotation process. Annotated data are essential to train algorithms to detect sensitive information in a data set. Now, we can observe that the complexity of privacy policies is a significant concern, and many contributions were dedicated to this issue. Significantly, the simplification and the attention increase towards privacy purposes received a fair amount of interest. Compliance with requirements affects many use cases, especially in the area of automation and the simplification of privacy regulating documents. Data Linkage affects all the use cases that aim for a privacy-preserving way of sharing data or challenges protecting sensitive information in unstructured data structures.

The disclosure of sensitive data might occur in use cases that attempt to protect sensitive data, share them in a private manner, or during the interaction with a voice-related service.

In mining or protecting sensitive data, the disclosure of sensitive data is an issue because the analysis bears the chance to infer sensitive information about the data subject.

The privacy issue resulting from the handling of sensitive information by applications causes many publications to render investigations to evaluate the privacy impact and raise awareness towards this issue. The issue of ”identification” accompanies use cases addressing the sharing of information, protection of sensitive information, the application of search engines, and the encounter of voice-related services.

The inflexibility of anonymization tools hinders the process in which privacy-preserving information exchange is rendered. To prevent the misuse of sensitive data, use cases were devised that address the issue with a privacy-preserving manner of data exchange, general protection of sensitive information within unstructured data sets or the simplification of privacy regulations are conducted. Profiling might originate in use cases that focus on browsing, mining, or protecting sensitive information in unstructured data sets. Most frequently, Profiling occurs in context with search engines and voice-based services.

One major privacy issue within this graph is the secondary use of unstructured clinical data occurring in use cases that aim for sharing information or protecting it. The existence of sensitive information within not medical data happens to occur in or be caused by the collection of annotations, the definition of privacy requirements, mining of data, privacy-preserving information sharing. The issue of unintended data disclosure originates in use

cases that share sensitive information or protect it. It also is subject to use cases in which search engines or voice-based use cases.

This graph illustrates the diversity of privacy-related issues, and in which category of use cases they either occur or which use cases they case. There is not one category of use case that is affected by just one. However, most of the privacy issues occur in use cases in which either sensitive information is tried to be protected in unstructured data sets or when the use case conducts the sharing of information. The following chart will elaborate on the development of privacy issues during the last years.

Domains involving NLP as a Privacy Enabler

After extracting the information about the privacy issues that were dealt with NLP and the corresponding use cases, we investigated in which domain the privacy issues are present. The result of our work is Figure 5.7. On the left side of the graph are the privacy issues. Next to each privacy issue is a bar that represents a 100 percent of use cases dedicated to it. each colour in the bar represents one category of use cases. The number in the box stands for the absolute number of the respective use cases of a given use case category.

On the first sight, the graph highlights the fact that NLP is frequently used within the medical domain in order to solve privacy issues. Likewise, the presence of the law sector in different privacy issues is revealed by this graph caused by the intense involvement of privacy policies or other privacy regulating documents. We observe that the categories ”Other” and ”General” are scattered around all privacy issues in high proportions. The privacy issues ”Complexity of privacy Policies”, ”Compliance with Requirements” and ”Secondary use of unstructured clinical data” are naturally predominated by the domain ”Law”,”Law” and ”Medicine”, respectively.

All in all, this graph shows us, that the occurrence of privacy issues solvable with NLP can happen in any domain listed here. But this also implies that other domains could utilize NLP more in order to preserve privacy.

Development of Privacy Issues solved with NLP as a Privacy Enabler

Figure 5.8 demonstrates the development of the variety of privacy-related issues that are solved with the support of NLP. On the x-axis of this chart, the years of publications are displayed. One instance in the graph has no assigned publication year because we were not able to find it. The numbers in the bar represent the number of publications contributed to one the privacy related issue with the corresponding color on the right side of the chart. If the box is too small to fit the number of contributions, it is written in the next bigger box with enough space, and it is highlighted by using a white font around the filling. For instance, the column assigned to 2020 has the following numbers, starting from the bottom of the column, ten and five, which belong to the categories ”Complexity of Privacy Policies” and the ”Compliance with Requirements”, respectively. Then, there are two empty fields. However, after these, there are two ”1” in the same colors as the empty fields indicating their reference. In this case, the privacy issues ”Data Linkage” and ”Disclosure of sensitive data for analysis”.

The same concept applies to the following numbers highlighted by the white color around the filling color. The y-axis of this graph represents the 100 percent of publications made in the corresponding year. At the top of every column, the total amount of publications for each year is written.

We observe that the variety and the amount of privacy-related issues solved with NLP increases. Notably, not just the almost every year presence of the privacy issue of "Unintended data disclosure" and the "Complexity of Privacy Policies", also the increased amount of attention contributed to the issue in the form of publications is well illustrated by the chart. A constant present within almost every year is the secondary use of unstructured clinical data, also assigned with growing numbers. In 2016, the variety and amount of publications received a significant intake compared to the year before. This is the same year in which General Data Protection Regulation was introduced by the European Union, and two years later, the country members needed to adapt to the law [16]. In the years afterward, the dedication towards the challenge of compliance also gained more attention. The development of the research field evolves. The publications start to address privacy concerns more specifically because privacy issues like identification, profiling, and data linkage are applied in more publications and delineate the problem of privacy as more than just a violation and address the problem's potential consequences.

5.3.2. Challenges for NLP as a Privacy Threat

In this section we attempt to answer the challenges that are privacy related and caused by NLP. First, we want to inspect the domains in which the privacy issues that are caused by NLP occur and we will point out which data type was mostly involved. Then, we present the issues and their distribution within this thesis. The last point will be a mapping of domains, data types and use cases to the respective privacy issue.

Domain Mapping Results

The mapping results for the sub category Domain are depicted in Figure 5.9. With 55.9 percent a majority of our findings work on generic or theoretical aspects for which we did not find an adequate domain. The "Cloud Computing", "Medicine" and "Home Automation" domain received 15.7, 14.2 and 4.7 percent, respectively. The "Other" domain achieved 9.4 percent of the papers. Now, we proceed with the results for the data type subcategory.

Data Type Mapping Results

Figure 5.10 illustrates the distribution of papers that conducted research on text or speech data. Apparently, there is majority dedicated to work with written data. The next section will discuss the results for the use case classification.

Use Case Classification Mapping Results

The specific mapping results for the use case classification are depicted in a figure located in A.3.1. Here, we will present the aggregated mapping results for the category use case classification contained by Figure 5.11. The dominant use case class is the topic referring to speech related services without disclosing the all the voice features with 42 papers matching it. A comparatively mediocre amount of papers were mapped to topics ”Model Training without Sharing Data”, ”Privacy-Utility-Trade-Off for NLP related Concept” counting 26, 20 and 15 papers, respectively. The topics ”Classification without Data Disclosure” and ”Similarity detection without Data Disclosure” achieved seven papers each. A fewer amount of papers were dedicated to the topics ”Investigating the Impact of NLP related Concept on Privacy”, ”Private Communication” and ”Summarization without Document Disclosure”. Next, we will present the mapping results for the privacy issues subcategory.

Mapping Results for Generalized Issue/Vulnerability solved for NLP

In Figure 5.12 the mapping results for this subcategory are depicted. 31.5 and 29.9 percent of the papers we found were mapped to the terms ”Direct Disclosure of sensitive data for NLP Tasks” and ”Direct Disclosure of sensitive data for NLP model training”, respectively. The last three topics within the chart are ”Exploitability of word embeddings”, ”Memorizability of NN” and ”Information Disclosure by Statistical Language Models” receiving 17.3, 15.0 and 6.3 percent of the papers included in this mapping study. In the following part, we will discuss the mapping results of final subcategory of this top category.

Domain Appearance of NLP as a Privacy Threat Domain

Figure 5.15 embodies the mapping of domains to the privacy issues caused by NLP. On the left side the privacy issues caused by NLP are listed and on the right side of the chart the domains are presented. Each color in the bar on the right of the listed privacy issue represent on domain. The number within the box describes the amount of publications dedicated towards the domain.

It is observable that the ”General” domain is predominant in all privacy issues. This implies that the research field still is in its beginnings. Since the medical domain has already conducted a lot of research towards privacy preservation in combination with NLP caused by [251], it is present in most of the detected privacy issues. A small proportion of specific domains are also present within the privacy issues. The next section will cover our analysis for the data types involved in privacy issues caused by NLP.

Data Types addressed by NLP as a Privacy Threat

This section will show a distribution of data types addressed by the privacy issues caused by NLP depicted in Figure 5.14. This table follows the same structure as Figure 5.15, but the difference is that we inspect the data type if it is written or in spoken form. As you can see, we have a clear focus on written data among the publication we included into this SMS. An

interesting fact is that the direct disclosure of sensitive data for NLP task is the only privacy issue that is predominated by speech data, mainly, because the voice itself is a bio-metric treat that needs to be treated with caution before disclosing it to any third party. In the next section, we will elaborate the use cases affected by NLP as a privacy threat.

Use Cases addressed by NLP as a Privacy Threat

Figure 5.13 shows the mapping of use cases on the privacy issues caused by NLP. It follows the same structure as Figure 5.15, however on the left side is a legend listing the use case categories and the corresponding color.

The direct disclosure of sensitive data to an NLP task are mainly addressed by use cases that want to train a model based on sensitive data or speech related services without the disclosure of the complete voice. A minority of use cases aim for the privacy-utility-trade-off of training data. The next privacy issue in the chart refers to the issue of direct disclosure of sensitive data for NLP tasks. The majority of use cases aim to protect the voice traits or want to store and conduct a search on data in a privacy preserving way. The exploitability of word embeddings occurs in the use case category of the privacy-utility-trade-off for NLP concepts. The ”Information Disclosure by Statistical Language Models” also occurs in the use case category of the privacy-utility-trade-off for NLP concepts among use cases of the type ”Speech related Service without complete Voice Feature Disclosure ” and the summarization without the disclosure of documents. The ”Memorizability of NN” causes mostly the use case of model training without sharing data and speech related services without fully disclosing all voice traits.

Again, this graph shows us the different use case categories which are caused because of the privacy issues we discovered or occur in the use case category. In the following part, we will discuss the solutions applied in order to preserve the privacy with NLP or for NLP.

5.4. What approaches are used to preserve privacy in and with NLP tasks and how can they be classified?

In this section, we will elaborate the solutions which were provided with the support of NLP or the applied PET in order to preserve the privacy within the NLP task. For the section dedicated to NLP as a privacy enabler, we will start with the mapping of privacy issue to the corresponding solutions. Then, we will specify the solutions based on the NLP concepts and method which were applied. For the part dedicated to solutions for NLP as a privacy threat, we also start with the mapping of privacy issues on the solutions provided by the literature we extracted.

5.4.1. Privacy Solutions Provided by NLP

In order to provide an answer for the question which privacy solutions are supported by NLP and how can they be classified, we start with the scheme we elaborated in the previous

chapter, then, we continue with the results for the applied NLP concept and the method type.

Generalized Privacy Issue Solution Mapping Results

Figure 5.16 shows an aggregated overview of the table located in subsection A.2.1. The most frequent class in this category was ”De-identification” with 73 publications. On the second place is the category ”Detection” with 38 publications. A comparable amount of papers were dedicated to the topics ”Designing”(27), ”Information Extraction”(26), ”Automation”(23) and ”Generation”(22). On a similar level of received publications are the topics ”Semantic Solutions”(19), ”Collected annotated corpus”(17), ”Speech de-identification” (16) and ”Overviews” (14). Lower attention was addressed towards the topics ”Mapping”(8), ”Suggestions”(7), ”Code-based Analysis” (7), ”Ontology based Solutions”(4), ”Encryption based Solutions”(2) and ”Demonstration of Threats”(1). The following part will discuss the mapping results for the applied NLP concepts.

Generalized Category of Applied NLP Concept Mapping Results

Here, we will illustrate the mapping results for the applied NLP concepts with two different levels of abstraction. First, we will discuss the results for various combinations we explained in section 4.5.1, in Figure 5.17, then, we will aggregate those results and map it to the major categories without any combinations. The result of it is displayed in Figure 5.18. Figure 5.17 depicts the fact that the papers we found have a strong focus on the semantic level and also on the morphological level or the combination of both of those. Speech Processing seems to be less popular. We attempted to find more appearances of combinations we delineated, but this was not the case. Figure 5.18 just stresses the fact that most of the research is done on the semantic level because of its more universal approach towards the natural language which also improves the dynamics of potential solution approaches. Another significant part is played by the morphological level supports to understand the task of words within a sentence or even am entire text corpus. The next section will elaborate the distribution of applied NLP method types within the extracted literature.

NLP Method Type Mapping Results

The last mapping results of the top category NLP as a privacy enabler is the method type that was applied in the papers in this top category. Again, we instrumentalized a two level abstraction process in Figure 5.19 the more specific one and Figure 5.20 displays the aggregated overview. We chose a pie chart, since we have a more suitable distribution of results. The top three are the pure methods ”Statistical”, ”NN” (Neural Networks) and the ”Rule based” approaches with 36.4, 21.4 and 12.9 percent, respectively. The most frequent combination we found was the combination of all three method types with 9.2 percent. Now, we will report about the mapping results for the sub categories of the other top category.

Mapping of Privacy Issues on Solutions provided by NLP

In this part, we will focus on the privacy preservation solutions contributed by NLP. On the left side of the Figure 5.21 the privacy solutions are listed. The bar next to each category represents the privacy issue classes with the corresponding color on the right side of the graph. The number within the box represents the number of contributions addressing the privacy issue category.

”Automation” was mostly used in order to solve issues regarding the complexity of privacy policies or the compliance with requirements. Also, ”Code-based Analysis” was used in order to resolve the same privacy related issues and, additionally, issue of handling sensitive information by applications. The collection of annotated corpora was applied in order to resolve the issues of the complexity of privacy policies and annotation quality. ”De-identification was applied mostly in order to make clinical unstructured data available fore research purposes. The solution categories "Designing and "Detection" provided a immense variety of solution towards multiple privacy issue categories. ”Encryption-based” solutions were used to either mitigate the disclosure of sensitive data or profiling. ”Generation” was mostly applied in order to solve the issues of the complexity of privacy policies or the compliance with requirements or to avoid the complete disclosure of data for analyzing purposes. The category of ”Information Extraction” was applied mostly for challenging the complexity of privacy policies same as the ”Mapping” solution category. 50 percent of the issues solved by an ontology-based approach aimed for profiling. The ”Overview” and the ”Suggestions” category offered a variety of solutions towards different privacy issues. Most of the solutions offered by ”Semantic Solutions” addressed issues related to privacy regulating documents or the compliance to them. ”Speech De-identification” was applied in order to mitigate ”Identification” or ”Profiling.

Mapping of NLP Concepts on Solutions provided by NLP

Next, the Figure 5.22 will delineate the level on which the analysis of the NLP tasks were applied. The chart follows the same rules as the charts discussed before, but in this case we inspect the different NLP domains listed in the legend on the right side of the chart. We are able to observe that most of the solution approaches apply the semantic analysis or a combination of it with the morphological analysis. A triple combination appears seldom.

Mapping of NLP Method Types on Solutions provided by NLP

In Figure 5.23 we are able to observe the distribution of applied method types for the provision of a solution towards a privacy issue. This chart follows the same logic as the previously mentioned ones in this chapter. We can say that almost every solution approach with NLP contains a variety of method types that are used in order to achieve there goal. Every solution approach applies neural networks or a mixed version of it. Highly prominent is also the application of statistical approaches or mixed version of it. Rather less frequent are approaches that are mixed versions of rule based approaches. It is noticeable that almost every solution approach applies the method type neural networks.

5.4.2. Solutions Provided for NLP Privacy Issues

This section will elaborate on the mappings to the provided solutions in form of PETs. We will map it on the threats they solve and in which use cases categories they were applied. Also, we were curious about the development of contributions applying PETs over the last few years.

In Figure 5.26 we observe the mapping of privacy issues caused by NLP on PETs. Also, this chart follows the same representation logic as the previous charts. Here, however, the left side of the chart are PETs listed and the bars next to it are filled with different colors representing the privacy issue caused by NLP. The numbers delineate the amount of publications addressing the corresponding privacy issue category.

PETs(RQ2) Mapping Results

In last subcategory in this section, we will inspect the mapping results from Figure 5.24 which contain the specific mapping results and Figure 5.25 represents the aggregated overview of the mapping results. Figure 5.24 displays the dominance of ”Homomorphic Encryption” and ”Obfuscation” having a mapping result of 36 and 30 papers, respectively. A significant amount of papers were mapped to the topics ”Differential Privacy (DP)”, ”Federated Learning”, ”None” and ”Secure Multiparty Computation”. There were just a few papers that were mapped to the topics that were combined PETs. Less popular was the topic ”Synthetic Data Generation” with just four papers.

Figure 5.25 displays a different result to us, since we counted the combinations of PETs to their respective topic. However, the results do not extremely differ from the specific view, it shows us the share of the different PETs. Homomorphic Encryption still holds the biggest share with 27.6 percent within the chart followed by Obfuscation with 22.4 percent and Differential Privacy with 14.9 percent. 9.7 of the publications did not include any PETs. 8.2 percent were dedicated towards the topic of Secure Multiparty Computation and the smallest amount of publications addressed the topic of synthetic data generation.

All in all, we started in this chapter with the definition of the research questions that we attempt to answer with the results of this mapping study. Then, we defined the parameters of the search process requiring search queries and an adequate selection of electronic data sources. After executing the search queries in the respective electronic data sources, we filtered the outcome of the search process, screened through the papers and included all those which fulfilled our criteria and validated them with the support of the advisor of this thesis. Ultimately, we executed the keywording of abstracts process in order to extract all categories that we attempt to map on all the papers. In the end, we started the mapping process and described the results of it at the end of this chapter. In the end, we executed the methodology according to Petersen’s paper [11]. The next chapter will contain the results of our interpretation of the mapping results and further analytical procedures.

Mapping of NLP Privacy Issues on PETs

"Differential Privacy" was applied in order to solve the exploitability of word embeddings or the disclosure of sensitive data for the training of a model or for a NLP task. Some use cases involving the issue of "NN memorizability" was also solved. In order to solve the issue of sharing sensitive data for model training, the combination of differential privacy with secure multiparty computation or federated learning and synthetic data generation were applied in order to solve issues that were related to the exposure of sensitive data towards model training. The direct disclosure of sensitive data for NLP tasks was mainly solved with the application of homomorphic encryption, obfuscation and secure multiparty computation. The issue of information disclosure by statistical language models was mostly solved with differential privacy, homomorphic encryption and obfuscation. The exploitablity of word embeddings is tackled by diverse PETs, namely differential privacy, federated learning, a combination of federated learning and homomorphic encryption [244], homomorphic encryption and obfuscation. The issue of memorizability of neural networks is also not just solved with one PET but by multiple. The most publications were contributed in the solution category of "Obfuscation", followed by the solution categories federated learning, secure multiparty computation, homomorphic encryption, differential privacy and a combination of federated learning and differential privacy [252]. The next chart will disclose the mapping of use case categories to PET.

Mapping of Use Case Categories on PETs

Figure 5.27 provides on overview over the PETs and the use case category they occur in. This illustration has a list of PETs and a few combinations on the left side and on the right are the different use case categories with a given color.

In the case of classification without data disclosure the PETs differential privacy, homomorphic encryption and secure multiparty computation were applied. The use cases that conducted an investigation to see the impact of NLP on privacy did not apply any PETs. The use cases focusing on the model training without sharing data were mostly encountered by the application of federated learning or a combination including it. Also, the application of differential privacy, homomophic encryption or secure multiparty computation were an option. The use cases referring to the Privacy-Utility-Trade-off were most frequently addressed by differential privacy, also homomorphic encryption and obfuscation were part of the solution domain. In order to make a private communication happen the application of obfuscation was introduced. Use cases addressing similarity detection without the disclosure of data were solved with different PETs. The most frequent publications addressing it were made with the usage of obfuscation. Other less frequent approaches were made with differential privacy and homomorphic encryption. Speech related services were mostly handled with the application of homomorphic encryption of obfuscation. Storing and searching data was mostly solved with homomorphic encryption. The next chart will focus on the development of publications over time.

Mapping of PETs on Years

Figure 5.28 shows use the amount of publications made during the last 14 years. On the left side of the graph is the list of PETs with their color within the bars that are on the right of the year number. Each bar represents a 100 percent of the number of publications made in the respective year. On the left of the chart is the toal amount of publications made in the respective year.

The popularity of PETs gained a lot of interest in the last three years. Especially, differential privacy which started to appear in 2018 and since then it contributes over 10 percent of the publications per year. A similar trend is also observable for federated learning and its combinations after having a two year absence between 2015 and 2018. But since 2018 at least one publication involving federated learning per year even in 2020 twelve publications were made. Still, the biggest coverage is provided by homomorphic encryption and by obfuscation. Secure multiparty computation has it first appearance in 2007 and had since then a few publications per year. Synthetic data generation has a few publications in 2019 and 2020.

5.5. What are the current research gaps and possible future research directions in the area of privacy-preserving NLP?

5.5.1. Research Gaps for NLP as a privacy Enabler

The complexity of privacy policies is one of the major pillar we detected as privacy issue within the domain NLP as a privacy enabler. The focus of future research should be to develop pipelines that support the idea of formulating privacy policies or privacy regulating documents in cooperation with technical and law experts to create a standard easy automatable.

Not just for the privacy related issues solved with NLP, but also for all privacy related research fields the setup of a standard schema is imperative. The standard should require every contribution addressing a standardized privacy issues to elaborate at least a few consequences that might come up if a certain privacy mechanism is not applied or is not sufficient enough. Avoiding the simple but still legit justification of a privacy violation. This would support the common understanding of the importance regarding privacy and the understanding of the consequences which a privacy violation might cause.

In the medical domain, we realized a high diversity of terms that needs to be standardized by the medical research community in order to avoid repetitive research, especially for the unstructured documents, because we observed a lot of synonyms.

Our results show that the solution approaches are frequently relying on statistical method types which require a lot amount of data and an alternative is presented by Feyisetan, Drake, Balle, and Diethe the application of active learning in order to reduce the required amount of data for model training purposes [240]. Of course, this is not the solution to the problem but an incentive in which direction the research might head. Another opportunity is the synthetic generation of data in order to tackle the problem of the requirement of a lot of data.

5.5.2. Research Gaps for NLP as a privacy Threat

Since this top category, we discovered, is upcoming, we noticed a lot of general approaches within this category, a potential gap is to use the solutions for the issues and apply the general approaches to specific scenarios. The combination of federated learning and differential privacy could enable business models in which costumers could contribute their data in a privacy preserving manner in exchange for some benefits to build a training data set. The application of the privacy preserving concepts in a business model would introduce the research field faster into society and increase its popularity.

We detected one paper applying quantum computing [253] that made us curious if the concept is also applicable for other NLP related tasks to preserve the privacy in them. For example, if this concept can also be applicable to text based tasks.

Based on our findings in section 5.3.2, speech data is still a topic that needs further research, especially, because of its tremendous privacy value it is imperative to protect it.

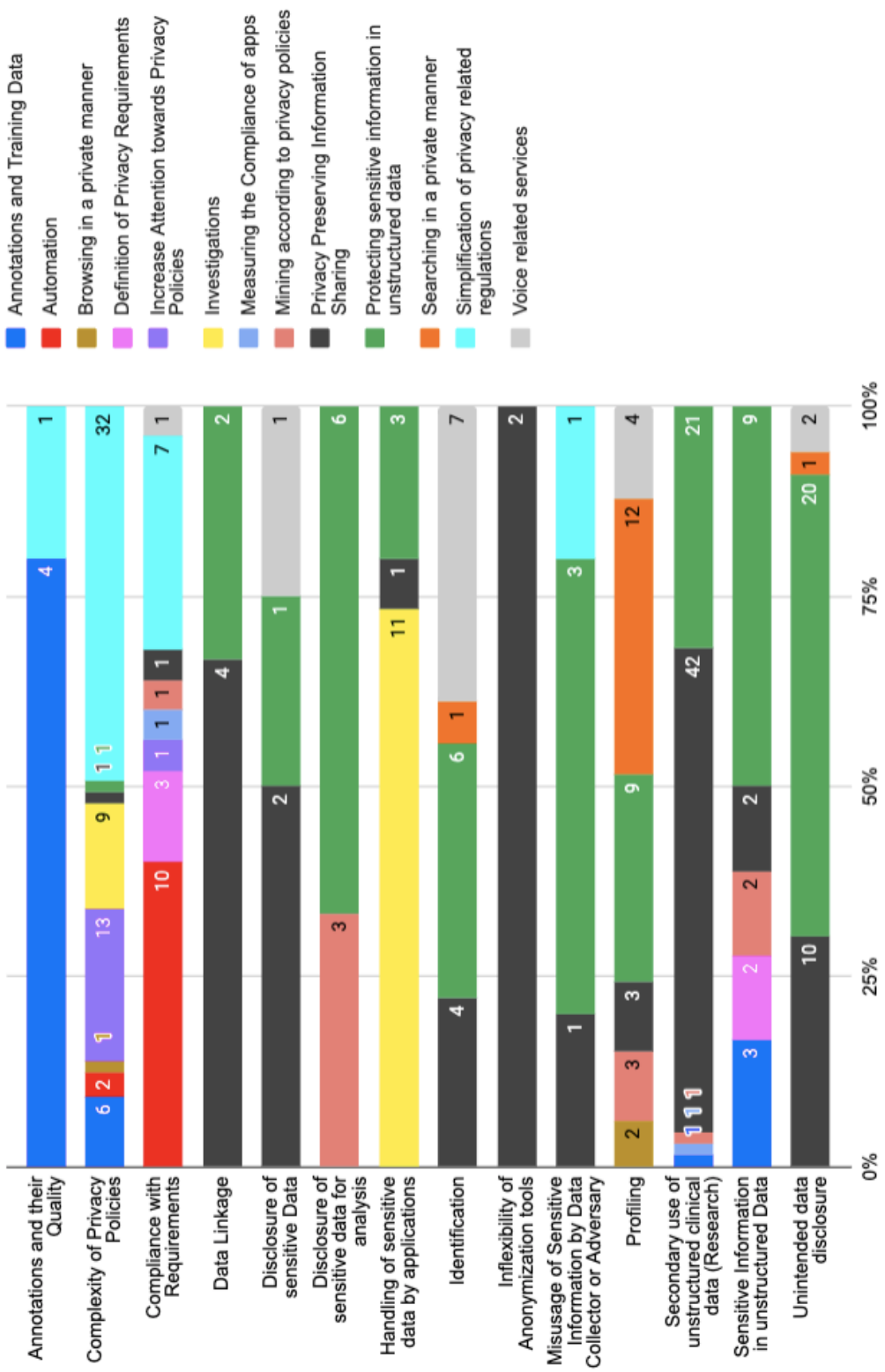


Figure 5.6.: Privacy Issues and Use Cases

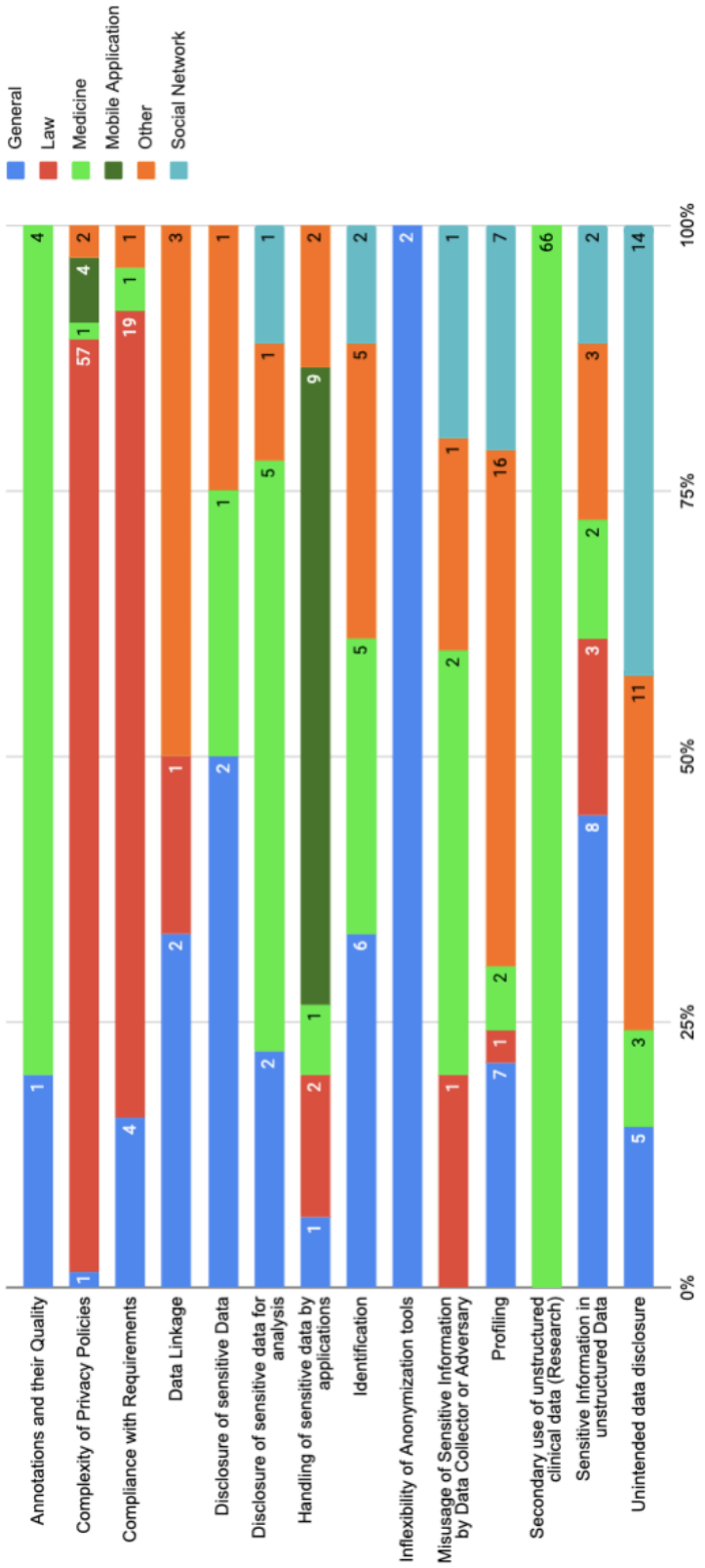


Figure 5.7.: Privacy Issues and Domains

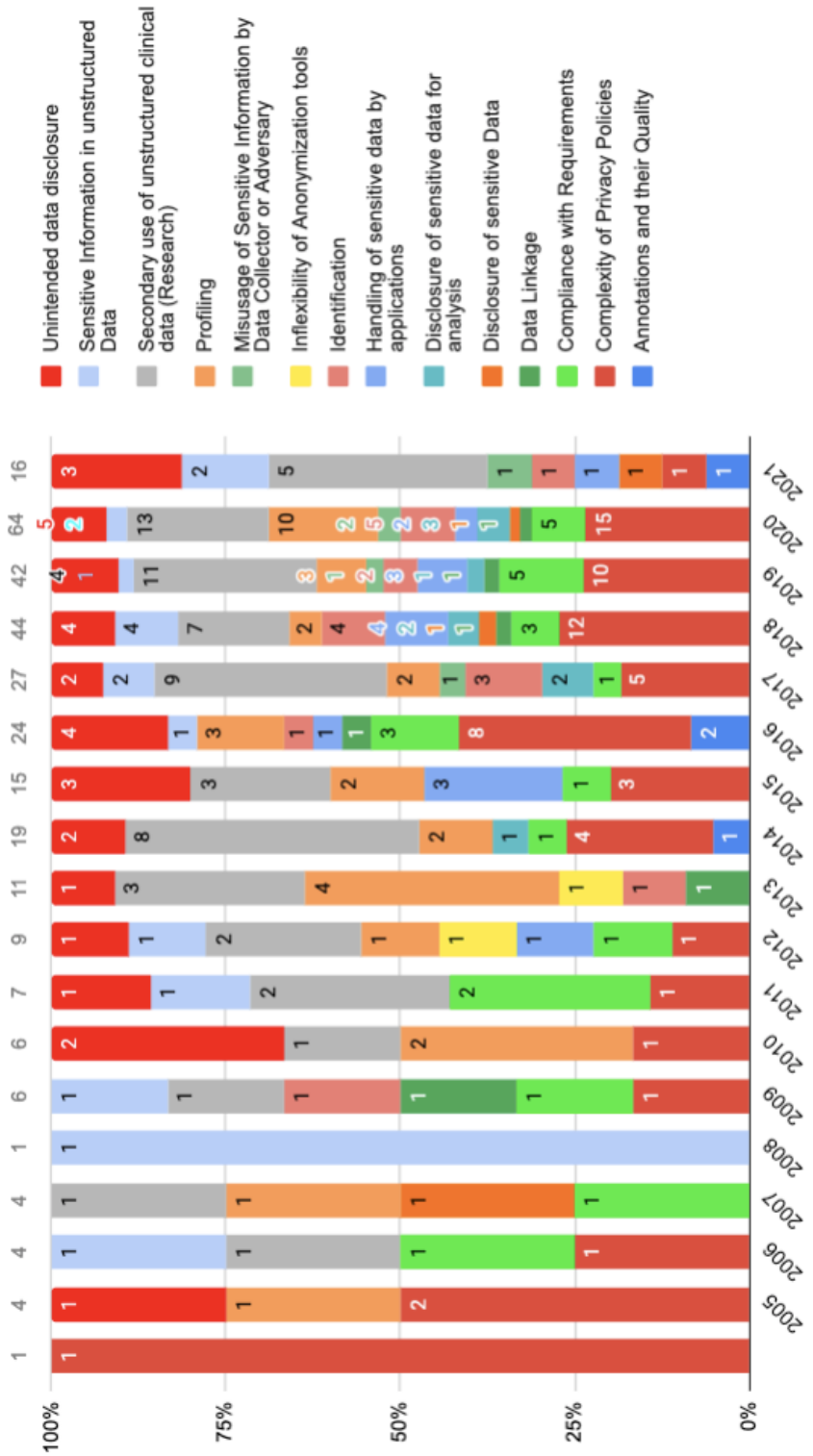


Figure 5.8.: Development of Privacy Issues

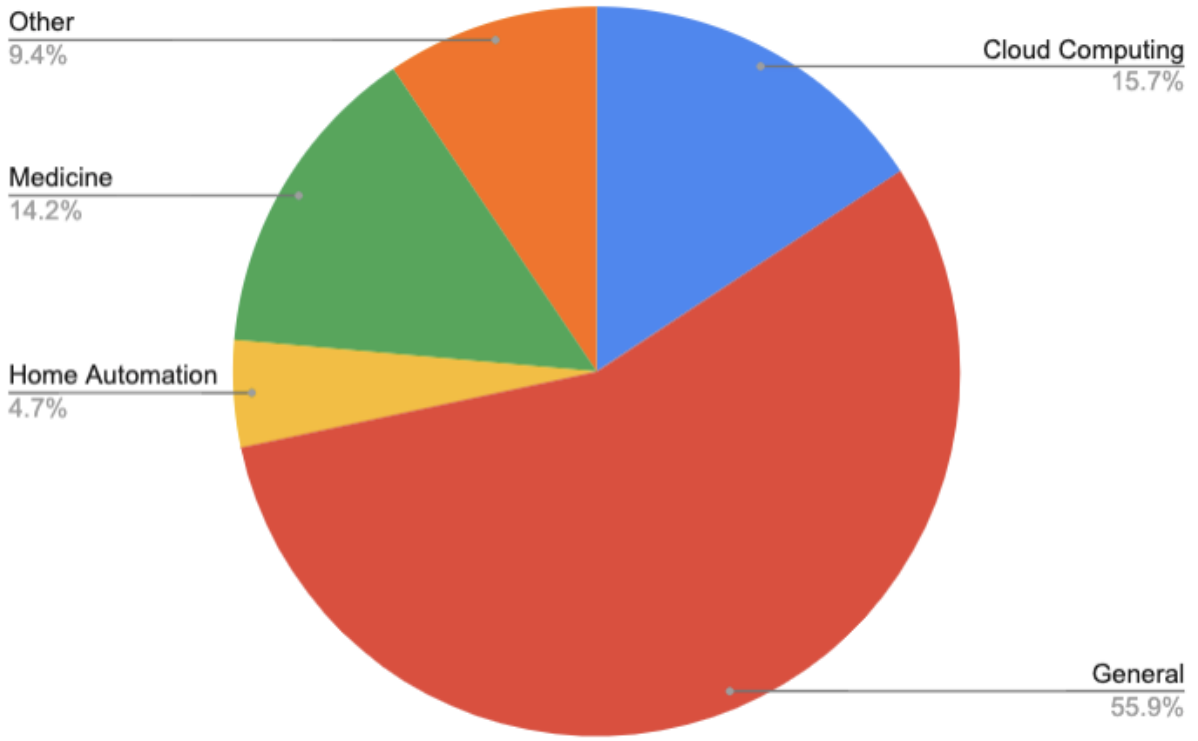


Figure 5.9.: Mapping Results for the Domain category in the top category NLP as a Privacy Threat

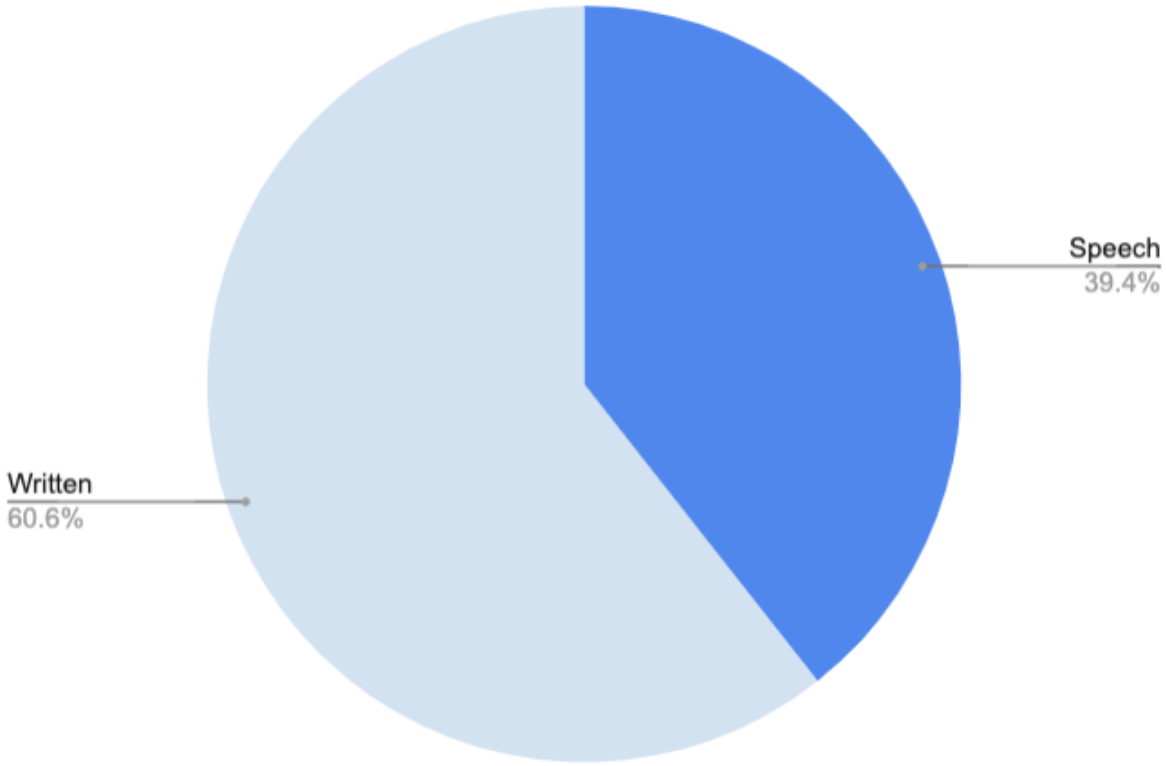


Figure 5.10.: Mapping Results for the Data Type category in the top category NLP as a Privacy Threat

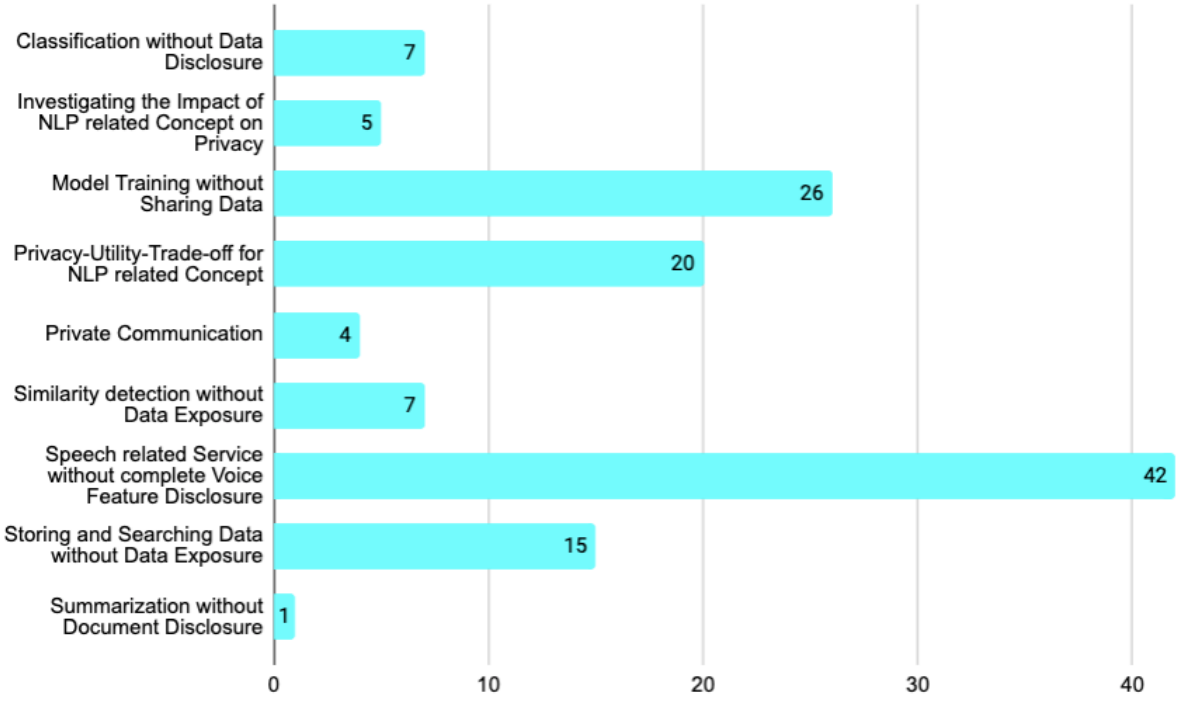


Figure 5.11.: Aggregated Mapping Results for the Use Case Classification category in the top category NLP as a Privacy Threat

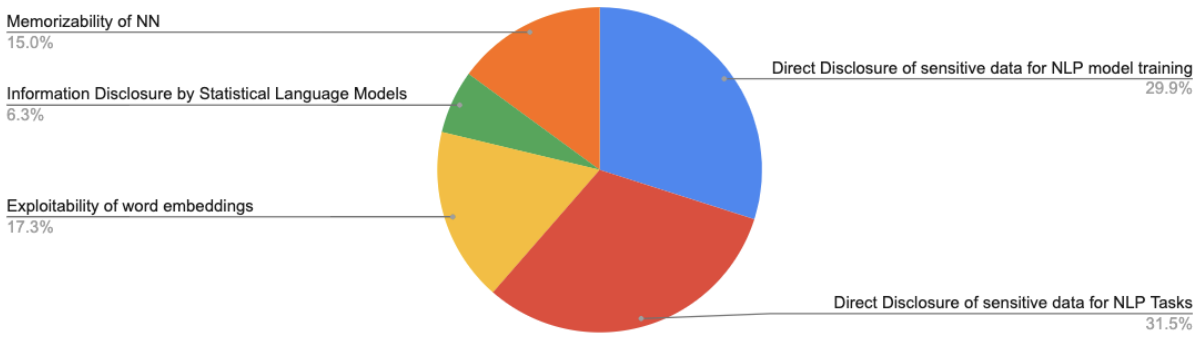


Figure 5.12.: Mapping Results for the Generalized Issue/Vulnerability solved for NLP category in the top category NLP as a Privacy Threat

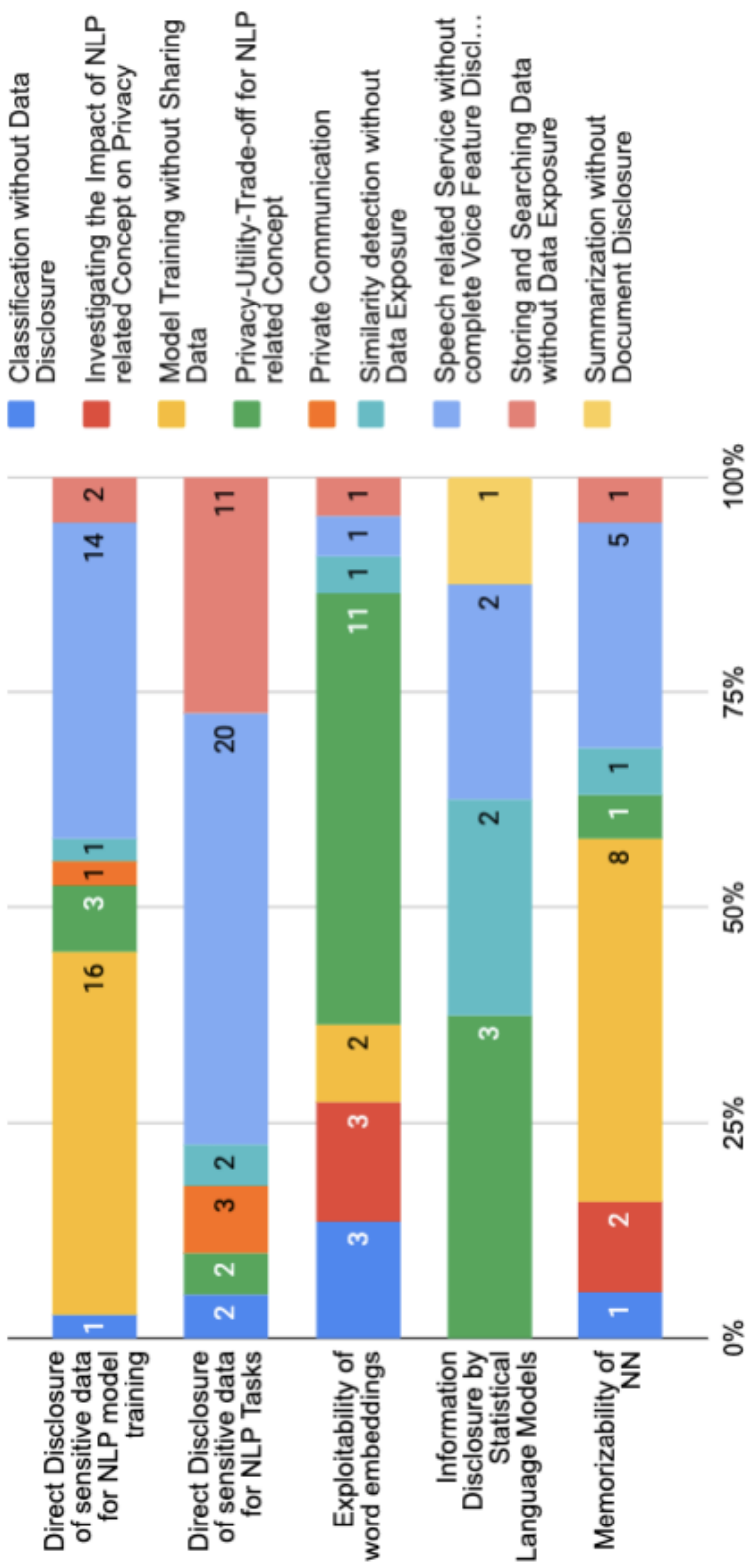


Figure 5.13.: NLP Privacy Issues and Use Cases

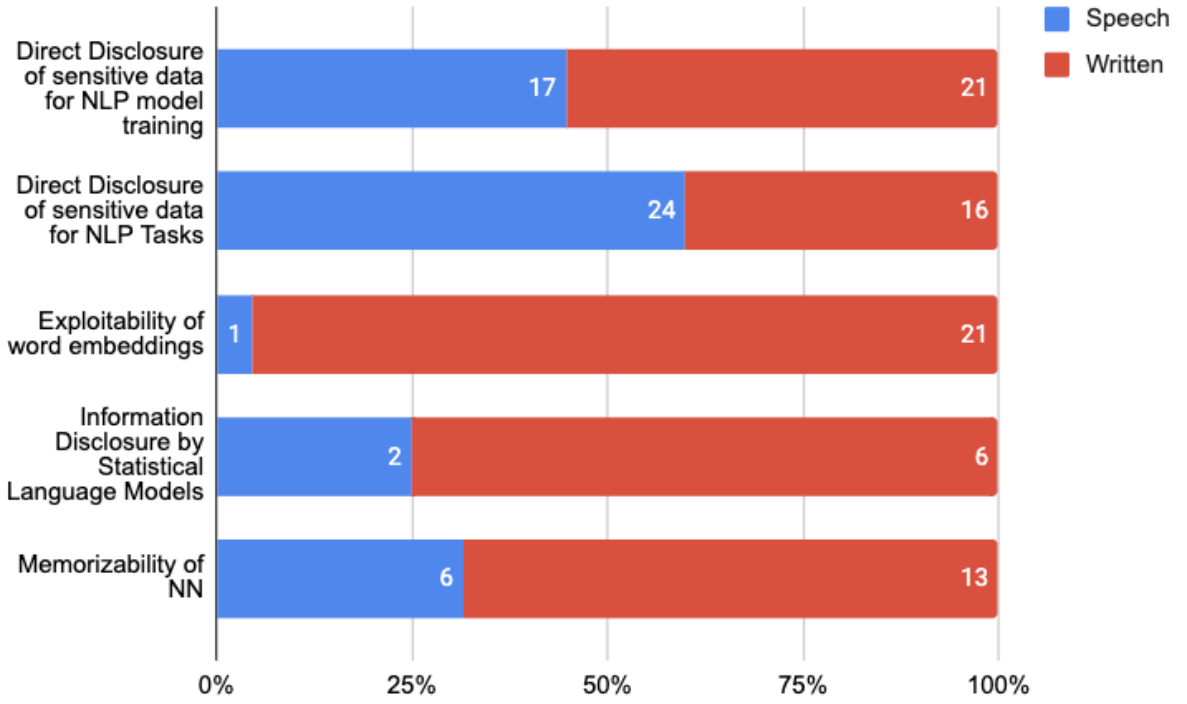


Figure 5.14.: NLP Privacy Issues and Data Type

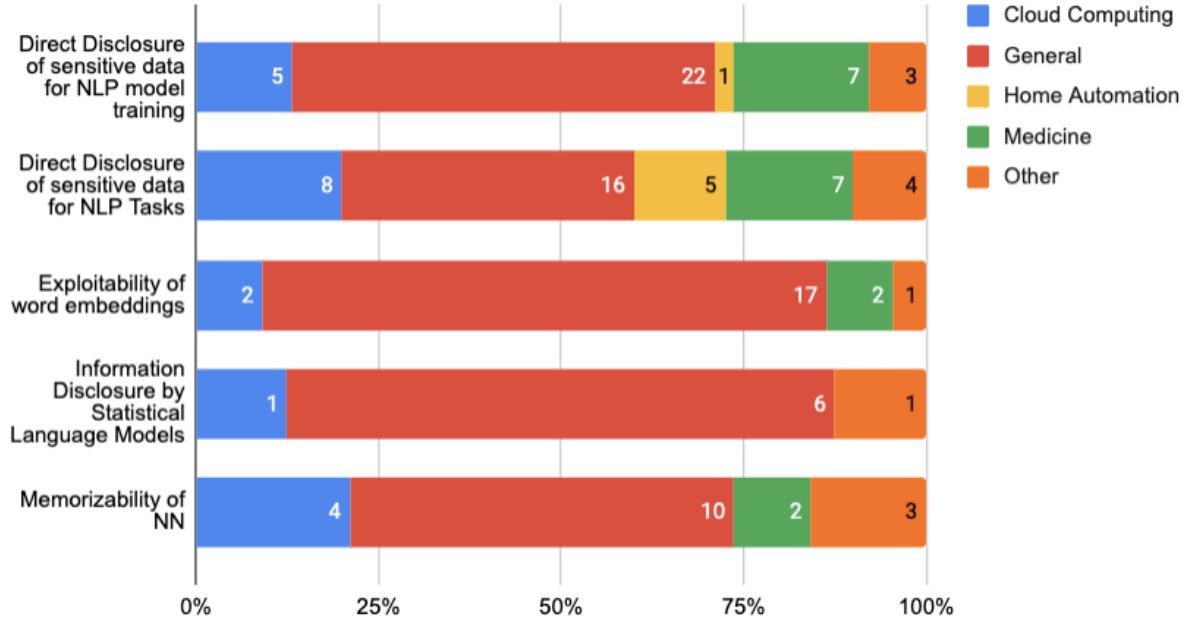


Figure 5.15.: NLP Privacy Issues and Domains

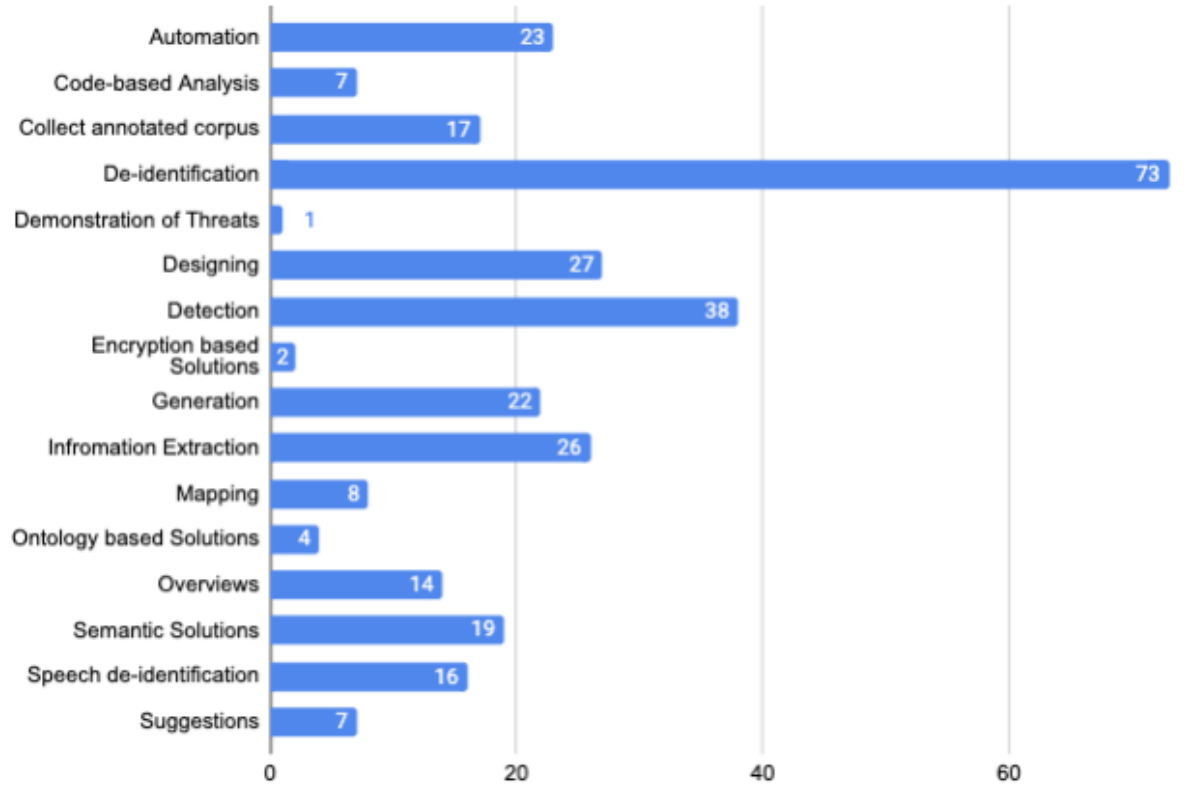


Figure 5.16.: Mapping Results for the Generalized Privacy Issue Solution category in the top category NLP as a Privacy Enabler

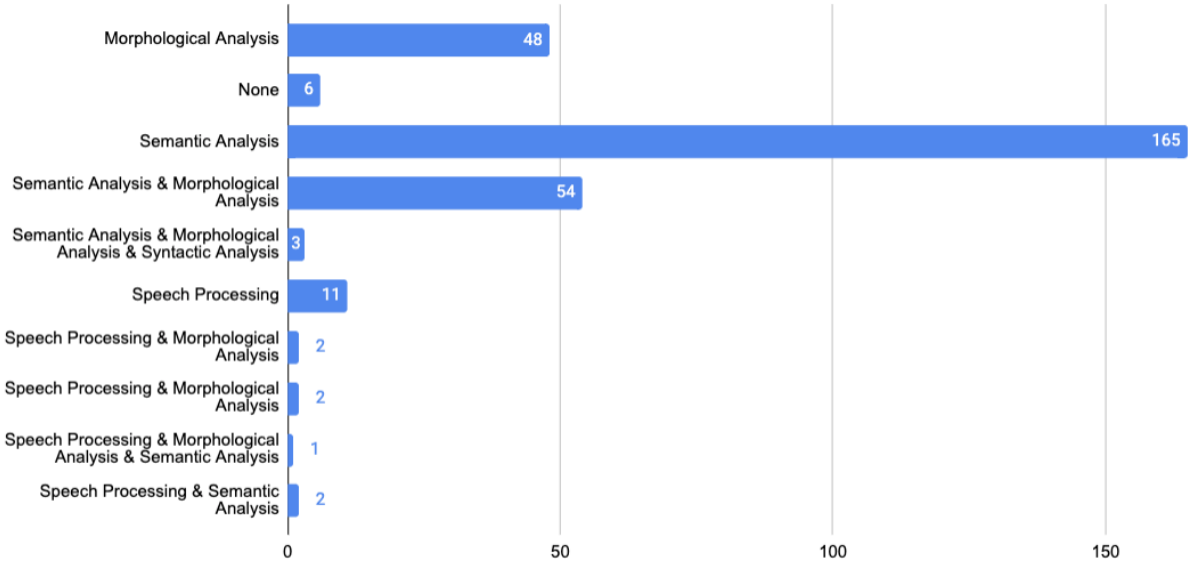


Figure 5.17.: Mapping Results for the Generalized Applied NLP Concept category in the top category NLP as a Privacy Enabler

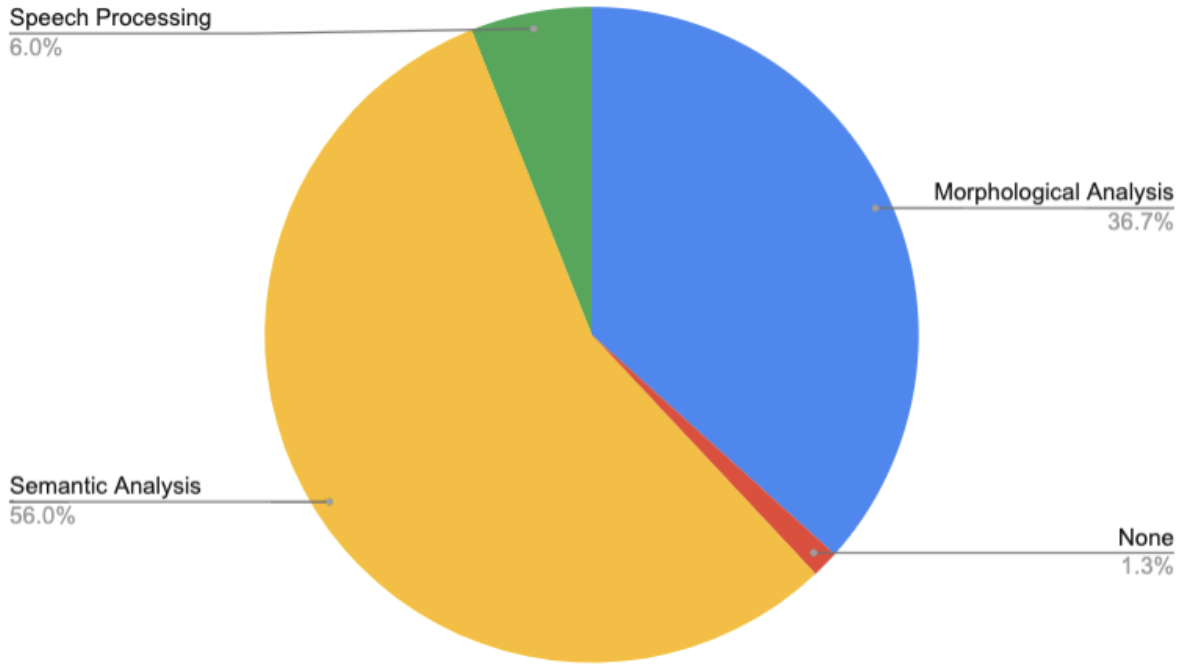


Figure 5.18.: Aggregated mapping results for the Generalized Applied NLP Concept category in the top category NLP as a Privacy Enabler

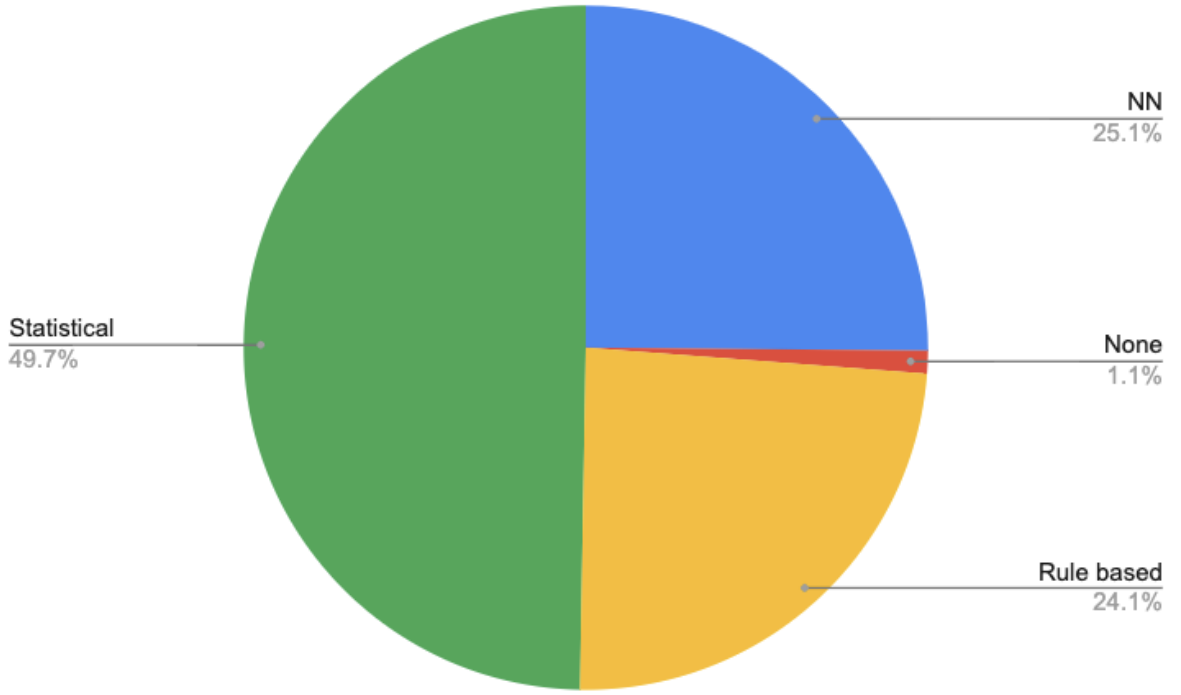


Figure 5.19.: Mapping Results for the Generalized Applied NLP Concept category in the top category NLP as a Privacy Enabler

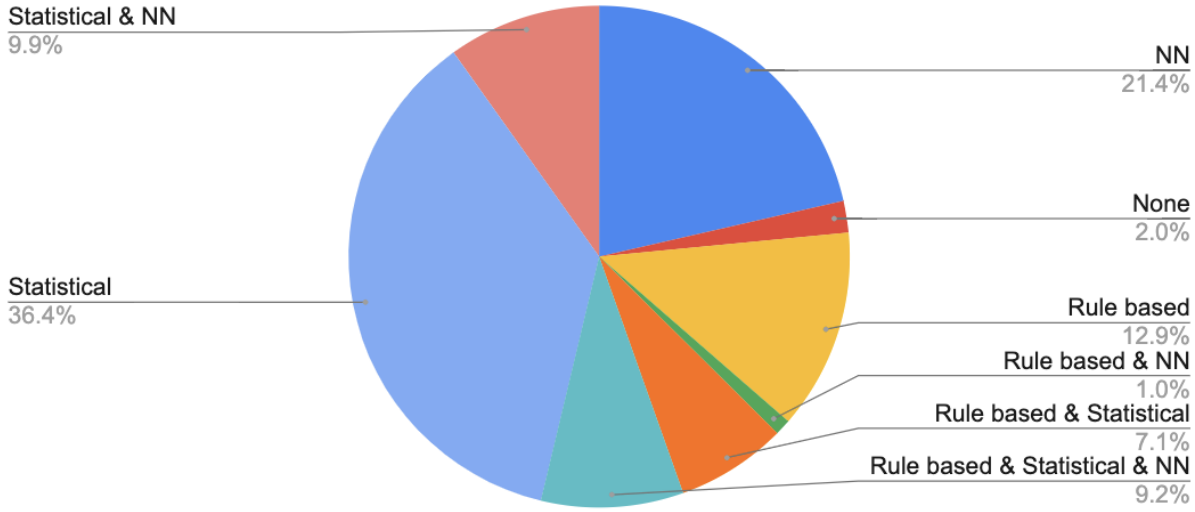


Figure 5.20.: Aggregated mapping results for the Generalized NLP Method category in the top category NLP as a Privacy Enabler

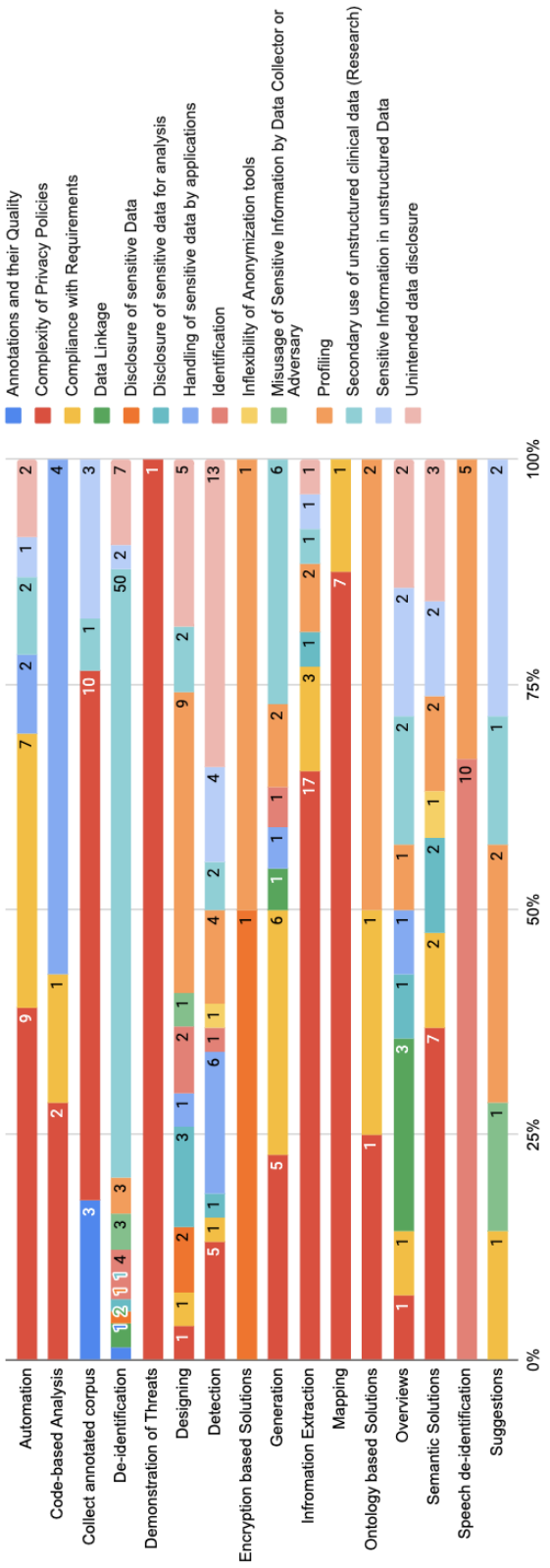


Figure 5.21.: Privacy solutions aiming to solve privacy issues

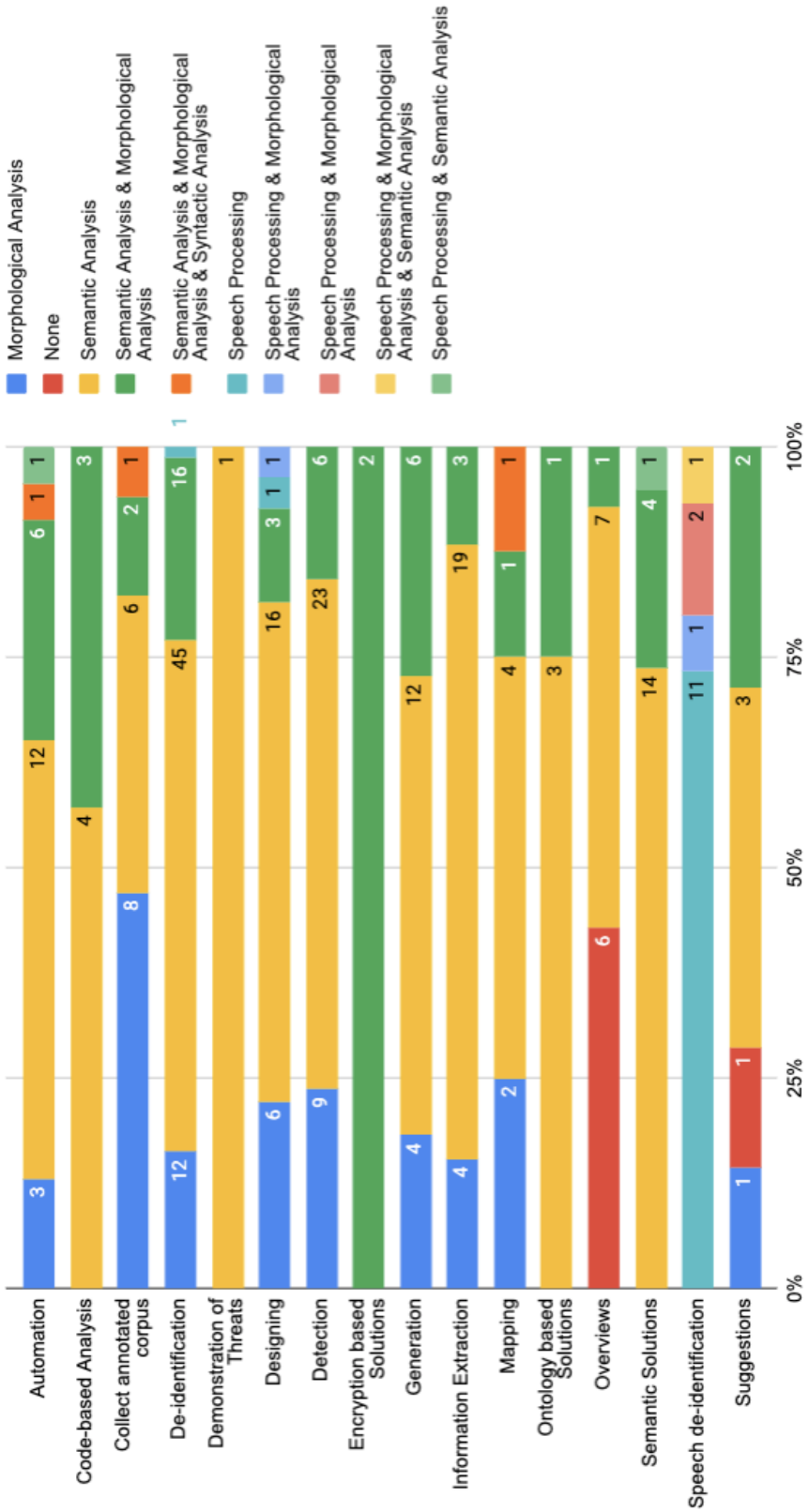


Figure 5.22.: Privacy solutions and their analysis levels

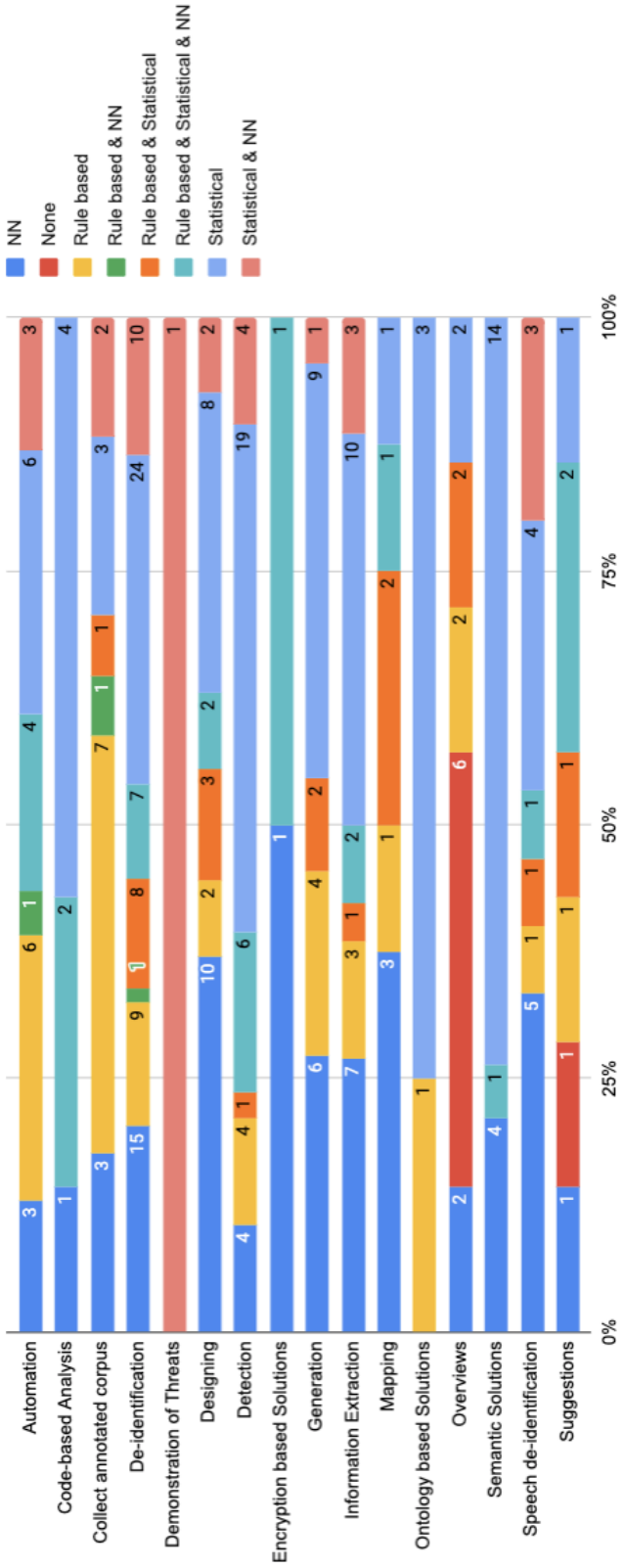


Figure 5.23.: Privacy solutions and their applied method category

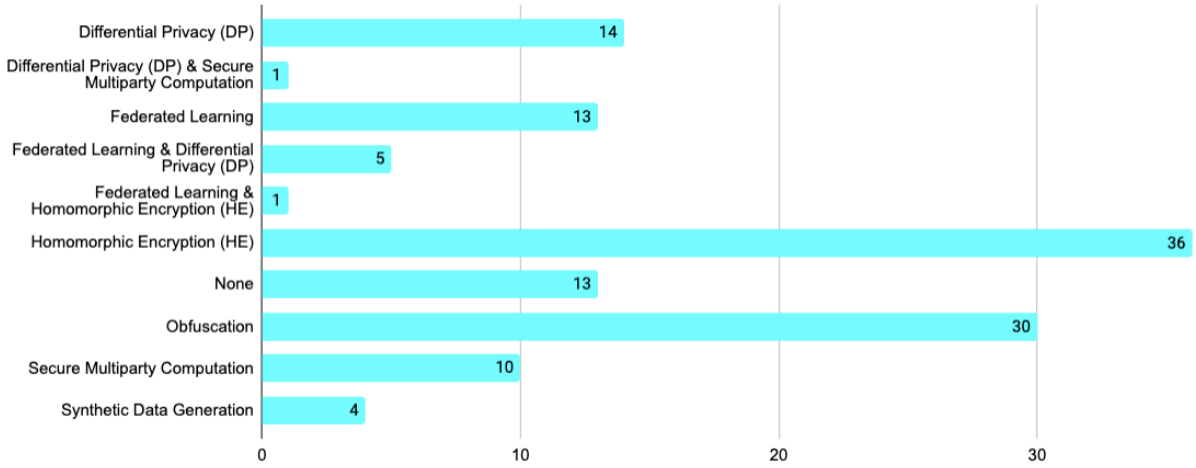


Figure 5.24.: Mapping Results for the Privacy Enhancing Technologies (PETs) category in the top category NLP as a Privacy Threat

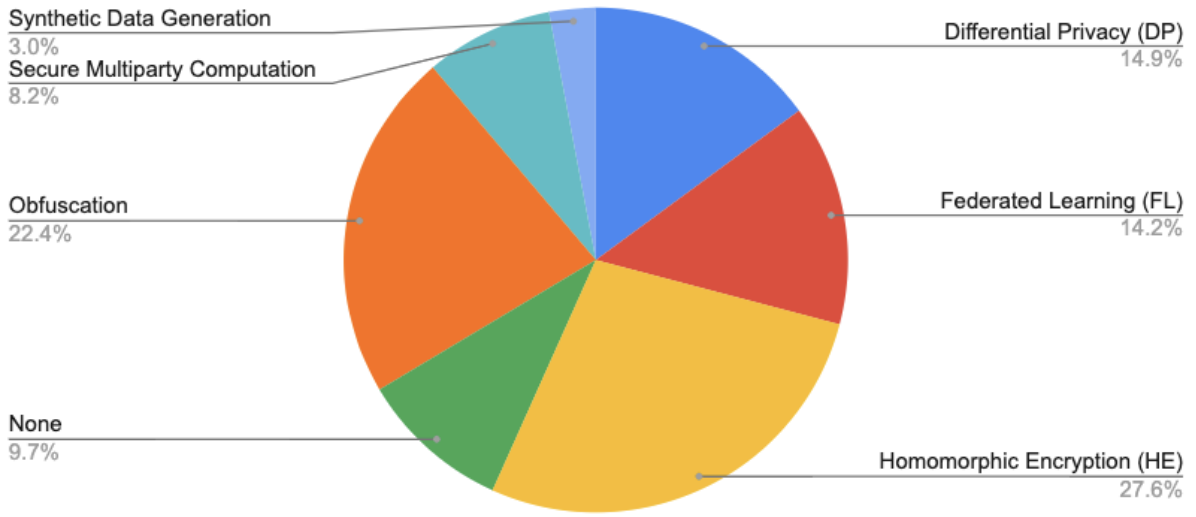


Figure 5.25.: Aggregated Mapping Results for the Privacy Enhancing Technologies (PETs) category in the top category NLP as a Privacy Threat

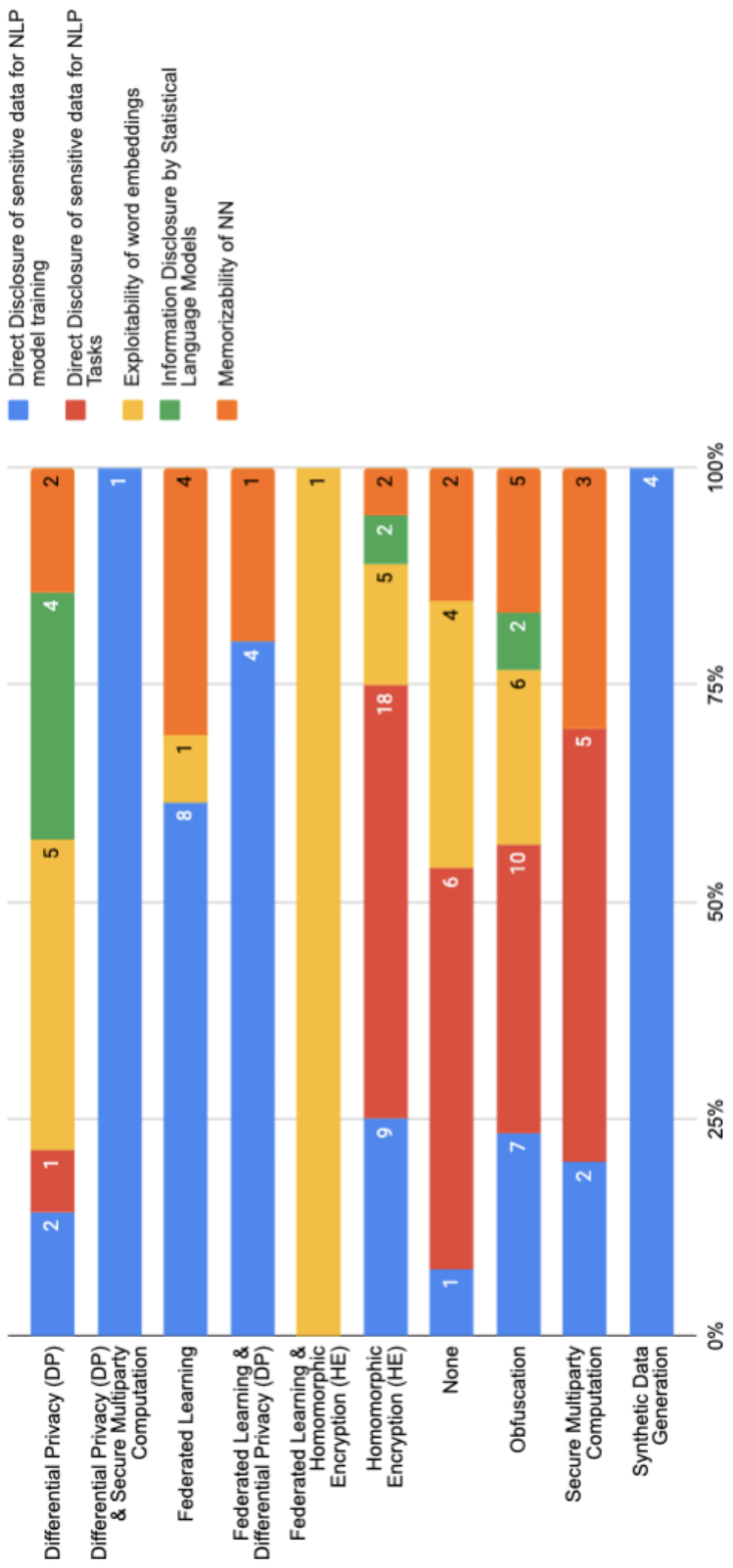


Figure 5.26.: NLP Privacy Threats and their Solutions

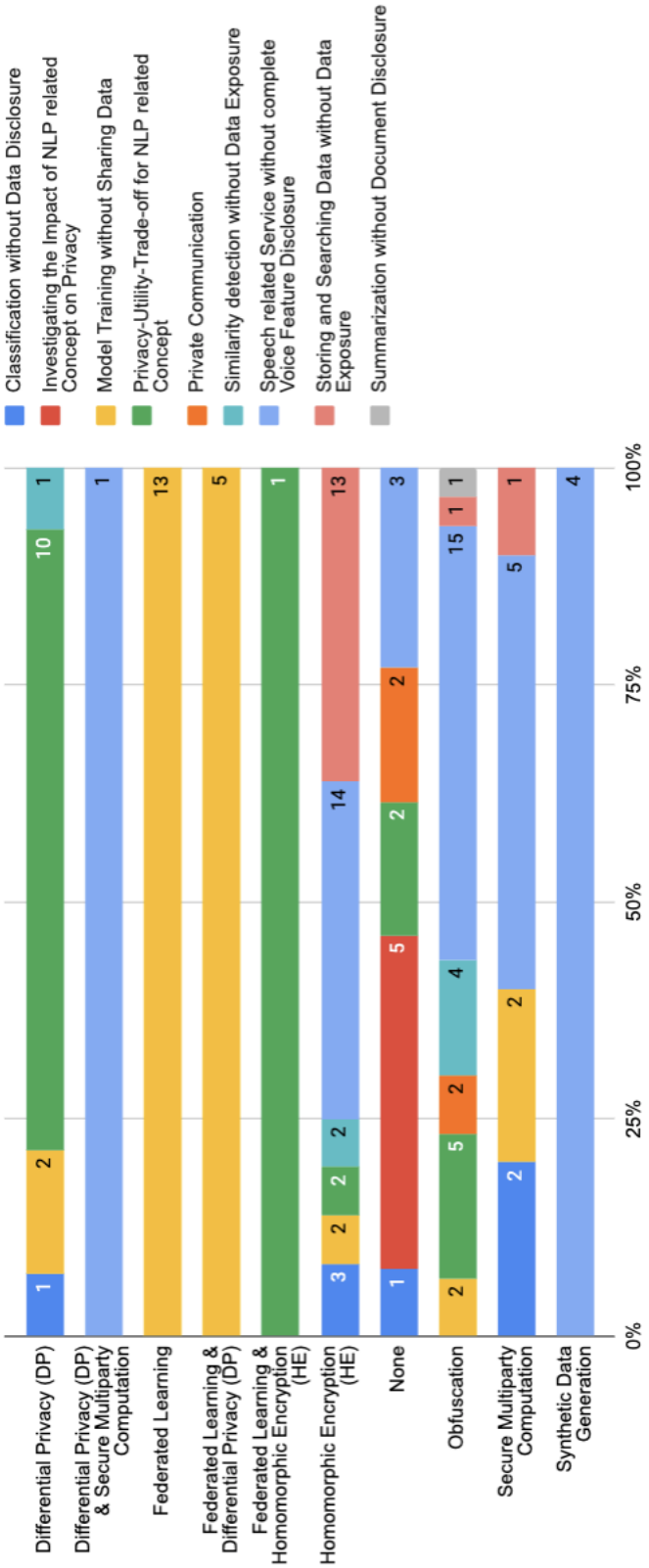


Figure 5.27.: NLP Privacy Threat Solutions and their Use Cases

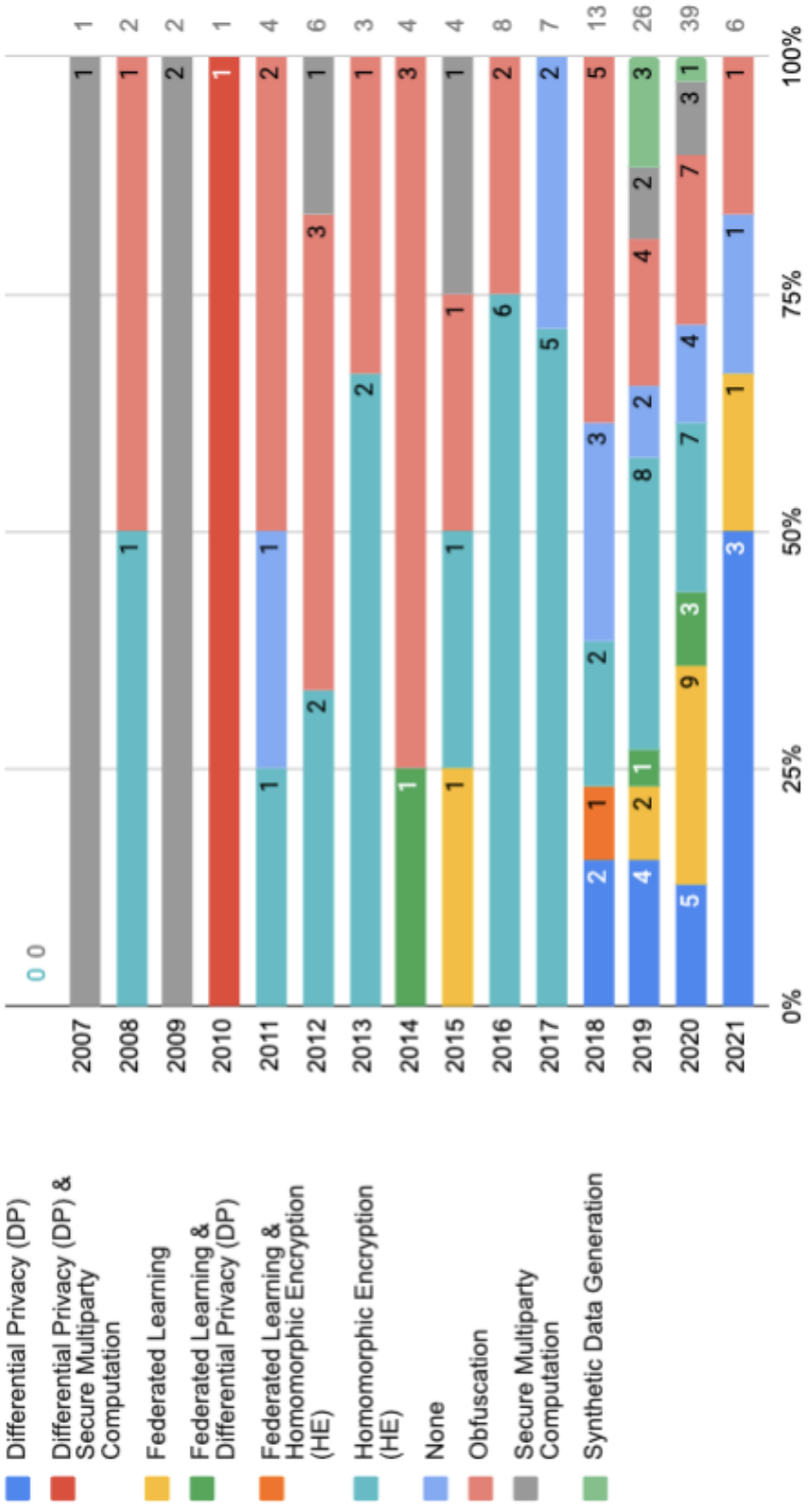


Figure 5.28.: NLP Privacy Threat Solutions and their Development over time

6. Discussion

This chapter will list all essential findings from the previous chapter. The essential findings are split into four parts. Two parts refer to the findings made towards the privacy-related solutions in which one part is dedicated to the interpretation that NLP is a privacy enabler and the other one that NLP as a privacy threat. The remaining two parts refer to the findings made for the solution approaches. Finally, the last part of this chapter will delineate the limitations.

6.1. Summary of Findings

This section will cover a summary of the results we discovered in the previous chapter. The first two parts refer to follow the suggestion of Kitchenham to prove the relevance of the topic by plotting the publication years and check the distribution of publications made by the single electronic data source [12]. We observed that our topic and our subtopics are relevant and gaining interest. Additionally, we realized that Google Scholar adds value as an electronic data source selection to a SMS. Furthermore, we noticed the need to distinguish between two top categories, namely NLP as a privacy enabler and as a privacy threat. The next part will list the essential findings categorized by the research questions and the belonging to its top category.

6.1.1. Main Privacy related Challenges for NLP as a Privacy Enabler

In this part of the thesis, we will point out the most important findings from based on the results made within the SMS.

Domains Dealing with Privacy related Challenges and NLP

We discovered that the main domains applying NLP within their solutions are law and medicine with 27.6 and 30.6 percent, respectively, meaning that over half of the publications we found were related to the two topics. Still, 8.9 and 4.3 percent were located in the domains of social networks and mobile applications, respectively.

Most frequent Use Case Categories affected by NLP solvable Privacy related Challenge

The three most frequent use case categories, we discovered, are protecting sensitive information in unstructured data sets, the privacy-preserving sharing of information, and the simplification of privacy-related regulations.

Most frequent Privacy related Challenges Solved by the application of NLP

According to our mapping results, we observed that the most frequent privacy issues are the secondary use of unstructured clinical data primarily for research purposes, the complexity of privacy regulating documents, unintended data disclosure, profiling, and compliance with requirements.

Domain Diversity of Privacy related Challenges solvable with NLP

Most of the privacy-related challenges we detected affected at least two or more domains. This highlights the fact that one privacy-related challenge is also applicable to multiple domains.

Use Cases addressed by the highest variety of Privacy related Challenges

The use case categories which are affected the most by privacy-related challenges are the privacy-preserving information sharing with 12 out of 14 and the protection of sensitive data in unstructured data being addressed by 10 out of 14 privacy-related challenges.

Increased Attention of Privacy related Challenges solvable with NLP

Since 2018, we realized that the number of publications addressing privacy-related challenges solvable with NLP and the diversity of categories of privacy-related challenges is increasing.

Increased Attention towards the Complexity of Privacy Policies

Since 2016, we observed that the amount of publications addressing the complexity of privacy regulating documents solvable with NLP is increasing.

6.1.2. Main Privacy related Challenges for NLP as a Privacy Threat

This section will summarize the findings within the result chapter.

General Domain mostly affected by NLP as a Privacy Threat

The mapping results regarding the domain affected by NLP as a privacy threat highlight the fact that most of the publications included in the SMS were mapped to the ”General” domain, indicating that NLP as a privacy threat is a relatively new topic.

Popularity of Publications Towards the Written Data Type

Most of the papers in the top category which interprets NLP as a privacy threat deal with the written data type more than with the speech data.

Most frequent Use Case Classes

The three most frequent use case classes identified within the thesis are speech-based services without the complete voice feature disclosure, model training without the disclosure of data, and the privacy-utility-trade-off for NLP related concepts.

Most frequent NLP Threats

The four most frequent NLP privacy threats are The direct disclosure of sensitive data for NLP model training or an NLP task, the exploitability of word embeddings, and the memorizability of NN.

Direct Disclosure of Sensitive Data dominated by Speech Data

Most of the privacy issues were predominated by the written data type. However, the disclosure of speech to a NLP task was the only one dominated by the speech data type.

Generality of Privacy Issues

As a result of our mapping of domains and the use case classes, we discovered that every privacy issue was at least affecting three out of five domains. However, the most considerable proportion was covered by the general domain, meaning that rather theoretical publications addressed the privacy issues without a specific application.

Most affected Use Case Classes

As a result of this study, we identified that speech related services are affected by every privacy issue we identified and that all privacy issues get addressed by the use case class ”Privacy-Utility-Trade-off for NLP related concepts” meaning that in every privacy issue research is conducted to find a balance between utility and privacy.

6.1.3. Solutions supported by NLP as a Privacy Enabler

Here, we summarize the results we collected for the domain in which we discuss privacy solutions supported by NLP.

Most frequent Solutions supported by NLP

This study received the most mapping results based on the publications that we included for De-identification, Detection, and Designing.

Most frequent Analysis Level supported by NLP

The two most often applied NLP concepts were semantic analysis and the combination with the morphological analysis covering over 50 percent of the publications in the top domain in which NLP is interpreted as privacy enabler.

Most frequently applied NLP Method

Our results show that almost 50 percent of the publications in which NLP is utilized as a privacy enabler are based on statistical approaches. The neural networks and rule-based approaches received 25.1 and 24.1 percent, respectively.

Diversity of Solution approaches towards Privacy Policy Complexity

We discovered that the widest variety of approaches towards solving the privacy-related challenge are made to ease the complexity of privacy policies. 12 out of the 16 categories for solving privacy-related challenges addressed the complexity of privacy policies. Most publications were made within the information extraction category.

High Coverage of Semantic Analysis

Almost all privacy issue solutions supported by NLP are covered by either semantic analysis or the combination with morphological analysis. No solution approach is purely based on one level of analysis. Mixed-level approaches are less frequent than pure ones.

High Coverage of Solutions Approaches supported by NLP based on Neural Networks

All solution categories have approaches in which neural networks are applied. The highest coverage is still dedicated to statistical approaches. Rule-based and mixed approaches are a minority.

6.1.4. Main Solutions for NLP as a Privacy Threat

In this section, we will summarize the results we received for the category in which we solve privacy issues caused by NLP.

Homomorphic Encryption as most applied PET

The three most frequent PETs according to our mapping results are homomorphic encryption, obfuscation, and differential privacy, achieving 36, 30, and 14 publications, respectively. Including the combinations into the count homomorphic encryption, obfuscation, and differential privacy achieve an overall coverage of 27.6, 22.4, and 14.9 percent, respectively.

Most frequent PET combinations

The PETs, which are mainly used for combinations, are federated learning and homomorphic encryption. The most prominent combination with the mapping results is federated learning and differential privacy with a count of five.

PETs with Highest Solution Coverage

Three PETs contain all five privacy issues caused by NLP, which proves the fact of their universal utilization possibilities, are differential privacy, homomorphic encryption, and obfuscation.

Differential Privacy for Privacy-Utility-Trade-off

Differential privacy is the PET which is applied the most to introduce a trade-off between privacy and utility into a data set to disclose data that still has value for a NLP task.

Federated Learning as main PET for Model Training

Federated learning is only applied for model training of data without sharing the raw data and does not solve any further privacy issues caused by NLP.

Highest Diversity regarding application by use cases

Homomorphic encryption and obfuscation are the PET with the highest diversity regarding being applied by six and seven out of nine use case categories.

Synthetic Data Generation as Solution for Speech related Services

We realized that mainly in the use case category referring to voice-based services, the PET synthetic data generation is applied.

2018 as the beginning of the Diverse Application of PETs

In 2018, not just the amount of publications regarding the application of PETs to solve NLP related privacy issues is increasing but also the diversity of approaches.

6.2. Limitations

Our systematic mapping study covers a lot of information that leads to a lot of thoughts. However, this thesis was limited by time. Therefore not every thought could be followed. Another major issue we faced during this thesis is the limited access to online papers that are either not covered within the online service of the university or a third-party library faces service problems that also lead to the fact that access to specific papers is not possible.

Furthermore, the quality of abstracts and titles was crucial for us, mainly because of the tremendous amount of papers and not always the title or abstracts provided a sufficient amount of information. Privacy-Preserving NLP is not a mature and clearly defined term; therefore, it might happen that some papers weren't inspected because the required vital words weren't used. Thus, they were not detected by the search engines of the electronic data sources. Another drawback was that not all electronic data sources did provide the optimal search functionalities like filtering of keywords in a particular part of the document. This lead to results that included the keywords but the topic covered in the document varied from our topic significantly. Subsequently, the methodology left out some important papers that are relevant to the topic. However, it would've been possible to find those papers with an extended search query that would have led to an even more enormous amount of papers to go through what would not be realistic in the given amount of time. Some examples for not found papers from the PrivateNLP Workshop [254] have the following titles:

- On Log-Loss Scores and (No) Privacy [255]
- A Differentially Private Text Perturbation Method Using Regularized Mahalanobis Metric [56]
- Identifying and Classifying Third-party Entities in Natural Language Privacy Policies [52]
- Surfacing Privacy Settings Using Semantic Matching [54]
- Differentially Private Language Models Benefit from Public Pre-training [55]

7. Conclusion and Future Work

In this chapter, we will conclude the thesis and delineate possible future work.

7.1. Conclusion

All in all, we asked ourselves which privacy-related challenges exist in Natural Language Processing. To answer this question, we conducted a systematic mapping study to investigate the literature addressing privacy preservation and natural language processing. We included 431 publications into our mapping study and realized that 304 and 127 publications have a different interpretation of privacy and NLP. 304 of them saw NLP as a privacy enabler that faces different challenges than NLP as a privacy threat. We were curious about the use cases and privacy issues those two interpretations contain and which methods and concepts were applied. In the end, we used five major NLP related privacy threats partially inspired by Pan, Carlini and Koppel [8, 239, 9] and 14 privacy-related challenges partially inspired by the paper by [146] Boukharrou, Chaouche, and Mahdjar within our selected literature. Through mappings of the use case categories on the privacy-related challenges, we gained a better understanding of the challenges and their environment. The second question we attempted to answer was addressing the solutions which the literature proposes to solve the privacy-related challenges and the possibility of categorizing them. We applied the categories suggested by Dilmegani [101] for our solutions for NLP privacy issues and applied Petersen's keywording approach [11] to extract the categories that describe privacy issue solution approaches supported by NLP. To see the potential of the different solution approaches for NLP related privacy issues or NLP as a privacy enabler, we mapped the privacy issues on the solutions to also gain a better understanding of their applicability and in which scenario they are used. In the end, we reported our findings and observations to provide an overview of the research field of Privacy-Preserving Natural Language Processing and its challenges and solutions. With this overview, we proposed different research activities and in which direction the research field might head.

7.2. Future Work

We realized that privacy preservation techniques were developed frequently during the mapping study or that some were reapplied. It would be interesting to investigate if there is a trend or if some tools are more used than others and why that is the case. Furthermore, our systematic mapping study delivers an overview for researchers that are interested in the topic of privacy preservation and NLP. This provides the opportunity to conduct systematic

literature reviews on one of the top categories identified during this thesis. This is a superficial analysis of a significantly more critical research field that can be extended. One example is to inspect further the applied NLP concepts in the context of privacy. Our research proves that the intersection between privacy and NLP gains more and more interest every year.

A. General Addenda

A.1. Work Sheets containing the analysis of the top categories

A.1.1. NLP as a Privacy Enabler Analysis Sheet

Document Title	Authors	Abstract	Year	Source	Generalized Dom	Generalized Data Category	(RQ1)Classification of Use Case	Generalized Privacy Issue(P	Generalized Privacy Issue S	Generalized Category of Ap	NLP Method
QTIP: multi-agent NLP and privacy arc	V. Keselj; D. Jutla	We present a generic natural	2005	IEEE	General	complex sensitive information	Browsing in a private manner	Profiling	Designing a multi-agent archi	Morphological Analysis	Rule based
The Effects of OCR Error on the Extra	Kazem TaghvaR	OCR error has been shown n	2006	Springer	Other	complex sensitive information	protecting sensitive Information in u	Sensitive Information in unstr	Overview of the current state	Semantic Analysis & Morphol	Rule based & Statistical
Theoretical considerations of ethics in	Suominen, H; Le	This paper discusses theoret	2006	Web of Science	Medicine	patient health information (PHI	Mining according to privacy policies	Secondary use of unstructure	Suggestion of security and pr	Semantic Analysis	Rule based & Statistical & NN
Evaluating the state-of-the-art in auton	Uzuner, O; Luo,	To facilitate and survey studie	2007	Web of Science	Medicine	patient health information (PHI	protecting patient privacy in unstruc	Disclosure of sensitive Data	De-identification	Semantic Analysis	Rule based & Statistical
Reconciling privacy policies and regula	Krachina, O; Ras	How well the privacy policy fo	2007	Web of Science	Law	Privacy Policies	Ease the automation process of priv	Compliance with Requiremen	Ontological semantics perspe	Semantic Analysis	Statistical
Privacy and Artificial Agents, or, Is Goo	Chopra, S; White	We investigate legal and philo	2007	Web of Science	Law	User Generated Content (UGC	protecting sensitive Information in u	Profiling	Suggestion of security and pr	Semantic Analysis & Morphol	Rule based & Statistical & NN
Distributed Latent Dirichlet allocation f	H. Wang; Z. Li; Y	The paper introduces the mo	2008	IEEE	General	complex sensitive information	Mining according to privacy policies	Sensitive Information in unstr	Semantic similarity based on	Semantic Analysis	Statistical
Finding Defects in Natural Language C	J. H. Weber-Jahn	Large-scale software systems	2009	IEEE	Law	Privacy Policies	Definition of Privacy Requirements	Compliance with Requiremen	Generation of Artefacts based	Semantic Analysis & Morphol	Rule based
Accurate Synthetic Generation of Rea	Peter ChristenAg	A large proportion of the mas	2009	Springer	General	Synthetic Data Generation	Privacy Preserving Information Sha	Data Linkage	Generation of Synthetic Data	Morphological Analysis	Rule based
Voice convergin: Speaker de-identifica	Q. Jin; A. R. Toth	Speaker identification might b	2009	IEEE	General	Speech Data	Privacy Preserving Information Sha	Identification	Speech De-Identification	Speech Processing	Statistical
A System for De-identifying Medical M	A. Benton; S. Hill	There are millions of public p	2010	IEEE	Medicine	User Generated Content (UGC	Protecting Sensitive Information on	Secondary use of unstructure	De-identification	Semantic Analysis & Morphol	Statistical
Detecting Revelation of Private Inform	N. Watanabe; H.	Online social networks are be	2010	IEEE	Social Network	User Generated Content (UGC	Protecting Sensitive Information on	Unintended data disclosure	Detecting privacy-sensitive in	Morphological Analysis	Statistical
Data Leak Prevention through Named	J. M. Gómez-Hid	The rise of the social web has	2010	IEEE	Social Network	User Generated Content (UGC	Protecting Sensitive Information on	Unintended data disclosure	Detecting privacy-sensitive in	Semantic Analysis	Rule based & Statistical & NN
Privacy Domain-Specific Ontology Bui	L. Cai; C. Lu; C.	With the rapid development o	2010	IEEE	General	complex sensitive information	Privacy Preserving Information Sha	Profiling	Ontology build for privacy	Semantic Analysis	Statistical
A Notation for Policies Using Feature S	Fujita, K; Tsukad	New security and privacy enh	2011	Web of Science	Law	Privacy Policies	Automated and Flexible Rule Enfor	Complexity of Privacy Policies	Automated Access Control ba	Morphological Analysis	Rule based
Privacy Measures for Free Text Docun	Liqiang GengYon	Privacy compliance for free te	2011	Springer	Medicine	patient health information (PHI	Measuring the Compliance of apps	Secondary use of unstructure	Automated Compliance Chec	Semantic Analysis	Rule based
Towards Natural-Language Understan	Papanikolaou, N	In this paper we survey existi	2011	Web of Science	Law	Privacy Policies	Automated and Flexible Rule Enfor	Compliance with Requiremen	Automatic policy enforcement	Semantic Analysis & Morphol	Rule based
Unlocking data for clinical research–th	Ganslandt, Thom	Objective: Data from clinical	2011	Google Scholar	Medicine	patient health information (PHI	Privacy Preserving Information Sha	Secondary use of unstructure	De-identification	Semantic Analysis	Rule based
On the Declassification of Confidential	Abril, D; Navarro	We introduce the anonymizat	2011	Web of Science	General	complex sensitive information	protecting sensitive Information in u	Sensitive Information in unstr	De-identification	Semantic Analysis	Statistical
Text Classification for Data Loss Preve	Michael HartPrat	Businesses, governments, an	2011	Springer	General	complex sensitive information	protecting sensitive Information in u	Unintended data disclosure	Detecting privacy-sensitive in	Semantic Analysis	Statistical
Automatic Anonymization of Natural La	H. Nguyen-Son;	One approach to overcoming	2012	IEEE	Social Network	User Generated Content (UGC	Protecting Sensitive Information on	Sensitive Information in unstr	Automatic Annonymization of	Morphological Analysis	Statistical
A machine learning solution to assess	Costante, Elisa;	A privacy policy is a legal doc	2012	Google Scholar	Law	Privacy Policies	Paying more Attention to Privacy Po	Complexity of Privacy Policies	Automatic Assessment of Priv	Semantic Analysis	Statistical
Evaluating current automatic de-identi	Ferrandez, O; Sc	Background: The increased u	2012	Web of Science	Medicine	patient health information (PHI	protecting patient privacy in unstruc	Secondary use of unstructure	De-identification	Semantic Analysis	Statistical
Using Profiling Techniques to Protect t	Alexandre ViejoD	The emergence of microblogg	2012	Springer	Social Network	User Generated Content (UGC	Privacy Preserving Information Sha	Profiling	Designing a scheme for a priv	Semantic Analysis & Morphol	Statistical
Detecting Sensitive Information from T	David SánchezM	Whenever a document conta	2012	Springer	General	User Generated Content (UGC	Privacy Preserving Information Sha	Inflexibility of annonymization	Detecting privacy-sensitive in	Semantic Analysis & Morphol	Statistical
P2P Watch: Personal Health Informati	Sokolova, M; El I	Background: Users of peer-to	2012	Web of Science	Medicine	patient health information (PHI	Privacy Preserving Information Sha	Unintended data disclosure	Detection of Personal Health	Semantic Analysis	Rule based
iDASH: integrating data for analysis, a	Ohno-Machado,	iDASH (integrating data for a	2012	Google Scholar	Medicine	patient health information (PHI	Privacy Preserving Information Sha	Handling of sensitive data by	Overview of algorithms and to	Semantic Analysis	Rule based & Statistical
Improved de-identification of physician	McMurry, AJ; Fitz	Background: Physician notes	2013	Web of Science	Medicine	patient health information (PHI	Privacy Preserving Information Sha	Secondary use of unstructure	De-identification	Morphological Analysis	Statistical
A framework for privacy-preserving me	Li, Xiao-Bai; Qin,	Health information systems h	2013	Google Scholar	Medicine	patient health information (PHI	Privacy Preserving Information Sha	Secondary use of unstructure	De-identification	Semantic Analysis	Statistical
Anonymouth revamped: Getting closer	McDonald, AW;	Ulman, Jeffrey; Barrowclift, Ma	2013	Google Scholar	Other	User Generated Content (UGC	protecting sensitive Information in u	Identification	De-identification / Obfuscating	Semantic Analysis	Rule based & Statistical
A Versatile Tool for Privacy-Enhanced	Avi ArampatzisG	We consider the problem of p	2013	Springer	Other	User Generated Content (UGC	Searching in a private manner	Profiling	Designing a privacy-preservin	Semantic Analysis	Statistical
Gateway to the Cloud - Case Study: A	R. Smith; J. Xu; S	We describe a study in the do	2013	IEEE	Medicine	patient health information (PHI	Privacy Preserving Information Sha	Secondary use of unstructure	Designing a tailor-made data	Semantic Analysis	Rule based & Statistical
Knowledge-based scheme to create p	SáNchez, David;	Web search engines (WSEs)	2013	Google Scholar	Other	User Generated Content (UGC	Searching in a private manner	Profiling	Generation of Synthetic Data	Semantic Analysis & Morphol	Statistical
A taxonomy of privacy-preserving reco	Vatsalan, Dinush	The process of identifying wh	2013	Google Scholar	Other	complex sensitive information	Privacy Preserving Information Sha	Data Linkage	Overview of techniques for pr	Semantic Analysis	Rule based
Minimizing the disclosure risk of sema	Sánchez, David;	Text sanitization is crucial to	2013	ScienceDirect	General	complex sensitive information	Privacy Preserving Information Sha	Inflexibility of annonymization	Semantic correlations in docu	Semantic Analysis	Rule based & Statistical & NN
Utility preserving query log anonymiza	Batet, Montserra	Query logs are of great intere	2013	ScienceDirect	Other	Query Data	Searching in a private manner	Profiling	Semantic Microaggregation fo	Semantic Analysis & Morphol	Statistical
A discussion of privacy challenges in u	Hasan, Omar; Ha	User profiling is the process	2013	Google Scholar	Other	complex sensitive information	Mining according to privacy policies	Profiling	Suggestion of security and pr	Semantic Analysis & Morphol	Rule based & Statistical
Privee: An architecture for automatical	Zimmeck, Sebas	Privacy policies on websites	2014	Google Scholar	Law	Privacy Policies	Paying more Attention to Privacy Po	Complexity of Privacy Policies	Automatic Analysis of Privacy	Semantic Analysis & Morphol	Rule based
Preparing an annotated gold standard	Deleger, L; Lingr	Objective: The current study	2014	Web of Science	Medicine	patient health information (PHI	Annotations with Gold Standard	Annotations and their Quality	Collect annotated corpus	Morphological Analysis	Rule based & Statistical
Evaluating the effects of machine pre-	South, BR; Mowe	The Health Insurance Portab	2014	Web of Science	Medicine	patient health information (PHI	Privacy Preserving Information Sha	Secondary use of unstructure	De-identification	Semantic Analysis	Rule based & Statistical
De-identification in natural language p	V. Vincze; R. Far	Natural language processing	2014	IEEE	Medicine	patient health information (PHI	Privacy Preserving Information Sha	Secondary use of unstructure	De-identification	Semantic Analysis	Rule based & Statistical & NN
De-identification of unstructured paper	Fenz, Stefan; He	Whenever personal data is pr	2014	Google Scholar	Medicine	patient health information (PHI	Privacy Preserving Information Sha	Secondary use of unstructure	De-identification	Semantic Analysis	Statistical
Text de-identification for privacy protec	Meystre, SM; Fe	As more and more electronic	2014	Web of Science	Medicine	patient health information (PHI	Privacy Preserving Information Sha	Secondary use of unstructure	De-identification	Semantic Analysis	Statistical
De-identification of clinical narratives t	Li, MQ; Carrell, D	Purpose: Electronic health re	2014	Web of Science	Medicine	patient health information (PHI	Privacy Preserving Information Sha	Secondary use of unstructure	De-identification	Semantic Analysis & Morphol	Statistical
Can Physicians Recognize Their Own	Meystre, S; Sher	The adoption of Electronic He	2014	Web of Science	Medicine	patient health information (PHI	Privacy Preserving Information Sha	Unintended data disclosure	De-identification	Semantic Analysis & Morphol	Rule based & Statistical
Profiling social networks to provide us	Viejo, Alexandre;	Web search engines (WSEs)	2014	Google Scholar	Social Network	User Generated Content (UGC	Searching in a private manner	Profiling	Designing a privacy-preservin	Semantic Analysis	Statistical
Privacy detective: Detecting private int	Caliskan Islam, A	Detecting the presence and a	2014	Google Scholar	Social Network	User Generated Content (UGC	Protecting Sensitive Information on	Profiling	Detecting privacy-sensitive in	Semantic Analysis	Statistical & NN
A platform for developing privacy pres	S. Ucan; H. Gu	Healthcare Information Techn	2014	IEEE	Medicine	patient health information (PHI	protecting patient privacy in unstruc	Disclosure of sensitive data fo	Information Extraction from H	Semantic Analysis	Statistical
Filtering Personal Queries from Mixed	Ary Fagundes Br	Queries performed against th	2014	Springer	Other	Query Data	Mining according to privacy policies	Compliance with Requiremen	Information Extraction from pr	Morphological Analysis	Statistical
AutoCog: Measuring the Description-to	Qu, ZY; Rastogi,	The booming popularity of sm	2014	Web of Science	Law	complex sensitive information	Ease the comprehension of Privacy	Complexity of Privacy Policies	Mapping of Description-to-per	Semantic Analysis & Morphol	Rule based & Statistical & NN
Latent semantic analysis for privacy pr	Selmi, Mouna; H	Today's e-learning systems e	2014	Google Scholar	Other	User Generated Content (UGC	protecting sensitive Information in u	Unintended data disclosure	Semantic analysis for privacy	Semantic Analysis	Statistical

Document Title	Authors	Abstract	Year	Source	Generalized Dom	Generalized Data Category	(RQ1)Classification of Use Case	Generalized Privacy Issue(P	Generalized Privacy Issue S	Generalized Category of Ap	NLP Method
The Impact of Anonymization for Auton	Shermis, Mark D	This study investigated the in	2015	Wiley	General	User Generated Content (UG	protecting sensitive Information in u	Handling of sensitive data by	Automated Essay Scoring	Semantic Analysis	Rule based & Statistical & NN
Annotating longitudinal clinical narrativ	Stubbs, A; Uzune	The 2014 i2b2/UTHealth natu	2015	Web of Science	Medicine	patient health information (PHI	Annotations with Gold Standard	Complexity of Privacy Policies	Collect annotated corpus	Morphological Analysis	Rule based
Iterative Classification for Sanitizing La	B. Li; Y. Vorobey	Cheap ubiquitous computing	2015	IEEE	General	complex sensitive information	Privacy Preserving Information Sha	Unintended data disclosure	De-identification	Semantic Analysis	Rule based & Statistical
Secure Obfuscation of Authoring Style	Hoi LeReihaneh	Anonymous authoring include	2015	Springer	Social Network	User Generated Content (UG	protecting sensitive Information in u	Profiling	De-identification / Obfuscating	Semantic Analysis	Statistical
MonkeyDroid: Detecting Unreasonable	Ma, K; Liu, MY; C	Static and dynamic taint-anal	2015	Web of Science	Mobile Application	complex sensitive information	Investigating the potential Privacy In	Handling of sensitive data by	Detecting privacy-sensitive in	Semantic Analysis	Statistical
A Novel Approach to Prevent Persona	N. A. Patil; A. S.	Online social network such as	2015	IEEE	Social Network	User Generated Content (UG	Protecting Sensitive Information on	Unintended data disclosure	Detecting privacy-sensitive in	Morphological Analysis	Rule based & Statistical
Oblivion: Mitigating Privacy Leaks by (	Milivoj Simeonov	Search engines are the preva	2015	Springer	Other	Query Data	Searching in a private manner	Unintended data disclosure	Detecting privacy-sensitive in	Semantic Analysis	Rule based & Statistical & NN
Autoppg: Towards automatic generatic	Yu, Le; Zhang, Ta	A privacy policy is a statemer	2015	Google Scholar	Law	Privacy Policies	Ease the writing process of privacy	Complexity of Privacy Policies	Generation of Artefacts based	Semantic Analysis	Statistical
Towards an information type lexicon fo	J. Bhatia; T. D. B	Privacy policies serve to infor	2015	IEEE	Law	Privacy Policies	Ease the comprehension of Privacy	Complexity of Privacy Policies	Mapping Privacy Policy Conte	Morphological Analysis	Rule based
Ontology-Enabled Access Control and	Marcel HeupelLa	Recent trends in ubiquitous c	2015	Springer	Social Network	User Generated Content (UG	Protecting Sensitive Information on	Profiling	Ontology-Enabled Access Co	Semantic Analysis & Morphol	Rule based
Privacy-driven access control in social	Imran-Daud, Mal	In online social networks (OS	2016	ScienceDirect	Social Network	User Generated Content (UG	Protecting Sensitive Information on	Unintended data disclosure	Automatic semantic annotatio	Semantic Analysis & Morphol	Statistical
Automatic Extraction of Metrics from S	S. Mittal; K. P. Jo	To effectively manage cloud b	2016	IEEE	Law	Privacy Policies	Ease the automation process of priv	Complexity of Privacy Policies	Automation process of SLAs	Semantic Analysis & Morphol	Rule based
Is the Juice Worth the Squeeze? Cost	Carrell, DS; Cron	Background: Clinical text con	2016	Web of Science	Medicine	patient health information (PHI	Annotations with Gold Standard	Annotations and their Quality	Collect annotated corpus	Morphological Analysis	Rule based
The Creation and Analysis of a Websit	Wilson, S; Schau	Website privacy policies are (	2016	Web of Science	Law	Privacy Policies	Paying more Attention to Privacy Po	Complexity of Privacy Policies	Collect annotated corpus	Morphological Analysis	Rule based
Optimizing annotation resources for na	Li, MQ; Carrell, D	Objective: Electronic medical	2016	Web of Science	Medicine	patient health information (PHI	Annotations with Gold Standard	Annotations and their Quality	De-identification	Morphological Analysis	Statistical
Data sanitization for privacy preservati	P. Tambe; D. Vor	Online Social Networks (OSN	2016	IEEE	Social Network	User Generated Content (UG	Protecting Sensitive Information on	Unintended data disclosure	De-identification	Semantic Analysis & Morphol	Rule based & Statistical & NN
New Challenge of Protecting Privacy o	L. Xu; Y. Wu	k-Anonymity is a good way to	2016	IEEE	Other	User Generated Content (UG	protecting sensitive Information in u	Unintended data disclosure	De-identification / Obfuscating	Morphological Analysis	Rule based & Statistical
Obfuscating gender in social media wr	Reddy, Sravana;	The vast availability of textua	2016	Google Scholar	Social Network	User Generated Content (UG	Protecting Sensitive Information on	Profiling	Designing a gender obfuscati	Semantic Analysis	Rule based & Statistical & NN
Working at the web search engine side	Pàmies-Estrems	The popularity of Web Search	2016	Google Scholar	Other	User Generated Content (UG	Privacy Preserving Information Sha	Unintended data disclosure	Designing a web search engi	Semantic Analysis	Statistical
Enforcing transparent access to privat	Viejo, Alexandre;	Social networks have becom	2016	ScienceDirect	Social Network	User Generated Content (UG	Protecting Sensitive Information on	Profiling	Detecting privacy-sensitive in	Semantic Analysis & Morphol	Statistical
PPMark: An Architecture to Generate I	de Pontes, DRG	Layman and non-layman use	2016	Web of Science	Law	Privacy Policies	Ease the comprehension of Privacy	Complexity of Privacy Policies	Generation of Artefacts based	Morphological Analysis	Statistical
If You Can't Measure It, You Can't Mar	M. Alohaly; H. Ta	Despite the best efforts of us	2016	IEEE	Law	Privacy Policies	Investigating the potential Privacy In	Handling of sensitive data by	Generation of Artefacts based	Semantic Analysis	Rule based & Statistical
Extracting keyword and keyphrase fro	Audich, Dhiren A	One of the key components o	2016	Google Scholar	Law	Privacy Policies	Ease the comprehension of Privacy	Complexity of Privacy Policies	Information Extraction from pr	Semantic Analysis	Statistical
Automatic Summarization of Privacy P	Tomuro, N; Lytine	When customers purchase a	2016	Web of Science	Law	Privacy Policies	Paying more Attention to Privacy Po	Complexity of Privacy Policies	Information Extraction from pr	Semantic Analysis	NN
Ambiguity in Privacy Policies and the I	Reidenberg, JR;	Website privacy policies ofter	2016	Web of Science	Law	Privacy Policies	Ease the comprehension of Privacy	Complexity of Privacy Policies	Mapping of Ambiguity on a sc	Semantic Analysis	Rule based & Statistical
Personal privacy protection in time of t	Sokolova, Marina	Personal privacy protection in	2016	Google Scholar	Other	patient health information (PHI	protecting sensitive Information in u	Data Linkage	Overview of Challenges and a	Semantic Analysis	Statistical
Privacy-preserving sound to degrade a	Hashimoto, Kei;	In this paper, a privacy protec	2016	Google Scholar	General	Speech Data	Voice protection in public	Identification	Speech De-Identification	Speech Processing	Statistical
A Privacy Guard Service	X. Ye; F. Wang	Mobile devices are changing	2017	IEEE	Other	complex sensitive information	protecting sensitive Information in u	Unintended data disclosure	Automatic Conversion of sens	Speech Processing & Seman	Statistical
A cascaded approach for Chinese clin	Jian, Z; Guo, XS	With rapid adoption of Electro	2017	Web of Science	Medicine	patient health information (PHI	Privacy Preserving Information Sha	Secondary use of unstructure	De-identification	Semantic Analysis	Rule based & Statistical
Semi-Automatic De-identification of Ho	I. Calapodescu; I	Patient medical records repre	2017	IEEE	Medicine	patient health information (PHI	Privacy Preserving Information Sha	Secondary use of unstructure	De-identification	Semantic Analysis	Statistical
De-Identification of Medical Narrative I	Foufi, V; Gaudet-	Maintaining data security and	2017	Web of Science	Medicine	patient health information (PHI	Privacy Preserving Information Sha	Secondary use of unstructure	De-identification	Morphological Analysis	Rule based
The UAB Informatics Institute and 201	Bui, DDA; Wyatt,	Clinical narratives (the text no	2017	Web of Science	Medicine	patient health information (PHI	Privacy Preserving Information Sha	Secondary use of unstructure	De-identification	Morphological Analysis	Rule based
De-identification of medical records us	Jiang, Zhipeng; Z	The CEGS N-GRID 2016 Sha	2017	ScienceDirect	Medicine	patient health information (PHI	protecting patient privacy in unstruc	Secondary use of unstructure	De-identification	Semantic Analysis	Statistical & NN
A natural language processing challen	Uzuner, Ozlem;	Stubbs, Amber; Filannino, Mic	2017	Google Scholar	Medicine	patient health information (PHI	protecting patient privacy in unstruc	Secondary use of unstructure	De-identification	Morphological Analysis	Rule based
PHIs (Protected Health Information) id	K. Rajput; G. Ch	To preserve patient confident	2017	IEEE	Medicine	patient health information (PHI	protecting patient privacy in unstruc	Secondary use of unstructure	De-identification	Semantic Analysis & Morphol	Rule based & Statistical & NN
Privacy-Aware Data Analysis Middlew	Thien-An Nguyer	Privacy preservation is an es	2017	Springer	Medicine	patient health information (PHI	Mining according to privacy policies	Disclosure of sensitive data fo	Designing Secure Views for p	Morphological Analysis	Rule based
Detecting Protected Health Informatio	Henriksson, A; K	To enable secondary use of h	2017	Web of Science	Medicine	patient health information (PHI	Privacy Preserving Information Sha	Secondary use of unstructure	Detecting privacy-sensitive in	Semantic Analysis	Statistical
Protecting privacy in the archives: Pre	T. Hutchinson	Natural language processing	2017	IEEE	General	complex sensitive information	Protecting Sensitive Information on	Sensitive Information in unstr	Detecting privacy-sensitive in	Semantic Analysis	Statistical
Social media data sensitivity and priva	A. Lokhande; S.	Now in these days the social	2017	IEEE	Social Network	User Generated Content (UG	Protecting Sensitive Information on	Unintended data disclosure	Detecting privacy-sensitive in	Semantic Analysis & Morphol	Statistical
An Evaluation of Constituency-Based	M. C. Evans; J. E	Requirements analysts can n	2017	IEEE	Law	Privacy Policies	Ease the comprehension of Privacy	Complexity of Privacy Policies	Detection of vagueness	Morphological Analysis	Rule based
Learning Data Privacy and Terms of S	M. Bahrami; M. S	People are using on daily bas	2017	IEEE	Law	Privacy Policies	Ease the comprehension of Privacy	Complexity of Privacy Policies	Information Extraction from pr	Semantic Analysis	Rule based
Large-scale readability analysis of priv	Fabian, Benjamir	Online privacy policies notify	2017	Google Scholar	Law	Privacy Policies	Paying more Attention to Privacy Po	Complexity of Privacy Policies	Information Extraction from pr	Semantic Analysis & Morphol	Statistical
Enhancing sensitivity classification wit	McDonald, Grah	Government documents mus	2017	Google Scholar	Other	Government Data	Privacy Preserving Information Sha	Sensitive Information in unstr	Semantic features using word	Semantic Analysis	NN
How Well Can WordNet Measure Priva	N. Zhu; M. Zhang	Privacy is a fundamental issu	2017	IEEE	General	User Generated Content (UG	Ease the automation process of priv	Compliance with Requiremen	Semantic Similarities Tool Co	Semantic Analysis	Statistical
Semantic Information Retrieval from P	Sicuranza, M; Es	This paper presents a novel a	2017	Web of Science	Medicine	patient health information (PHI	protecting patient privacy in unstruc	Disclosure of sensitive data fo	Semantic-centered Rules	Semantic Analysis	Statistical
Influence of speaker de-identification i	Lopez-Otero, Pa	Depression is a common mer	2017	Wiley	Medicine	Speech Data	Voice-Based Healthcare in a private	Identification	Speech De-Identification	Speech Processing & Morpho	Statistical
Voicemask: Anonymize and sanitize vo	Qian, Jianwei; D	Voice input has been tremen	2017	Google Scholar	Other	Speech Data	Voice-based Service in a private ma	Identification	Speech de-identification	Speech Processing	NN
A Data Purpose Case Study of Privacy	J. Bhatia; T. D. B	Privacy laws and internationa	2017	IEEE	Law	Privacy Policies	Ease the comprehension of Privacy	Misusage of Sensitive Informa	Suggestion of security and pr	Semantic Analysis	Statistical
Privacy Matters: Detecting Nocuous P	Baumer, FS; Gro	Consulting a physician was lo	2017	Web of Science	Medicine	patient health information (PHI	protecting patient privacy in unstruc	Identification	Unintended data disclosure	Semantic Analysis	Rule based
Privacy Preserving Information Sharin	Tian, Yuan;	Users share a large amount o	2018	Google Scholar	Law	Privacy Policies	Privacy Preserving Information Sha	Complexity of Privacy Policies	Automated Access Control	Semantic Analysis & Morphol	Rule based & Statistical & NN
Privacy and Security Issues Due to Pe	N. Chiluka; A. K.	The security and privacy issu	2018	IEEE	Mobile Application	User Generated Content (UG	Investigating the potential Privacy In	Handling of sensitive data by	Code-based privacy analysis	Semantic Analysis & Morphol	Rule based & Statistical & NN
FlowCog: Context-aware Semantics E	Pan, X; Cao, YZ;	Android apps having access	2018	Web of Science	Mobile Application	complex sensitive information	Investigating the potential Privacy In	Handling of sensitive data by	Code-based privacy analysis	Semantic Analysis & Morphol	Rule based & Statistical & NN

Document Title	Authors	Abstract	Year	Source	Generalized Dom	Generalized Data Category	(RQ1)Classification of Use Case	Generalized Privacy Issue(F	Generalized Privacy Issue S	Generalized Category of Ap	NLP Method
Finding Clues for Your Secrets: Semar	Nan, Yuhong; Ya	A long-standing challenge in	2018	Google Scholar	Mobile Application	User Generated Content (UGC	Investigating the potential Privacy Ir	Handling of sensitive data by	Code-based privacy analysis	Semantic Analysis & Morphol	Statistical
Protecting Privacy in the Archives: Sup	T. Hutchinson	This paper documents the ite	2018	IEEE	General	complex sensitive information	Annotations with Gold Standard	Sensitive Information in unstr	Collect annotated corpus	Semantic Analysis	Statistical
Query-Based Linked Data Anonymizat	Remy DelanauxA	We introduce and develop a	2018	Springer	Law	Privacy Policies	Privacy Preserving Information Sha	Data Linkage	De-identification	Semantic Analysis	Rule based
Redaction of Protected Health Informa	A. Madan; A. M.	This paper describes the de-i	2018	IEEE	Medicine	patient health information (PHI	Privacy Preserving Information Sha	Secondary use of unstructure	De-identification	Semantic Analysis	Statistical & NN
Numerical Age Variations within Clinic	D. Hanauer; Q. M	Many kinds of numbers and r	2018	IEEE	Medicine	patient health information (PHI	protecting patient privacy in unstruc	Secondary use of unstructure	De-identification	Semantic Analysis	Statistical
Processing Text for Privacy: An Inform	Natasha Fernanc	The problem of text documen	2018	Springer	Other	User Generated Content (UGC	protecting sensitive Information in u	Identification	De-identification / Obfuscating	Speech Processing	Statistical & NN
Privacy preserving, crowd sourced crir	Mohler, George;	Social sensing plays an impo	2018	Google Scholar	Social Network	User Generated Content (UGC	Privacy Preserving Information Sha	Identification	Designing a framework for sh	Semantic Analysis	Rule based & Statistical
Privacy preserving network security da	DeYoung, Mark E	An incessant rhythm of data l	2018	Google Scholar	General	complex sensitive information	Privacy Preserving Information Sha	Disclosure of sensitive Data	Desinging a system that supp	Semantic Analysis & Morphol	Rule based & Statistical
Detecting Complex Sensitive Informati	Jan NeerbekIra A	State-of-the-art sensitive info	2018	Springer	General	complex sensitive information	Protecting sensitive Information in u	Sensitive Information in unstr	Detecting privacy-sensitive in	Semantic Analysis	NN
Anonymization of Unstructured Data v	Fadi HassanJose	The anonymization of structu	2018	Springer	General	complex sensitive information	protecting sensitive Information in u	Unintended data disclosure	Detecting privacy-sensitive in	Semantic Analysis	Statistical
P-GENT: Privacy-preserving geocodin	Wang, Shuo; Sin	With the widespread prolifera	2018	Google Scholar	General	User-generated content (UGC	Protecting Sensitive Information on	Disclosure of sensitive data fo	Detection of Locations withou	Semantic Analysis & Morphol	Statistical
Towards an Application-Based Notion	M. M. Al Sobeihy	Detecting privacy leakage in A	2018	IEEE	Mobile Application	Privacy Policies & Code	Investigating the potential Privacy Ir	Complexity of Privacy Policies	Detection of potential pitfalls i	Semantic Analysis	Statistical & NN
An Investigation Into Android Run-Tim	G. L. Scoccia; S.	To protect the privacy of end	2018	IEEE	Mobile Application	User Generated Content (UGC	Investigating the potential Privacy Ir	Handling of sensitive data by	Detection of the Correlation b	Morphological Analysis	Statistical
Modeling Security and Privacy Require	Mai, PX; Goknil,	Context Modem internet-base	2018	Web of Science	Law	Privacy Policies	Definition of Privacy Requirements	Compliance with Requiremen	Generation of Artefacts based	Semantic Analysis	Statistical
SynthNotes: A Generator Framework f	E. Begoli; K. Bro	One of the key, emerging cha	2018	IEEE	Medicine	Synthetic Data Generation	Privacy Preserving Information Sha	Secondary use of unstructure	Generation of Synthetic Data	Morphological Analysis	Statistical
Email security level classification of im	Huang, Jen-Wei;	Email is far more convenient	2018	ScienceDirect	Other	User Generated Content (UGC	protecting sensitive Information in u	Unintended data disclosure	Information Extraction from E	Morphological Analysis	Statistical & NN
PrivacyGuide: Towards an Implementa	Tesfay, WB; Hofn	Nowadays Internet services h	2018	Web of Science	Law	Privacy Policies	Ease the comprehension of Privacy	Complexity of Privacy Policies	Information Extraction from pr	Semantic Analysis	Statistical
How Dangerous Permissions are Dec	Baalous, R; Poet	Google requires Android apps	2018	Web of Science	Law	Privacy Policies	Investigating the potential Privacy Ir	Complexity of Privacy Policies	Information Extraction from pr	Morphological Analysis	Statistical
RECIPE: Applying Open Domain Ques	Shvartzshanider,	We describe our experiences	2018	Web of Science	Law	Privacy Policies	Paying more Attention to Privacy Po	Compliance with Requiremen	Mapping Privacy Policies to C	Semantic Analysis	NN
KnIGHT: Mapping Privacy Policies to C	Najmeh Mousavi	Although the use of apps and	2018	Springer	Law	Privacy Policies	Paying more Attention to Privacy Po	Complexity of Privacy Policies	Mapping Privacy Policies to G	Semantic Analysis	NN
Stories unfold: Issues and challenges	Cinco, Jeffrey C;	An emerging trend in the cyb	2018	Google Scholar	Other	complex sensitive information	protecting sensitive Information in u	Unintended data disclosure	Overview over the research fi	Semantic Analysis	Statistical
PrivOnto: A semantic framework for th	Oltramari, A; Pira	Privacy policies are intended	2018	Web of Science	Law	Privacy Policies	Paying more Attention to Privacy Po	Complexity of Privacy Policies	Semantic Framework for the A	Semantic Analysis	Statistical
Semantic Incompleteness in Privacy P	J. Bhatia; T. D. B	Companies that collect perso	2018	IEEE	Law	Privacy Policies	Ease the comprehension of Privacy	Complexity of Privacy Policies	Semantic Incompleteness De	Semantic Analysis	Statistical
Semantic Inference from Natural Lang	Hosseini, MB	Mobile apps collect different	2018	Web of Science	Law	Privacy Policies	Ease the comprehension of Privacy	Complexity of Privacy Policies	Semantic Inference from Priva	Semantic Analysis	NN
Towards privacy-preserving speech da	Qian, Jianwei; Ha	Privacy-preserving data publi	2018	Google Scholar	General	Speech Data	Privacy Preserving Information Sha	Identification	Speech de-identification	Speech Processing & Morpho	Rule based & Statistical & NN
Towards Smart Citizen Security Based	J. Roa; G. Jacob	Citizen security is a fundame	2018	IEEE	General	Speech Data	protecting sensitive Information in u	Identification	Speech de-identification	Speech Processing	Statistical & NN
Extraction of Natural Language Requir	H. Guo; Ö. Kafali	We address the problem of e	2018	IEEE	Other	complex sensitive information	Definition of Privacy Requirements	Sensitive Information in unstr	Suggestion of security and pr	Semantic Analysis	NN
VACCINE: Using Contextual Integrity f	Shvartzshnaider,	Modern enterprises rely on D	2019	Web of Science	Law	Privacy Policies	Automated and Flexible Rule Enfor	Compliance with Requiremen	Automated Compliance Chec	Semantic Analysis	NN
Automatic Anonymization of Textual D	F. Hassan; D. Sá	Data sharing is key in a wide	2019	IEEE	General	complex sensitive information	Privacy Preserving Information Sha	Secondary use of unstructure	Automatic Anonymization of T	Semantic Analysis	NN
Revealing the unrevealed: Mining sma	Hatamian, M; Se	Popular smartphone apps ma	2019	Web of Science	Mobile Application	User Generated Content (UGC	Ease the comprehension of privacy	Complexity of Privacy Policies	Automatic Summarization of U	Semantic Analysis	Statistical
A Multilateral Privacy Impact Analysis	Majid HatamianN	Smartphone apps have the p	2019	Springer	Law	Privacy Policies	Investigating the potential Privacy Ir	Complexity of Privacy Policies	Code-based privacy analysis	Semantic Analysis	Statistical
ESARA: A Framework for Enterprise S	Hatamian, M; Pa	Protecting enterprise's confid	2019	Web of Science	Mobile Application	complex sensitive information	Investigating the potential Privacy Ir	Handling of sensitive data by	Code-based privacy analysis	Semantic Analysis	Statistical
The case for a gdpr-specific annotated	Gallé, Matthias;	In this position paper we anal	2019	Google Scholar	Law	Privacy Policies	Annotation Revision	Complexity of Privacy Policies	Collect annotated corpus	Semantic Analysis & Morphol	Rule based
On GDPR Compliance of Companies'	Nicolas M. Mülle	We introduce a data set of pr	2019	Springer	Law	Privacy Policies	Collection of Privacy Policies	Complexity of Privacy Policies	Collect annotated corpus	Semantic Analysis	Statistical & NN
Towards privacy preserving unstructur	Mehta, B; Rao, U	Various sources and sophistic	2019	Web of Science	General	complex sensitive information	Privacy Preserving Information Sha	Data Linkage	De-identification	Semantic Analysis	Statistical
Named Entity Recognition in Clinical T	Changjian LiuJia	Clinical Named Entity Recogr	2019	Springer	Medicine	patient health information (PHI	Privacy Preserving Information Sha	Secondary use of unstructure	De-identification	Semantic Analysis	NN
Impact of De-Identification on Clinical	Obeid, JS; Heide	Clinical text de-identification	2019	Web of Science	Medicine	patient health information (PHI	Privacy Preserving Information Sha	Secondary use of unstructure	De-identification	Semantic Analysis & Morphol	Statistical & NN
An Extensible De-Identification Frame	Braghin, S; Bette	The volume of unstructured h	2019	Web of Science	Medicine	patient health information (PHI	Privacy Preserving Information Sha	Secondary use of unstructure	De-identification	Semantic Analysis & Morphol	Statistical & NN
A study of deep learning methods for c	Yang, X; Lyu, TC	Background: De-identification	2019	Web of Science	Medicine	patient health information (PHI	protecting patient privacy in unstruc	Secondary use of unstructure	De-identification	Semantic Analysis & Morphol	NN
Privacy- And utility-preserving textual a	Feyisetan O., Ba	Accurately learning from user	2019	SCOPUS	General	text location data	Mining according to privacy policies	Profiling	Designing a geo-indistinguish	Semantic Analysis	NN
Privacy Disclosures Detection in Natur	Mehdy, Nuhil; Ke	An increasing number of peo	2019	Google Scholar	Social Network	User Generated Content (UGC	Privacy Preserving Information Sha	Unintended data disclosure	Designing a methodology for	Semantic Analysis & Morphol	NN
iCAT: An Interactive Customizable Ano	Oqaily, M; Jarray	Today's data owners usually	2019	Web of Science	General	complex sensitive information	Ease the automation process of priv	Compliance with Requiremen	Designing a tailor-made data	Morphological Analysis	Rule based & Statistical & NN
Privacy in Text Documents	Dias, M; Ferreira	The process of sensitive data	2019	Web of Science	General	complex sensitive information	protecting sensitive Information in u	Sensitive Information in unstr	Detecting privacy-sensitive in	Semantic Analysis	Statistical
A DNS Tunneling Detection Method Ba	Jiacheng ZhangL	DNS tunneling is a typical DN	2019	Springer	Other	complex sensitive information	Protecting sensitive Information in u	Profiling	Detecting privacy-sensitive in	Semantic Analysis	NN
A Nlp-based Solution to Prevent from I	Canfora, G; Di S	Private and sensitive informa	2019	Web of Science	Social Network	User Generated Content (UGC	Protecting Sensitive Information on	Unintended data disclosure	Detecting privacy-sensitive in	Morphological Analysis	Rule based & Statistical & NN
Detecting Private Information in Large	De Luca, Pasqua	The violation of privacy, other	2019	Google Scholar	Social Network	User Generated Content (UGC	Protecting Sensitive Information on	Unintended data disclosure	Detecting privacy-sensitive in	Semantic Analysis	Statistical
Short Text, Large Effect: Measuring th	D. C. Nguyen; E.	Application markets streamlin	2019	IEEE	Mobile Application	User Generated Content (UGC	Investigating the potential Privacy Ir	Handling of sensitive data by	Detection of the Correlation b	Morphological Analysis	Statistical
PolicyLint: Investigating Internal Privac	Andow, B; Mahm	Privacy policies are the prima	2019	Web of Science	Law	Privacy Policies	Ease the comprehension of Privacy	Complexity of Privacy Policies	Generation of Artefacts based	Semantic Analysis & Morphol	Statistical & NN
Automatic Detection and Analysis of D	S. P. Nayak; S. R	Due to introduction of Genera	2019	IEEE	Law	Privacy Policies	Automated and Flexible Rule Enfor	Compliance with Requiremen	Information Extraction from pr	Semantic Analysis	Rule based
Natural language processing for mobil	Story, Peter; Zim	Many Internet services collec	2019	Google Scholar	Law	Privacy Policies	Ease the comparison of Privacy Po	Compliance with Requiremen	Information Extraction from pr	Semantic Analysis	Statistical
Automated and Personalized Privacy I	Cheng ChangHu	Along with the popularity of m	2019	Springer	Law	Privacy Policies	Ease the comprehension of Privacy	Complexity of Privacy Policies	Information Extraction from pr	Semantic Analysis	NN
Quantifying the effect of in-domain dis	Kumar, Vinayshe	Privacy policies are documen	2019	Google Scholar	Law	Privacy Policies	Ease the comprehension of Privacy	Complexity of Privacy Policies	Information Extraction out of P	Semantic Analysis	Statistical & NN

Document Title	Authors	Abstract	Year	Source	Generalized Dom	Generalized Data Category	(RQ1)Classification of Use Case	Generalized Privacy Issue(P	Generalized Privacy Issue S	Generalized Category of Ap	NLP Method
Adapting State-of-the-Art Deep Langu	Zhou, LY; Suomi	Background: Deep learning (	2019	Web of Science	Medicine	patient health information (PHI	protecting patient privacy in unstruc	Secondary use of unstructure	Overview of Challenges and a	Semantic Analysis	NN
Towards a Privacy Compliant Cloud Ar	Blohm, M; Dukin	Natural language processing	2019	Web of Science	General	complex sensitive information	Automated and Flexible Rule Enforc	Compliance with Requiremen	Overview of challenges of wo	Semantic Analysis	NN
Privacy-preserving social media forens	Naqvi, Syed; En	Social media is extensively u	2019	Google Scholar	Social Network	User Generated Content (UG	Protecting Sensitive Information on	Disclosure of sensitive data fo	Semantic Analysis of social m	Speech Processing & Seman	Statistical
Identifying incompleteness in privacy p	Bhatia, J; Evans,	Companies that collect perso	2019	Web of Science	Law	Privacy Policies	Ease the comprehension of Privacy	Complexity of Privacy Policies	Semantic Incompleteness De	Semantic Analysis & Morphol	Statistical
Deep Reinforcement Learning-based T	Mosallanezhad, A	User-generated textual data i	2019	Google Scholar	General	Use of third party / sharing ser	Privacy Preserving Information Sha	Unintended data disclosure	Semantic-based text pertubat	Semantic Analysis	NN
Speech sanitizer: Speech content des	Qian, Jianwei; D	Voice input users' speech rec	2019	Google Scholar	General	Speech Data	Voice-based Service in a private ma	Profiling	Speech De-Identification	Speech Processing & Morpho	Rule based & Statistical
An AI-assisted Approach for Checking	D. Torre; S. Abua	Privacy policies are critical fo	2020	IEEE	Law	Privacy Policies	Ease the compliance process throu	Compliance with Requiremen	Automated Compliance Chec	Semantic Analysis	Statistical & NN
Establishing a Strong Baseline for Priv	Najmeh Mousavi	Digital service users are routi	2020	Springer	Law	Privacy Policies	Paying more Attention to Privacy Po	Complexity of Privacy Policies	Automated Privacy Policy Cla	Semantic Analysis	Statistical
A Comparative Study of Sequence Cla	Lindner, Zachary	Privacy policies are legal doc	2020	Google Scholar	Law	Privacy Policies	Ease the comprehension of Privacy	Complexity of Privacy Policies	Automated Privacy Policy Co	Semantic Analysis	Statistical & NN
Code Element Vector Representations	Heaps, John;	The increasing popularity of r	2020	Google Scholar	Law	User Generated Content (UG	Automated and Flexible Rule Enforc	Compliance with Requiremen	Code-based privacy analysis	Semantic Analysis	NN
Correlating UI Contexts with Sensitive	J. Liu; D. He; D.	The Android framework provi	2020	IEEE	Mobile Application	complex sensitive information	Investigating the access legitimacy	Complexity of Privacy Policies	Code-based privacy analysis	Semantic Analysis	Statistical
Enhanced Privacy and Data Protection	F. Martinelli; F. M	Artificial Intelligence systems	2020	IEEE	Law	complex sensitive information	Annotation Collection	Sensitive Information in unstr	Collect annotated corpus	Semantic Analysis & Morphol	NN
From Prescription to Description: Map	POPLAVSKA, El	The European Union's Gener	2020	Google Scholar	Law	Privacy Policies	Annotations for research acceleratic	Complexity of Privacy Policies	Collect annotated corpus	Morphological Analysis	Rule based
Privacy Policies over Time: Curation a	Amos, Ryan; Aca	Automated analysis of privac	2020	Google Scholar	Law	Privacy Policies	Collection of Privacy Policies	Complexity of Privacy Policies	Collect annotated corpus	Morphological Analysis	Rule based
Crosslingual named entity recognition	Catelli, Rosario;	The COrona VIrus Disease 1	2020	ScienceDirect	Medicine	patient health information (PHI	Privacy Preserving Information Sha	Secondary use of unstructure	De-identification	Semantic Analysis	NN
Detecting Protected Health Information	B. Singh; Q. Sun	Clinical narratives host vast a	2020	IEEE	Medicine	patient health information (PHI	Privacy Preserving Information Sha	Secondary use of unstructure	De-identification	Semantic Analysis	NN
N-Sanitization: A semantic privacy-pre	Iwendi, Celestine	The introduction and rapid gr	2020	Google Scholar	Medicine	patient health information (PHI	Privacy Preserving Information Sha	Secondary use of unstructure	De-identification	Semantic Analysis	Rule based & Statistical & NN
Using word embeddings to improve th	Abdalla, M; Abda	Objective: In this work, we int	2020	Web of Science	Medicine	patient health information (PHI	protecting patient privacy in unstruc	Secondary use of unstructure	De-identification	Morphological Analysis	Rule based & NN
An Embedding-based Medical Note De	H. Zhou; D. Ruan	Medical note de-identification	2020	IEEE	Medicine	patient health information (PHI	protecting patient privacy in unstruc	Secondary use of unstructure	De-identification	Semantic Analysis	NN
Privacy guarantees for de-identifying t	Adelani, David If	Machine Learning approache	2020	Google Scholar	Medicine	complex sensitive information	protecting sensitive Information in u	Misusage of Sensitive Informa	De-identification	Semantic Analysis & Morphol	NN
On divergence-based author obfuscati	Bevendorff, Jane	Authorship verification is the	2020	Google Scholar	Other	User Generated Content (UG	protecting sensitive Information in u	Profiling	De-identification / Obfuscating	Semantic Analysis	Statistical
Understanding the Potential Risks of S	Ü. Meteriz; N. Fa	The extensive use of smartph	2020	IEEE	Law	complex sensitive information	Investigating the potential Privacy In	Complexity of Privacy Policies	Demonstration of Threats	Semantic Analysis	Statistical & NN
DatashareNetwork: A Decentralized Pr	Edalatnejad, Kas	Investigative journalists colle	2020	Google Scholar	Other	User-Centric Privacy Guidanc	Searching in a private manner	Identification	Designing a decentralized pe	Morphological Analysis	Statistical & NN
Assuring privacy-preservation in minin	Ma, Bo; Wu, Jins	Currently, there is a very larg	2020	Google Scholar	Medicine	patient health information (PHI	protecting patient privacy in unstruc	Secondary use of unstructure	Designing a privacy preserve	Semantic Analysis	NN
TIPRDC: task-independent privacy-res	Li, Ang; Duan, Yi	The success of deep learning	2020	Google Scholar	Social Network	User Generated Content (UG	Privacy Preserving Information Sha	Misusage of Sensitive Informa	Designing a task-independen	Semantic Analysis	NN
Preserving Privacy in Analyses of Text	Diethe, Tom; Fey	Amazon prides itself on being	2020	Google Scholar	General	Use of third party / storing/sen	Mining according to privacy policies	Disclosure of sensitive data fo	Designing a text perturbation	Semantic Analysis	NN
Privacy and Utility Trade-Off for Textua	Jingye TangTian	In recent years, the problem	2020	Springer	Other	User Generated Content (UG	protecting sensitive Information in u	Disclosure of sensitive data fo	Designing a text perturbation	Semantic Analysis	NN
A User-Centric and Sentiment Aware R	Nuhil Mehdy, AK	Data and information privacy	2020	Google Scholar	Social Network	User Generated Content (UG	Privacy Preserving Information Sha	Unintended data disclosure	Designing A User-Centric Priv	Semantic Analysis	NN
Research on Intelligent Security Prote	H. Yang; L. Huan	Based on the analysis of the	2020	IEEE	Other	Government Data	Privacy Preserving Information Sha	Unintended data disclosure	Detecting privacy-sensitive in	Semantic Analysis	Rule based & Statistical & NN
Using Natural Language Processing to	Silva, P; Goncalv	As information systems deal	2020	Web of Science	Law	Privacy Policies	Protecting sensitive Information in u	Complexity of Privacy Policies	Detecting privacy-sensitive in	Semantic Analysis	Rule based & Statistical & NN
Tweet Classification Using Deep Learn	R. GeethaS. Kar	Twitter is one of the most suc	2020	Springer	Social Network	User Generated Content (UG	Protecting Sensitive Information on	Unintended data disclosure	Detecting privacy-sensitive in	Semantic Analysis	Statistical & NN
Using NLP and Machine Learning to D	Silva, Paulo; Gon	Privacy concerns are constan	2020	Google Scholar	Law	complex sensitive information	Protecting Sensitive Information on	Sensitive Information in unstr	Detection of Data Privacy Vio	Semantic Analysis & Morphol	Rule based & Statistical & NN
On the Blockchain-Based Decentralize	R. Doku; D. B. R	It is human nature to anticipa	2020	IEEE	General	Data set containing sensitive i	Privacy Preserving Information Sha	Disclosure of sensitive Data	Encryption based on Events	Semantic Analysis & Morphol	NN
Privacy Policy Classification with XLNe	Mustapha, Majd;	Popularization of privacy poli	2020	Google Scholar	Law	Privacy Policies	Ease the comprehension of Privacy	Complexity of Privacy Policies	Generation of Artefacts based	Semantic Analysis & Morphol	NN
Privacy-Preserving Data Generation a	Shuo WangLingj	In this paper, we propose a p	2020	Springer	General	User Generated Content (UG	Privacy Preserving Information Sha	Identification	Generation of Synthetic Data	Semantic Analysis & Morphol	NN
Generation and evaluation of artificial	Ive, Julia; Viani,	A serious obstacle to the dev	2020	Google Scholar	Medicine	patient health information (PHI	Privacy Preserving Information Sha	Secondary use of unstructure	Generation of Synthetic Data	Semantic Analysis	NN
Differential Privacy and Natural Langu	Panchal, Kunjal;	Honey Encryption is an appro	2020	Google Scholar	Other	User Generated Content (UG	Searching in a private manner	Profiling	Generation of Synthetic Data	Semantic Analysis	NN
PolicyQA: A Reading Comprehension	Ahmad, Wasi Ud	Privacy policy documents are	2020	Google Scholar	Law	Privacy Policies	Ease the comprehension of Privacy	Complexity of Privacy Policies	Information Extraction from pr	Semantic Analysis	NN
Surfacing Privacy Settings Using Sem	Khandelwal, Rish	Online services utilize privacy	2020	Google Scholar	Other	complex sensitive information	Paying more Attention to Privacy Po	Complexity of Privacy Policies	Information Extraction from pr	Semantic Analysis	Statistical
Lucene-P2: A Distributed Platform for I	Uplavikar, Nitish;	Information retrieval (IR) play	2020	Google Scholar	Other	Query Data	Searching in a private manner	Profiling	Information Extraction if inforr	Semantic Analysis	Rule based
Chatbot Security and Privacy in the Ag	W. Ye; Q. Li	The rise of personal assistant	2020	IEEE	Other	Speech Data	Voice-based Assistance in a privacy	Unintended data disclosure	Overview of existing dialogue	None	None
A Survey on Privacy-Preserving Data I	Yang, Yunlu; Zho	In recent years, the increase	2020	Google Scholar	Other	complex sensitive information	Mining according to privacy policies	Profiling	Overview over the research fi	None	None
Data Leakage Detection and Preventio	Suvendu Kumar	Disclosure of confidential dat	2020	Springer	Other	complex sensitive information	protecting sensitive Information in u	Data Linkage	Overview over the research fi	None	None
Enhancing Privacy Preservation in Sp	Zhang, Guanglin	In speech data publishing, us	2020	Google Scholar	General	Speech Data	Privacy Preserving Information Sha	Profiling	Speech de-identification	Speech Processing	Statistical & NN
Privacy-Enhanced Emotion Recognitio	M. ThenmozhiK.	Speech recognition also knov	2020	Springer	Medicine	Speech Data	Voice-Based Healthcare in a private	Identification	Speech De-Identification	Speech Processing	NN
Exploiting Privacy-preserving Voice Q	T. Altuwaiyan; M.	Voice Assistant Systems (VAS	2020	IEEE	Medicine	Speech Data	Voice-Based Healthcare in a private	Profiling	Speech De-Identification	Speech Processing & Morpho	Statistical
Speaker Anonymization for Personal I	Yoo, IC; Lee, K;	As speech-based user interfa	2020	Web of Science	General	Speech Data	Voice-based Service in a private ma	Identification	Speech De-Identification	Speech Processing	NN
Voice-indistinguishability: Protecting v	Han, Yaowei; Li,	With the development of sma	2020	Google Scholar	Other	Speech Data	Voice-based Service in a private ma	Identification	Speech De-Identification	Speech Processing	Statistical & NN
Privacy-Enabled Smart Home Framew	Singh, Deepika;	Smart home environment pla	2020	Google Scholar	Other	Speech Data	Voice-based Service in a private ma	Profiling	Speech De-Identification	Speech Processing	NN
Anonymization for the GDPR in the Co	Francopoulo, Gil	The General Data Protection	2020	Google Scholar	Law	Privacy Policies	Ease the automation process of priv	Compliance with Requiremen	Suggestion of security and pr	None	None
A Machine Learning Based Methodolo	Beniamino Di Ma	Textual resources annotation	2021	Springer	Law	complex sensitive information	Annotation Automatization	Sensitive Information in unstr	Collect annotated corpus	Semantic Analysis & Morphol	NN
A Novel COVID-19 Data Set and an Ef	R. Catelli; F. Gar	In the last years, the need to	2021	IEEE	Medicine	patient health information (PHI	Annotation Collection	Annotations and their Quality	Collect annotated corpus	Semantic Analysis	NN

Document Title	Authors	Abstract	Year	Source	Generalized Dom	Generalized Data Category	(RQ1)Classification of Use Case	Generalized Privacy Issue(F	Generalized Privacy Issue S	Generalized Category of Ap	NLP Method
Combining contextualized word repres	Catelli, Rosario;	Clinical de-identification aims	2021	ScienceDirect	Medicine	patient health information (PHI	Privacy Preserving Information Sha	Secondary use of unstructure	De-identification	Semantic Analysis	NN
A deep reinforcement learning model f	Ahmed, Usman;	User-generated textual data i	2021	Google Scholar	Other	User Generated Content (UGC	protecting sensitive Information in u	Misusage of Sensitive Informa	De-identification / Obfuscating	Semantic Analysis	NN
A Conceptual Framework for Sensitive	Nancy VictorDap	Big data can be referred to as	2021	Springer	Social Network	User Generated Content (UGC	Privacy Preserving Information Sha	Unintended data disclosure	Designing a Big Data Framew	Semantic Analysis	Statistical
Artificial Empathy for Clinical Compani	Miguel Vargas M	We present a prototype wher	2021	Springer	Medicine	Speech Data	Voice-Based Healthcare in a private	Unintended data disclosure	Designing a locally deployed	Speech Processing	NN
Toward a Privacy Guard for Cloud-Bas	Radja Boukharro	The Internet of Things is a tec	2021	Springer	Other	Speech Data	Voice-based Assistance in a privacy	Disclosure of sensitive Data	Designing a Privacy Guard fo	Speech Processing & Morpho	NN
Context-Rich Privacy Leakage Analysi	Y. Luo; L. Cheng	Emerging Internet of Things (	2021	IEEE	Other	complex sensitive information	Investigating the potential Privacy In	Handling of sensitive data by	Detecting privacy-sensitive in	Semantic Analysis	Statistical & NN
An OOV Recognition Based Approach	Xiao LiangNingy	Sensitive word recognition te	2021	Springer	Other	complex sensitive information	Protecting sensitive Information in u	Unintended data disclosure	Detecting privacy-sensitive in	Semantic Analysis	NN
A Method for Generating Synthetic Ele	J. Guan; R. Li; S	Machine learning (ML) and N	2021	IEEE	Medicine	Synthetic Data Generation	Privacy Preserving Information Sha	Secondary use of unstructure	Generation of Synthetic Data	Semantic Analysis	NN
Exsense: Extract sensitive information	Guo, Yongyan; L	Large-scale sensitive informa	2021	ScienceDirect	General	complex sensitive information	protecting sensitive Information in u	Sensitive Information in unstr	Information Extraction from la	Semantic Analysis	NN
Analysis of gender and identity issues	Lopez-Otero, Pa	Research in the area of autor	2021	ScienceDirect	Medicine	Speech Data	Voice-Based Healthcare in a private	Identification	Speech De-Identification	Speech Processing	NN
Semantic knowledge and privacy in th	Das P.K., Kashya	In the past few years, the Inte	2016	SCOPUS	Law	Privacy Policies	Automated and Flexible Rule Enfor	Compliance with Requiremen	Automated Compliance Chec	Morphological Analysis	Rule based & Statistical & NN
VerHealth: Vetting Medical Voice Appli	Shezan, Faysal H	Healthcare applications on Ve	2020	ACM	Medicine	Speech Data	Voice-Based Healthcare in a private	Compliance with Requiremen	Automated Privacy Assessme	Semantic Analysis & Morphol	Rule based & NN
Privacy-aware text rewriting	Xu Q., Qu L., Xu	Biased decisions made by au	2019	SCOPUS	Other	User Generated Content (UGC	protecting sensitive Information in u	Handling of sensitive data by	Automated Rewriting	Semantic Analysis	Statistical & NN
Towards integrating the FLG framewor	Rabinia A., Drag	Automatic modeling of privacy regulation		SCOPUS	Law	Privacy Policies	Automatic modeling of privacy regu	Complexity of Privacy Policies	Automatic modeling of privacy	Semantic Analysis & Morphol	Rule based & Statistical & NN
Usable privacy and security for person	Karat C.-M., Bro	IBM T.J. Watson Research C	2006	SCOPUS	Law	Privacy Policies	Automated and Flexible Rule Enfor	Compliance with Requiremen	Automatic policy enforcement	Semantic Analysis	Rule based
Automatic policy enforcement on sema	Nguyen T.-V.T., F	Web-based data collection of	2015	SCOPUS	Law	Privacy Policies	Automated and Flexible Rule Enfor	Compliance with Requiremen	Automatic policy enforcement	Semantic Analysis	NN
On privacy preservation in text and do	Olsson F.	The preservation of the privac	2009	SCOPUS	General	complex sensitive information	Annotation Process Support	Complexity of Privacy Policies	Collect annotated corpus	Semantic Analysis	Rule based
A framenet for cancer information in cl	Roberts K., Si Y.	This paper presents a pilot pr	2018	SCOPUS	Medicine	patient health information (PHI	Annotations for research acceleratio	Secondary use of unstructure	Collect annotated corpus	Semantic Analysis	Statistical & NN
Analyzing Privacy Policies at Scale: Fr	Wilson, Shomir;	Website privacy policies are c	2018	ACM	Law	Privacy Policies	Ease the comprehension of Privacy	Complexity of Privacy Policies	Collect annotated corpus	Morphological Analysis	Statistical
A Large Publicly Available Corpus of W	Zaeem, Razieh N	Studies have shown website	2021	Google Scholar	Law	Privacy Policies	Ease the comprehension of Privacy	Complexity of Privacy Policies	Collect annotated corpus	Semantic Analysis	Statistical
Question answering for privacy policie	Ravichander A.,	Privacy policies are long and	2019	SCOPUS	Law	Privacy Policies	Paying more Attention to Privacy Po	Complexity of Privacy Policies	Collect annotated corpus	Morphological Analysis	Rule based & NN
An emerging strategy for privacy prese	Rashid F., Miri A.	Data De-identification and Di	2020	SCOPUS	Medicine	complex sensitive information	Mining according to privacy policies	Disclosure of sensitive data fo	De-identification	Morphological Analysis	Statistical
Anonimytext: Anonimization of unstruc	Perez-Lainez R.,	The anonymization of unstruc	2009	SCOPUS	Medicine	patient health information (PHI	Mining according to privacy policies	Sensitive Information in unstr	De-identification	Morphological Analysis	Rule based
Secure secondary use of clinical data	Christoph J., Grie	Objectives: The secondary us	2015	SCOPUS	Medicine	patient health information (PHI	Privacy Preserving Information Sha	Secondary use of unstructure	De-identification	Morphological Analysis	Statistical & NN
Anonymization of sensitive information	Saluja B., Kumar	Due to privacy constraints, cl	2019	SCOPUS	Medicine	patient health information (PHI	Privacy Preserving Information Sha	Secondary use of unstructure	De-identification	Semantic Analysis	NN
De-identification of free-text medical re	Johnson A.E.W.,	The ability of caregivers and	2020	SCOPUS	Medicine	patient health information (PHI	Privacy Preserving Information Sha	Secondary use of unstructure	De-identification	Semantic Analysis	NN
NLNDE: The neither-language-nor-dor	Lange L., Adel H	Natural language processing	2020	SCOPUS	Medicine	patient health information (PHI	Privacy Preserving Information Sha	Secondary use of unstructure	De-identification	Semantic Analysis	NN
Sensitive data detection and classifica	García-Pablos A.	Massive digital data processi	2020	SCOPUS	Medicine	patient health information (PHI	Privacy Preserving Information Sha	Secondary use of unstructure	De-identification	Semantic Analysis	NN
Developing a standard for de-identifyir	Velupillai S., Dali	Background: Electronic patie	2009	SCOPUS	Medicine	patient health information (PHI	Privacy Preserving Information Sha	Secondary use of unstructure	De-identification	Semantic Analysis	Rule based & Statistical
Evaluation of PHI Hunter in Natural La	Redd A., Pickard	OBJECTIVES: We introduce	2015	SCOPUS	Medicine	patient health information (PHI	Privacy Preserving Information Sha	Secondary use of unstructure	De-identification	Semantic Analysis	Statistical
Generalizability and comparison of aut	Ferrández O., Sc	In this paper, we present an e	2012	SCOPUS	Medicine	patient health information (PHI	Privacy Preserving Information Sha	Secondary use of unstructure	De-identification	Semantic Analysis	Statistical
A deep learning-based system for the	Jiang D., Shen Y	Due to privacy constraints, de	2019	SCOPUS	Medicine	patient health information (PHI	Privacy Preserving Information Sha	Secondary use of unstructure	De-identification	Semantic Analysis	Statistical & NN
Automatic de-identification of medical	Marimon M., Gor	There is an increasing interes	2019	SCOPUS	Medicine	patient health information (PHI	Privacy Preserving Information Sha	Secondary use of unstructure	De-identification	Semantic Analysis	Statistical & NN
Technical Note: An embedding-based	Zhou, Hanyue; R	Purpose Medical note de-iden	2021	Wiley	Medicine	patient health information (PHI	Privacy Preserving Information Sha	Secondary use of unstructure	De-identification	Semantic Analysis	Rule based & Statistical & NN
Protected health information recognitio	Colón-Ruiz C., S	Medical records contain relev	2019	SCOPUS	Medicine	patient health information (PHI	Privacy Preserving Information Sha	Secondary use of unstructure	De-identification	Semantic Analysis	Statistical & NN
Utility-preserving privacy protection of	Sánchez D., Bat	The adoption of ITs by medic	2014	SCOPUS	Medicine	patient health information (PHI	Privacy Preserving Information Sha	Secondary use of unstructure	De-identification	Semantic Analysis & Morphol	Statistical
A machine learning based approach to	Du L., Xia C., De	Background: With the increas	2018	SCOPUS	Medicine	patient health information (PHI	Privacy Preserving Information Sha	Secondary use of unstructure	De-identification	Semantic Analysis & Morphol	Statistical
A patient like me - An algorithm-based	Koren G., Souro	To date, consumer health too	2019	SCOPUS	Medicine	patient health information (PHI	Privacy Preserving Information Sha	Secondary use of unstructure	De-identification	Semantic Analysis & Morphol	Statistical
De-identifying Swedish Ehr text using	Chomutare T., Yi	Sensitive data is normally req	2020	SCOPUS	Medicine	patient health information (PHI	protecting patient privacy in unstruc	Secondary use of unstructure	De-identification	Semantic Analysis	NN
Data Science and Natural Language P	Vydiswaran V.G.	In the past decade, a growing	2021	SCOPUS	Medicine	patient health information (PHI	protecting patient privacy in unstruc	Secondary use of unstructure	De-identification	Semantic Analysis	NN
Deidentification of free-text medical re	Johnson A.E.W.,	The ability of caregivers and	2020	SCOPUS	Medicine	patient health information (PHI	protecting patient privacy in unstruc	Secondary use of unstructure	De-identification	Semantic Analysis	NN
De-identification of psychiatric intake r	Stubbs A., Filann	The 2016 CEGS N-GRID sha	2017	SCOPUS	Medicine	patient health information (PHI	protecting patient privacy in unstruc	Secondary use of unstructure	De-identification	Semantic Analysis & Morphol	Rule based & Statistical & NN
A Privacy-Preserving Natural Languag	Pinto, Jeffrey Ag	Automated clinical informatio	2018	Google Scholar	Medicine	patient health information (PHI	protecting patient privacy in unstruc	Secondary use of unstructure	De-identification	Semantic Analysis & Morphol	Statistical & NN
The pattern of name tokens in narrativ	Kayaalp M., Brov	Objective: To understand the	2014	SCOPUS	Medicine	patient health information (PHI	protecting patient privacy in unstruc	Secondary use of unstructure	De-identification	Semantic Analysis & Morphol	Rule based
De-identification of emails: Pseudonym	Eder E., Krieg-H	We deal with the pseudonym	2019	SCOPUS	Social Network	User Generated Content (UGC	protecting patient privacy in unstruc	Identification	De-identification	Semantic Analysis	Statistical
Personal information privacy: What's r	Hammoud K., Be	In recent events, user-privacy	2019	SCOPUS	Medicine	patient health information (PHI	protecting sensitive Information in u	Misusage of Sensitive Informa	De-identification	Semantic Analysis	Rule based & Statistical & NN
Code Alltag 2.0 - A pseudonymized Ge	Eder E., Krieg-H	The vast amount of social co	2020	SCOPUS	Social Network	User Generated Content (UGC	Protecting Sensitive Information on	Unintended data disclosure	De-identification	Semantic Analysis	Rule based
Novel location de-identification for ma	Taguchi K., Aram	In recent years, the protectio	2018	SCOPUS	Social Network	User Generated Content (UGC	Protecting Sensitive Information on	Unintended data disclosure	De-identification	Semantic Analysis & Morphol	Statistical
Information leakage through documen	Lopresti D., Law	It has been recently demonst	2005	SCOPUS	General	complex sensitive information	protecting sensitive Information in u	Unintended data disclosure	De-identification / Obfuscating	Morphological Analysis	Statistical
Don't Let Google Know I'm Lonely	Aonghusa, P\'{o}	From buying books to finding	2016	ACM	Other	User Generated Content (UGC	Searching in a private manner	Profiling	De-identification / Obfuscating	Morphological Analysis	Statistical
LN-Annote: An alternative approach to	Jung Y.H., Strato	Personal mobile devices offe	2015	SCOPUS	Mobile Application	User Generated Content (UGC	protecting sensitive Information in u	Handling of sensitive data by	Designing a locally deployed	Semantic Analysis	NN
Distortion Search–A Web Search Priva	Mivule, Kato; Ho	Search engines have vast tec	2017	Google Scholar	Other	User Generated Content (UGC	Searching in a private manner	Profiling	Designing a privacy-preservin	Semantic Analysis	Statistical & NN

Document Title	Authors	Abstract	Year	Source	Generalized Dom	Generalized Data Category	(RQ1)Classification of Use Case	Generalized Privacy Issue(P	Generalized Privacy Issue S	Generalized Category of Ap	NLP Method
Towards query logs for privacy studies	Biega A.J., Schm	Detailed query histories often	2020	SCOPUS	Other	Query Data	Searching in a private manner	Profiling	Designing a scheme for a priv	Morphological Analysis	Statistical
Interactive Topic Search System Base	Chen, LC	In this paper, we develop an i	2020	Web of Science	General	User Generated Content (UGC	Searching in a private manner	Profiling	Designing a search tree witho	Morphological Analysis	Statistical
Design of an Inclusive Financial Privac	Akanfe, Oluwafe	Financial privacy is an import	2020	ACM	Other	Privacy Policies	Investigating the potential Privacy In	Complexity of Privacy Policies	Designing an Inclusive Financ	Semantic Analysis	Statistical
A Framework for Estimating Privacy R	Chang K.C., Zae	With the rapidly growing popu	2020	SCOPUS	Law	Privacy Policies	Investigating the potential Privacy In	Handling of sensitive data by	Detecting privacy-sensitive in	Morphological Analysis	Statistical
Aquilis: Using Contextual Integrity for I	Kumar, Abhishek	Smartphones are nowadays t	2020	ACM	Mobile Application	complex sensitive information	Investigating the potential Privacy In	Handling of sensitive data by	Detecting privacy-sensitive in	Semantic Analysis	Statistical
Detecting privacy-sensitive events in n	Jindal P., Gunter	In this paper, we present a nc	2014	SCOPUS	Medicine	patient health information (PHI	protecting patient privacy in unstruc	Secondary use of unstructure	Detecting privacy-sensitive in	Morphological Analysis	Rule based
Clustering Help-Seeking Behaviors in	Liang C., Abbott	Online Lesbian, Gay, Bisexua	2019	SCOPUS	Medicine	User Generated Content (UGC	Protecting Sensitive Information on	Identification	Detecting privacy-sensitive in	Morphological Analysis	Statistical
Detecting and editing privacy policy pit	Santos C., Gang	Privacy policies are the locus	2017	SCOPUS	Law	Privacy Policies	Paying more Attention to Privacy Po	Complexity of Privacy Policies	Detection of Inconsistencies v	Semantic Analysis	Statistical
Towards a multi-stage approach to det	Bäumer F.S., Ke	Physician Review Websites a	2018	SCOPUS	Medicine	patient health information (PHI	protecting patient privacy in unstruc	Profiling	Detection of Privacy Breaches	Semantic Analysis & Morphol	Statistical
Automated Detection of Privacy Sensit	Bouhaddou O., D	Care coordination across hea	2016	SCOPUS	Law	Privacy Policies	Privacy Preserving Information Sha	Compliance with Requiremen	Detection of Privacy Sensitive	Semantic Analysis	Rule based
Automatic detection of vague words ar	Lebanoff L., Liu F	Website privacy policies repre	2018	SCOPUS	Law	Privacy Policies	Ease the comprehension of Privacy	Complexity of Privacy Policies	Detection of vagueness	Semantic Analysis	NN
Mitigating file-injection attacks with nat	Liu H., Wang B.	Searchable Encryption can b	2020	SCOPUS	Other	Use of third party / storing/sen	Searching in a private manner	Profiling	Encryption-based search syst	Semantic Analysis & Morphol	Rule based & Statistical & NN
Automated Understanding Of Cloud Te	Papanikolaou, N	We argue in favour of a set o	2011	Google Scholar	Law	Privacy Policies	Automated and Flexible Rule Enforc	Compliance with Requiremen	Generation of Artefacts based	Semantic Analysis	Rule based & Statistical
Natural language processing of rules a	Papanikolaou N.	We discuss ongoing work on	2012	SCOPUS	Law	Privacy Policies	Automated and Flexible Rule Enforc	Compliance with Requiremen	Generation of Artefacts based	Semantic Analysis	Statistical
Mining Privacy Goals from Privacy Pol	Bhatia, Jaspreet;	Privacy policies describe high	2016	ACM	Law	Privacy Policies	Definition of Privacy Requirements	Compliance with Requiremen	Generation of Artefacts based	Semantic Analysis & Morphol	Statistical
An empirical study of natural language	Brodie C.A., Kara	Today organizations do not h	2006	SCOPUS	Law	Privacy Policies	Ease the implementation of written	Complexity of Privacy Policies	Generation of Artefacts based	Semantic Analysis	Rule based
Design of a Compliance Index for Priv	Akanfe O., Valec	Many nations have adopted c	2020	SCOPUS	Law	Privacy Policies	Measuring the Compliance of apps	Compliance with Requiremen	Generation of Artefacts based	Semantic Analysis	Statistical
Sharing copies of synthetic clinical cor	Lohr C., Buechel	The legal culture in the Europ	2018	SCOPUS	Medicine	patient health information (PHI	Privacy Preserving Information Sha	Secondary use of unstructure	Generation of Synthetic Data	Morphological Analysis	Rule based
Resilience of clinical text de-identified	Carrell D.S., Mal	Objective: Effective, scalable	2020	SCOPUS	Medicine	Synthetic Data Generation	Privacy Preserving Information Sha	Secondary use of unstructure	Generation of Synthetic Data	Semantic Analysis	Statistical
Challenges and opportunities beyond	Tayefi, Maryam;	Abstract Electronic health rec	2021	Wiley	Medicine	patient health information (PHI	protecting patient privacy in unstruc	Secondary use of unstructure	Generation of Synthetic Data	Semantic Analysis	NN
Applying language technology to nursi	Suominen H., Le	Objectives: The present study	2007	SCOPUS	Medicine	patient health information (PHI	protecting patient privacy in unstruc	Secondary use of unstructure	Information Extraction from nu	Semantic Analysis & Morphol	Rule based & Statistical
Chatbot for IT security training: Using	Gulenko I.	We conduct a pre-study with	2014	SCOPUS	General	complex sensitive information	Browsing in a private manner	Complexity of Privacy Policies	Information Extraction from pr	Semantic Analysis	NN
MyAdChoices: Bringing Tra	Parra-Arnau, Jav	The intrusiveness and the inc	2017	ACM	Other	complex sensitive information	Browsing in a private manner	Profiling	Information Extraction from pr	Semantic Analysis	Statistical
Pre-processing legal text: Policy parsir	Waterman K.K.	One of the most significant ch	2010	SCOPUS	Law	Privacy Policies	Ease the automation process of priv	Complexity of Privacy Policies	Information Extraction from pr	Semantic Analysis & Morphol	Rule based & Statistical & NN
Identifying the provision of choices in p	Sathyendra K.M.	Websites' and mobile apps' p	2017	SCOPUS	Law	Privacy Policies	Ease the comprehension of Privacy	Complexity of Privacy Policies	Information Extraction from pr	Morphological Analysis	Rule based & Statistical & NN
Polisis: Automated analysis and prese	Harkous H., Faw	Privacy policies are the prima	2018	SCOPUS	Law	Privacy Policies	Ease the comprehension of Privacy	Complexity of Privacy Policies	Information Extraction from pr	Semantic Analysis	Statistical & NN
Understanding Privacy Awareness in A	Feichtner J., Gru	Permissions are a key factor	2020	SCOPUS	Mobile Application	complex sensitive information	Investigating the permission usage	Complexity of Privacy Policies	Information Extraction from pr	Semantic Analysis	NN
PrivacyCheck: Automatic Summarizati	Zaeem, Razieh N	Prior research shows that onl	2018	ACM	Law	Privacy Policies	Paying more Attention to Privacy Po	Complexity of Privacy Policies	Information Extraction from pr	Semantic Analysis	NN
Automatic extraction of opt-out choice	Sathyendra K.M.	Online "notice and choice" is	2016	SCOPUS	Law	Privacy Policies	Paying more Attention to Privacy Po	Complexity of Privacy Policies	Information Extraction from pr	Semantic Analysis	Statistical
A step towards usable privacy policy: A	Liu F., Ramanath	With the rapid development o	2014	SCOPUS	Law	Privacy Policies	Ease the comprehension of Privacy	Complexity of Privacy Policies	Mapping of Privacy Policies to	Morphological Analysis	Statistical
The Effect of the GDPR on Privacy Po	Zaeem, Razieh N	The General Data Protection	2020	ACM	Law	Privacy Policies	Investigating the Impact of GDPR w	Complexity of Privacy Policies	Mapping Privacy Policies to G	Semantic Analysis	Rule based & Statistical
The role of vocabulary mediation to dis	Leone V., Di Car	To date, the effort made by ex	2020	SCOPUS	Law	Privacy Policies	Ease the comprehension of Privacy	Complexity of Privacy Policies	Mapping Privacy Policy Conte	Semantic Analysis & Morphol	NN
P2Onto: Making Privacy Policies Trans	Novikova E., Doy	The privacy issue is highly re	2020	SCOPUS	Law	Privacy Policies	Ease the comprehension of Privacy	Complexity of Privacy Policies	Ontology used for transparen	Semantic Analysis	Statistical
De-identification of unstructured clinica	Meystre S.M.	The adoption of Electronic He	2015	SCOPUS	Medicine	patient health information (PHI	protecting patient privacy in unstruc	Secondary use of unstructure	Overview of Challenges and a	None	None
Challenges in detecting privacy reveal	Tesfay W.B., Ser	This paper discusses the cha	2016	SCOPUS	Medicine	patient health information (PHI	protecting sensitive Information in u	Sensitive Information in unstr	Overview of challenges in det	None	None
GDPR privacy policies in CLAUDETTE	Liepin R., Contis	The latest developments in na	2019	SCOPUS	Law	Privacy Policies	Investigating the Impact of GDPR w	Complexity of Privacy Policies	Overview of Challenges of on	Semantic Analysis	Rule based
Data processing and text mining techn	Sun W., Cai Z., L	Currently, medical institutes g	2018	SCOPUS	Medicine	patient health information (PHI	protecting patient privacy in unstruc	Disclosure of sensitive data fo	Overview over the research fi	None	None
Deriving semantic models from privacy	Breaux T.D., Ante	Natural language policies des	2005	SCOPUS	Law	Privacy Policies	Ease the comparison of Privacy Po	Complexity of Privacy Policies	Semantic Model Creation bas	Semantic Analysis & Morphol	Statistical
Modeling language vagueness in priva	Liu F., Fella N.L.,	Website privacy policies are t	2016	SCOPUS	Law	Privacy Policies	Ease the comprehension of Privacy	Complexity of Privacy Policies	Semantic Modeling of langua	Semantic Analysis	NN
Opening public deliberations: Transpa	Bassi E., Leoni D	The open data movement is c	2013	SCOPUS	Other	Government Data	Privacy Preserving Information Sha	Unintended data disclosure	Semantic open source stack	Semantic Analysis & Morphol	Statistical
On the Suitability of Applying WordNet	Zhu N., Wang S.	Privacy protection is a fundar	2018	SCOPUS	General	User Generated Content (UGC	Ease the automation process of priv	Compliance with Requiremen	Semantic Similarities Tool Co	Semantic Analysis	Statistical
Enforcing vocabulary k-anonymity by s	Liu J., Wang K.	Web query logs provide a rich	2010	SCOPUS	General	Query Data	Searching in a private manner	Profiling	Semantic similarity based on	Semantic Analysis	Statistical
Mining rule semantics to understand le	Breaux T.D., Ante	Organizations in privacy-regu	2005	SCOPUS	Law	Privacy Policies	Ease the automation process of priv	Complexity of Privacy Policies	Semantics of Rules Mining	Semantic Analysis	Statistical
She Knows Too Much-Voice Comman	Furey E., Blue J.	Voice controlled Internet of Th	2018	SCOPUS	Other	Speech Data	Voice-based Service in a private ma	Profiling	Speech de-identification	Speech Processing	Rule based
Partakable technology	Osman N.	This paper proposes a shift in	2018	SCOPUS	Social Network	User Generated Content (UGC	Definition of Privacy Requirements	Sensitive Information in unstr	Suggestion of security and pr	Morphological Analysis	Rule based

A.1.2. NLP as a Privacy Threat Analysis Sheet

Document Title	Authors	Abstract	Year	Source	Domain	Data Type	Use Cases	Generalized Issue/Vulnerability sol	PETs(RQ2) 1
A Framework for Secure Speech Recognition	P. Smaragdis; I	We present an alg	2007	IEEE	General	Speech	Speech Recognition without Dis	Direct Disclosure of sensitive data for	Secure Multiparty Comp
Identity verification using voice and its use in a p	Çamlıkaya, Ere	Since security has	2008	Google Scholar	Medicine	Speech	Speech Verification without Disc	memorizability of NN	Obfuscation
Slice-based architecture for biometrics: Prototyp	B. K. Sy	This research inve	2009	IEEE	Medicine	Speech	Speech Verification without Disc	Direct Disclosure of sensitive data for	Secure Multiparty Comp
Privacy Preserving Techniques for Speech Proc	Pathak, M;	Speech is perhaps	2010	Google Scholar	General	Speech	Speech Processing without Disc	Direct Disclosure of sensitive data for	Differential Privacy (DP)
Privacy-preserving document similarity detectior	Khelik, Ksenia;	The document sim	2011	Google Scholar	General	Written	Similarity detection without Data	Information Disclosure by Statistical L	Homomorphic Encryptio
A Strategy for Deploying Secure Cloud-Based N	D. Carrell	Natural language	2011	IEEE	Medicine	Written	Classification without Data Disc	Direct Disclosure of sensitive data for	None
Privacy-preserving machine learning for speech	Pathak, Manas	Speech is one of t	2012	Google Scholar	General	Speech	Speech Processing without Disc	Direct Disclosure of sensitive data for	Homomorphic Encryptio
An Efficient and Secure Nonlinear Programming	Madhura, M; S	Cloud Computing	2012	Google Scholar	Cloud Computing	Written	Model Training without Sharing	memorizability of NN	Homomorphic Encryptio
Privacy-preserving speaker authentication	Pathak, Manas	Speaker authentic	2012	Google Scholar	General	Speech	Speech Verification without Disc	Direct Disclosure of sensitive data for	Obfuscation
HMM Based Privacy Preserving Approach for V	Prashantini, S;	Pre-processing of	2013	Google Scholar	General	Speech	Speech Communication without	Direct Disclosure of sensitive data for	Homomorphic Encryptio
Privacy-preserving speech processing: cryptogr	Pathak, Manas	Speech is one of t	2013	Google Scholar	General	Speech	Speech Processing without Disc	Direct Disclosure of sensitive data for	Homomorphic Encryptio
Collaborative search log sanitization: Toward dif	Hong, Yuan; Va	Severe privacy lea	2014	Google Scholar	Other	Written	Model Training without Sharing	Direct Disclosure of sensitive data for	Federated Learning & D
Privacy-preserving speaker verification using ga	Portêlo, José; I	In this paper we p	2014	Google Scholar	General	Speech	Speech Processing without Disc	Direct Disclosure of sensitive data for	Obfuscation
Privacy-preserving important passage retrieval	Marujo, Luís; P	State-of-the-art im	2014	Google Scholar	General	Written	Similarity detection without Data	exploitability of word embeddings	Obfuscation
A Federated Network for Translational Cancer R	Jacobson, RS;	Advances in canc	2015	Web of Science	Medicine	Written	Model Training without Sharing	Direct Disclosure of sensitive data for	Federated Learning
A Full-Text Retrieval Algorithm for Encrypted Da	Wei SongYihui	Nowadays, more a	2015	Springer	Cloud Computing	Written	Storing and Searching Data with	Direct Disclosure of sensitive data for	Homomorphic Encryptio
Privacy-preserving multi-document summarizati	Marujo, Luís; P	State-of-the-art ex	2015	Google Scholar	General	Written	Summarization without Docume	Information Disclosure by Statistical L	Obfuscation
Privacy-preserving frameworks for speech minir	Portêlo, José M	Security agencies	2015	Google Scholar	General	Speech	Speech Processing without Disc	Direct Disclosure of sensitive data for	Secure Multiparty Comp
Preserving privacy of encrypted data stored in c	Dharini, M; Sas	In cloud computin	2016	Google Scholar	Cloud Computing	Written	Storing and Searching Data with	Direct Disclosure of sensitive data for	Homomorphic Encryptio
Edit Distance Based Encryption and Its Applicati	Tran Viet Xuan	Edit distance, alsc	2016	Springer	Medicine	Written	Similarity detection without Data	Direct Disclosure of sensitive data for	Homomorphic Encryptio
Encrypted domain cloud-based speech noise re	M. A. Yakubu; I	During the acquisi	2016	IEEE	Cloud Computing	Speech	Storing and Searching Data with	Direct Disclosure of sensitive data for	Homomorphic Encryptio
Learning low-dimensional representations of me	Choi, Youngdu	We show how to l	2016	Google Scholar	General	Written	Privacy-Utility-Trade-off for Wor	exploitability of word embeddings	Obfuscation
Efficient and Privacy-Preserving Voice-Based Se	M. Hadian; T. A	In-home IoT devic	2017	IEEE	Medicine	Speech	Speech Processing without Disc	Direct Disclosure of sensitive data for	Homomorphic Encryptio
Privacy Preserving Vector Quantization Based S	Ene, Andrei; To	In the recent years	2017	Google Scholar	Cloud Computing	Speech	Speech Recognition without Dis	Direct Disclosure of sensitive data for	Homomorphic Encryptio
Privacy preserving encrypted phonetic search o	C. Glackin; G.	This paper presen	2017	IEEE	Cloud Computing	Speech	Storing and Searching Data with	Direct Disclosure of sensitive data for	Homomorphic Encryptio
Privacy-Preserving Speech Emotion Recognitior	Gareta, Alberto	Machine learning	2017	Google Scholar	General	Speech	Speech Emotion Recognition w	Information Disclosure by Statistical L	Homomorphic Encryptio
Beyond Big Data: What Can We Learn from AI M	Caliskan, Aylin	My research involv	2017	Google Scholar	Other	Written	Investigating the Impact of NLP	exploitability of word embeddings	None
Deep models under the GAN: information leaka	Hitaj, Briland; A	Deep Learning ha	2017	Google Scholar	General	Written	Investigating the Impact of Colla	memorizability of NN	None
Author obfuscation using generalised differentia	Fernandes, Na	The problem of ob	2018	Google Scholar	General	Written	Privacy-Utility-Trade-off for Train	Direct Disclosure of sensitive data for	Differential Privacy (DP)
Syntf: Synthetic and differentially private term fre	Weggenmann,	Text mining and in	2018	Google Scholar	General	Written	Privacy-Utility-Trade-off for Train	Information Disclosure by Statistical L	Differential Privacy (DP)
Privacy-preserving collaborative model learning:	Wang, Qian; D	Nowadays, machi	2018	Google Scholar	General	Written	Privacy-Utility-Trade-off for Train	exploitability of word embeddings	Federated Learning & H
Exploring Hashing and Cryptonet Based Approa	M. Dias; A. Aba	The outsourcing o	2018	IEEE	General	Speech	Speech Emotion Recognition w	Direct Disclosure of sensitive data for	Homomorphic Encryptio
Toward practical privacy-preserving analytics for	Sharma, Sagar	Modern healthcare	2018	Google Scholar	Medicine	Written	Privacy-Utility-Trade-off for Train	Direct Disclosure of sensitive data for	None
Smart Bears don't talk to strangers: analysing pr	Demetzou, Kat	The “Smart Bear”	2018	Google Scholar	Other	Speech	Private Communication	Direct Disclosure of sensitive data for	None
Privacy-preserving neural representations of tex	Coavoux, Maxi	This article deals	2018	Google Scholar	Cloud Computing	Written	Privacy-Utility-Trade-off for Neu	exploitability of word embeddings	None
VoiceGuard: Secure and Private Speech Proces	Brasser, Ferdir	With the advent of	2018	Google Scholar	Home Automation	Speech	Speech Processing without Disc	Direct Disclosure of sensitive data for	Obfuscation
Towards robust and privacy-preserving text repr	Li, Yitong; Bald	Written text often	2018	Google Scholar	General	Written	Privacy-Utility-Trade-off for Train	exploitability of word embeddings	Obfuscation
Privacy-preserving active learning on sensitive d	Feyisetan, Olu	Active learning ho	2019	Google Scholar	General	Written	Model Training without Sharing	Direct Disclosure of sensitive data for	Differential Privacy (DP)
Data Anonymization for Privacy Aware Machine	David Nizar Jal	The increase of da	2019	Springer	General	Written	Privacy-Utility-Trade-off for Train	Direct Disclosure of sensitive data for	Differential Privacy (DP)
Generalised differential privacy for text documer	Fernandes, Na	We address the pr	2019	Google Scholar	General	Written	Privacy-Utility-Trade-off for Train	Information Disclosure by Statistical L	Differential Privacy (DP)
I am not what i write: Privacy preserving text rep	Beigi, Ghazale	Online users gene	2019	Google Scholar	Other	Written	Privacy-Utility-Trade-off for Train	Information Disclosure by Statistical L	Differential Privacy (DP)
Learning Private Neural Language Modeling wit	S. Ji; S. Pan; G	Mobile keyboard s	2019	IEEE	General	Written	Model Training without Sharing	Direct Disclosure of sensitive data for	Federated Learning
Generative models for effective ML on private, d	Augenstein, Se	To improve real-w	2019	Google Scholar	General	Written	Model Training without Sharing	Direct Disclosure of sensitive data for	Federated Learning & D
A privacy-preserving distributed filtering framew	Sadat, MN; Azi	Background Medi	2019	Web of Science	Medicine	Written	Privacy-Utility-Trade-off for Train	Direct Disclosure of sensitive data for	Homomorphic Encryptio

Document Title	Authors	Abstract	Year	Source	Domain	Data Type	Use Cases	Generalized Issue/Vulnerability sol	PETs(RQ2) 1
Encrypted Speech Recognition Using Deep Poly	S. Zhang; Y. G	The cloud-based s	2019	IEEE	Cloud Computing	Speech	Speech Recognition without Dis	Direct Disclosure of sensitive data for	Homomorphic Encryptio
Privacy-preserving voice-based search over mH	Hadian, Mohan	Voice-enabled dev	2019	Google Scholar	Medicine	Speech	Speech Processing without Disc	Direct Disclosure of sensitive data for	Homomorphic Encryptio
Obfuscation for privacy-preserving syntactic par	Hu, Zhifeng; Ha	The goal of homo	2019	Google Scholar	General	Written	Privacy-Utility-Trade-off for Trair	exploitability of word embeddings	Homomorphic Encryptio
An Efficient and Dynamic Semantic-Aware Multi	X. Dai; H. Dai;	Traditional search	2019	IEEE	Cloud Computing	Written	Storing and Searching Data with	exploitability of word embeddings	Homomorphic Encryptio
Semantic-aware multi-keyword ranked search s	Dai, Hua; Dai,	Traditional search	2019	ScienceDirect	Cloud Computing	Written	Storing and Searching Data with	memorizability of NN	Homomorphic Encryptio
Compromising Speech Privacy under Continuou	S. A. Anand; P.	This paper explore	2019	IEEE	Other	Speech	Speech Processing without Disc	Direct Disclosure of sensitive data for	None
Adversarial Training for Privacy-Preserving Dee	M. Alawad; S.	Collaboration amo	2019	IEEE	Medicine	Written	Model Training without Sharing	Direct Disclosure of sensitive data for	Obfuscation
Adversarial Learning of Privacy-Preserving Text	Friedrich, Max;	De-identification is	2019	Google Scholar	Medicine	Written	Privacy-Utility-Trade-off for Trair	Direct Disclosure of sensitive data for	Obfuscation
Privacy-aware Document Ranking with Neural S	Shao, JJ; Ji, SY	The recent work o	2019	Web of Science	Cloud Computing	Written	Similarity detection without Data	memorizability of NN	Obfuscation
Privacy-preserving outsourced speech recogniti	Ma, Zhuo; Liu,	Most of the curren	2019	Google Scholar	Other	Speech	Speech Recognition without Dis	memorizability of NN	Secure Multiparty Comp
Privacy-preserving adversarial representation le	Srivastava, Brij	Automatic speech	2019	Google Scholar	General	Speech	Speech Recognition without Dis	Direct Disclosure of sensitive data for	Synthetic Data Generati
You talk too much: Limiting privacy exposure via	Vaidya, Tavish;	Voice synthesis us	2019	Google Scholar	Home Automation	Speech	Speech Recognition without Dis	Direct Disclosure of sensitive data for	Synthetic Data Generati
Towards differentially private text representation	Lyu, Lingjuan;	Most deep learnin	2020	Google Scholar	General	Written	Privacy-Utility-Trade-off for Wor	exploitability of word embeddings	Differential Privacy (DP)
Calibrating Mechanisms for Privacy Preserving	Feyisetan, Olu	This talk presents	2020	Google Scholar	General	Written	Privacy-Utility-Trade-off for Wor	exploitability of word embeddings	Differential Privacy (DP)
Hyperbolic Embeddings for Preserving Privacy a	Feyisetan, Olu	User's goal: meet	2020	Google Scholar	General	Written	Privacy-Utility-Trade-off for Wor	exploitability of word embeddings	Differential Privacy (DP)
Differentially private set union	Gopi, Sivakanth	We study the basi	2020	Google Scholar	General	Written	Similarity detection without Data	Information Disclosure by Statistical L	Differential Privacy (DP)
Differentially Private Representation for NLP: Fo	Lyu, Lingjuan;	It has been demor	2020	Google Scholar	General	Written	Privacy-Utility-Trade-off for Neu	memorizability of NN	Differential Privacy (DP)
Building a Personally Identifiable Information Re	Hathurusinghe,	This thesis explore	2020	Google Scholar	General	Written	Model Training without Sharing	Direct Disclosure of sensitive data for	Federated Learning
Federated learning for healthcare informatics	Xu, Jie; Glicksb	With the rapid dev	2020	Google Scholar	Medicine	Written	Model Training without Sharing	Direct Disclosure of sensitive data for	Federated Learning
Federated Acoustic Model Optimization for Auto	Conghui TanDi	Traditional Automa	2020	Springer	Other	Speech	Model Training without Sharing	Direct Disclosure of sensitive data for	Federated Learning
Privacy-Preserving Deep Learning NLP Models	M. Alawad; H.	Population cancer	2020	IEEE	Medicine	Written	Model Training without Sharing	exploitability of word embeddings	Federated Learning
Texthide: Tackling data privacy in language unde	Huang, Yangsib	An unsolved chall	2020	Google Scholar	General	Written	Model Training without Sharing	memorizability of NN	Federated Learning
Task-Agnostic Privacy-Preserving Representatio	Li, Ang; Yang,	The availability of	2020	Google Scholar	General	Written	Model Training without Sharing	memorizability of NN	Federated Learning
Decentralizing feature extraction with quantum c	Yang, Chao-Ha	We propose a nov	2020	Google Scholar	General	Speech	Model Training without Sharing	memorizability of NN	Federated Learning
Fold-stratified cross-validation for unbiased and	Bey, Romain; C	Objective: We intr	2020	Google Scholar	Medicine	Written	Model Training without Sharing	memorizability of NN	Federated Learning
Empirical Studies of Institutional Federated Lear	Zhu, Xinghua;	Federated learnin	2020	Google Scholar	General	Written	Model Training without Sharing	Direct Disclosure of sensitive data for	Federated Learning & D
Privacy-Preserving Collaborative Deep Learning	L. Zhao; Q. Wa	With powerful para	2020	IEEE	General	Written	Model Training without Sharing	memorizability of NN	Federated Learning & D
Generic cost optimized and secured sensitive at	Sumathi, M; Sa	Cloud computing s	2020	Web of Science	Cloud Computing	Written	Model Training without Sharing	Direct Disclosure of sensitive data for	Homomorphic Encryptio
Cross-lingual multi-keyword rank search with se	Guan, Zhitao; L	The emergence of	2020	ScienceDirect	General	Written	Storing and Searching Data with	Direct Disclosure of sensitive data for	Homomorphic Encryptio
Privacy Preserving Chatbot Conversations	D. Biswas	With chatbots gair	2020	IEEE	General	Written	Storing and Searching Data with	Direct Disclosure of sensitive data for	Homomorphic Encryptio
Multi-user searchable encryption voice in home	Li, Wei; Xiao, Y	With the developn	2020	ScienceDirect	Home Automation	Speech	Storing and Searching Data with	Direct Disclosure of sensitive data for	Homomorphic Encryptio
PrivFT: Private and Fast Text Classification With	A. A. Badawi; L	We present an eff	2020	IEEE	General	Written	Classification on encrypted Data	exploitability of word embeddings	Homomorphic Encryptio
PAIGE: towards a hybrid-edge design for privac	Liang, Yilei; O'l	Intelligent Persona	2020	Google Scholar	Home Automation	Speech	Speech Processing without Disc	Direct Disclosure of sensitive data for	None
Privacy Risks of General-Purpose Language Mo	X. Pan; M. Zha	Recently, a new p	2020	IEEE	General	Written	Investigating the Impact of Word	exploitability of word embeddings	None
Exploring the Privacy-Preserving Properties of V	Abdalla, M; Abd	Background: Word	2020	Web of Science	Medicine	Written	Investigating the Impact of Word	exploitability of word embeddings	None
Investigating the Impact of Pre-trained Word Em	Thomas, A; Ad	The sensitive infor	2020	Web of Science	General	Written	Investigating the Impact of Pre-t	memorizability of NN	None
Privacy Preserving Acoustic Model Training for S	Y. Tachioka	In-domain speech	2020	IEEE	General	Speech	Model Training without Sharing	Direct Disclosure of sensitive data for	Obfuscation
Performance Evaluation of Voice Encryption Tec	A. M. Raheema	With the substanti	2020	IEEE	General	Speech	Speech Communication without	Direct Disclosure of sensitive data for	Obfuscation
Privacy-and utility-preserving textual analysis via	Feyisetan, Olu	Accurately learnin	2020	Google Scholar	General	Written	Privacy-Utility-Trade-off for Trair	exploitability of word embeddings	Obfuscation
Preech: A system for privacy-preserving speech	Ahmed, Shima	New advances in	2020	Google Scholar	Cloud Computing	Speech	Speech Transcription without Di	Information Disclosure by Statistical L	Obfuscation
Privacy-preserving Voice Analysis via Disentang	Aloufi, Ranya;	Voice User Interfa	2020	Google Scholar	Other	Speech	Speech Processing without Disc	memorizability of NN	Obfuscation
A novel privacy-preserving speech recognition fr	Wang, QR; Fer	Utilizing speech a	2020	Web of Science	Other	Speech	Speech Recognition without Dis	memorizability of NN	Obfuscation
Privacy-Aware Best-Balanced Multilingual Comr	Pituxcoosuvarr	In machine transla	2020	Web of Science	General	Written	Classification on encrypted Data	Direct Disclosure of sensitive data for	Secure Multiparty Comp
Privacy-preserving Feature Extraction via Adver	Ding, Xiaofeng	Deep learning is ir	2020	Google Scholar	Cloud Computing	Written	Model Training without Sharing	memorizability of NN	Secure Multiparty Comp

Document Title	Authors	Abstract	Year	Source	Domain	Data Type	Use Cases	Generalized Issue/Vulnerability sol	PETs(RQ2) 1
SecureNLP: A system for multi-party privacy-pre	Feng, Qi; He, D	Natural language	2020	Google Scholar	General	Written	Model Training without Sharing	memorizability of NN	Secure Multiparty Comp
Adversarial representation learning for private s	Ericsson, Davic	As more and more	2020	Google Scholar	General	Speech	Speech Characteristics Obfusca	Direct Disclosure of sensitive data for	Synthetic Data Generati
Privacy-Preserving Knowledge Transfer with Bo	Hong-Jun Yoor	There is a need to	2021	Springer	General	Written	Model Training without Sharing	exploitability of word embeddings	Differential Privacy (DP)
ADePT: Auto-encoder based Differentially Privat	Krishna, Satya	Privacy is an impo	2021	Google Scholar	General	Written	Privacy-Utility-Trade-off for Train	exploitability of word embeddings	Differential Privacy (DP)
Privacy-Preserving Graph Convolutional Networ	Igamberdiev, T	Graph convolution	2021	Google Scholar	General	Written	Classification without Data Disc	memorizability of NN	Differential Privacy (DP)
Exploiting peer-to-peer communications for que	Tran, Bang; Lia	Voice assistant sy	2021	Google Scholar	Home Automation	Speech	Private Communication	Direct Disclosure of sensitive data for	Obfuscation
Federated learning of N-gram language models	Chen M., Sures	We propose algor	2019	SCOPUS	General	Written	Model Training without Sharing	Direct Disclosure of sensitive data for	Federated Learning
Poster abstract: Federated learning for speech e	Latif S., Khalifa	Privacy concerns	2020	SCOPUS	General	Speech	Model Training without Sharing	Direct Disclosure of sensitive data for	Federated Learning
Industrial Federated Topic Modeling	Jiang, Di; Tong	Probabilistic topic	2021	ACM	Medicine	Written	Model Training without Sharing	Direct Disclosure of sensitive data for	Federated Learning
Improving on-device speaker verification using f	Granqvist F., S	Information on spe	2020	SCOPUS	General	Speech	Model Training without Sharing	Direct Disclosure of sensitive data for	Federated Learning & D
Secure computation for privacy preserving biom	Sy B.	The goal of this re	2008	SCOPUS	General	Written	Speech Communication without	Direct Disclosure of sensitive data for	Homomorphic Encryptio
Privacy-preserving PLDA speaker verification us	Treiber A., Nau	The usage of biom	2019	SCOPUS	General	Speech	Speech Verification without Disc	Direct Disclosure of sensitive data for	Homomorphic Encryptio
Achieving efficient similar document search ove	Aritomo D., Wa	Cloud computing,	2019	SCOPUS	Cloud Computing	Written	Storing and Searching Data with	Direct Disclosure of sensitive data for	Homomorphic Encryptio
Privacy preserving speech, face and fingerprint	Dinesh A., Bijo	Biometrics repres	2017	SCOPUS	General	Speech	Speech Processing without Disc	Direct Disclosure of sensitive data for	Homomorphic Encryptio
Efficient and Privacy-Preserving Speaker Verific	Gao X., Li K., C	Speaker recognitio	2020	SCOPUS	Home Automation	Speech	Speech Verification without Disc	Direct Disclosure of sensitive data for	Homomorphic Encryptio
Encrypted Domain Mel-Frequency Cepstral Coe	Chen J., Chen	Audio has become	2018	SCOPUS	Cloud Computing	Written	Speech Watermarking	Direct Disclosure of sensitive data for	Homomorphic Encryptio
Efficient searching with multiple keyword over e	Santhi K., Deep	In Cloud Computir	2016	SCOPUS	Cloud Computing	Written	Storing and Searching Data with	Direct Disclosure of sensitive data for	Homomorphic Encryptio
Toward Efficient Multi-Keyword Fuzzy Search ov	Fu Z., Wu X., C	Keyword-based se	2016	SCOPUS	Cloud Computing	Written	Storing and Searching Data with	Direct Disclosure of sensitive data for	Homomorphic Encryptio
Privacy preserving similarity based text retrieval	Kumari P., Jane	Cloud computing i	2016	SCOPUS	Cloud Computing	Written	Storing and Searching Data with	Direct Disclosure of sensitive data for	Homomorphic Encryptio
Classification of Encrypted Word Embeddings u	Podschwadt R.	Deep learning has	2020	SCOPUS	General	Written	Classification on encrypted Data	exploitability of word embeddings	Homomorphic Encryptio
Privacy-Preserving Character Language Modelli	Thaine, Patricia	Some of the most sensitive informat		Google Scholar	General	Written	Classification on encrypted Data	exploitability of word embeddings	Homomorphic Encryptio
Continuous improvement process (CIP)-based p	Yankson B.	Advances within th	2021	SCOPUS	Other	Written	Private Communication	Direct Disclosure of sensitive data for	None
Preserving privacy in speaker and speech chara	Nautsch A., Jin	Speech recording	2019	SCOPUS	Medicine	Speech	Speech Verification without Disc	Direct Disclosure of sensitive data for	None
Privacy-aware personalized entity representatio	Melnick L., Elm	Representation le	2020	SCOPUS	General	Written	Private Communication	Direct Disclosure of sensitive data for	Obfuscation
An analysis of blocking methods for private reco	Etienne B., Che	The field of Big Da	2016	SCOPUS	Other	Written	Similarity detection without Data	Direct Disclosure of sensitive data for	Obfuscation
Redesign of Gaussian mixture model for efficien	Rahulamathava	This paper propos	2018	SCOPUS	General	Speech	Speech Recognition without Dis	Direct Disclosure of sensitive data for	Obfuscation
A privacy preserving efficient protocol for seman	Hawashin B., F	During the similari	2011	SCOPUS	General	Written	Similarity detection without Data	Direct Disclosure of sensitive data for	Obfuscation
Privacy-preserving speaker verification and iden	Pathak M.A., R	Speech being a u	2012	SCOPUS	General	Speech	Speech Verification without Disc	Direct Disclosure of sensitive data for	Obfuscation
Privacy-preserving speaker verification as passv	Pathak M.A., R	We present a text-	2012	SCOPUS	General	Speech	Speech Verification without Disc	Direct Disclosure of sensitive data for	Obfuscation
Privacy-preserving ivector-based speaker verific	Rahulamathava	This paper introdu	2018	SCOPUS	General	Speech	Speech Verification without Disc	Direct Disclosure of sensitive data for	Obfuscation
Secure binary embeddings of front-end factor an	Portêlo J., Aba	Remote speaker v	2013	SCOPUS	General	Written	Speech Verification without Disc	Direct Disclosure of sensitive data for	Obfuscation
Biomedical Data Privacy Enhancement Architec	Singh N., Lakh	The Collaborative	2018	SCOPUS	Medicine	Written	Storing and Searching Data with	Direct Disclosure of sensitive data for	Obfuscation
PIVOT: Privacy-preserving outsourcing of text da	Li Y., Wang W.I	In this paper, we c	2019	SCOPUS	General	Written	Privacy-Utility-Trade-off for Wor	exploitability of word embeddings	Obfuscation
Privacy-preserving speaker verification using se	Portêlo J., Raj	Remote speaker v	2014	SCOPUS	General	Speech	Speech Verification without Disc	exploitability of word embeddings	Obfuscation
Privacy preserving speaker verification using ad	Pathak M.A., R	In this paper we p	2011	SCOPUS	General	Speech	Speech Verification without Disc	memorizability of NN	Obfuscation
Privacy-preserving classification of personal tex	Reich D., Todo	Classification of p	2019	SCOPUS	General	Written	Classification without Data Discl	Direct Disclosure of sensitive data for	Secure Multiparty Comp
Secure computation for biometric data security-a	Sy B.K.	The goal of this re	2009	SCOPUS	General	Speech	Speech Verification without Disc	Direct Disclosure of sensitive data for	Secure Multiparty Comp
Attacking a privacy preserving music matching a	Portêlo J., Raj	Secure multi-party	2012	SCOPUS	Other	Speech	Storing and Searching Data with	Direct Disclosure of sensitive data for	Secure Multiparty Comp
Privacy preserving speech analysis using emoti	Aloufi R., Hadd	Voice controlled d	2019	SCOPUS	Cloud Computing	Speech	Speech Recognition without Dis	Direct Disclosure of sensitive data for	Synthetic Data Generati

A.2. Detailed Category Tables with Aggregation Mapping

A.2.1. Privacy Issue Solutions for NLP as a Privacy Enabler

This list is taken from the ”Privacy Issue Solution” column, contained by the work sheet located in subsection A.1.1.

Generalized Privacy Issue Solution (RQ2)	Amount		
Automated Access Control	1	Automation	23
Automated Access Control based on notation	1		
Automated Compliance Checker	4		
Automated Essay Scoring	1		
Automated Privacy Assessment of health Related Alexa Application	1		
Automated Privacy Policy Classification	1		
Automated Privacy Policy Coverage Check with Sequence Classification Models	1		
Automated Rewriting	1		
Automatic Analysis of Privacy Policies	1		
Automatic Anonymization of Text Posts	1		
Automatic Anonymization of Textual Documents	1		
Automatic Assessment of Privacy Policiy Completness	1		
Automatic Conversion of sensitive information in text	1		
Automatic modeling of privacy regulations	1		
Automatic policy enforcement	2		
Automatic policy enforcement on semantic social data	1		
Automatic semantic annotation mechanism	1		
Automatic Summarization of User Reviews	1		
Automation process of SLAs	1		
Code-based privacy analysis of Smart phone apps	6	Code-based Analysis	7
Code-based privacy analysis of web applications	1		
Collect annotated corpus	17	Collect annotated corpus	17
De-identification	66	De-identification	74
De-identification / Obfuscating Authorship	8		
Demonstration of Threats	1	Demonstration of Threats	1
Designing a Big Data Framework for Publishing Social Media Data	1	Designing	27
Designing a decentralized peer-to-peer private document search engine	1		
Designing a framework for sharing of sensitive information	1		
Designing a gender obfuscation tool	1		
Designing a geo-indistinguishability text pertubation algorithm	1		
Designing a locally deployed system	2		
Designing a methodology for providing extra safety precautions without being intrusive	1		
Designing a multi-agent architecture coupled with privacy preserving techniques	1		
Designing a Privacy Guard for Cloud-Based Home Assistants and IoT Devices	1		
Designing a privacy preserved medical text data analysis	1		
Designing a privacy-preserving web search engine	3		
Designing a scheme for a privacy preserving search log analysis	1		
Designing a scheme for a privacy preserving text analysis	1		
Designing a search tree without tracking user interaction	1		
Designing a tailor-made data annonymity approach	2		
Designing a task-independent privacy-respecting data crowdsourcing framework	1		
Designing a text perturbation mechanism for a privacy preserving text analysis	2		
Designing A User-Centric Privacy-Disclosure Detection Framework	1		
Designing a web search engine side to generate privacy-preserving user profiles	1		
Designing an Inclusive Financial Privacy Index	1		
Designing Secure Views for privacy preserving data analysis	1		
Desinging a system that supports privacy preserving data publication of network secu	1		
Detecting privacy-sensitive information / activities	27	Detection	38
Detection of Data Privacy Violations	1		
Detection of Inconsistencies within Privacy Policies	1		
Detection of Locations without user involvement	1		
Detection of Personal Health Information in Peer-to-Peer File-Sharing Networks	1		

Detection of potential pitfalls in the privacy policies of companies on the We	1		
Detection of Privacy Breaches in Physican Reviews	1		
Detection of Privacy Sensitive Conditions in C-CDAs	1		
Detection of the Correlation between User Reviews and Privacy Issues	2		
Detection of vagueness	2		
Encryption based on Events	1	Encryption based Solution	2
Encryption-based search system mitigating file-Injection Attacks	1		
Generation of Artefacts based on Privacy Policy Analysis	12	Generation	22
Generation of Synthetic Data	10		
Information Extraction from Emails	1	Infromation Extraction	26
Information Extraction from Health Records	1		
Information Extraction from large-scale unstructured textual data	1		
Information Extraction from nursing documents	1		
Information Extraction from privacy policies	20		
Information Extraction if information is harboured by a second party	1		
Information Extraction out of Privacy Policies with Word Embeddings	1		
Mapping of Ambiguity on a score board	1	Mapping	8
Mapping of Description-to-permission Fidelity on a scale	1		
Mapping of Privacy Policies to Privacy Issues	1		
Mapping Privacy Policies to Contextual Integrity (CI) with Q&A	1		
Mapping Privacy Policies to GDPR	2		
Mapping Privacy Policy Content to selected Dictionary	2		
Ontological semantics perspective for checking Privacy Policies	1	Ontology based Solutions	4
Ontology build for privacy	1		
Ontology used for transparency in Privacy Policies	1		
Ontology-Enabled Access Control and Privacy Recommendations	1		
Overview of algorithms and tools for sharing data in a privacy-preserving manner	1	Overviews	14
Overview of Challenges and applied methods for protection of personal health informa	3		
Overview of challenges in detecting privacy revealing information in unstructured text	1		
Overview of Challenges of omission, context and multilingualism	1		
Overview of challenges of working with personal and particularly sensitive data in prac	1		
Overview of existing dialogue system vulnerabilities in security and privacy.	1		
Overview of techniques for privacy preserving data linkage	1		
Overview of the current state of the legal regulations and analyse different data protec	1		
Overview over the research field	4		
Semantic analysis for privacy preserving peer feedback	1	Semantic Solutions	19
Semantic Analysis of social media forensic analysis for preventive policing of online a	1		
Semantic correlations in document sanitization to Minimizing risk disclosure	1		
Semantic features using word embeddings for classification	1		
Semantic Framework for the Analysis of Privacy Policies	1		
Semantic Incompleteness Detection in Privacy Policy Goals	2		
Semantic Inference from Privacy Policies	1		
Semantic Microaggregation for Anonymization of query logs to preserve utility	1		
Semantic Model Creation based on Privacy Policies	1		
Semantic Modeling of language vagueness	1		
Semantic open source stack	1		
Semantic Similarities Tool Comparison	2		
Semantic similarity based on clustering and k-annonymity	2		
Semantic-based text pertubation approach	1		
Semantic-centered Rules	1		
Semantics of Rules Mining	1		
Speech De-Identification	15	Speech de-identification	16
Suggestion of security and privacy requirements	3	Suggestions	7

Suggestion of security and privacy requirements by involving users	1
Suggestion of security and privacy requirements for text mining	3
Grand Total	**304**

A.2.2. Privacy Issue Solutions for NLP as a Privacy Threat

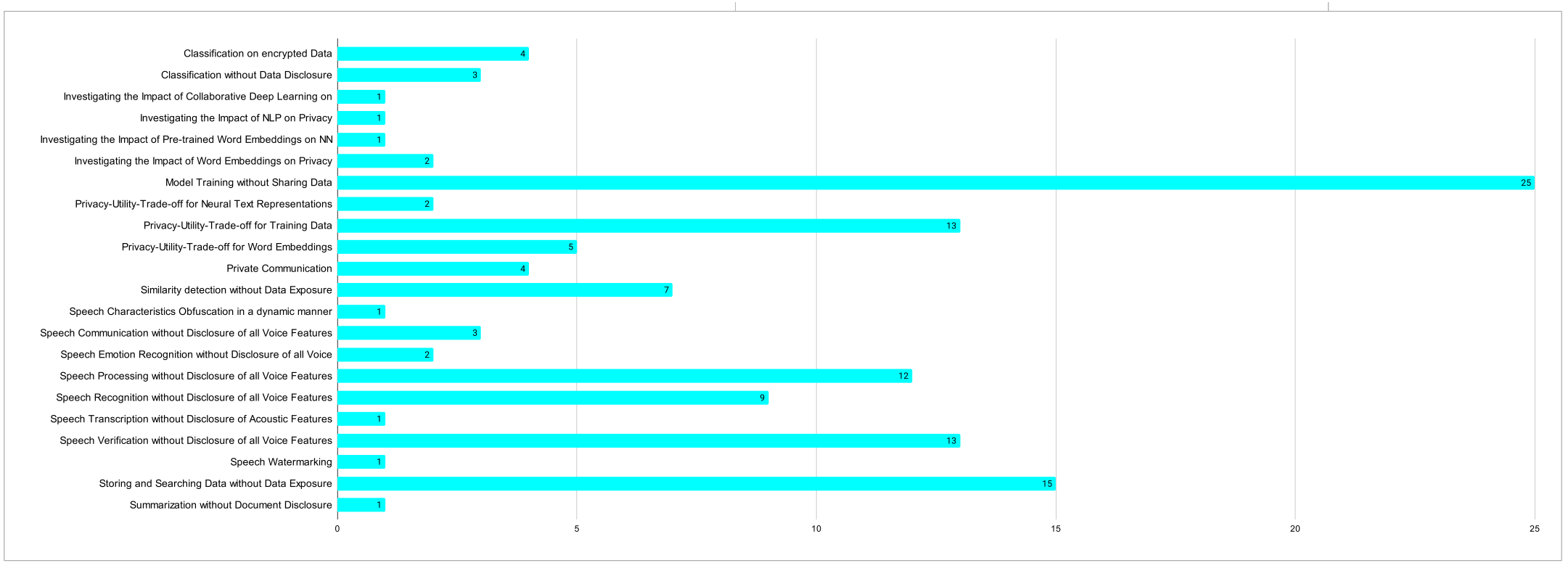
This list is taken from the ”Use Cases” column, contained by the work sheet located in subsection A.1.2.

Model Training without Sharing Data	COUNTA of Mod		
Classification on encrypted Data	4	Classification without Data Disclosure	7
Classification without Data Disclosure	3		
Investigating the Impact of Collaborative Deep Learning on Priva	1	Investigating the Impact of NLP related Concept on Privacy	5
Investigating the Impact of NLP on Privacy	1		
Investigating the Impact of Pre-trained Word Embeddings on NN	1		
Investigating the Impact of Word Embeddings on Privacy	2		
Model Training without Sharing Data	25	Model Training without Sharing Data	26
Privacy-Utility-Trade-off for Neural Text Representations	2	Privacy-Utility-Trade-off for NLP related Concept	20
Privacy-Utility-Trade-off for Training Data	13		
Privacy-Utility-Trade-off for Word Embeddings	5		
Private Communication	4	Private Communication	4
Similarity detection without Data Exposure	7	Similarity detection without Data Exposure	7
Speech Characteristics Obfuscation in a dynamic manner	1	Speech related Service without complete Voice Feature Disclo	42
Speech Communication without Disclosure of all Voice Features	3		
Speech Emotion Recognition without Disclosure of all Voice Fea	2		
Speech Processing without Disclosure of all Voice Features	12		
Speech Recognition without Disclosure of all Voice Features	9		
Speech Transcription without Disclosure of Acoustic Features	1		
Speech Verification without Disclosure of all Voice Features	13		
Speech Watermarking	1		
Storing and Searching Data without Data Exposure	15	Storing and Searching Data without Data Exposure	15
Summarization without Document Disclosure	1	Summarization without Document Disclosure	1
Grand Total	**126**		

A.3. Figures for Mapping Results

A.3.1. Use Case Classification for NLP as a Privacy Treat

These values were taken from the work sheet located in subsection A.1.2.


Classification on encrypted Data
4
Classification without Data Disclosure
3
Investigating the Impact of Collaborative Deep Learning on
1
Investigating the Impact of NLP on Privacy
1
Investigating the Impact of Pre-trained Word Embeddings on NN
1
Investigating the Impact of Word Embeddings on Privacy
2
Model Training without Sharing Data
25
Privacy-Utility-Trade-off for Neural Text Representations
2
Privacy-Utility-Trade-off for Training Data
13
Privacy-Utility-Trade-off for Word Embeddings
5
Private Communication
4
Similarity detection without Data Exposure
7
Speech Characteristics Obfuscation in a dynamic manner
1
Speech Communication without Disclosure of all Voice Features
3
Speech Emotion Recognition without Disclosure of all Voice
2
Speech Processing without Disclosure of all Voice Features
12
Speech Recognition without Disclosure of all Voice Features
9
Speech Transcription without Disclosure of Acoustic Features
1
Speech Verification without Disclosure of all Voice Features
13
Speech Watermarking
1
Storing and Searching Data without Data Exposure
15
Summarization without Document Disclosure
1
0
5
10
15
20
25

List of Figures

1.1. Trends in Data Science and Big Data 2
1.2. Overview of the Systematic Mapping Study (SMS) taken from [11] 5
1.3. Amount of papers during the different SMS phases 5
1.4. Keywording abstracts to build classification schemes taken from [11] 6

3.1. Overview of privacy preservation methods in deep learning taken from [44] . 17
3.2. Overview of privacy preservation metrics in deep learning taken from [44] . . 18
3.3. Overview of privacy preservation challenges and weaknesses taken from [45] 18

4.1. Search Term Segmentation 23
4.2. Search Query Results 26
4.3. Filtered Search Query Results 27
4.4. Proportion of remaining papers 30

5.1. Publications per year 49
5.2. Publications per electronic data source 50
5.3. Mapping Results for the Domain category in the top category NLP as a Privacy Enabler 51
5.4. Mapping Results for the Use Case Classification category in the top category NLP as a Privacy Enabler 52
5.5. Mapping Results for the Generalized Privacy Issue category in the top category NLP as a Privacy Enabler 53
5.6. Privacy Issues and Use Cases 65
5.7. Privacy Issues and Domains 66
5.8. Development of Privacy Issues 67
5.9. Mapping Results for the Domain category in the top category NLP as a Privacy Threat 68
5.10. Mapping Results for the Data Type category in the top category NLP as a Privacy Threat 69
5.11. Aggregated Mapping Results for the Use Case Classification category in the top category NLP as a Privacy Threat 70
5.12. Mapping Results for the Generalized Issue/Vulnerability solved for NLP category in the top category NLP as a Privacy Threat 70
5.13. NLP Privacy Issues and Use Cases 71
5.14. NLP Privacy Issues and Data Type 72
5.15. NLP Privacy Issues and Domains 72

5.16. Mapping Results for the Generalized Privacy Issue Solution category in the top category NLP as a Privacy Enabler 73
5.17. Mapping Results for the Generalized Applied NLP Concept category in the top category NLP as a Privacy Enabler 73
5.18. Aggregated mapping results for the Generalized Applied NLP Concept category in the top category NLP as a Privacy Enabler 74
5.19. Mapping Results for the Generalized Applied NLP Concept category in the top category NLP as a Privacy Enabler 75
5.20. Aggregated mapping results for the Generalized NLP Method category in the top category NLP as a Privacy Enabler 75
5.21. Privacy solutions aiming to solve privacy issues 76
5.22. Privacy solutions and their analysis levels 77
5.23. Privacy solutions and their applied method category 78
5.24. Mapping Results for the Privacy Enhancing Technologies (PETs) category in the top category NLP as a Privacy Threat 79
5.25. Aggregated Mapping Results for the Privacy Enhancing Technologies (PETs) category in the top category NLP as a Privacy Threat 79
5.26. NLP Privacy Threats and their Solutions 80
5.27. NLP Privacy Threat Solutions and their Use Cases 81
5.28. NLP Privacy Threat Solutions and their Development over time 82

List of Tables

1.1. Table of Research Questions 3

4.1. Search Queries 24
4.2. Proposed Electronic Data Sources 24
4.3. Selected Electronic Data Sources 25
4.4. Amount of Papers after Filtering 28
4.5. Selection of Papers for the Validation Process 28
4.6. Criteria Table 29
4.7. Table with Advisor Comments 31
4.8. Summary of Comments 33
4.9. Subcategories within the two top categories 34
4.10. Domains for NLP as a Privacy Enabler 35
4.11. Classification of Use Cases 44
4.12. Generalized Privacy Issues 45
4.13. Terms of Generalized Privacy Issue Solution 45
4.14. All Terms in Generalized Category of Applied NLP Concept 46
4.15. NLP Method Types 46
4.16. Domains for NLP as a Privacy Threat 46
4.17. Use Cases for NLP as a Privacy Threat 47
4.18. Generalized Issue/Vulnerability solved for NLP 47
4.19. Privacy Enhancing Technologies 47

Acronyms

NLP Natural Language Processing. 2–4, 6, 9–23, 28–30, 32–35, 37–43, 48, 50–52, 55–62, 64, 83–90

PET Privacy Enhancing Technology. 4, 42, 58, 61–63, 86, 87

PP NLP Privacy-Preserving Natural Language Processing. 3–5, 10, 18, 23, 27, 48

SMS Systematic Mapping Study. 4, 5, 22, 57, 83, 84, 110

Bibliography

[1] *The History of the General Data Protection Regulation*. URL: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en.

[2] L. Jarvis. "The Age of Big Data Analytics: A cross-national comparison of the implementation of Article 23 of the GDPR in the United Kingdom, France, Germany and Italy". In: (2019).

[3] J. Wolff and N. Atallah. "Early GDPR Penalties: Analysis of Implementation and Fines Through May 2020". In: *Available at SSRN 3748837* (2020).

[4] *GDPR Enforcement Tracker*. URL: https://www.enforcementtracker.com/.

[5] R. Chan. "The Cambridge Analytica whistleblower explains how the firm used Facebook data to sway elections". In: *Business Insider. Retrieved* 12 (2020).

[6] D. R. Raban and A. Gordon. "The evolution of data science and big data research: A bibliometric analysis". In: *Scientometrics* 122.3 (2020), pp. 1563–1581.

[7] W. B. Tesfay, J. Serna, and S. Pape. "Challenges in Detecting Privacy Revealing Information in Unstructured Text." In: *PrivOn@ ISWC*. 2016.

[8] N. Carlini, C. Liu, Ú. Erlingsson, J. Kos, and D. Song. "The secret sharer: Evaluating and testing unintended memorization in neural networks". In: *28th {USENIX} Security Symposium ({USENIX} Security 19)*. 2019, pp. 267–284.

[9] X. Pan, M. Zhang, S. Ji, and M. Yang. "Privacy risks of general-purpose language models". In: *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE. 2020, pp. 1314–1331.

[10] M. Abdalla, M. Abdalla, G. Hirst, and F. Rudzicz. "Exploring the Privacy-Preserving Properties of Word Embeddings: Algorithmic Validation Study". In: *Journal of medical Internet research* 22.7 (2020), e18055.

[11] K. Petersen, R. Feldt, S. Mujtaba, and M. Mattsson. "Systematic mapping studies in software engineering". In: *12th International Conference on Evaluation and Assessment in Software Engineering (EASE) 12*. 2008, pp. 1–10.

[12] B. A. Kitchenham, D. Budgen, and P. Brereton. *Evidence-based software engineering and systematic reviews*. Vol. 4. CRC press, 2015.

[13] K. Petersen, S. Vakkalanka, and L. Kuzniarz. "Guidelines for conducting systematic mapping studies in software engineering: An update". In: *Information and Software Technology* 64 (2015), pp. 1–18.

[14] A. Lukács. "what is privacy? The history and definition of privacy". In: (2016).

[15] A. F. Westin. "Social and political dimensions of privacy". In: *Journal of social issues* 59.2 (2003), pp. 431–453.

[16] *Art. 4 GDPR – Definitions*. Mar. 2018. URL: https://gdpr-info.eu/art-4-gdpr/.

[17] P. M. Schwartz and D. J. Solove. "The PII problem: Privacy and a new concept of personally identifiable information". In: *NYUL rev.* 86 (2011), p. 1814.

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

[19] S. L. Garfinkel et al. "De-identification of personal information". In: *National institute of standards and technology* (2015).

[20] C. Dwork. "The differential privacy frontier". In: *Theory of Cryptography Conference*. Springer. 2009, pp. 496–502.

[21] H. H. Pang, X. Xiao, and J. Shen. "Obfuscating the topical intention in enterprise text search". In: *2012 IEEE 28th International Conference on Data Engineering*. IEEE. 2012, pp. 1168–1179.

[22] K. El Emam. "Seven ways to evaluate the utility of synthetic data". In: *IEEE Security & Privacy* 18.4 (2020), pp. 56–59.

[23] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas. "Communication-efficient learning of deep networks from decentralized data". In: *Artificial Intelligence and Statistics*. PMLR. 2017, pp. 1273–1282.

[24] R. Cramer, I. B. Damgård, et al. *Secure multiparty computation*. Cambridge University Press, 2015.

[25] C. Fontaine and F. Galand. "A survey of homomorphic encryption for nonspecialists". In: *EURASIP Journal on Information Security* 2007 (2007), pp. 1–10.

[26] E. D. Liddy. "Natural language processing". In: (2001).

[27] S. Wu, E. M. Ponti, and R. Cotterell. "Differentiable Generative Phonology". In: *arXiv preprint arXiv:2102.05717* (2021).

[28] A. Voutilainen. "Part-of-speech tagging". In: *The Oxford handbook of computational linguistics* (2003), pp. 219–232.

[29] A. R. Hippisley. "Lexical analysis". In: (2010).

[30] M. Marrero, J. Urbano, S. Sánchez-Cuadrado, J. Morato, and J. M. Gómez-Berbıs. "Named entity recognition: fallacies, challenges and opportunities". In: *Computer Standards & Interfaces* 35.5 (2013), pp. 482–489.

[31] URL: https://sites.google.com/view/privatenlp/home/emnlp-2020?authuser=0.

[32] URL: https://sites.google.com/view/privatenlp/home?authuser=0.

[33] *PrivateNLP 2020*. URL: https://sites.google.com/view/wsdm-privatenlp-2020.

[34] Q. Feng, D. He, Z. Liu, H. Wang, and K.-K. R. Choo. "SecureNLP: A system for multi-party privacy-preserving natural language processing". In: *IEEE Transactions on Information Forensics and Security* 15 (2020), pp. 3709–3721.

[35] P. Ram, J. Markkula, V. Friman, and A. Raz. "Security and privacy concerns in connected cars: a systematic mapping study". In: *2018 44th Euromicro Conference on Software Engineering and Advanced Applications (SEAA)*. IEEE. 2018, pp. 124–131.

[36] L. H. Iwaya, A. Ahmad, and M. A. Babar. "Security and Privacy for mHealth and uHealth Systems: a Systematic Mapping Study". In: *IEEE Access* 8 (2020), pp. 150081–150112.

[37] N. Papanikolaou, S. Pearson, and M. C. Mont. "Towards natural-language understanding and automated enforcement of privacy rules and regulations in the cloud: survey and bibliography". In: *FTRA International Conference on Secure and Trust Computing, Data Management, and Application*. Springer. 2011, pp. 166–173.

[38] P. Silva, C. Gonçalves, C. Godinho, N. Antunes, and M. Curado. "Using natural language processing to detect privacy violations in online contracts". In: *Proceedings of the 35th Annual ACM Symposium on Applied Computing*. 2020, pp. 1305–1307.

[39] L. Zhao, W. Alhoshan, A. Ferrari, K. J. Letsholo, M. A. Ajagbe, E.-V. Chioasca, and R. T. Batista-Navarro. "Natural Language Processing (NLP) for Requirements Engineering: A Systematic Mapping Study". In: *arXiv preprint arXiv:2004.01099* (2020).

[40] W. Khan, A. Daud, J. A. Nasir, and T. Amjad. "A survey on the state-of-the-art machine learning models in the context of NLP". In: *Kuwait journal of Science* 43.4 (2016).

[41] Z. Ji, Z. C. Lipton, and C. Elkan. "Differential privacy and machine learning: a survey and review". In: *arXiv preprint arXiv:1412.7584* (2014).

[42] M. Gong, Y. Xie, K. Pan, K. Feng, and A. K. Qin. "A survey on differentially private machine learning". In: *IEEE Computational Intelligence Magazine* 15.2 (2020), pp. 49–64.

[43] D. Zhang, X. Chen, D. Wang, and J. Shi. "A survey on collaborative deep learning and privacy-preserving". In: *2018 IEEE Third International Conference on Data Science in Cyberspace (DSC)*. IEEE. 2018, pp. 652–658.

[44] H. C. Tanuwidjaja, R. Choi, and K. Kim. "A survey on deep learning techniques for privacy-preserving". In: *International Conference on Machine Learning for Cyber Security*. Springer. 2019, pp. 29–46.

[45] H. C. Tanuwidjaja, R. Choi, S. Baek, and K. Kim. "Privacy-Preserving Deep Learning on Machine Learning as a Service—a Comprehensive Survey". In: *IEEE Access* 8 (2020), pp. 167425–167447.

[46] T. Bolton, T. Dargahi, S. Belguith, M. S. Al-Rakhami, and A. H. Sodhro. "On the security and privacy challenges of virtual assistants". In: *Sensors* 21.7 (2021), p. 2312.

[47] L. M. H. E. V. Polychronopoulos, G. Lopez, Y. T. O. Z. K. Ye, and Y. W. C. Quirk. "Privacy-Aware Personalized Entity Representations for Improved User Understanding". In: (2020).

[48] A. N. Mehdy and H. Mehrpouyan. "A User-Centric and Sentiment Aware Privacy-Disclosure Detection Framework based on Multi-input Neural Network." In: *PrivateNLP@ WSDM*. 2020, pp. 21–26.

[49] R. Podschwadt and D. Takabi. "Classification of Encrypted Word Embeddings using Recurrent Neural Networks." In: *PrivateNLP@ WSDM*. 2020, pp. 27–31.

[50] V. Jain and S. Ghanavati. "Is It Possible to Preserve Privacy in the Age of AI?" In: *PrivateNLP@ WSDM*. 2020, pp. 32–36.

[51] Y. Huang, Z. Song, D. Chen, K. Li, and S. Arora. "Texthide: Tackling data privacy in language understanding tasks". In: *arXiv preprint arXiv:2010.06053* (2020).

[52] M. B. Hosseini, K. Pragyan, I. Reyes, and S. Egelman. "Identifying and Classifying Third-party Entities in Natural Language Privacy Policies". In: *Proceedings of the Second Workshop on Privacy in NLP*. 2020, pp. 18–27.

[53] C. Akiti, A. Squicciarini, and S. Rajtmajer. "A Semantics-based Approach to Disclosure Classification in User-Generated Online Content". In: *Proceedings of the 2020 Conference on Empirical Methods in Natural Language Processing: Findings*. 2020, pp. 3490–3499.

[54] R. Khandelwal, A. Nayak, Y. Yao, and K. Fawaz. "Surfacing Privacy Settings Using Semantic Matching". In: *Proceedings of the Second Workshop on Privacy in NLP*. 2020, pp. 28–38.

[55] G. Kerrigan, D. Slack, and J. Tuyls. "Differentially Private Language Models Benefit from Public Pre-training". In: *arXiv preprint arXiv:2009.05886* (2020).

[56] Z. Xu, A. Aggarwal, O. Feyisetan, and N. Teissier. "A Differentially Private Text Perturbation Method Using a Regularized Mahalanobis Metric". In: *arXiv preprint arXiv:2010.11947* (2020).

[57] M. Kuhrmann, D. M. Fernández, and M. Daneva. *On the Pragmatic Design of Literature Studies in Software Engineering: An Experience-based Guideline*. 2016. arXiv: 1612.03583 [cs.SE].

[58] URL: https://dl.acm.org/search/advanced.

[59] *Operators - Data Studio Help*. URL: https://support.google.com/datastudio/answer/10468382?hl=en.

[60] URL: https://ieeexplore.ieee.org/Xplorehelp/searching-ieee-xplore/search-examples.

[61] Elsevier. *How do I use the advanced search?* URL: https://service.elsevier.com/app/answers/detail/a_id/25974/supporthub/sciencedirect/.

[62] Elsevier. *How can I best use the Advanced search?* URL: https://service.elsevier.com/app/answers/detail/a_id/11365/c/10545/supporthub/scopus/.

[63] *Search Tips*. URL: https://link.springer.com/searchhelp.

[64] *index*. URL: https://images.webofknowledge.com/WOKRS535R111/help/WOS/hp_search.html.

[65] *Search Tips (Video)*. Nov. 1970. URL: https://www.wiley.com/customer-success/wiley-digital-archives-training-hub/search-tips-video.

[66] K. Pandey. "Natural Language Processing: An Overview". In: *Advances in Science & Technology* (), p. 24.

[67] L. Chen, M. A. Babar, and H. Zhang. "Towards an evidence-based understanding of electronic data sources". In: *14th International Conference on Evaluation and Assessment in Software Engineering (EASE)*. 2010, pp. 1–4.

[68] Elsevier. *Ei Compendex: Most complete Engineering Database*. URL: https://www.elsevier.com/solutions/engineering-village/content/compendex.

[69] URL: https://www.google.com/sheets/about/.

[70] *Free Reference Manager - Stay on top of your Literature*. URL: https://www.jabref.org/.

[71] *COUNTUNIQUE - Docs Editors Help*. URL: https://support.google.com/docs/answer/3093405?hl=en.

[72] *QUERY function - Docs Editors Help*. URL: https://support.google.com/docs/answer/3093343?hl=en.

[73] *SORT function - Docs Editors Help*. URL: https://support.google.com/docs/answer/3093150?hl=en.

[74] Prashanth, By, and Prashanth. *SORTN Tie Modes in Google Sheets - The Four Tiebreakers*. Oct. 2018. URL: https://infoinspired.com/google-docs/spreadsheet/sortn-tie-modes-in-google-sheets/.

[75] T. Angelanda and R. Colomo-Palaciosa. "Deep Learning for Single Image Super-Resolution: A Systematic Mapping Study". In: ().

[76] J. Zhang, L. Yang, S. Yu, and J. Ma. "A DNS tunneling detection method based on deep learning models to prevent data exfiltration". In: *International Conference on Network and System Security*. Springer. 2019, pp. 520–535.

[77] W. Song, Y. Cui, and Z. Peng. "A full-text retrieval algorithm for encrypted data in cloud storage applications". In: *Natural Language Processing and Chinese Computing*. Springer, 2015, pp. 229–241.

[78] L. Li, Y. Fan, M. Tse, and K.-Y. Lin. "A review of applications in federated learning". In: *Computers & Industrial Engineering* (2020), p. 106854.

[79] K. Meenakshi and G. Maragatham. "A review on security attacks and protective strategies of machine learning". In: *International Conference on Emerging Current Trends in Computing and Expert Technology*. Springer. 2019, pp. 1076–1087.

[80] Q. Liu, P. Li, W. Zhao, W. Cai, S. Yu, and V. C. Leung. "A survey on security threats and defensive techniques of machine learning: A data driven view". In: *IEEE access* 6 (2018), pp. 12103–12117.

[81] A. Lutskiv and N. Popovych. "Adaptable Text Corpus Development for Specific Linguistic Research". In: *2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T)*. IEEE. 2019, pp. 217–223.

[82] F. Rashid and A. Miri. "An Emerging Strategy for Privacy Preserving Databases: Differential Privacy". In: *International Conference on Human-Computer Interaction*. Springer. 2020, pp. 487–498.

[83] Y.-C. Tsai, S.-L. Wang, I.-H. Ting, and T.-P. Hong. "Flexible Anonymization of Transactions with Sensitive Items". In: *2018 5th International Conference on Behavioral, Economic, and Socio-Cultural Computing (BESC)*. IEEE. 2018, pp. 201–206.

[84] J. Ji, B. Chen, and H. Jiang. "Fully-connected LSTM–CRF on medical concept extraction". In: *International Journal of Machine Learning and Cybernetics* 11.9 (2020), pp. 1971–1979.

[85] R. Delanaux, A. Bonifati, M.-C. Rousset, and R. Thion. "Query-based linked data anonymization". In: *International Semantic Web Conference*. Springer. 2018, pp. 530–546.

[86] Q. Li, Z. Yang, L. Luo, L. Wang, Y. Zhang, H. Lin, J. Wang, L. Yang, K. Xu, and Y. Zhang. "A multi-task learning based approach to biomedical entity relation extraction". In: *2018 IEEE International Conference on Bioinformatics and Biomedicine (BIBM)*. IEEE. 2018, pp. 680–682.

[87] M. Pikuliak, M. Simko, and M. Bielikova. "Towards combining multitask and multilingual learning". In: *International Conference on Current Trends in Theory and Practice of Informatics*. Springer. 2019, pp. 435–446.

[88] H. Zhou, X. Li, W. Yao, C. Lang, and S. Ning. "Dut-nlp at mediqa 2019: an adversarial multi-task network to jointly model recognizing question entailment and question answering". In: *Proceedings of the 18th BioNLP Workshop and Shared Task*. 2019, pp. 437–445.

[89] K. Roberts, Y. Si, A. Gandhi, and E. Bernstam. "A framenet for cancer information in clinical narratives: schema and annotation". In: *Proceedings of the Eleventh International Conference on Language Resources and Evaluation (LREC 2018)*. 2018.

[90] N. Niknami, M. Abadi, and F. Deldar. "SpatialPDP: A personalized differentially private mechanism for range counting queries over spatial databases". In: *2014 4th International Conference on Computer and Knowledge Engineering (ICCKE)*. IEEE. 2014, pp. 709–715.

[91] J. Friginal, S. Gambs, J. Guiochet, and M.-O. Killijian. "Towards privacy-driven design of a dynamic carpooling system". In: *Pervasive and mobile computing* 14 (2014), pp. 71–82.

[92] R. Shokri, G. Theodorakopoulos, J.-Y. Le Boudec, and J.-P. Hubaux. "Quantifying location privacy". In: *2011 IEEE symposium on security and privacy*. IEEE. 2011, pp. 247–262.

[93] M. Gong, K. Pan, Y. Xie, A. K. Qin, and Z. Tang. "Preserving differential privacy in deep neural networks with relevance-based adaptive noise imposition". In: *Neural Networks* 125 (2020), pp. 131–141.

[94] S. Al-Fedaghi. "Perceived privacy". In: *2012 Ninth International Conference on Information Technology-New Generations*. IEEE. 2012, pp. 355–360.

[95] H. Wang, Z. Li, and Y. Cheng. "Distributed Latent Dirichlet allocation for objects-distributed cluster ensemble". In: *2008 International Conference on Natural Language Processing and Knowledge Engineering*. IEEE. 2008, pp. 1–7.

[96] P. Sun, Z. Wang, Y. Feng, L. Wu, Y. Li, H. Qi, and Z. Wang. "Towards personalized privacy-preserving incentive for truth discovery in crowdsourced binary-choice question answering". In: *IEEE INFOCOM 2020-IEEE Conference on Computer Communications*. IEEE. 2020, pp. 1133–1142.

[97] D. Z. Hakkani-Tur, Y. Saygin, M. Tang, and G. Tur. *Preserving privacy in natural language databases*. US Patent 8,473,451. June 2013.

[98] M. Ç. Demir and Ş. Ertekin. "Identifying textual personal information using bidirectional LSTM networks". In: *2018 26th Signal Processing and Communications Applications Conference (SIU)*. IEEE. 2018, pp. 1–4.

[99] P. Thaine and G. Penn. "Reasoning about unstructured data de-identification". In: *Journal of Data Protection & Privacy* 3.3 (2020), pp. 299–309.

[100] H. Wang, T. Feng, Z. Ren, L. Gao, and J. Zheng. "Towards Efficient Privacy-Preserving Personal Information in User Daily Life". In: *International Conference on Internet of Things as a Service*. Springer. 2019, pp. 503–513.

[101] C. Dilmegani. *Top 10 Privacy Enhancing Technologies (PETs) in 2021*. July 2021. URL: https://research.aimultiple.com/privacy-enhancing-technologies/.

[102] *Domain*. URL: https://www.merriam-webster.com/dictionary/domain.

[103] N. M. Nejad, P. Jabat, R. Nedelchev, S. Scerri, and D. Graux. "Establishing a strong baseline for privacy policy classification". In: *IFIP International Conference on ICT Systems Security and Privacy Protection*. Springer. 2020, pp. 370–383.

[104] E. Poplavska, T. B. Norton, S. Wilson, and N. Sadeh. "From Prescription to Description: Mapping the GDPR to a Privacy Policy Corpus Annotation Scheme". In: *Legal Knowledge and Information Systems*. IOS Press, 2020, pp. 243–246.

[105] M. Bahrami, M. Singhal, and W.-P. Chen. "Learning Data Privacy and Terms of Service from Different Cloud Service Providers". In: *2017 IEEE International Conference on Smart Cloud (SmartCloud)*. IEEE. 2017, pp. 250–257.

[106] Z. Qu, V. Rastogi, X. Zhang, Y. Chen, T. Zhu, and Z. Chen. "Autocog: Measuring the description-to-permission fidelity in android applications". In: *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. 2014, pp. 1354–1365.

[107] R. Catelli, F. Gargiulo, V. Casola, G. De Pietro, H. Fujita, and M. Esposito. "Crosslingual named entity recognition for clinical de-identification applied to a COVID-19 Italian data set". In: *Applied Soft Computing* 97 (2020), p. 106779.

[108] A. E. Johnson, L. Bulgarelli, and T. J. Pollard. "Deidentification of free-text medical records using pre-trained bidirectional transformers". In: *Proceedings of the ACM Conference on Health, Inference, and Learning*. 2020, pp. 214–221.

[109] B. Singh, Q. Sun, Y. S. Koh, J. Lee, and E. Zhang. "Detecting Protected Health Information with an Incremental Learning Ensemble: A Case Study on New Zealand Clinical Text". In: *2020 IEEE 7th International Conference on Data Science and Advanced Analytics (DSAA)*. IEEE. 2020, pp. 719–728.

[110] L. Lange, H. Adel, and J. Strötgen. "NLNDE: The Neither-Language-Nor-Domain-Experts' Way of Spanish Medical Document De-Identification". In: *arXiv preprint arXiv:2007.01030* (2020).

[111] D. C. Nguyen, E. Derr, M. Backes, and S. Bugiel. "Short text, large effect: Measuring the impact of user reviews on android app security & privacy". In: *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE. 2019, pp. 555–569.

[112] G. L. Scoccia, S. Ruberto, I. Malavolta, M. Autili, and P. Inverardi. "An investigation into Android run-time permissions from the end users' perspective". In: *Proceedings of the 5th international conference on mobile software engineering and systems*. 2018, pp. 45–55.

[113] N. Victor and D. Lopez. "A Conceptual Framework for Sensitive Big Data Publishing". In: *Proceedings of International Conference on Communication and Computational Technologies*. Springer. 2021, pp. 523–533.

[114] G. Canfora, A. Di Sorbo, E. Emanuele, S. Forootani, and C. A. Visaggio. "A NLP-based solution to prevent from privacy leaks in social network posts". In: *Proceedings of the 13th International Conference on Availability, Reliability and Security*. 2018, pp. 1–6.

[115] A. F. B. Neto, P. Desaulniers, P. A. Duboue, and A. Smirnov. "Filtering Personal Queries from Mixed-Use Query Logs". In: *Canadian Conference on Artificial Intelligence*. Springer. 2014, pp. 47–58.

[116] M. Sokolova and S. Matwin. "Personal privacy protection in time of big data". In: *Challenges in computational statistics and data mining*. Springer, 2016, pp. 365–380.

[117] O. Akanfe, R. Valecha, and H. R. Rao. "Design of an inclusive financial privacy index (INF-PIE): a financial privacy and digital financial inclusion perspective". In: *ACM Transactions on Management Information Systems (TMIS)* 12.1 (2020), pp. 1–21.

[118] F. Olsson. "On privacy preservation in text and document-based active learning for named entity recognition". In: *Proceedings of the ACM first international workshop on Privacy and anonymity for very large databases*. 2009, pp. 53–60.

[119] M. Blohm, C. Dukino, M. Kintz, M. Kochanowski, F. Koetter, and T. Renner. "Towards a Privacy Compliant Cloud Architecture for Natural Language Processing Platforms." In: *ICEIS (1)*. 2019, pp. 454–461.

[120] M. Gallé, A. Christofi, and H. Elsahar. "The case for a GDPR-specific annotated dataset of privacy policies". In: *AAAI Symposium on Privacy-Enhancing AI and HLT Technologies*. 2019.

[121] R. Catelli, F. Gargiulo, V. Casola, G. De Pietro, H. Fujita, and M. Esposito. "A novel covid-19 data set and an effective deep learning approach for the de-identification of italian medical records". In: *IEEE Access* 9 (2021), pp. 19097–19110.

[122] D. S. Carrell, D. J. Cronkite, B. A. Malin, J. S. Aberdeen, and L. Hirschman. "Is the juice worth the squeeze? Costs and benefits of multiple human annotators for clinical text de-identification". In: *Methods of information in medicine* 55.04 (2016), pp. 356–364.

[123] T.-V. T. Nguyen, N. Fornara, and F. Marfia. "Automatic policy enforcement on semantic social data". In: *Multiagent and Grid Systems* 11.3 (2015), pp. 121–146.

[124] N. Papanikolaou, S. Pearson, and M. C. Mont. "Automated Understanding Of Cloud Terms Of Service And SLAs". In: ().

[125] V. Keselj and D. Jutla. "QTIP: multi-agent NLP and privacy architecture for information retrieval in usable Web privacy software". In: *The 2005 IEEE/WIC/ACM International Conference on Web Intelligence (WI'05)*. IEEE. 2005, pp. 718–724.

[126] J. Parra-Arnau, J. P. Achara, and C. Castelluccia. "Myadchoices: Bringing transparency and control to online advertising". In: *ACM Transactions on the Web (TWEB)* 11.1 (2017), pp. 1–47.

[127] P. X. Mai, A. Goknil, L. K. Shar, F. Pastore, L. C. Briand, and S. Shaame. "Modeling security and privacy requirements: a use case-driven approach". In: *Information and Software Technology* 100 (2018), pp. 165–182.

[128] J. H. Weber-Jahnke and A. Onabajo. "Finding defects in natural language confidentiality requirements". In: *2009 17th IEEE International Requirements Engineering Conference*. IEEE. 2009, pp. 213–222.

[129] Z. Lindner. "A Comparative Study of Sequence Classification Models for Privacy Policy Coverage Analysis". In: *arXiv preprint arXiv:2003.04972* (2020).

[130] R. N. Zaeem and K. S. Barber. "A Large Publicly Available Corpus of Website Privacy Policies Based on DMOZ." In: *CODASPY*. 2021, pp. 143–148.

[131] T. D. Breaux and A. I. Antón. "Deriving semantic models from privacy policies". In: *Sixth IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY'05)*. IEEE. 2005, pp. 67–76.

[132] D. Torre, S. Abualhaija, M. Sabetzadeh, L. Briand, K. Baetens, P. Goes, and S. Forastier. "An ai-assisted approach for checking the completeness of privacy policies against gdpr". In: *2020 IEEE 28th International Requirements Engineering Conference (RE)*. IEEE. 2020, pp. 136–146.

[133] L. Yu, T. Zhang, X. Luo, and L. Xue. "Autoppg: Towards automatic generation of privacy policy for android applications". In: *Proceedings of the 5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices*. 2015, pp. 39–50.

[134] C. A. Brodie, C.-M. Karat, and J. Karat. "An empirical study of natural language parsing of privacy policy rules using the SPARCLE policy workbench". In: *Proceedings of the second symposium on Usable privacy and security*. 2006, pp. 8–19.

[135] Y. Luo, L. Cheng, H. Hu, G. Peng, and D. Yao. "Context-Rich Privacy Leakage Analysis Through Inferring Apps in Smart Home IoT". In: *IEEE Internet of Things Journal* 8.4 (2020), pp. 2736–2750.

[136] J. Liu and K. Wang. "Enforcing vocabulary k-anonymity by semantic similarity based clustering". In: *2010 IEEE International Conference on Data Mining*. IEEE. 2010, pp. 899–904.

[137] T. Diethe and O. Feyisetan. "Preserving privacy in analyses of textual data". In: *PrivateNLP@ WSDM*. 2020.

[138] Y. Shvartzshanider, A. Balashankar, T. Wies, and L. Subramanian. "RECIPE: Applying open domain question answering to privacy policies". In: *Proceedings of the Workshop on Machine Reading for Question Answering*. 2018, pp. 71–77.

[139] R. Doku, D. B. Rawat, and C. Liu. "On the Blockchain-Based Decentralized Data Sharing for Event Based Encryption to Combat Adversarial Attacks". In: *IEEE Transactions on Network Science and Engineering* (2020).

[140] J. Qian, F. Han, J. Hou, C. Zhang, Y. Wang, and X.-Y. Li. "Towards privacy-preserving speech data publishing". In: *IEEE INFOCOM 2018-IEEE Conference on Computer Communications*. IEEE. 2018, pp. 1079–1087.

[141] Y. Tian. "Privacy Preserving Information Sharing in Modern and Emerging Platforms". PhD thesis. Carnegie Mellon University, 2018.

[142] M. D. Shermis, S. Lottridge, and E. Mayfield. "The impact of anonymization for automated essay scoring". In: *Journal of Educational Measurement* 52.4 (2015), pp. 419–436.

[143] S. Ucan and H. Gu. "A platform for developing privacy preserving diagnosis mobile applications". In: *IEEE-EMBS International Conference on Biomedical and Health Informatics (BHI)*. IEEE. 2014, pp. 509–512.

[144] S. Wang, R. Sinnott, and S. Nepal. "P-GENT: Privacy-preserving geocoding of non-geotagged tweets". In: *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*. IEEE. 2018, pp. 972–983.

[145] K. Hashimoto, J. Yamagishi, and I. Echizen. "Privacy-preserving sound to degrade automatic speaker verification performance". In: *2016 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE. 2016, pp. 5500–5504.

[146] R. Boukharrou, A.-C. Chaouche, and K. Mahdjar. "Toward a Privacy Guard for Cloud-Based Home Assistants and IoT Devices". In: *International Conference on Mobile, Secure, and Programmable Networking*. Springer. 2020, pp. 177–194.

[147] F. H. Shezan, H. Hu, G. Wang, and Y. Tian. "VerHealth: Vetting Medical Voice Applications through Policy Enforcement". In: *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 4.4 (2020), pp. 1–21.

[148] P. Lopez-Otero and L. Docio-Fernandez. "Analysis of gender and identity issues in depression detection on de-identified speech". In: *Computer Speech & Language* 65 (2021), p. 101118.

[149] J. Tang, T. Zhu, P. Xiong, Y. Wang, and W. Ren. "Privacy and Utility Trade-Off for Textual Analysis via Calibrated Multivariate Perturbations". In: *International Conference on Network and System Security*. Springer. 2020, pp. 342–353.

[150] Ö. Uzuner, Y. Luo, and P. Szolovits. "Evaluating the state-of-the-art in automatic de-identification". In: *Journal of the American Medical Informatics Association* 14.5 (2007), pp. 550–563.

[151] X. Ye and F. Wang. "A Privacy Guard Service". In: *2017 IEEE International Conference on Cognitive Computing (ICCC)*. IEEE. 2017, pp. 48–55.

[152] E. Eder, U. Krieg-Holz, and U. Hahn. "CODE ALLTAG 2.0—A Pseudonymized German-Language Email Corpus". In: *Proceedings of the 12th Language Resources and Evaluation Conference*. 2020, pp. 4466–4477.

[153] K. Fujita and Y. Tsukada. "A notation for policies using feature structures". In: *Data Privacy Management and Autonomous Spontaneous Security*. Springer, 2010, pp. 140–154.

[154] P. K. Das, A. L. Kashyap, G. Singh, C. Matuszek, T. Finin, A. Joshi, et al. "Semantic knowledge and privacy in the physical web". In: *Proceedings of the 4th Workshop on Society, Privacy and the Semantic Web-Policy and Technology (PrivOn2016) co-located with 15th International Semantic Web Conference (ISWC 2016)*. 2016.

[155] J. Heaps. "Code Element Vector Representations Through the Application of Natural Language Processing Techniques for Automation of Software Privacy Analysis". PhD thesis. The University of Texas at San Antonio, 2020.

[156] N. Papanikolaou. "Natural language processing of rules and regulations for compliance in the cloud". In: *OTM Confederated International Conferences" On the Move to Meaningful Internet Systems"*. Springer. 2012, pp. 620–627.

[157] C. Iwendi, S. A. Moqurrab, A. Anjum, S. Khan, S. Mohan, and G. Srivastava. "N-sanitization: A semantic privacy-preserving framework for unstructured medical datasets". In: *Computer Communications* 161 (2020), pp. 160–171.

[158] Z. Jian, X. Guo, S. Liu, H. Ma, S. Zhang, R. Zhang, and J. Lei. "A cascaded approach for Chinese clinical text de-identification with less annotation effort". In: *Journal of biomedical informatics* 73 (2017), pp. 76–83.

[159] Q. Xu, L. Qu, C. Xu, and R. Cui. "Privacy-aware text rewriting". In: *Proceedings of the 12th International Conference on Natural Language Generation*. 2019, pp. 247–257.

[160] K. Hammoud, S. Benbernou, M. Ouziri, Y. Saygın, R. Haque, and Y. Taher. "Personal information privacy: what's next?" In: CEUR Workshop Proceedings. 2019.

[161] D. I. Adelani, A. Davody, T. Kleinbauer, and D. Klakow. "Privacy guarantees for de-identifying text transformations". In: *arXiv preprint arXiv:2008.03101* (2020).

[162] D. Sánchez, M. Batet, and A. Viejo. "Minimizing the disclosure risk of semantic correlations in document sanitization". In: *Information Sciences* 249 (2013), pp. 110–123.

[163] L. Deleger, T. Lingren, Y. Ni, M. Kaiser, L. Stoutenborough, K. Marsolo, M. Kouril, K. Molnar, and I. Solti. "Preparing an annotated gold standard corpus to share with extramural investigators for de-identification research". In: *Journal of biomedical informatics* 50 (2014), pp. 173–183.

[164] F. Martinelli, F. Marulli, F. Mercaldo, S. Marrone, and A. Santone. "Enhanced Privacy and Data Protection using Natural Language Processing and Artificial Intelligence". In: *2020 International Joint Conference on Neural Networks (IJCNN)*. IEEE. 2020, pp. 1–8.

[165] D. Abril, G. Navarro-Arribas, and V. Torra. "On the declassification of confidential documents". In: *International Conference on Modeling Decisions for Artificial Intelligence*. Springer. 2011, pp. 235–246.

[166] J. Neerbek, I. Assent, and P. Dolog. "Detecting complex sensitive information via phrase structure in recursive neural networks". In: *Pacific-Asia Conference on Knowledge Discovery and Data Mining*. Springer. 2018, pp. 373–385.

[167] C.-M. Karat, C. Brodie, and J. Karat. "Usable privacy and security for personal information management". In: *Communications of the ACM* 49.1 (2006), pp. 56–57.

[168] S. Zimmeck and S. M. Bellovin. "Privee: An architecture for automatically analyzing web privacy policies". In: *23rd {USENIX} Security Symposium ({USENIX} Security 14)*. 2014, pp. 1–16.

[169] Y. Shvartzshnaider, Z. Pavlinovic, A. Balashankar, T. Wies, L. Subramanian, H. Nissenbaum, and P. Mittal. "Vaccine: Using contextual integrity for data leakage detection". In: *The World Wide Web Conference*. 2019, pp. 1702–1712.

[170] A. Stubbs and Ö. Uzuner. "Annotating longitudinal clinical narratives for de-identification: The 2014 i2b2/UTHealth corpus". In: *Journal of biomedical informatics* 58 (2015), S20–S29.

[171] J. Liu, D. He, D. Wu, and J. Xue. "Correlating UI Contexts with Sensitive API Calls: Dynamic Semantic Extraction and Analysis". In: *2020 IEEE 31st International Symposium on Software Reliability Engineering (ISSRE)*. IEEE. 2020, pp. 241–252.

[172] M. Hatamian, N. Momen, L. Fritsch, and K. Rannenberg. "A multilateral privacy impact analysis method for android apps". In: *Annual Privacy Forum*. Springer. 2019, pp. 87–106.

[173] P. M. Aonghusa and D. J. Leith. "Don't let Google know I'm lonely". In: *ACM Transactions on Privacy and Security (TOPS)* 19.1 (2016), pp. 1–25.

[174] D. P. Lopresti and A. L. Spitz. "Information leakage through document redaction: attacks and countermeasures". In: *Document recognition and retrieval XII*. Vol. 5676. International Society for Optics and Photonics. 2005, pp. 183–190.

[175] Ü. Meteriz, N. F. Yıldıran, J. Kim, and D. Mohaisen. "Understanding the Potential Risks of Sharing Elevation Information on Fitness Applications". In: *2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS)*. IEEE. 2020, pp. 464–473.

[176] D. Pàmies-Estrems, J. Castellà-Roca, and A. Viejo. "Working at the web search engine side to generate privacy-preserving user profiles". In: *Expert Systems with Applications* 64 (2016), pp. 523–535.

[177] K. Mivule and K. Hopkinson. "Distortion Search–A Web Search Privacy Heuristic". In: ().

[178] A. Li, Y. Duan, H. Yang, Y. Chen, and J. Yang. "TIPRDC: task-independent privacy-respecting data crowdsourcing framework for deep learning with anonymized intermediate representations". In: *Proceedings of the 26th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining*. 2020, pp. 824–832.

[179] S. Reddy and K. Knight. "Obfuscating gender in social media writing". In: *Proceedings of the First Workshop on NLP and Computational Social Science*. 2016, pp. 17–26.

[180] P. Silva, C. Gonçalves, C. Godinho, N. Antunes, and M. Curado. "Using NLP and machine learning to detect data privacy violations". In: *IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE. 2020, pp. 972–977.

[181] C. Santos, A. Gangemi, and M. Alam. "Detecting and Editing Privacy Policy Pitfalls on the Web." In: *TERECOM@ JURIX*. 2017, pp. 87–99.

[182] P. Jindal, C. A. Gunter, and D. Roth. "Detecting privacy-sensitive events in medical text". In: *Proceedings of the 5th ACM Conference on Bioinformatics, Computational Biology, and Health Informatics*. 2014, pp. 617–620.

[183] C. Liang, D. Abbott, Y. A. Hong, M. Madadi, and A. White. "Clustering Help-Seeking Behaviors in LGBT Online Communities: A Prospective Trial". In: *International Conference on Human-Computer Interaction*. Springer. 2019, pp. 345–355.

[184] H. Liu and B. Wang. "Mitigating File-Injection Attacks with Natural Language Processing". In: *Proceedings of the Sixth International Workshop on Security and Privacy Analytics*. 2020, pp. 3–13.

[185] D. R. G. de Pontes and S. D. Zorzo. "PPMark: An Architecture to Generate Privacy Labels Using TF-IDF Techniques and the Rabin Karp Algorithm". In: *Information Technology: New Generations*. Springer, 2016, pp. 1029–1040.

[186] M. Mustapha, K. Krasnashchok, A. Al Bassit, and S. Skhiri. "Privacy Policy Classification with XLNet (Short Paper)". In: *Data Privacy Management, Cryptocurrencies and Blockchain Technology*. Springer, 2020, pp. 250–257.

[187] E. Begoli, K. Brown, S. Srinivas, and S. Tamang. "SynthNotes: A Generator Framework for High-volume, High-fidelity Synthetic Mental Health Notes". In: *2018 IEEE International Conference on Big Data (Big Data)*. IEEE. 2018, pp. 951–958.

[188] J. Guan, R. Li, S. Yu, and X. Zhang. "A method for generating synthetic electronic medical record text". In: *IEEE/ACM transactions on computational biology and bioinformatics* (2019).

[189] K. M. Sathyendra, S. Wilson, F. Schaub, S. Zimmeck, and N. Sadeh. "Identifying the provision of choices in privacy policy text". In: *Proceedings of the 2017 Conference on Empirical Methods in Natural Language Processing*. 2017, pp. 2774–2779.

[190] R. Baalous and R. Poet. "How Dangerous Permissions are Described in Android Apps' Privacy Policies?" In: *Proceedings of the 11th International Conference on Security of Information and Networks*. 2018, pp. 1–2.

[191] J. R. Reidenberg, J. Bhatia, T. D. Breaux, and T. B. Norton. "Ambiguity in privacy policies and the impact of regulation". In: *The Journal of Legal Studies* 45.S2 (2016), S163–S190.

[192] N. M. Nejad, S. Scerri, and J. Lehmann. "Knight: Mapping privacy policies to GDPR". In: *European Knowledge Acquisition Workshop*. Springer. 2018, pp. 258–272.

[193] R. N. Zaeem and K. S. Barber. "The effect of the GDPR on privacy policies: Recent progress and future promise". In: *ACM Transactions on Management Information Systems (TMIS)* 12.1 (2020), pp. 1–20.

[194] O. Krachina, V. Raskin, and K. Triezenberg. "Reconciling privacy policies and regulations: Ontological semantics perspective". In: *Symposium on Human Interface and the Management of Information*. Springer. 2007, pp. 730–739.

[195] L. Cai, C. Lu, and C. Zhang. "Privacy domain-specific ontology building and consistency analysis". In: *2010 international conference on internet technology and applications*. IEEE. 2010, pp. 1–6.

[196] S. M. Meystre. "De-identification of unstructured clinical data for patient privacy protection". In: *Medical Data Privacy Handbook*. Springer, 2015, pp. 697–716.

[197] L. Zhou, H. Suominen, T. Gedeon, et al. "Adapting state-of-the-art deep language models to clinical information extraction systems: Potentials, challenges, and solutions". In: *JMIR medical informatics* 7.2 (2019), e11499.

[198] S. K. Nayak and A. C. Ojha. "Data Leakage Detection and Prevention: Review and Research Directions". In: *Machine Learning and Information Processing; Springer: Singapore* (2020), pp. 203–212.

[199] W. Sun, Z. Cai, Y. Li, F. Liu, S. Fang, and G. Wang. "Data processing and text mining technologies on electronic medical records: a review". In: *Journal of healthcare engineering* 2018 (2018).

[200] N. Zhu, M. Zhang, D. Feng, and J. He. "How Well Can WordNet Measure Privacy: A Comparative Study?" In: *2017 13th International Conference on Semantics, Knowledge and Grids (SKG)*. IEEE. 2017, pp. 45–49.

[201] I.-C. Yoo, K. Lee, S. Leem, H. Oh, B. Ko, and D. Yook. "Speaker Anonymization for Personal Information Protection Using Voice Conversion Techniques". In: *IEEE Access* 8 (2020), pp. 198637–198645.

[202] G. Francopoulo and L. Schaub. "Anonymization for the GDPR in the Context of Citizen and Customer Relationship Management and NLP". In: *workshop on Legal and Ethical Issues (Legal2020)*. ELRA. 2020, pp. 9–14.

[203] H. Suominen, T. Lehtikunnas, B. Back, H. Karsten, T. Salakoski, and S. Salantera. "Theoretical considerations of ethics in text mining of nursing documents". In: *Studies in health technology and informatics* 122 (2006), p. 359.

[204] O. Hasan, B. Habegger, L. Brunie, N. Bennani, and E. Damiani. "A discussion of privacy challenges in user profiling with big data techniques: The EEXCESS use case". In: *2013 IEEE International Congress on Big Data*. IEEE. 2013, pp. 25–30.

[205] W. Ye and Q. Li. "Chatbot Security and Privacy in the Age of Personal Assistants". In: *2020 IEEE/ACM Symposium on Edge Computing (SEC)*. IEEE. 2020, pp. 388–393.

[206] F. Hassan, D. Sánchez, J. Soria-Comas, and J. Domingo-Ferrer. "Automatic anonymization of textual documents: Detecting sensitive information via word embeddings". In: *2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*. IEEE. 2019, pp. 358–365.

[207] B. Di Martino, F. Marulli, P. Lupi, and A. Cataldi. "A Machine Learning Based Methodology for Automatic Annotation and Anonymisation of Privacy-Related Items in Textual Documents for Justice Domain". In: *Conference on Complex, Intelligent, and Software Intensive Systems*. Springer. 2020, pp. 530–539.

[208] S. Wilson, F. Schaub, A. A. Dara, F. Liu, S. Cherivirala, P. G. Leon, M. S. Andersen, S. Zimmeck, K. M. Sathyendra, N. C. Russell, et al. "The creation and analysis of a website privacy policy corpus". In: *Proceedings of the 54th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*. 2016, pp. 1330–1340.

[209] A. Ravichander, A. W. Black, S. Wilson, T. Norton, and N. Sadeh. "Question answering for privacy policies: Combining computational and legal perspectives". In: *arXiv preprint arXiv:1911.00841* (2019).

[210] C. D. Manning, M. Surdeanu, J. Bauer, J. R. Finkel, S. Bethard, and D. McClosky. "The Stanford CoreNLP natural language processing toolkit". In: *Proceedings of 52nd annual meeting of the association for computational linguistics: system demonstrations*. 2014, pp. 55–60.

[211] X. Pan, Y. Cao, X. Du, B. He, G. Fang, R. Shao, and Y. Chen. "Flowcog: context-aware semantics extraction and analysis of information flow leaks in android apps". In: *27th {USENIX} Security Symposium ({USENIX} Security 18)*. 2018, pp. 1669–1685.

[212] M. Dharini and R. Sasikumar. "Preserving privacy of encrypted data stored in cloud and enabling efficient retrieval of encrypted data through blind storage". In: *Advances in Natural and Applied Sciences* 10.10 SE (2016), pp. 72–77.

[213] X. Dai, H. Dai, G. Yang, X. Yi, and H. Huang. "An efficient and dynamic semantic-aware multikeyword ranked search scheme over encrypted cloud data". In: *IEEE Access* 7 (2019), pp. 142855–142865.

[214] H. Dai, X. Dai, X. Yi, G. Yang, and H. Huang. "Semantic-aware multi-keyword ranked search scheme over encrypted cloud data". In: *Journal of Network and Computer Applications* 147 (2019), p. 102442.

[215] W. Li, Y. Xiao, C. Tang, X. Huang, and J. Xue. "Multi-user searchable encryption voice in home IoT system". In: *Internet of Things* 11 (2020), p. 100180.

[216] Y. Liang, D. O'Keeffe, and N. Sastry. "PAIGE: towards a hybrid-edge design for privacy-preserving intelligent personal assistants". In: *Proceedings of the Third ACM International Workshop on Edge Systems, Analytics and Networking*. 2020, pp. 55–60.

[217] M. Hadian, T. Altuwaiyan, X. Liang, and W. Li. "Privacy-preserving voice-based search over mhealth data". In: *Smart Health* 12 (2019), pp. 24–34.

[218] M. Friedrich, A. Köhn, G. Wiedemann, and C. Biemann. "Adversarial learning of privacy-preserving text representations for de-identification of medical records". In: *arXiv preprint arXiv:1906.05000* (2019).

[219] S. Krishna, R. Gupta, and C. Dupuy. "ADePT: Auto-encoder based Differentially Private Text Transformation". In: *arXiv preprint arXiv:2102.01502* (2021).

[220] B. Weggenmann and F. Kerschbaum. "Syntf: Synthetic and differentially private term frequency vectors for privacy-preserving text mining". In: *The 41st International ACM SIGIR Conference on Research & Development in Information Retrieval*. 2018, pp. 305–314.

[221] G. Beigi, K. Shu, R. Guo, S. Wang, and H. Liu. "I am not what i write: Privacy preserving text representation learning". In: *arXiv preprint arXiv:1907.03189* (2019).

[222] C. Tan, D. Jiang, H. Mo, J. Peng, Y. Tong, W. Zhao, C. Chen, R. Lian, Y. Song, and Q. Xu. "Federated acoustic model optimization for automatic speech recognition". In: *International Conference on Database Systems for Advanced Applications*. Springer. 2020, pp. 771–774.

[223] D. Reich, A. Todoki, R. Dowsley, M. De Cock, and A. C. Nascimento. "Privacy-preserving classification of personal text messages with secure multi-party computation: An application to hate-speech detection". In: *arXiv preprint arXiv:1906.02325* (2019).

[224] B. Hitaj, G. Ateniese, and F. Perez-Cruz. "Deep models under the GAN: information leakage from collaborative deep learning". In: *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. 2017, pp. 603–618.

[225] X. Ding, H. Fang, Z. Zhang, K.-K. R. Choo, and H. Jin. "Privacy-preserving Feature Extraction via Adversarial Training". In: *IEEE Transactions on Knowledge and Data Engineering* (2020).

[226] X. Zhu, J. Wang, Z. Hong, and J. Xiao. "Empirical studies of institutional federated learning for natural language processing". In: *Proceedings of the 2020 Conference on Empirical Methods in Natural Language Processing: Findings*. 2020, pp. 625–634.

[227] M. Chen, A. T. Suresh, R. Mathews, A. Wong, C. Allauzen, F. Beaufays, and M. Riley. "Federated learning of n-gram language models". In: *arXiv preprint arXiv:1910.03432* (2019).

[228] M. Coavoux, S. Narayan, and S. B. Cohen. "Privacy-preserving neural representations of text". In: *arXiv preprint arXiv:1808.09408* (2018).

[229] L. Lyu, Y. Li, X. He, and T. Xiao. "Towards differentially private text representations". In: *Proceedings of the 43rd International ACM SIGIR Conference on Research and Development in Information Retrieval*. 2020, pp. 1813–1816.

[230] B. Tran and X. Liang. "Exploiting peer-to-peer communications for query privacy preservation in voice assistant systems". In: *Peer-to-Peer Networking and Applications* 14.3 (2021), pp. 1475–1487.

[231] J. Shao, S. Ji, and T. Yang. "Privacy-aware document ranking with neural signals". In: *Proceedings of the 42nd International ACM SIGIR Conference on Research and Development in Information Retrieval*. 2019, pp. 305–314.

[232] K. Khelik. "Privacy-preserving document similarity detection". MA thesis. Universitetet i Agder/University of Agder, 2011.

[233] A. A. Gareta. "Privacy-Preserving Speech Emotion Recognition". In: (2017).

[234] S. Ahmed, A. R. Chowdhury, K. Fawaz, and P. Ramanathan. "Preech: a system for privacy-preserving speech transcription". In: *29th {USENIX} Security Symposium ({USENIX} Security 20)*. 2020, pp. 2703–2720.

[235] A. Treiber, A. Nautsch, J. Kolberg, T. Schneider, and C. Busch. "Privacy-preserving PLDA speaker verification using outsourced secure computation". In: *Speech Communication* 114 (2019), pp. 60–71.

[236] D. Aritomo and C. Watanabe. "Achieving efficient similar document search over encrypted data on the cloud". In: *2019 IEEE International Conference on Smart Computing (SMARTCOMP)*. IEEE. 2019, pp. 1–6.

[237] Z. Fu, X. Wu, C. Guan, X. Sun, and K. Ren. "Toward efficient multi-keyword fuzzy search over encrypted outsourced data with accuracy improvement". In: *IEEE Transactions on Information Forensics and Security* 11.12 (2016), pp. 2706–2716.

[238] L. Marujo, J. Portêlo, W. Ling, D. M. de Matos, J. P. Neto, A. Gershman, J. Carbonell, I. Trancoso, and B. Raj. "Privacy-preserving multi-document summarization". In: *arXiv preprint arXiv:1508.01420* (2015).

[239] M. Koppel, S. Argamon, and A. R. Shimoni. "Automatically categorizing written texts by author gender". In: *Literary and linguistic computing* 17.4 (2002), pp. 401–412.

[240] O. Feyisetan, T. Drake, B. Balle, and T. Diethe. "Privacy-preserving active learning on sensitive data for user intent classification". In: *arXiv preprint arXiv:1903.11112* (2019).

[241] M. Pathak. "Privacy Preserving Techniques for Speech Processing". In: *Dec* 1 (2010), pp. 1–54.

[242] S. Augenstein, H. B. McMahan, D. Ramage, S. Ramaswamy, P. Kairouz, M. Chen, R. Mathews, et al. "Generative models for effective ML on private, decentralized datasets". In: *arXiv preprint arXiv:1911.06679* (2019).

[243] F. Granqvist, M. Seigel, R. van Dalen, Á. Cahill, S. Shum, and M. Paulik. "Improving on-device speaker verification using federated learning with privacy". In: *arXiv preprint arXiv:2008.02651* (2020).

[244] Q. Wang, M. Du, X. Chen, Y. Chen, P. Zhou, X. Chen, and X. Huang. "Privacy-preserving collaborative model learning: The case of word vector training". In: *IEEE Transactions on Knowledge and Data Engineering* 30.12 (2018), pp. 2381–2393.

[245] S. A. Anand, P. Walker, and N. Saxena. "Compromising Speech Privacy under Continuous Masking in Personal Spaces". In: *2019 17th International Conference on Privacy, Security and Trust (PST)*. IEEE. 2019, pp. 1–10.

[246] D. Carrell. "A strategy for deploying secure cloud-based natural language processing systems for applied research involving clinical text". In: *2011 44th Hawaii International Conference on System Sciences*. IEEE. 2011, pp. 1–11.

[247] K. Demetzou, L. Böck, and O. Hanteer. "Smart Bears don't talk to strangers: analysing privacy concerns and technical solutions in smart toys for children". In: (2018).

[248] A. Rabinia, S. Ghanavati, and M. Dragoni. "Towards Integrating the FLG Framework with the NLP Combinatory Framework". In: ().

[249] P. Thaine and G. Penn. "Privacy-Preserving Character Language Modelling". In: ().

[250] E. D. Lopez-Cozar, E. Orduna-Malea, and A. Martin-Martin. "Google Scholar as a data source for research assessment". In: *Springer handbook of science and technology indicators*. Springer, 2019, pp. 95–127.

[251] R. Nosowsky and T. J. Giordano. "The Health Insurance Portability and Accountability Act of 1996 (HIPAA) privacy rule: implications for clinical research". In: *Annu. Rev. Med.* 57 (2006), pp. 575–590.

[252] L. Zhao, Q. Wang, Q. Zou, Y. Zhang, and Y. Chen. "Privacy-preserving collaborative deep learning with unreliable participants". In: *IEEE Transactions on Information Forensics and Security* 15 (2019), pp. 1486–1500.

[253] C.-H. H. Yang, J. Qi, S. Y.-C. Chen, P.-Y. Chen, S. M. Siniscalchi, X. Ma, and C.-H. Lee. "Decentralizing feature extraction with quantum convolutional neural network for automatic speech recognition". In: *ICASSP 2021-2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE. 2021, pp. 6523–6527.

[254] O. Feyisetan, S. Ghanavati, S. Malmasi, and P. Thaine. "Proceedings of the Second Workshop on Privacy in NLP". In: *Proceedings of the Second Workshop on Privacy in NLP*. 2020.

[255] A. Aggarwal, Z. Xu, O. Feyisetan, and N. Teissier. "On Log-Loss Scores and (No) Privacy". In: *Proceedings of the Second Workshop on Privacy in NLP*. 2020, pp. 1–6.